Region Uppsala

Granskning av implementation av Heroma

Mars 2023

Kvalitetssäkrare: Rebecka Hansson
Projektledare: Martin Westholm
Projektmedlem: Markus Månsson

Innehållsförteckning

3	Sammanfattning
4	Rekommendationer
5-7	Inledning - Bakgrund - Syfte och revisionsfrågor - Revisionskriterier - Avgränsning - Metod - Inledande reflektion
8-17	Granskningsresultat - Har förberedelser (behovsanalys och kravspecifikation) och upphandlingsprocess varit tillräcklig med avseende på projektets omfattning? - Har utbildningen av medarbetare varit tillräcklig för att ge användarna förutsättningar att hantera systemet korrekt? - Har implementationen hanterats på ett sätt som skapar bra förutsättningar för funktion och integritet i det nya systemet? - Har behörighetsfrågan och GDPR hanterats på ett korrekt sätt? - Finns tillräcklig kontroll i rutiner kring lönehanteringen – systemmässig/automatisk kontra manuell hantering (inmatning eller kontroll)?
18-19	Samlad bedömning
20-23	Bilagor

Sammanfattning

PwC har på uppdrag av Region Uppsalas revisorer genomfört en granskning av regionens införande av ett nytt HR-system. Syftet med granskningen var att granska och utvärdera implementationen av Heroma och om den skett med tillräcklig styrning och intern kontroll.

Utifrån genomförd granskning är vår samlade bedömning att införandet **delvis** skett med tillräcklig styrning och intern kontroll.

Granskningen har utgått från fem revisionsfrågor. Nedan anges bedömning för respektive revisionsfråga. För fullständiga bedömningar se respektive revisionsfråga i rapporten eller det avslutande avsnittet “Sammanfattande bedömningar utifrån revisionsfrågor”.

Revisionsfrågor	**Bedömning**
Har förberedelser (behovsanalys och kravspecifikation) och upphandlingsprocess varit tillräcklig med avseende på projektets omfattning?	**Delvis**
Har utbildningen av medarbetare varit tillräcklig för att ge användarna förutsättningar att hantera systemet korrekt?	**Delvis**
Har implementationen hanterats på ett sätt som skapar bra förutsättningar för funktion och integritet i det nya systemet?	**Delvis**
Har behörighetsfrågan och GDPR hanterats på ett korrekt sätt?	**Delvis**
Finns tillräcklig kontroll i rutiner kring lönehanteringen – systemmässig/automatisk kontra manuell hantering (inmatning eller kontroll)?	**Uppfylld**

Rekommendationer

Gällande Heroma och kringliggande aktiviteter

- Avsätt resurser för att utbilda organisationen i hur lönespecifikationerna i Heroma ska läsas och tolkas
- Säkerställ att det pågående arbetet med att bygga upp det nya organisationsträdet i Heroma fortsatt prioriteras och färdigställs.
- Etablera rutiner och arbetssätt för att följa upp loggade användaraktiviteter. Det bör exempelvis tydliggöras vad som är avvikande användaraktiviteter och hur avvikelserna ska hanteras.
- Se över om regionens register över personuppgiftsbehandlingar behöver uppdateras i och med genomförandet av detta projekt.

För kommande projekt

- Säkerställ att supportfunktionen har förstärkt och adekvat bemanning vid driftstart av verksamhetskritiska system.
- Säkerställ att verksamheten avsätter tid för att genomföra utbildning vid lansering av verksamhetskritiska system.
- Säkerställ att det finns ändamålsenliga säkerhetsfunktioner (exempelvis för lösenordshantering) upprättade inför framtida lanseringar av IT-lösningar.
- Säkerställ att verksamheten avsätter ändamålsenliga resurser för att bedriva lokala anpassningsprojekt, bedriva verksamhetsspecifika utbildningar och för att tillsätta superanvändare vid genomförande av implementationer av större system. Det behöver även tydligt kommuniceras och förankras att verksamheten har detta ansvaret. Det behöver även säkerställas att de medarbetare i verksamheten som deltar i projekt får möjlighet att avsätta tid för det.
- Se över om regionens medvetenhet och rutiner för att identifiera och hantera personuppgiftsincidenter behöver uppdateras. Detta för att säkerställa att personuppgiftsincidenter identifieras på ett ändamålsenligt sätt och att anmälan till IMY sker i linje med lagkraven.
- Vid tillämpliga fall bör det säkerställas att en konsekvensbedömning ur ett dataskyddsperspektiv genomförs redan innan införandet av IT-lösningar (i linje med artikel 35 i Dataskyddsförordningen) för att på så sätt förebygga risker innan de uppkommer.
- Tillse att det finns en projektekonom tillsatt för styrning och uppföljning av det ekonomiska utfallet i kommande projekt
- Säkerställ extra extern resurstilldelning vid stora projekt då dessa oftast inte kan drivas med enbart befintliga resurser

1

Inledning

Inledning

Bakgrund

Regionen hade tidigare olika system för lön, schemaläggning, tidregistrering och vikariehantering. 2015 togs ett beslut om att genomföra en förstudie inför upphandling av ett gemensamt HR-system. En upphandling genomfördes och Heroma valdes som nytt HR-system. Centralt i valet av leverantör var att systemstödet för ovan områden skulle uppfattas som ett system. Avtalet med leverantören skrevs under i september 2019 och systemet driftsattes februari 2022.

Det har varit problem efter och i samband med implementeringen, som exempel har medarbetare fått fel lön och jour- och komptid samt även att semesterdagar inte har stämt. Omständigheterna har även varit föremål för viss mediabevakning.

Brister i lönesystemet innebär en stor risk för felaktig lönehantering och potentiell påverkan på de anställdas ersättning och förmåner.
Revisorerna i Region Uppsala ser därför i sin risk- och väsentlighetsbedömning att implementationen av Heroma är viktig att granska och utvärdera.

Syfte och revisionsfrågor

Syfte med granskningen är att granska och utvärdera implementationen av Heroma och om den skett med tillräcklig styrning och intern kontroll.

Följande revisionsfråga ska besvaras inom ramen av granskningen:

- Har implementationen av systemet Heroma hanterats på ett sätt som skapar bra förutsättningar för en trygg och säker lönehantering

Den övergripande granskningen av implementationen av Heroma skall utreda följande frågeställningar:

- Har förberedelser (behovsanalys och kravspecifikation) och upphandlingsprocess varit tillräcklig med avseende på projektets omfattning?
- Har utbildningen av medarbetare varit tillräcklig för att ge användarna förutsättningar att hantera systemet korrekt?
- Har implementationen hanterats på ett sätt som skapar bra förutsättningar för funktion och integritet i det nya systemet (övergång från tidigare system, test av Heroma, migration av data från tidigare system till Heroma, integrering med ekonomisystem)?
- Har behörighetsfrågan och GDPR hanterats på ett korrekt sätt?
- Finns tillräcklig kontroll i rutiner kring lönehanteringen – systemmässig/automatisk kontra manuell hantering (inmatning eller kontroll)?

Revisionskriterier

- Offentlighets- och sekretesslagen
- Verksamheternas interna styrande dokument relevanta för granskningen
- Regelverk/lagkrav samt interna policys gällande GDPR

Metod och avgränsningar

Granskningen har genomförts genom intervjuer med projektledning och projektdeltagare samt ansvariga tjänstemän och systemadministratörer. Dokumentation med relevans för införandet av Heroma har även inhämtats och granskats.

Tekniska tester av systemet har ej genomförts inom ramen för granskningen.

Inledande reflektion

Vår erfarenhet från liknande granskningar är att det är både ***komplext samt resurs- och tidskrävande att genomföra stora IT-relaterade projekt.*** Det är vanligt förekommande att projekt som avser att byta ut eller implementera ett nytt IT-stöd antingen tar längre tid än planerat, inte uppnår önskad kvalitet eller att projektets budget överskrids. Detta är även vanligt i organisationer som har mångårig vana att driva och arbeta i IT-relaterade projekt.

Ofta underskattas komplexiteten och omfattningen i IT-projekt inför uppstart och baserat på vad som framkommit i denna utvärdering bedöms det som sannolikt att detta till viss del även skett i Region Uppsala och implementationen av Heroma. I denna komplexitet ingår även att förstå hur arbetssätt och rutiner ändras för användare/medarbetare i samband med utveckling av system och att förändring är olika svårt att hantera för olika människor. Detta införande har även genomförts under den tidsperiod då pandemin påverkade verksamheten som mest, vilket gjorde det svårare att få resurser till projektet samt även påverkade möjligheten att genomföra lärarledda utbildningar. Det var även en redan ansträngd organisation som skulle ta emot ett nytt system, vilket skapade ytterligare svårigheter.

Möjligheten att lyckas med dessa typer av projekt är starkt beroende av en tydlig styrning och ledning, samsyn och effektivitet avseende metodik och arbetssätt. Även organisationens IT-mognad och möjlighet att förändras behöver beaktas.

De främsta förbättringsområden som identifierats i denna utvärdering berör bland annat bristande utbildningsmaterial för vissa områden (tolkning av lönespecifikationer och schemaläggning) som skapat mycket frustration i verksamheten. Det har även avsatts bristande resurser i verksamheten för att genomföra lokala införandeprojekt och utse superanvändare som skulle stötta användare. Projektet har även kunnat se att de som ej tagit sig tid eller haft möjlighet att gå erforderlig utbildning har haft större utmaningar med att arbeta effektivt i Heroma. Samtidigt hade medarbetare det svårt att få svar på frågor och problem som uppstod både inför- och efter driftsättning, bland annat på grund av hög belastning på supporten. Detta påverkade verksamhetens förståelse för systemet.

Införandet har även påverkats negativt av att kravställningen för vissa viktiga områden (exempelvis schemaläggning) inte var tillräckligt genomarbetad.

Den gemensamma bilden som lyfts fram under intervjuer är dock att genomförandet samt resultatet av programmet överlag har varit lyckat, även om det funnits brister avseende vissa områden, det är viktigt att ta med sig framåt. Vissa av dessa brister kan härledas till pandemins effekter, men det finns även andra lärdomar att dra inför kommande projekt.Vi har dock inte identifierat några väsentliga brister gällande hur projektet bedrivits eller i införandet av systemet i organisationen.

Vår förhoppning är att denna utvärdering och slutrapport kan bidra till att belysa lärdomar som Region Uppsala kan ta med sig inför framtida program och projekt samt för det kontinuerliga förbättringsarbetet.

2

Granskningsresultat

Revisionsfrågor:

1. **Har förberedelser (behovsanalys och kravspecifikation) och upphandlingsprocess varit tillräcklig med avseende på projektets omfattning?**
2. **Har utbildningen av medarbetare varit tillräcklig för att ge användarna förutsättningar att hantera systemet korrekt?**
3. **Har implementationen hanterats på ett sätt som skapar bra förutsättningar för funktion och integritet i det nya systemet (övergång från tidigare system, test av Heroma, migration av data från tidigare system till Heroma, integrering med ekonomisystem)?**
4. **Har behörighetsfrågan och GDPR hanterats på ett korrekt sätt?**
5. **Finns tillräcklig kontroll i rutiner kring lönehanteringen – systemmässig/automatisk kontra manuell hantering (inmatning eller kontroll)?**

Revisionsfråga 1: Har förberedelser (behovsanalys och kravspecifikation) och upphandlingsprocess varit tillräcklig med avseende på projektets omfattning?

Iaktagelser

Regiondirektören beslutade hösten 2015 att starta en förstudie inför upphandling av nytt HR-system. En förstudie genomfördes under hösten 2016 och inom ramen för förstudien genomfördes exempelvis workshops med verksamheten samt även studiebesök på plats hos två andra regioner. Resultatet dokumenterades i en förstudierapport och presenterades för Regionstyrelsens personalutskott i januari 2017. Regionstyrelsen beslutade om upphandling av ett nytt HR-system under våren 2017 och därefter startades ett arbete med att identifiera behov och krav mer ingående. I september 2019 skrevs avtal med leverantören CGI.

I granskningen framgår att en extern projektledare anlitades för att driva arbetet med kravställning och upphandling tillsammans med medarbetare inom regionen (exempelvis en kravgrupp). Totalt togs ca 600 krav fram, innehållandes både funktionella och tekniska krav och med en uppdelning på ska- och bör-krav. För att identifiera organisationens behov och krav genomfördes workshops och intervjuer med representanter och yrkesgrupper i verksamheterna. Därefter var flera personer involverade i arbetet med att dokumentera och specificera kraven. Arbetssättet gick ut på att en person fick i uppgift att dokumentera kravet och att flera personer därefter kvalitetssäkrade skrivningen. En utmaning som lyfts fram i detta arbetet är att verksamheten inte tillsatte resurser i önskad omfattning för att delta i arbetet med att identifiera behov och krav, vilket medförde att vissa perspektiv ej belystes i tillräcklig utsträckning.

Anbudsunderlaget gick ut under våren 2019 och den leverantör som vann upphandlingen hade svarat ja på alla ska-krav. Inför upphandlingen testades 15 olika testfall inom lösningen av utsedda testgrupper från regionens verksamheter utefter den framtagna kravspecifikationen. Utvärderingen av testfallen var positiv där endast ett bör-krav inte uppfylldes. I granskningen framgår dock att testningen borde varit mer omfattande och exempelvis inkluderat testning av schemaläggning på ett bättre sätt.

Det framgår även i granskningen att en kostnadsuppskattning genomfördes inför upphandlingen samt att två personer från regionens upphandlingsenhet var involverade i upphandlingen. Regionen tog även referenser på två andra organisationer som använde Heroma för åtminstone områdena lön samt schema och bemanning sedan tidigare. Det uppges även att fackliga referensgrupper involverades inför att upphandlingen genomfördes.

På en övergripande nivå är de intervjuade nöjda med den fastställda kravspecifikationen. Men för vissa områden borde kraven ha varit tydligare och mer detaljerade, dels för att nå önskad funktionalitet på bättre sätt och dels för att öka verifierbarheten och minska utrymmet för olika tolkningar. Detta gäller exempelvis området schemaläggning där mer tid och resurser borde ha lagts på att utreda och detaljera kraven eftersom en fungerande schemaläggning är en så viktig del i verksamheten.

Att alla krav inte var tillräckligt tydliga har medfört att vissa krav inte har implementerats och att det finns en restlista med krav och områden som ska åtgärdas. Det har även medfört att vissa krav implementerats på ett sätt som inte uppfyller regionens faktiska behov. Regionen anser dock inte att leverantören brister i sin leverans avseende flera av dessa krav, då kraven inte var tillräckligt tydliga i sin formulering.

Enligt vår granskning genomfördes strukturerade riskanalyser innan uppstart av projektet gällande såväl verksamhetens mottagande av systemet som ur ett IT- och leverantörsperspektiv, vilket skapar bättre förutsättningar att lyckas med projektet så länge riskerna hanteras på ett ändamålsenligt sätt.

Revisionsfråga 1: Har förberedelser (behovsanalys och kravspecifikation) och upphandlingsprocess varit tillräcklig med avseende på projektets omfattning?

Bedömning

Utifrån iakttagelser från dokumentationsgranskning samt intervjuer är PwC:s bedömning att revisionsfrågan är **delvis uppfylld**.

Bedömningen baseras på att:

- Förstudie genomfördes inför beslut om upphandling.
- Workshops och intervjuer genomfördes med verksamheten i arbetet med att identifiera behov och krav.
- Det inför upphandlingen testades 15 olika testfall inom lösningen av utsedda testgrupper från regionens verksamheter utefter den framtagna kravspecifikationen. Testningen bedöms dock inte ha varit tillräckligt omfattande.
- Upphandlingsenheten och fackliga representanter involverades i arbetet inför upphandlingen.
- De intervjuade är nöjda med kravspecifikationen på en övergripande nivå, men kraven för vissa områden (exempelvis för schemaläggning) var inte tillräckligt genomarbetade.
- Det genomfördes strukturerade riskanalyser inför uppstart av projektet i syfte att identifiera väsentliga risker och fokusområden.

Revisionsfråga 2: Har utbildningen av medarbetare varit tillräcklig för att ge användarna förutsättningar att hantera systemet korrekt?

Iaktagelser

Utbildning av medarbetare i Heroma har bedrivits som ett delprojekt i införandet av Heroma. Den ursprungliga intentionen var att främst erbjuda en kombination av lärarledda fysiska utbildningar, digitala utbildningar och digitala guider. Men på grund av pandemin och de restriktioner som infördes så kunde inte fysiska utbildningar genomföras. Istället togs sex längre utbildningsfilmer utifrån olika ämnesområden fram. Som komplement till utbildningsfilmerna skapades även över 100 st guider som är integrerade i systemet och som kan tas del av genom både skrift och tal. Det skapades även ett antal manualer/lathundar, övningshäften samt en testmiljö för vissa användargrupper. Utbildningspaketet lanserades september 2021. Inför driftsättning genomfördes även ett flertal utbildningsworkshops med representanter från alla förvaltningarna. Det sattes även upp en telefonsupport dit användare kunde ringa för att ställa frågor (dock inte lönefrågor) och rapportera fel. Ärenden kunde även skapas digitalt genom regionens ärendehanteringssystem.

Inom ramen för projektet genomfördes uppföljning av hur organisationen upplevde och mottog utbildningarna. Önskemålet från organisationen var framförallt att kunna delta i lärarledda utbildningar. Detta började därför att erbjudas via Teams senare under våren 2022 (dvs. en tid efter driftsättning). I samband med detta började det även erbjudas bokningsbara utbildningsresurser som besökte verksamheter för att ge stöd på plats.

I granskningen framkommer några utmaningar och brister i arbetet med utbildning. Återkommande är att projektet borde ha genomfört mer utbildningsinsatser och tagit fram mer utbildningsmaterial för vissa områden, främst avseende schemaläggning och tolkning av lönespecifikationer. Detta borde även ha tillgängliggjorts i ett tidigare stadie inom projektet (redan inför driftsättning). Brister avseende detta har medfört mycket kritik och irritation hos medarbetare i organisationen. Det har även tagit mycket resurser från verksamheten att hantera de utmaningar som följt av detta.

Det har under införandet funnits en utmaning med att medarbetare inte har tagit del av utbildningsmaterialet i tillräcklig omfattning inför driftsättningen, vilket medförde att dessa användare hade bristande förutsättningar för att kunna hantera systemet på ett bra sätt. Värt att notera är dock att många medarbetare hade svårt att avsätta tid för att genomföra utbildningar under hösten/vintern 2021 då de under denna tidsperiod hade en hög arbetsbelastning från andra arbetsuppgifter som en konsekvens av pandemin. Vidare anges att det ej har genomförts uppföljning på individnivå i tillräcklig omfattning för att säkerställa att medarbetare tagit del av utbildningsmaterialet i tid.

Det lyfts även fram att verksamheten hade svårt att ta till sig av utbildningsmaterielet innan driftsättningen genomfördes då systemet inte var färdigbyggt. Detta medförde att utbildningarna blev abstrakta att genomföra samt att det var svårt för medarbetare att få tydliga svar från projektet om problem som uppstod. Vidare anges att det var ett hårt tryck på supporten vid driftsättning, vilket medförde att det tog lång tid för användare att få svar på vissa ärenden.

En annan utmaning som identifierats är att resurser i form av lokala projektledare och superanvändare inte tillsattes i nödvändig omfattning i vissa verksamheter. Dessa roller hade exempelvis i uppgift att fungera som lokala utbildare och organisera lokala utbildningsinsatser. Flera personer som hade dessa roller behövde avsätta tid för detta utöver sina ordinarie arbetsuppgifter. Detta medförde en hög arbetsbelastning för dessa personer samt påverkade stödet och utbildningar till användare på lokal nivå negativt. Pandemin och bristande resurser i kombinationen med att verksamheterna inte helt förstått sitt ansvar beskrivs som främsta anledningar till dessa utmaningar.

En aspekt som generellt uppges ha fungerat väl avseende utbildningar är att utbildningsmaterialet har uppdaterats kontinuerligt samt att det har varit tydligt för medarbetarna vart utbildningsmaterialet fanns att ta del av.

Revisionsfråga 2: Har utbildningen av medarbetare varit tillräcklig för att ge användarna förutsättningar att hantera systemet korrekt?

Bedömning

Utifrån iakttagelser från dokumentationsgranskning samt intervjuer är PwC:s bedömning att revisionsfrågan är **delvis uppfylld**.

Bedömningen baseras på att:

- Ett utbildningspaket med filmer, manualer och integrerade guider lanserades hösten 2021. Utbildningsmaterialet har även utvecklats och uppdaterats löpande sedan dess.
- Användare kunde ställa frågor och rapportera fel både via telefon och via regionens ärendehanteringssystem. Vid driftsättning var det dock hög belastning och det tog lång tid att få svar på vissa ärenden. Inför driftsättningen var det även svårt för verksamheten att få svar på frågor om hur systemet skulle fungera i praktiken, då systemet inte var färdigbyggt.
- Projektet borde ha genomfört mer utbildningsinsatser och tagit fram mer utbildningsmaterial för vissa områden, exempelvis avseende schemaläggning och tolkning av lönespecifikationer. Detta borde även ha tillgängliggjorts i ett tidigare stadie inom projektet (redan inför driftsättning). Brister avseende detta har medfört mycket kritik och irritation hos medarbetare i organisationen.
- Medarbetare inom vissa delar av organisationen har inte tagit del av utbildningsmaterial i tillräcklig omfattning inför driftsättningen, delvis på grund av pandemins effekter
- Vissa delar av verksamheten avsatte inte tillräckliga resurser för att arbeta med lokala projekt och med att tillsätta superanvändare. Detta påverkade innehållet och genomförandet av vissa utbildningar anpassade efter särskilda yrkesgrupper samt det lokala användarstödet negativt. Det medförde även en hög arbetsbelastning för de medarbetare som arbetade med de lokala projekten utöver sina ordinarie arbetsuppgifter.

Revisionsfråga 3: Har implementationen hanterats på ett sätt som skapar bra förutsättningar för funktion och integritet i det nya systemet?

Iaktagelser

Vi har i vår genomgång granskat övergripande projektmetodik och projektstruktur, hur Heroma och integrationer med andra system har testats innan driftstart samt hur projektet säkerställt att all data konverterats och migrerats fullständigt och riktigt från Primula till Heroma.

Vår granskning visar att projektet baserats på en strukturerad och väl dokumenterad projektplan där väsentliga delområden finns specificerade och utgör en bra grund för projektet. Vi har även gjort en genomlysning av den projektorganisation som etablerats och bedömer att den speglar verksamheten och intressentgrupperna på ett ändamålsenligt sätt. Vidare har även avstämningar med fackliga företrädare skett kontinuerligt under och efter projektets genomförande.

Projekt- och styrgruppsmöten har genomförts med fast periodicitet och beslut har tagits på olika nivåer beroende på påverkan på projektet. Mötesdiskussioner och beslut har dokumenterats i anteckningar från projektgruppsmöten samt i styrgruppsprotokoll.

Vår granskning visar att det genomförts kontinuerliga riskanalyser under projektets gång i syfte att identifiera risker med potentiell påverkan på tid, kostnad eller kvalitet för genomförandet. Riskanalyserna finns dokumenterade där vidtagna åtgärder och ansvarsområden framgår. Som vi noterat tidigare saknas dock en strukturerad riskanlys inför projektets uppstart i syfte att identifiera väsentliga fokusområden.

Testningen av systemet och dess integrationer har baserats på en initial testplan med syftet att beskriva upplägget och förutsättningarna för testarbetet. Utöver det har en teststrategi utarbetats, med liknande innehåll som testplanen. Testfall har erhållits från systemleverantören CGI och dessa har bearbetats för att anpassas till Region Uppsalas specifika förutsättningar.

I syfte att testa de specifika förutsättningar och avtal som finns inom Region Uppsala har två piloter genomförts, där delar av verksamheten varit involverade. Detta har sedan kompletterats med parallelltest, där utfall från Heroma och Primula jämförts för att säkerställa riktigheten i utfallet av lönekörningarna. Vi har i vår genomgång verifierat testarbetet genom granskning av den testdokumentation som tagits fram i samband med utförandet. Testningen av lönehanteringsfunktionerna i systemet har varit tillfredsställande, dock upplevs brister gällande test av schema- och bemanningsrutinerna i den nya miljön.

Migrering av data från Primula till Heroma gjordes inför driftstart med hjälp av instruktioner från CGI, genom två testmigreringar och en skarp migrering av data. Testmigreringarna verifierades av projektteamet och visade endast på mindre avvikelser, vilka kunde åtgärdas inför den skarpa migreringen. I samband med den skarpa migreringen noterades mindre avvikelser gällande kompsaldo av de som drabbats, vilket åtgärdades i samband med upptäckten.

Vid registrering av läkarnas löneavtal i Heroma gjorde Region Uppsala en alternativ tolkning av avtalet, jämfört med hur det hanterats i Primula. Tolkning av avtalet gjordes i samråd med SKR, utan att involvera eller informera läkarföreningen. Detta har medfört att läkarnas löner gällande jour- och beredskap har förändrats samt att avrundningsregler fungerar annorlunda mot tidigare, vilket dock beslutats vara den korrekta tolkningen av avtalet.

Även utbildningen av användarna inför driftstart har stor påverkan på hanteringen av systemet och därmed även integriteten i informationen i systemet. Vi har berört detta i tidigare avsnitt och identifierat vissa brister gällande genomförandet av utbildningen, vilket får stor påverkan på såväl användarnas upplevelse av systemet som riktigheten i utfallet från systemet.

Vår uppfattning efter de intervjuer som genomförts med projektledning och projektdeltagare är att det trots pandemin och den påverkan det fått på organisationen och tillgången på resurser, funnits ett stort engagemang och en förståelse för vikten av projektet.

Revisionsfråga 3: Har implementationen hanterats på ett sätt som skapar bra förutsättningar för funktion och integritet i det nya systemet?

Bedömning

Utifrån iakttagelser från dokumentationsgranskning samt intervjuer är PwC:s bedömning att revisionsfrågan är **delvis uppfylld**.

Bedömningen baseras på att:

- Projektmodellen har varit väl strukturerad och det har funnits en bra styrningsmodell genom projektet
- Projektorganisationen har speglat verksamheten på ett ändamålsenligt sätt och involverat externa referensgrupper
- Riskanalyser har utförts och uppdaterats kontinuerligt under projektets gång
- Utbildningen, vilket vi skrivit om tidigare, var i vissa avseenden bristfällig och det säkerställdes inte att användarna genomgick utbildning innan behörighet tilldelades. Användarnas hantering av systemet är en viktig faktor för integriteten i informationen i systemet.
- Testplanen som tagits fram är relativt kortfattad och översiktlig och upplevs inte som färdigbearbetad. Den innehåller ingen översikt av de områden som ska testas eller vilka integrationer eller beroenden som bör beaktas i testningen. Ett gediget förarbete skapar bättre förutsättningar för ett lyckat genomförande och utfall.
- Upplägget på testningen, med pilottester och parallelltester, skapar bra förutsättningar för att testa ett stort och representativt urval av den framtida populationen och jämförelsen av utfall mellan Primula och Heroma identifierar tydligt eventuella brister. Vår bedömning är att testningen av lönehanteringen i Heroma utfördes på ett tillfredsställande sätt, men att det enligt ovan finns utrymme för förbättring gällande den beskrivande dokumentationen av testningen.
- Testning av funktionalitet för schema/bemanning påbörjades i ett sent skede och utfördes ej i tillräcklig omfattning för att minimera risken för brister vid driftstart
- Migreringen av data har hanterats på ett strukturerat sätt med ändamålsenlig verifiering av utfallet
- Det kvarstår viss osäkerhet inom organisationen kring riktigheten i nuvarande löneutbetalningar från Heroma. Denna osäkerhet behöver analyseras och adresseras av HR-funktionen i syfte att öka förtroendet för Heroma i organisationen.

Revisionsfråga 4: Har behörighetsfrågan och GDPR hanterats på ett korrekt sätt?

Iaktagelser

Uppsättning av roller och behörigheter har bedrivits som ett av delprojekten i införande av Heroma och utgick bland annat från de system som Heroma skulle ersätta.

Informationssäkerhet har funnits med som ett av perspektiven i kravställningen som genomfördes inför upphandlingen. Under projektet har det dock mellan Region Uppsala och leverantören uppstått olika syn på inloggnings- och lösenordshanteringen för Kom & Gå (lösningen för tidsregistrering). Detta medförde att det inför driftsättning av lösningen saknades en ändamålsenlig uppsatt lösenordshantering. Trots detta valde regionen att driftsätta lösningen, vilket medförde att medarbetare kunde logga in på andra anställdas användarkonton i Kom&Gå genom att ange användarnamn och användar-ID (samt genom att vara ansluten till regionens nätverk). Den information som kunde tas del av var exempelvis namn på personen, in- och utstämplingar under de senaste 8 dagarna, om personen begärt frånvaro (dock inte typ av frånvaro) samt dagens- och morgondagens arbetstid. Vissa uppgifter kunde även ändras av den som loggade in. En riskanalys ur detta perspektiv genomfördes inte i samband med driftsättningen. Att obehöriga kunde ta del av denna typ av information om andra medarbetare är en brist ur ett konfidentialitets- och integritetsperspektiv. Hösten 2022 implementerade regionen en egen lösenordshantering och användare behöver nu logga in genom anställningskort eller lösenord. Under intervju lyfts det fram som en lärdom att denna lösenordshantering borde ha implementerats tidigare.

Om en incident har inträffat som sannolikt leder till risker för de registrerades fri- och rättigheter ska det anmälas till Integritetsskyddsmyndigheten (IMY) inom 72 timmar från det att incidenten upptäcktes. I granskningen noteras att regionens anmälan till IMY gjordes hösten 2022, dvs flera månader efter driftsättning. Detta indikerar brister i regionens rutiner för hantering av personuppgiftsincidenter.

I övrigt visar granskningen att en manual för behörighetsadministration har utvecklats inom projektet. Användares behörigheter styrs av roll, PA-team och organisation. I dagsläget finns 12 olika typer av roller uppsatta inom systemet och vid utdelning av behörigheter finns kontroller i form av att en chef godkänner behörighetstilldelning. Initialt användes blanketter för att dokumentera behörighetsbeställningar, men sedan sommaren 2022 används ett ärendehanteringssystem för att stödja i arbetet med att tilldela, ändra och ta bort behörigheter. Det finns även en integration med regionens Active Directory (AD) som stöd i arbetet med att hantera och organisera användare och behörigheter. Det framgår även att antalet höga behörigheter begränsas till ett minimum och att regelbundna kontroller genomförs att medarbetare har rätt behörighet.

En utmaning som lyfts fram är att organisationsträdet i systemet inte har varit ändamålsenligt uppsatt. Detta har medfört att medarbetares attestfrågor om exempelvis jourersättning, semester, tjänstledighet gått till fel chef i organisationen, vilket bidragit till ökad administration för chefer. En annan brist som identifieras i granskningen är att det saknas arbetssätt och rutiner för att följa upp systemets loggar av användaraktiviteter.

Avseende GDPR har ett personuppgiftsbiträdesavtal tecknats med leverantören som en del av huvudavtalet. Avtalet reglerar exempelvis personuppgiftsbiträdets åtaganden, användandet av underbiträden samt överföring till tredje land. Det har även etablerats förutsättningar för att säkerställa de registrerades rättigheter samt automatiska gallringsrutiner för radering av personuppgifter utefter särskilda intervall. Vidare framkommer att en konsekvensbedömning (som görs i syfte att förebygga risker ur ett dataskyddsperspektiv) påbörjades inför upphandlingen av Heroma, men att den ej färdigställdes innan införandet. Konsekvensbedömningen slutfördes dock efter införandet av Heroma (hösten 2022). Det har inom ramen för projektet ej heller utretts om regionens behandlingsregister behöver uppdateras med anledning av införandet.

Revisionsfråga 4: Har behörighetsfrågan och GDPR hanterats på ett korrekt sätt?

Bedömning

Utifrån iakttagelser från dokumentationsgranskning samt intervjuer är PwC:s bedömning att revisionsfrågan är **delvis uppfylld**.

Bedömningen baseras på att:

- Heromas applikation för tidsregistrering, Kom & Gå, driftsattes utan en ändamålsenlig lösenordshantering var etablerad, vilket medförde att medarbetare kunde logga in på andra anställdas konton. En mer ändamålsenlig lösning för lösenordshantering lanserades november 2022.
  - Anmälan till IMY gjordes flera månader efter att incidenten upptäcktes, vilket indikerar brister i rutinerna för hantering av personuppgiftsincidenter inom regionen.
- En manual för behörighetshantering har etablerats inom projektet och regelbundna kontroller genomförs för att säkerställa att medarbetare har rätt behörighet.
- Ett ärendehanteringssystem används i hanteringen av behörigheter för att stärka spårbarheten.
- Loggning av användaraktiviteter finns aktiverat, men det saknas rutiner och arbetssätt för att följa upp loggarna.
- Personuppgiftsbiträdesavtal ingår som en bilaga till huvudavtalet.
- Förutsättningar för att hantera de registrerades rättigheter har etablerats.
- Automatiska gallringsrutiner för radering av personuppgifter har etablerats.
- En konsekvensbedömning avseende implementeringen av Heroma slutfördes ej inför införandet, vilket är en brist eftersom syftet med en konsekvensbedömning är att förebygga risker innan de uppkommer.
- Det har inom ramen för projektet ej utretts om regionens behandlingsregister behöver uppdateras med anledning av införandet.

Revisionsfråga 5: Finns tillräcklig kontroll i rutiner kring lönehanteringen – systemmässig/automatisk kontra manuell hantering (inmatning eller kontroll)?

Iaktagelser

För att skapa en trygg och säker lönehantering är det viktigt att rutinerna i löneprocessen har god intern kontroll. Vi har som en del av vår granskning gått igenom och verifierat de kontrollmoment som utförs i den löpande lönehanteringen i syfte att säkerställa korrekta utbetalningar till de anställda inom regionen.

Heroma har en strikt behörighetsstruktur med ett stort antal roller som tilldelas användare baserat på ansvar i verksamheten. Detta är grunden till en säker lönehantering, att rätt personer har tillgång till rätt information och funktioner i systemet. Vår granskning visar att behörighetsstrukturen i Heroma är ändamålsenlig och följer de ansvarsområden som finns i verksamheten.

Underhåll och förändring av fasta data kan enbart utföras av löneadministratörer och alla förändringar loggas och möjlighet finns att ta ut loggrapporter vid behov. Region Uppsala gör ingen regelbunden kontroll av loggar i syfte att proaktivt identifiera avvikelser utan använder dem enbart vid specifika behov.

Heroma har en helt digitaliserad process från tidrapportering till utbetalning av lön samt ett flertal förebyggande automatiska systemkontroller som ska säkerställa indata och dataflödet i systemet, vilket minskar risken för fel i hanteringen av löner så länge grunduppgifterna i systemet är riktiga. Detta är en förbättring jämfört med hanteringen i Primula. Utöver de automatiska kontrollerna utförs även uppföljande kontroller och analyser av lönekonsulterna i samband med lönekörning i syfte att upptäcka felaktigheter. Detta till stor del baserat på fellistor från Heroma. Vidare ligger det ett ansvar på verksamheten att säkerställa att medarbetarna ligger på rätt avtal och att tidrapporteringen hanteras korrekt och slutförs.

Bedömning

Utifrån iakttagelser från dokumentationsgranskning samt intervjuer är PwC:s bedömning att revisionsfrågan är **uppfylld**.

Bedömningen baseras på att:

- Väsentliga kontrollmoment finns implementerade i löneprocessen och rutindokumentation finns i allt väsentligt framtagen i syfte att tydliggöra arbetsmoment och väsentliga kontroller. Det kvarstår visst arbete med rutindokumentation för lönekonsulternas ansvarsområden.
- Det finns en separat dokumentation av de nyckelkontroller som ska utföras i processen. Dokumentationen behöver dock vidareutvecklas för att tydliggöra respektive kontrollmoment samt ansvarsfördelningen gällande utförandet.
- Behörighetsstrukturen i Heroma är genomarbetad och följer de ansvar som finns i verksamheten
- Flödet är till stor del digitaliserat och automatiskt i Heroma, med systemkontroller genom hela flödet som satts upp för att minska risken för fel
- Loggfunktion finns som möjliggör uppföljning av alla förändringar i fast data.

3

Samlad bedömning

Samlad bedömning

Granskningen syfte var att granska och utvärdera implementationen av Heroma och om den skett med tillräcklig styrning och intern kontroll. Utifrån genomförd granskning är vår samlade bedömning att införandet **delvis** skett med tillräcklig styrning och intern kontroll.

Revisionsfrågor	Bedömning	
1. Har förberedelser (behovsanalys och kravspecifikation) och upphandlingsprocess varit tillräcklig med avseende på projektets omfattning?	**Delvis** - En förstudie genomfördes inför beslut om upphandling och upphandlingsenheten samt fackliga representanter involverades i arbetet inför upphandlingen. Kraven för vissa områden (exempelvis för schemaläggning) var inte tillräckligt genomarbetade.	
2. Har utbildningen av medarbetare varit tillräcklig för att ge användarna förutsättningar att hantera systemet korrekt?	**Delvis** - Ett omfattande utbildningspaket har lanserats, men mer utbildningsinsatser borde ha genomförts avseende schemaläggning och tolkning av lönespecifikationer. Medarbetare hade även svårt att få hjälp med problem som uppstod både inför- och efter driftsättning.	
3. Har implementationen hanterats på ett sätt som skapar bra förutsättningar för funktion och integritet i det nya systemet?	**Delvis** - Vår bedömning baseras på att det funnits en strukturerad projektorganisation och metodik under införandet och att migreringen av data genomförts på ett ändamålsenligt sätt. Vissa iakttagelser har gjort vad gäller systemtestning av funktionalitet samt utbildningen inför driftstart.	
4. Har behörighetsfrågan och GDPR hanterats på ett korrekt sätt?	**Delvis** - Heromas applikation för tidsregistrering driftsattes utan en ändamålsenlig lösenordshantering var etablerad. En manual för behörighetshantering har etablerats inom projektet. Organisationsträdet i systemet är inte ändamålsenligt uppsatt. Förutsättningar för att hantera de registrerades rättigheter har och automatiskt galla personuppgifter har etablerats.	
5. Finns tillräcklig kontroll i rutiner kring lönehanteringen – systemmässig/automatisk kontra manuell hantering (inmatning eller kontroll)?	**Uppfyllt** - Vår bedömning baseras på att det finns en ändamålsenlig behörighetsstruktur uppsatt i Heroma samt implementerade kontroller i lönehanteringsprocessen. Processen har även digitaliserats och automatiserats ytterligare vid införande av Heroma och endast ett fåtal manuella moment kvarstår.	

4

Bilagor

Dokumentationslista

I vårt arbete har vi tagit del av en stor mängd dokumentation kopplat till projektet i syfte att sätt oss in i projektets förutsättningar samt bedöma ändamålsenligheten i den projektdokumentation som projektet arbetat efter. Vi har även granskat dokumentation samt det som tagits fram under projektets gång. De kategorier av dokumentation vi tagit del av är enligt nedan.

- Policy’s och riktlinjer gällande upphandling inom Region Uppsala
- Krav och behovsanalys / projektförberedande dokumentation
- Risk- och konsekvensanalyser
- Grundläggande projektdokumentation
- Avtalsdokumentation systemleverantör
- Mötesprotokoll och beslutsunderlag
- Testdokumentation systemtester och migrering av data
- Utbildningsplan
- Manual behörighetshantering
- Processdokumentation och rutinbeskrivningar löneprocessen

Intervjupersoner

UTKAST

De roller som intervjuats inom ramen för granskningen är följande:

- Projektledare
- Delprojektledare - Utbildning
- Delprojektledare - Behörigheter
- Delprojektledare Teknik och Integrationer
- Testledare
- Deltagare projektforum
- Representanter från verksamheten
- Representanter från Upplands allmänna läkarförening
- Systemförvaltare
- Chef HR verksamhetsstöd
- HR-direktör
- Chef HR-center/Objektledare HR-objektet
- Lönekonsulter

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av Region Uppsala enligt de villkor och under de förutsättningar som framgår av projektplan från den 2022-12-08. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.

2023-03-14

Rebecka Hansson	**Martin Westholm**
Uppdragsledare	Projektledare