# Granskning av Regionens anpassning mot lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster

**Region Örebro län**

**Juni 2020**

*Rebecka Hansson*
*David Dymmel*
*Jessica Garpvall*
*Josefine Bäck*

**Revisionsrapport**

# Innehållsförteckning


**Sammanfattning och rekommendationer** 2

**Inledning** 5

1.1 Bakgrund 8

1.2 Syfte och revisionsfråga 8

1.3 Revisionskriterier 8

1.4 Kontrollmål 8

1.5 Avgränsning 8

1.6 Metod 6

**2. Iakttagelser och bedömningar** 8

2.1 Identifiering av samhällsviktiga och digitala tjänster 8

2.2 Systematiskt och riskbaserat informationssäkerhetsarbete 10

2.3 Incidentrapportering av NIS-incidenter 14

2.4 Riskanalys och tillhörande åtgärdsplan 15

2.5 Kontinuitetshantering 17

**3. Revisionella bedömningar** 19

**Bilagor** 22

**Bilaga 1 - Granskad dokumentation** 22

**Bilaga 2 - Revisionella bedömningsgrunder** 23

# Sammanfattning och rekommendationer

**Vi bedömer att Hälso- och sjukvårdsnämnden i Region Örebro län ("regionen"), med de åtgärder som vidtagits, inte uppfyller de krav som ställs på leverantörer av samhällsviktig verksamhet genom lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174).**

Inom ramen för regionens revision 2020 har PwC på uppdrag av regionens förtroendevalda revisorer granskat de åtgärder regionen vidtagit för att säkerställa att de leverantörer av samhällsviktiga och digitala tjänster som regionen äger eller på annat sätt ansvarar för anpassat sin verksamhet till lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (lag 2018:1174), inom verksamheter knutna till Hälso- och sjukvårdsnämnden i Region Örebro län.

Regionen arbetar löpande med informationssäkerhet och med sin anpassning mot lag 2018:1174 sedan 2018. Arbetet med informationssäkerhet drivs av enheten för juridik och informationssäkerhet, som rapporterar till Regionstyrelsen. Arbetet med anpassning mot lag 2018:1174 har påbörjats inom Hälso- och sjukvårdsnämndens verksamheter, men det finns vid tidpunkten för granskningen en otydlig fördelning av ansvar samt en avsaknad av aktiviteter med konkreta arbets- samt tidsplaner för anpassning till lagen. Informationssäkerhetsarbete i mer generella termer är en del av Hälso- och sjukvårdsnämndens verksamheters arbete redan idag. Detta arbete genomförs med utgångspunkt i standarden ISO/IEC 27001:2017 (Ledningssystem för informationssäkerhet) och de metoder och riktlinjer som finns på plats berör till viss del kraven genom lag 2018:1174, då arbetet som genomförts har syftat till att upprätthålla ett systematiskt och riskbaserat informationssäkerhetsarbete inom verksamheterna. Dock är dokumentation, metoder och riktlinjer inte heltäckande för att möta lagkraven och inte heller specifikt utvecklade mot bakgrund av lag 2018:1174.

Efter genomförd granskning bedömer vi att Region Örebro län **inte uppfyller** de krav som ställs genom lagen om informationssäkerhet för samhällsviktiga och digitala tjänster. Även om vissa åtgärder har vidtagits är dessa och planerade inte tillräckliga för att uppfylla kraven. Regionens åtgärder kopplade till införandet av lag 2018:1174 bedöms framförallt brista avseende:

- detaljerad kartläggning av verksamheten i syfte att specifikt identifiera samhällsviktig verksamhet, vilket leder till att regionen inte har kunskap om sina specifika beroenden till nätverk och informationssystem för leverans av sina samhällsviktiga tjänster,
- att peka ut tydliga och uppföljningsbara ansvars- och ledningsförhållanden för att utveckla och genomdriva nödvändiga åtgärder,
- rutiner och vägledningar för hantering och rapportering av incidenter i nätverk och informationssystem, internt likväl som till ansvarig myndighet.

För sammanställd bedömning av respektive kontrollmål se kapitel 3, Revisionell bedömning.

Utifrån granskningens resultat rekommenderar vi Region Örebro län att:

- tydliggöra ledning och styrning samt det formella ansvaret för att utveckla , implementera och rapportera åtgärder kopplade till lagen (kontrollmål I),

- utveckla och dokumentera rollbeskrivningar med definierade ansvarsområden för implementering av åtgärder på verksamhetsnivå (Kontrollmål I),

- etablera en roll/funktion i verksamheten med ansvar för informationssäkerhet syftandes till att säkerställa förståelse och kompetens inom informationssäkerhet samt möjlighet till förenklad kommunikation på verksamhetsnivå. Denna roll/funktion bör tilldelas ansvar och ägarskap på verksamhetsnivå för åtgärder kopplade till lagen. Denna roll/funktion kan med fördel vara motpart och kontaktpunkt till IT och enheten för juridik och säkerhet i frågor som rör IT- och informationssäkerhet (kontrollmål II),

- genomföra en detaljerad verksamhetskartläggning i syfte att identifiera samhällsviktiga verksamheter. Utifrån denna verksamhetskartläggning bör regionen definiera vilka beroenden till nätverk och informationssystem som är särskilt kritiska för att leverera identifierade samhällsviktiga verksamheter. Vidare bör det vara incidenter relaterade till dessa identifierade nätverk och informationssystem som leder till en incidentrapport i enlighet med lag 2018:1174, se vidare rekommendation 8 nedan (kontrollmål II),

- utveckla en planering för kommunikation, övning och utbildning inom området informationssäkerhet vilken inkluderar regionens samtliga medarbetare (kontrollmål (II & V),

- öka kompetens inom informationsklassning genom rekrytering och utbildning för att säkerställa att information klassas kontinuerligt och rätt. Genom att sprida kunskap om informationsklassning till fler kan regionen minska personberoendet, frigöra resurser och därigenom fokusera mer på strategisk utveckling inom informationssäkerhetsområdet (kontrollmål II),

- tydliggöra former för uppföljning, utvärdering och erfarenhetsåterföring vid utbildnings- och övningsverksamhet samt vid skarpa händelser kopplat till informationssäkerhet (kontrollmål II),

- definiera vad som klassificeras som en s.k. "NIS-incident" och skapa rutin för incidentrapportering (kontrollmål III),

- uppdatera relevanta styrdokument med utgångspunkt i lag (2018:1174) (kontrollmål IV)

- utse objektägare med ansvar för nätverk och informationssystem som ansvariga för att genomföra riskanalyser på sina objekt kopplade till samhällsviktiga leveranser (kontrollmål IV),

- utse ägare och leveransdatum för att genomföra övergripande riskanalys i enlighet med lagtexten (kontrollmål IV),
- fortsätt arbetet med framtagandet av kontinuitetsplaner för Hälso- och sjukvårdsnämndens kritiska och samhällsviktiga tjänster och beroenden. (Kontrollmål V),
- säkerställ att samtliga verksamheter har kontinuerligt reviderade och implementerade kontinuitetsplaner som bygger på krav om genomförd verksamhetskonsekvensanalys enligt regionens gällande riktlinjer. (Kontrollmål V).

# 1. Inledning

## 1.1 Bakgrund

I enlighet med upprättad revisionsplan för 2020 har vi granskat Hälso- och sjukvårdsnämnden i Region Örebro läns vidtagna åtgärder för att efterleva krav i enlighet med lag 2018:1174.

Europaparlamentet antog i juli 2016 ett direktiv för att uppnå en hög gemensam lägstanivå inom cybersäkerhet i unionen. Syftet med direktivet är att säkerställa säkerheten i nätverk och informationssystem för samhällsviktiga tjänster inom sektorerna; energi, transport, bankverksamhet, finansmarknadsinfrastruktur, hälso- och sjukvård, leverans och distribution av dricksvatten samt säkerheten i nätverk och informationssystem för digital infrastruktur. Direktivet infördes i Sverige genom lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster.

Enligt lagen ska leverantörer av samhällsviktiga tjänster bedriva ett systematiskt och riskbaserat informationssäkerhetsarbete. Bland annat ska en riskanalys genomföras och en åtgärdsplan utvecklas.

Därtill är leverantörerna enligt samma lag ålagda att säkerställa en incidentrapporteringsstruktur för incidenter som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst som de tillhandahåller.

Uppfyller inte leverantörerna av samhällsviktiga tjänster sina skyldigheter kan sanktionsavgifter upp till 10 miljoner kronor komma att utfärdas.

Sveriges regioner levererar direkt eller indirekt genom regionägda bolag samhällsviktiga och digitala tjänster inom flertalet av de identifierade sektorerna till sina medborgare och omfattas således av den nya lagstiftningen.

Revisorerna har med utgångspunkt i väsentlighet och risk funnit det angeläget att granska efterlevnad av lagen om informationssäkerhet för samhällsviktiga och digitala tjänster inom verksamheter knutna till Hälso- och sjukvårdsnämnden i Region Örebro län.

## 1.2 Syfte och revisionsfråga

Har Hälso- och sjukvårdsnämnden säkerställt att de leverantörer av samhällsviktiga och digitala tjänster som nämnden (regionen) äger eller på annat sätt ansvarar för anpassat sin verksamhet till lagen om informationssäkerhet för samhällsviktiga och digitala tjänster?

## 1.3 Revisionskriterier

- Lag (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster
- Förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster
- MSB:s och tillsynsmyndigheternas föreskrifter inom området
- Regionens/nämndens egna riktlinjer inom området

## 1.4 Kontrollmål

I. Har regionen identifierat de samhällsviktiga och digitala tjänster som faller under deras ansvar och vilka som levererar dessa?
II. Arbetar leverantörerna av dessa samhällsviktiga och digitala tjänster systematiskt och riskbaserat med sitt informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster?
III. Har leverantörerna av dessa samhällsviktiga och digitala tjänster en rutin för incidentrapportering av s.k. "NIS-incidenter"?
IV. Har leverantörerna av dessa samhällsviktiga och digitala tjänster utfört en riskanalys med ingående åtgärdsplan?
V. Har leverantörerna av dessa samhällsviktiga och digitala tjänster tagit fram kontinuitetsplaner för att säkerställa kontinuiteten i tjänsterna?

## 1.5 Avgränsning

Granskningen omfattar de samhällsviktiga tjänster som ligger inom Hälso-och sjukvårdsnämndens ansvarsområde tillsammans med de informationssystem och nätverk som dessa tjänster är beroende av.

Det har under arbetet med denna granskning framkommit att Region Örebro län inte ställt några specifika krav på sina leverantörer mot bakgrund av lag 2018:1174 och därför har en avgränsning för denna granskning varit att endast titta på regionens verksamhet och utesluta leverantörerna.

## 1.6 Metod

Granskningen har genomförts under januari till mars 2020 av Jessica Garpvall, Josefine Bäck och David Dymmel och har kvalitetssäkrats av Rebecca Hansson. Granskningen har dels genomförts på plats i Örebro genom workshopar och dels genom intervjuer över telefon med nyckelpersoner inom Region Örebro län och dels genom dokumentgenomgång.

Metoden innefattar granskning genom workshop och intervjuer med berörda tjänstemän och politiker i Region Örebro län tillsammans med granskning och sammanställning av relevant dokumentation.

Följande funktioner vid regionen har medverkat till denna granskning:

- Avdelningschef, Drift och Teknik
- Avdelningschef, Medicintekniska IT-system
- Chefsläkare, Hälso- och sjukvårdsförvaltningen
- Enhetschef, Enheten för juridik och informationssäkerhet
- Förvaltningsledare, Avdelning vårdsystem
- Gruppchef, Datakom
- Gruppchef, Serverdrift
- Informationssäkerhetssamordnare, Enheten för juridik och informationssäkerhet
- IT-samordnare, Vårdnära IT-stöd
- IT-säkerhetsansvarig
- Kanslichef, Regionkansliet
- Ordförande Hälso- och sjukvårdsnämnden

- Områdeschef (Thorax, kärl och diagnostik, Psykiatrin, Närsjukvårdsvårdområde Örebro och Söder inkl. AK-mottagningen USÖ)
- Systemtekniker, Avdelning vårdsystem
- Verksamhetschef (Psykiatrisk akut- och heldygnsvård, Primärvården VC Freja, Kopparberg och Storå)

Se bilaga 1 för förteckning över granskad dokumentation.

# 2. Iakttagelser och bedömningar

## 2.1 Identifiering av samhällsviktiga och digitala tjänster

***Kontrollmål I:*** *Har regionen identifierat de samhällsviktiga och digitala tjänster som faller under deras ansvar och vilka som levererar dessa?*

### *2.1.1 Iakttagelser*

En analys för att undersöka hur lag 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster påverkar Region Örebro län har genomförts. Efter diskussioner i en arbetsgrupp, där enheten för juridik och informationssäkerhet var sammankallande tillsammans med representanter från Länstrafiken, Hälso- och sjukvårdsförvaltningen, Folktandvården, Regionservice IT, Beredskap och säkerhet samt Medicinteknik, konstaterade regionen att hälso- och sjukvården med klinisk forskning samt Folktandvården[1] identifierats som samhällsviktiga tjänster under regionens ansvar. Ingen ytterligare detaljnivå i fråga om identifierade samhällsviktiga tjänster har enligt regionen utvecklats. Regionen har inga digitala tjänster som de beskrivs i lagen[2]. Regionens analys av lagstiftningen och hur den påverkar regionen utgick ifrån MSBFS 2018:7 föreskrifter om anmälan och identifiering av leverantörer av samhällsviktiga tjänster. Denna analys har dock inte dokumenterats eller fastställts i andra forum utöver den arbetsgrupp som diskuterade frågan. Vidare har inga handlingsplaner eller annan dokumentation för åtgärder som säkerställer efterlevnad av lagen tagits fram. Externa leverantörer som tillhandahåller tjänster för regionen uppges inte heller ha mottagit någon formell kommunikation kring uppdaterade krav i förhållande till lagen.

Enligt 23 § i lag 2018:1174 har leverantörer av samhällsviktiga tjänster en anmälningsskyldighet till respektive tillsynsmyndighet. För hälso- och sjukvårdssektorn är det Inspektionen för vård och omsorg (IVO) som är utpekad tillsynsmyndighet. En anmälan ska enligt lagen ske utan dröjsmål och i anmälan ska det framgå om leverantören tillhandahåller en samhällsviktig tjänst i två eller flera medlemsstater inom Europeiska unionen. Regionen anmälde 2019 Hälso- och sjukvårdsförvaltningen[3] som samhällsviktig tjänst till Inspektionen för vård och omsorg.[4] Utöver anmälan efterfrågas i lagen (12 §) en riskanalys vilken ska ligga till grund för säkerhetsåtgärder. Vidare ska det enligt lagen ingå en åtgärdsplan i denna riskanalys och den ska dokumenteras och uppdateras årligen. En sådan riskanalys med tillhörande åtgärdsplan har regionen i dagsläget inte tagit fram.

Ansvaret för att implementera lag 2018:1174 inom regionen har överlämnats till HSF från den ursprungliga arbetsgruppen som drevs av enheten för juridik och informationssäkerhet. Det är således förvaltningen med tillhörande verksamhet som har

---

[1] Folktandvården är exkluderad utifrån granskningens omfattning, där fokus ligger på hälso- och sjukvårdens ansvarsområde.

[2] Digitala tjänster definieras som internetbaserad marknadsplats, internetbaserad sökmotor, molntjänst (2 § Lag 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster

[3] Hädanefter även omnämnd som HSF

[4] NIS-anmälan.pdf

givits ansvaret internt inom regionen att säkerställa att regionen lever upp till kraven enligt lag 2018:1174.

Det uppges vid intervjuer att HSF i sitt arbete med att implementera lag 2018:1174 haft stöd från de centrala funktionerna (framförallt regionservice IT och enheten för juridik och informationssäkerhet). Erhållet stöd till HSF i denna fråga har inte varit formaliserat och har skett på behovsbasis.

Även om ansvaret för att leva upp till lag 2018:1174 har fördelats från enheten för juridik och informationssäkerhet till HSF uppges detta inte tydligt ha kommunicerats och inte heller implementerats inom region Örebro. Det framkommer vid intervjuer att ansvaret för implementering av 2018:1174 är otydligt.

Regionens bedömning om att viss verksamhet inom dess ansvarsområde identifierats som samhällsviktig och att denna verksamhet därmed omfattas av lag 2018:1174 har endast kommunicerats till delar av hälso- och sjukvårdsförvaltningens olika verksamheter och medarbetare. Det framkommer att en del medarbetare som till exempel intervjuade områdescheferna känner till lagen och vet i stora drag vad den innebär men att det på andra nivåer och delar av verksamheterna helt saknar kännedom om lagen och dess innebörd och effekter.

Det saknas dokumenterade rollbeskrivningar och definierade ansvarsområden för arbete med lag 2018:1174 inom HSF och under intervjuer framkom det att ansvarsfördelningen rörande implementering av åtgärder till följd av lagen är oklar, där vissa områden uppger att det är IT:s ansvar medan andra uppger att det är verksamheten som ska sköta det.

### *2.1.2 Bedömning*

Kontrollmålet bedöms vara **delvis uppfyllt.**

Bedömningen baseras på att det i denna granskning framkommit att regionen påbörjat ett arbete med att analysera hur och i vilken omfattning de berörs av lag 2018:1174. Regionen har som ett led i detta arbete identifierat och anmält den samhällsviktiga tjänsten, hälso- och sjukvård, till tillsynsmyndigheten IVO. Beslutet har även i viss utsträckning kommunicerats internt.

Regionens analyser och bedömningar kopplat till tolkning av samt implementering av lag 2018:1174 har dock inte dokumenterats. Regionen har inte i detalj identifierat och prioriterat verksamheter som samhällsviktiga för att därigenom kostnadseffektivisera och förenkla arbetet med lag 2018:1174. Genom att ytterligare urskilja vilka verksamheter, processer och aktiviteter inom den nu anmälda bredare definitionen av all hälso- och sjukvård inom regionen som särskilt viktiga för det svenska samhället kan regionen enklare kravställa leveranser i de informationssystem och nätverk som stödjer just dessa prioriterade verksamheter och därmed minska kostnader för andra delar.

Vidare har regionens beslut om åtgärder i relation till lag 2018:1174 i den mån det finns några, inte kommunicerats till samtliga berörda delar av verksamheten. Det saknas också uppgifter om att tredje part, det vill säga externa leverantörer till underliggande informationssystem och nätverk skulle ha mottagit någon information alls eller ytterligare

krav i relation till sin leverans av tjänster till regionen. Det har även framkommit att det råder en otydlighet över hur arbetet ska struktureras och implementeras i verksamheten. Det saknas dokumenterade rollbeskrivningar och definierade ansvarsområden inom tjänstemannaorganisationen (vilka innehar ansvaret att implementera åtgärder) vilket i sin tur riskerar att leda till att kraven i lag 2018:1174 inte kan efterlevas.

## 2.2 Systematiskt och riskbaserat informationssäkerhetsarbete

***Kontrollmål II:*** *Arbetar leverantörerna av dessa samhällsviktiga och digitala tjänster systematiskt och riskbaserat med sitt informationssäkerhetsarbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster?*

### *2.2.1 Iakttagelser*

**Ledning och styrning**

**Politisk ledning**

IT- och informationssäkerhet är ett ämne som uppges finnas på agendan för den politiska ledningen inom Region Örebro län. Det har under 2019 skett en organisatorisk förändring inom den politiska organisationen och det var i samband med den förändringen som Hälso- och sjukvårdsnämnden[5] skapades, med ansvar för Hälso- och sjukvårdsförvaltningens olika verksamhetsområden.

Det uppges vid intervju med ordförande för HSN att arbetet med lag 2018:1174 om informationssäkerhet för samhällsviktiga och digitala tjänster är under uppbyggnad och att det i dagsläget inte är fastställt hur detta arbete ska organiseras eller vilken eventuell påverkan detta arbete får på styrande dokumentation. Dock ligger ansvaret för informationssäkerhet under Regionstyrelsen som enheten för juridik och informationssäkerhet rapporterar till. Inom hälso- och sjukvården berörs informationssäkerhet inom ramen för rapportering rörande patientsäkerhet, vilket vid intervju uppges fungera adekvat.

**Tjänstemannaorganisation**

Enheten för juridik och informationssäkerhet driver arbetet med informationssäkerhet inom regionen och sammanställer årligen en verksamhetsrapport. Rapporten beskriver vid sidan av verksamhetens framdrift även hur arbetet följs upp och poängterar ett antal förbättringsåtgärder, för att säkerställa att arbetet kan fortgå och utvecklas. I dagsläget skickas en förfrågan till verksamheterna ut från Enheten för juridik och informationssäkerhet, där de ombeds inkomma med underlag för hur arbetet fortskridit under året. Återrapporteringen sker inte i enhetliga mallar, men det finns en ambition att insamling av information ska ske på ett mer strukturerat och organiserat vis.

Det finns i regionen en informationssäkerhetssamordnare som dedikerad resurs för arbetet med informationssäkerhet. Samordnaren arbetar dedikerat med frågorna, men flertalet inom enheten är involverade i arbetet vilket uppges ha underlättats efter att resurserna på enheten har utökats med två tillsatta tjänster (jurister).

[5] Hädanefter även omnämnd som HSN

Det finns även ett informationssäkerhetsråd med representanter från samtliga förvaltningar, som syftar till att förmedla arbetet med informationssäkerhet ut i verksamheterna. Enligt intervjusvar saknas det dock naturliga motparter på verksamhetsnivå när det kommer till frågor som rör informationssäkerhet.

**Dokumentation**

Regionens riskarbete med hänsyn till IT- och informationssäkerhet genomförs med utgångspunkt i standarden ISO/IEC 27001:2017 (Ledningssystem för informationssäkerhet). Regionen har tagit fram flertalet styrdokument samt stödjande material inom området för att koordinera och driva arbetet.

Dokumentationen som finns på plats berör till viss del lag 2018:1174, då dessa syftar till att upprätthålla ett systematiskt och riskbaserat informationssäkerhetsarbete;

- Informationssäkerhetspolicyn beskriver tio grundläggande principer som ska styra regionens arbete med informationssäkerhet.
- Riktlinjen och vägledningen för informationsklassning samt säkerhetsåtgärder baserat på informationsklassning har samtliga blivit reviderade under 2017. Denna dokumentation ska fungera som ett stöd för verksamheten i genomförandet av informationsklassning.
- Regionen har även instruktioner, mallar och metoder för genomförandet av riskanalyser. Riskanalys genomförs löpande inom regionen, men inga med utgångspunkt i lag 2018:1174.

Direkt kopplat till lagen har en checklista för rapportering av NIS-incidenter till MSB tagits fram, vilket gjordes under 2020.

Samtliga styrande och stödjande dokument finns tillgängliga via intranätet, vilket vid intervjuer visar sig vara känt i verksamheten. De intervjuade uppger att de vet var de ska leta om de vill hitta underlag kopplat till informationssäkerhetsområdet.

**Identifiering av tillgångar**

En systematisk kartläggning av systemstöd som används inom Region Örebro län genomfördes i samband med att Dataskyddsförordningen (GDPR) trädde i kraft 2018, där verksamheterna fick rapportera in system och appar som användes. De system som används inom Hälso- och sjukvårdsförvaltningens verksamheter finns således kartlagda i ett system (BASIS). Där redogörs även relationen och beroendena mellan systemen (både interna och externa system). Dock framkom det i denna granskning att verksamheter i vissa fall själva köper in system och appar, vilket innebär att det finns en risk att inte samtliga system och appar som används har kartlagts, vilket vid intervjuer uppges vara troligt.

Det finns även ett pågående projekt som drivs av IT-säkerhetsansvarig, i vilket en kartläggning av tillgångar (system och appar) med tillhörande prioriteringsordning genomförs. Resultatet av detta ska sedan ligga till grund för regionens kontinuitetsplaner som är under framtagande. HSF har varit involverade i denna kartläggning och uppgav då att intranätet bedömdes var en viktig informationskanal vid ett avbrott. Detta för att säkerställa informationsutbytet. Andra system såsom

exempelvis journal och patientsystem uppges kunna hanteras manuellt, och påverkar således inte leveranser av tjänster inom HSF:s område. Denna analys finns inte dokumenterad.

Lag 2018:1174 kräver att leverantörer av samhällsviktiga tjänster säkerställer leverans i samtliga led som kan påverkas vid en störning, vilket således även inkluderar nätverk och informationssystem som tillhandahålls av tredje part. Region Örebro driftar majoriteten av de system som återfinns inom HSF internt, men visst systemstöd som kan ha påverkan på leverans av tjänster (exempelvis telekommunikation) förses av externa aktörer. Det uppges vid intervjuer att befintliga avtal inte uppdateras med hänsyn till lagen, utan att detta är en aspekt som kommer inkluderas i tecknande av nya samt vid förlängning av existerande avtal. Det finns dock inga konkreta planer på att uppdatera eller utveckla nuvarande upphandlingsstöd med instruktioner relaterat till lag 2018:1174.

**Riskanalys och informationsklassificering**

Samtliga verksamheter inom Region Örebro län ska genomföra riskanalyser och informationsklassificeringar.

Det finns en riktlinje samt en vägledning för informationsklassning som beskriver arbetsprocessen för informationsklassificering där klassningen görs utifrån principerna om konfidentialitet, riktighet, tillgänglighet och spårbarhet. Utfallet från informationsklassificeringar ska sedan resultera i olika säkerhetsåtgärder, i enlighet med dokumentet "Säkerhetsåtgärder baserade på informationsklassning".

Enligt intervjusvar så framgår det att det finns en diskrepans mellan uppsatta riktlinjer och hur arbetet med informationssklassificeringar egentligen går till i verksamheten, vilket uppges bero på verksamheterna saknar relevant kompetens samt att arbetet inte genomförs i den utsträckning som det finns formulerat. Detta resulterar i att de resurser som besitter förmåga och kompetens behöver involveras i stor utsträckning när verksamheterna genomför klassningar, vilket har lett till att det strategiska arbetet med IT- och informationssäkerhet prioriterats ned då dessa resurser därmed behöver involveras operativt i stor utsträckning.

Det uppges att arbetet har förbättrats, och det pågår även initiativ som syftar till att förenkla den stödjande dokumentation för informationsklassning. Detta initiativ drivs av informationssäkerhetssamordnaren.

Verksamheterna inom HSF genomför riskanalyser kontinuerligt, men då med ett fokus på områden såsom patientsäkerhet och arbetsmiljö där informationssäkerhet inte uppges vara en naturlig del av analysen. Dock uppges det att IT-sidan som involveras vid analyserna brukar bidra med det perspektivet. Se kapitel 2.4 för vidare genomgång av riskanalysarbetet.

**Övning, utbildning och uppföljning**

Det finns inga generella krav på utbildning och övning inom informationssäkerhet som gjorts obligatoriska för samtliga Regionens medarbetare. Regionen arbetar dock med



pwc

att tillhandahålla både övning och utbildning i olika format beroende på ansvarsområde och roll i verksamheten. Områdeschefer och verksamhetschefer inom HSF har exempelvis under hösten 2019 genomgått en obligatorisk kurs i flera delar om informationssäkerhet som Myndigheten för Samhällsskydd och Beredskap (MSB) tagit fram, vilket initierades av enheten för juridik och informationssäkerhet.

Inom verksamheterna är det sedan respektive verksamhetschef som ansvarar för att medarbetare får den utbildning som behövs. Inom HSF:s verksamheter är det enbart de som kommer i kontakt med patientuppgifter som genomför en obligatorisk utbildning kopplat till området, men det uppges vid intervjuer att verksamhetscheferna har ett gott samarbete med enheten för juridik och informationssäkerhet och att när behov av flera insatser identifieras så anordnas detta (exempelvis föreläsningar och utbildningar).

På regionens intranät finns det även tillgänglig dokumentation om IT- och informationssäkerhet, där medarbetarna delges kunskap om hur information skall hanteras på ett säkert sätt.

När det kommer till övningsverksamhet har främst stabsövningar genomförts inom HSF:s verksamheter, men ett behov av att öva mer med ett fokus på andra delar av verksamheterna har identifieras. Det är framförallt de reservrutiner som återfinns inom samtliga delar av HSF, vilka redogör för hur medarbetare ska agera vid störningar i ordinarie verksamheter, som behövs övas. Verksamheterna har behövt använda sina reservrutiner skarpt vid flera tillfällen, men det har konstaterats av chefsläkare samt HSF:s IT-samordnare att det finns ett behov av att öva mer regelbundet och under lugnare omständigheter.

Efter övningar, utbildningar och inträffade incidenter sker utvärdering av det arbete som genomförts i varierad utsträckning. Utbildningarna följs exempelvis inte upp systematiskt, och det finns inte heller standardiserade mallar för erfarenhetsåterföring.

### *2.2.2 Bedömning*

Kontrollmålet bedöms vara **delvis uppfyllt.**

Bedömningen grundas i att det i denna granskning framkommit att det delvis finns ett systematiskt och riskbaserat informationssäkerhetsarbete inom regionen. Styrande dokumentation finns på plats. Det finns även framtagna stödjande dokument för exempelvis informationsklassificering och riskanalyser. Verksamheterna kan således genomföra efterfrågade analyser. Däremot finns det ett behov av utökad kompetens bland verksamheterna för att säkerställa ett genomgående likartat och adekvat resultat. Det saknas även naturliga motparter för frågor som rör informationssäkerhet ute i verksamheterna.

En systematisk kartläggning av tillgångar (systemstöd) gjordes i samband med att Dataskyddsförordningen (GDPR) trädde i kraft 2018, men det råder en osäkerhet kring huruvida samtliga regionens informationssystem är inkluderade. Detta som ett resultat av att verksamheten i viss utsträckning köper in egna system och att dessa därmed inte inkluderats i genomförd kartläggning. Utöver detta saknas även en prioriteringsordning dvs vilka system som bör prioriteras vid en störning, även om detta är ett pågående arbete. Analysen som har gjorts inom Hälso- och

sjukvårdsförvaltningen där nuvarande, manuella rutiner uppges fungera i så stor utsträckning att leverans ej påverkas vid störning bör ses över med utgångspunkt i lagen och tillhörande förordningar, för att säkerställa att analysen är i enlighet med faktisk kapacitet, samt att den baseras på leveransen av den samhällsviktiga tjänsten och de krav som ställs.

Övning och utbildning sker men det saknas ett systematiskt arbete med utvärdering och uppföljning, vilket innebär att viktiga erfarenheter riskerar att gå förlorade och inte bli inkorporerade i det vidare arbetet.

## 2.3 Incidentrapportering av NIS-incidenter

***Kontrollmål III:*** *Har leverantörerna av dessa samhällsviktiga och digitala tjänster en rutin för incidentrapportering av s.k. "NIS-incidenter"?*

### *2.3.1 Iakttagelse*

Enligt lag 2018:1174 ska en leverantör av en samhällsviktig tjänst "utan onödigt dröjsmål" rapportera incidenter som har en betydande inverkan på kontinuiteten i den samhällsviktiga tjänst som de tillhandahåller (18 §), vilket enligt MSBFS 2018:9 (7 kap.) innebär incidenter som

1. innebär att anmälningsskyldighet inträder enligt 3 kap. 5 § första stycket patientsäkerhetslagen (2010:659),
2. har påverkat tillhandahållandet av ambulans och ambulanssjukvård enligt 7 kap. 6 § hälso- och sjukvårdslagen (2017:30),
3. innebär att sådan hälso- och sjukvård som baseras på system som insamlar, bearbetar, lagrar eller distribuerar och presenterar information inte kan tillhandahållas i minst två timmar, eller
4. har pågått i minst sex timmar.

Rapportering ska ske till utvald myndighet, vilket är Myndigheten för Samhällsskydd och Beredskap (MSB). Inom Hälso- och sjukvårdsförvaltningens verksamheter finns det vid granskningens genomförande etablerade processer för rapportering av avvikelser och incidenter, både verksamhetsrelaterade vilket sker i systemet Platina och för IT-relaterade vilket sker i ärendehanteringssystemet. Det finns även fastställda och fungerande rutiner för IT-incidenthantering (2017) och större händelser kopplat till IT-miljön, vilka Regionservice IT ansvarar för (framtagande samt faktisk hantering). Det finns vidare en NIS-checklista framtagen, i vilken instruktioner för rapportering till MSB återfinns. Det finns däremot ingen fastställd definition för vad som ska klassificeras som en "NIS-incident". En intern rutin för rapportering av NIS-incidenter finns inte heller på plats. Vidare finns det i dagsläget inte någon fullständig kartläggning av samtliga informationssystem och nätverk som används inom HSF och inte heller någon analys med utgångspunkt i lag 2018:1174 över vilka system som är kritiska för regionens samhällsviktiga leveranser.

Det har uttryckts önskemål från både chefsläkare samt IT-samordnare inom HSF om att få en skriftlig definition samt en intern rutin på plats, vilket har diskuterats vidare i

arbetsgruppen. Det uppges finnas en ambition för framtagande av definition samt rutin, ett arbete som enheten för juridik och informationssäkerhet i så fall skulle driva, men det finns inga planerade aktiviteter för detta. I dagsläget sker diskussioner och bedömningar kring incidenter som möjligtvis kan klassificeras som en NIS-incident mellan chefsläkare på HSF eller IT-säkerhetsansvarig (Regionservice IT) och enheten för juridik och informationssäkerhet (framförallt med informationssäkerhetssamordnaren). Denna kontaktkedja uppges fungera väl.

Det har vid tidpunkten för denna granskning genomförande enligt regionens bedömning inte inträffat någon incident som skulle kunna klassificeras som en NIS-incident i enlighet med lag 2018:1174, även om inträffade incidenter har diskuterats med utgångspunkt i huruvida dessa omfattas av lagen.

### *2.3.2 Bedömning*

Kontrollmålet bedöms vara **inte uppfyllt.**

Detta då en rutin för intern incidentrapportering av NIS-incidenter inte existerar. Det existerar inte heller en definition av vad en NIS-incident inom regionen innebär. Enligt lagen behöver en incidentrapporteringsstruktur för incidenter som har betydande inverkan på kontinuiteten i den samhällsviktiga tjänsten eller ett likvärdigt alternativ finnas. Då det även vid granskningens tidpunkt saknas en analys med utgångspunkt i lagen över vilka system som är kritiska för leveransen av den samhällsviktiga tjänsten riskerar det även att vara oklart vilka system som berörs av rapporteringskravet.

Regionen har däremot upprättat ett internt dokument för rapportering av incidenter, baserat på de rutiner för rapportering av NIS-incidenter MSB har tagit fram. Eftersom det inte finns en tydlig definition av vad som bör definieras som en NIS-incident riskerar dock identifiering av incidenter samt rapportering av dessa inte fullföljas i enlighet med lagstiftningen.

## 2.4 Riskanalys och tillhörande åtgärdsplan

***Kontrollmål IV:*** *Har leverantörerna av dessa samhällsviktiga och digitala tjänster utfört en riskanalys med ingående åtgärdsplan?*

### *2.4.1 Iakttagelse*

Enligt lagen om informationssäkerhet för samhällsviktiga och digitala tjänster ska en riskanalys ligga till grund för val av säkerhetsåtgärder. I analysen ska det ingå en åtgärdsplan som dokumenteras och uppdateras årligen (12 §).

Det är respektive objektägare som har det övergripande ansvaret för riskbedömningar för system, det vill säga att objektägaren har ansvar för att identifiera risker samt fatta beslut om åtgärd för systemet. Detta ska identifieras genom en riskanalys, vilken ska genomföras tillsammans med relevanta aktörer (representanter från verksamheten, från IT och från andra områden som av objektägaren bedöms vara relevanta) där frågor diskuteras i workshopsformat. Analysen ska genomföras i enlighet med det underlag (mallar och riktlinjer) som finns framtagna (vilka är giltiga för hela regionen).

Det finns dock i dagsläget, vilket även noterades i den uppföljande granskning av IT- och informationssäkerhet som genomfördes hösten 2019[6], inte någon process för när, hur och varför en riskanalys ska genomföras kopplade till IT-tjänster även om det uppges vid intervjuer att det ska genomföras vid inköp av nya system och vid större förändringar. Detta är dock inte formaliserat eller dokumenterat. Det finns inte heller någon analys specifikt kopplat till informationssäkerhet, även om detta är inkluderat som en utgångspunkt att ta i beaktande när risken värderas och bedöms. Det saknas även en tydlig koppling mellan de riskanalyser och informationsklassificeringar som genomförs, även om riskanalysens resultat och åtgärder som framkommer där lyfts i den dokumentation för säkerhetsåtgärder baserade på informationsklassning.

Det pågår även ett riskanalysarbete på Regionservice IT, där identifierade risker jämförs med verksamhetsnyttan, vilket görs genom ifyllande av en blankett där analysobjektet undersöks utifrån hotbild, brister och svagheter. Syftet med detta är att säkerställa att nya system som tas in i miljön är tillräckligt säkra. Utöver detta har även större system gått igenom en informationsklassificering. Samtliga system har dock inte analyserats, vare sig från ett riskperspektiv eller utifrån informationen som lagras.

Det uppges finnas få resurser inom organisationen med tillräcklig kompetens för att genomföra riskanalyser, vilket innebär att specifika personer krävs vid genomförandet för att säkerställa adekvata analyser.

För att säkerställa en högre nivå och adekvata resultat av de analyser som genomförs pågår ett arbete på enheten för juridik och informationssäkerhet med att ta fram rutiner för riskanalyser. Detta då det upplevs bli ett felaktig fokus på de analyser som görs, där informationsflödet och informationstillgångar hamnar utanför. Denna problematik återkommer även i intervjuer med verksamheten, där informationssäkerhet uppges vara ett område som inte naturligt inkluderas. Arbetet med att ta fram rutiner beräknas vara färdigställt under våren 2020.

Inga direkta åtgärder har vidtagits med utgångspunkt i lagen, och de åtgärdsplaner som tas fram i dagsläget tar inte kritikalitet och nödvändighet för leverans av samhällsviktig tjänst i beaktande.

### *2.4.2 Bedömning*

Kontrollmålet bedöms vara **delvis uppfyllt.**

Bedömningen grundas i att riskanalyser genomförs i verksamheten, där IT- och informationssäkerhet tas i beaktande. En formaliserad process (ansvarsfördelning, frekvens samt vilken typ av riskanalys som är relevant) för genomförande saknas dock. Nuvarande rutiner och riktlinjer tar inte heller kritikalitet rörande leverans av samhällsviktig tjänst i beaktande. Säkerhetsåtgärder som följer på informationsklassificering är ej heller integrerade med den riskanalys som genomförs.

Det finns ett fåtal resurser i dagsläget som har adekvat kompetens och kunskap för att genomföra riskanalyser och informationsklassificeringar på efterfrågat vis med önskat resultat, vilket innebär en risk för personberoende samt att de analyser och

[6] Uppföljande granskning av Region Örebros IT- och informationssäkerhetsarbete (2019)

klassificeringar som görs utan stöd från dessa resurser inte lever upp till de krav som ställs.

## 2.5 Kontinuitetshantering

***Kontrollmål V:*** *Har leverantörerna av dessa samhällsviktiga och digitala tjänster tagit fram kontinuitetsplaner för att säkerställa kontinuiteten i tjänsterna?*

### *2.5.1 Iakttagelse*

Enligt MSBFS 2018:8 föreskrifter och allmänna råd om informationssäkerhet för leverantörer av samhällsviktiga tjänster ska regionen ha interna regler och arbetssätt för att identifiera och upprätthålla kontinuiteten inom hälso- och sjukvården samt minska effekterna av incidenter.

Enligt intervjusvar så finns det ett pågående arbete på den centrala IT-avdelningen (Regionservice IT) med att ta fram kontinuitetsplaner, där arbetet drivs av IT-säkerhetschefen. Målet är att involvera samtliga verksamheter inom Hälso- och sjukvårdsförvaltningen i syfte att kunna identifiera och prioritera de mest kritiska systemen och processer, vilket sedan ligger till grund för upprättandet av kontinuitetsplaner.

Som även noterat i den granskning som genomfördes 2019[7] så uppges det finnas problem att få in information från verksamhetens enheter om vilka system som är viktigast och mest kritiska för deras verksamhet, vilket försvårar arbetet med framtagande av planer och i längden prioritering av system vid en incident eller större störning. Det finns dock en kartläggning av de nätverks- och informationssystem som driftas och förvaltas inom regionen, där det även redogörs för beroenden mellan dessa samt till externa system och vid intervjuer uppges att de system som tillhör hälso- och sjukvården automatiskt klassificeras som kritiska. Det saknas dock prioriteringsordning bland dessa system.

Vid intervjuer uppges det att Hälso- och sjukvårdsförvaltningen har gjort efterfrågad prioriteringsordning, där intranätet exempelvis bedömdes vara en viktig informationskanal vid ett avbrott. Detta för att information behöver kunna delas vid en störning, och att det redan finns manuella rutiner för att säkerställa leverans om övriga system skulle gå ner. Analysen gjordes av förvaltningsledare, HSF:s IT-samordnare samt verksamhetsnära funktioner. Den finns inte dokumenterad.

Vid intervjuer uppges det att verksamheterna inom Hälso- och sjukvårdsförvaltningen både har vanan och förmågan att minimera avbrottstider samt skapa förutsättningar för att återgå till och återställa verksamheten efter ett avbrott. Samtliga avdelningar i verksamheten har tagit fram egna reservrutiner ifall ett avbrott skulle ske vilka finns tillgängliga på intranätet. Enligt intervjusvar så har ett behov av mer regelbunden övning av reservrutinerna identifierats. Idag används de främst i skarpa situationer och ett behov av att tillsammans på ett mer metodiskt sätt gå igenom rutinerna har identifieras.

System som används inom HSF har i dagsläget Service Level Agreements (SLA:er), i vilka servicenivåer som ska uppfyllas av Regionservice IT finns definierade. Dessa servicenivåer varierar och ska enligt intervjusvar bestämmas baserat på

[7] Uppföljande granskning av Region Örebros IT- och informationssäkerhetsarbete (2019)

informationsklassificering och de rekommenderade säkerhetsåtgärder som framkommer av den. Detta har skett för nya system, men nivåer för äldre system uppges inte vara baserade på någon känd analys. Någon distinktion har inte heller gjorts utifrån lag 2018:1174 och om hur systemen påverkar den samhällsviktiga tjänsten.

Det har även identifierats ett behov från HSF av en kontinuitetssamordnare eller liknande resurs, som kan fokusera på kontinuitets- och beredskapsfrågor inom regionen. En förfrågan om detta har ställts, men inte blivit godkänd.

### *2.5.2 Bedömning*

Kontrollmålet bedöms vara **inte uppfyllt.**

Detta då regionen inte har färdigställda kontinuitetsplaner att arbeta efter i händelse av ett störning eller avbrott, vilket innebär att de i dagsläget inte vet vad som ska prioriteras vid en större incident eller en incident i ett system som är kritiskt för leveransen i verksamheten. Däremot finns det redundans inom verksamheten i form av reservrutiner och god vana att arbeta med manuella processer.

# 3. Revisionella bedömningar

| Kontrollmål | Kommentar |
|---|---|
| I. Har regionen identifierat de samhällsviktiga och digitala tjänster som faller under deras ansvar och vilka som levererar dessa? | **Delvis uppfyllt**<br>Regionen har påbörjat arbetet med att analysera hur och i vilken omfattning de beröras av lag 2018:1174, samt vilka som levererar samhällsviktiga tjänster inom regionen. Analys och bedömning är dock inte dokumenterad och samtliga berörda delar av regionen har inte blivit informerade om beslutet vilket även inkluderar externa leverantörer. Det råder även en otydlighet kring hur arbetet ska struktureras och implementeras, och det saknas dokumenterade rollbeskrivningar och definierade ansvarsområden inom tjänstemannaorganisationen (vilka innehar ansvaret att implementera åtgärder) vilket i sin tur riskerar att leda till att kraven i lag 2018:1174 inte kan efterlevas. |
| II. Arbetar leverantörerna av dessa samhällsviktiga och digitala tjänster systematiskt och riskbaserat med sitt informationssäkerhets arbete avseende nätverk och informationssystem som de använder för att tillhandahålla samhällsviktiga tjänster? | **Delvis uppfyllt**<br>Regionen arbetar i viss utsträckning systematiskt och riskbaserat i sitt informationssäkerhetsarbete, och informationsklassificering samt riskanalyser genomförs i verksamheterna. Däremot saknas ett fokus på leveransen av den samhällsviktiga tjänsten, där en kartläggning av tillgångar samt beroendeförhållanden med en tillhörande prioriteringsordning saknas. Vidare genomförs riskanalyser och informationsklassificeringar ute i verksamheterna med ett varierat resultat till följ av en varierad kunskapsnivå hos utförare. Det saknas även ett systematiskt arbete med utvärdering och uppföljning. |
| III.Har leverantörerna av dessa samhällsviktiga och digitala tjänster en rutin för incidentrapportering av | **Inte uppfyllt**<br>Regionen har inte skapat en intern rutin för incidentrapportering av s.k. NIS-incidenter. Det saknas även en definition på vad som klassificeras som en sådan incident. Vidare |

| | |
|---|---|
| s.k. "NIS-incidenter"? | saknas även en analys med utgångspunkt i lagen över vilka system som är kritiska för leveransen av den samhällsviktiga tjänsten, vilket leder till oklarhet i vilka system som berörs av rapporteringskravet. |
| IV. Har leverantörerna av dessa samhällsviktiga och digitala tjänster utfört en riskanalys med ingående åtgärdsplan? | **Delvis uppfyllt**<br>Riskanalyser där IT- och informationssäkerhet tas i beaktande genomförs, vilka resulterar i åtgärdsplaner. En formaliserad process för genomförande (ansvarsfördelning, frekvens samt vilken typ av riskanalys som är relevant) saknas dock. Nuvarande rutiner och riktlinjer tar inte heller lag 2018:1174 i beaktande, i exempelvis kritikalitet rörande leverans av samhällsviktig tjänst. Det finns inte heller en övergripande riskanalys med ingående åtgärdsplan. |
| V. Har leverantörerna av dessa samhällsviktiga och digitala tjänster tagit fram kontinuitetsplaner för att säkerställa kontinuiteten i tjänsterna? | **Inte uppfyllt**<br>Regionen har inga kontinuitetsplaner för att säkerställa kontinuiteten i den samhällsviktiga tjänsten. Däremot finns det framtagna reservrutiner ifall en störning eller avbrott i verksamheten skulle ske, med manuella rutiner som har använts vid flera tillfällen. |

# Bilagor

## Bilaga 1 - Granskad dokumentation

Inom ramen för uppdraget har PwC tagit del av följanden dokumentation:

- Anmälan tillsynsmyndighet
- Arbetsflöde för att säkerställa reservrutiner vid driftstopp i VårdIT-system
- Arbetsbeskrivning - IT-SIRT
- Behörighet för elektronisk åtkomst och direktåtkomst
- Checklista NIS
- Driftstopp Allvarlig händelse, Regionservice IT
- Informationsklassning (riktlinje)
- Informationssäkerhetspolicy
- IT-Arkitektur
- Kris- och katastrofmedicinsk beredskap Region Örebro län
- Reservrutin Läkemedelslista Planerade Oplanerade vid driftstopp
- Mall ISAK Excel 2016 20191008 (informationsklassificeringsinstruktion)
- NIS-anmälan
- Process för IT-Incidenthantering
- Processbeskrivning Samarbete med externa leverantörer i fastighetssystem ver 2
- Reservrutin Infomedix Klinisk portal och ordinationslista vid driftstopp
- Reservrutin Läkemedelslista Planerade Oplanerade vid driftstopp
- Reservrutiner vårdsystem websida
- Riskanalys (mall)
- Riskanalysschema_Fastighetssystem
- Roller för IT-Incidenthantering
- Rätt att ta del av uppgifter i patientjournal
- Säkerhetsåtgärder baserade på informationsklassning
- Slutrapport Fastigheters interna system och molntjänst
- Tilldelning, förändring, borttagning och uppföljning av behörighet i vårdsystem
- Vägledning informationsklassning
- Verktyg-riskanalysblankett
- Övningsplan 2020 - Regionservice

## Bilaga 2 - Revisionella bedömningsgrunder

**Uppfyllt**: Kontrollmålet bedöms till största delen vara uppfyllt, mindre avvikelser kan förekomma. Men verksamheten fungerar i huvudsak ändamålsenligt.

**Delvis uppfyllt:** Kontrollmålet bedöms endast delvis vara uppfyllt, det finns en större eller flera mindre avvikelser som påverkar verksamhetens ändamålsenlighet.

**Inte uppfyllt:** Kontrollmålet bedöms inte vara uppfyllt. Det finns avvikelser som måste åtgärdas snarast för att verksamheten ska fungera ändamålsenligt.

**Ej bedömt**: Kontrollmålet går ej att bedöma

.

2020-10-08

*Rebecka Hansson* *XX*

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av [regionens revisorer] enligt de villkor och under de förutsättningar som framgår av projektplan från den [2019-01-09]. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.