Stockholms läns landsting

Landstingsrådsberedningen

SKRIVELSE
2016-03-23

LS 2016-0192

Landstingsstyrelsen

Yttrande över landstingsrevisorernas projektrapport nr 9/2015, Ledningssystem för informationssäkerhet - arbetet med genomförande

Föredragande landstingsråd: Daniel Forslund

Ärendebeskrivning

Landstingsrevisorerna i revisorsgrupp II har lämnat projektrapport 9/2015, Ledningssystem för informationssäkerhet – arbetet med genomförande för yttrande.

Förslag till beslut

Landstingsrådsberedningen föreslår landstingsstyrelsen besluta

att avge yttrande till landstingsrevisorerna över landstingsrevisorernas projektrapport 9/2015, Ledningssystem för informationssäkerhet – arbetet med genomförande, enligt landstingsdirektörens tjänsteutlåtande.

Landstingsrådsberedningens motivering

Stockholms län landsting behöver ständigt utveckla sitt arbete med informationssäkerhet. Den snabba IT-utvecklingen och den ökade informationsdelningen inom landstinget kräver säkra processer för informationshantering. Ett handlingsprogram för informationssäkerhet för åren 2016-2020 har tagits fram i syfte att införa ett systematiskt säkerhetsarbete i landstingets samtliga verksamheter.

Landstingets ledningssystem för informationssäkerhet, s.k. LIS, skapar en struktur för styrning och ständiga förbättringar. Landstingsrevisorerna granskning av implementeringen visar att det återstår arbete innan landstinget har nått en tillfredsställande nivå. Landstingsrådsberedningen delar revisorernas och landstingsstyrelsens förvaltnings slutsats att det är angeläget att öka tempot i införandet på både lokal och central nivå.

De rekommendationer som revisorerna för fram ligger i linje med det arbete som redan har påbörjats och arbetet kommer att intensifieras ytterligare i enlighet med rekommendationerna. Det är särskilt angeläget att informationssäkerhet ses som en strategisk ledningsfråga och prioriteras av ansvarig förvaltningschef eller VD i syfte att hela verksamheten ska genomsyras av ett högt säkerhetsmedvetande. Ett ambitiöst arbete har inletts utifrån det nya handlingsprogrammet och insatser kommer att genomföras för att den nya så kallade compliance-processen skyndsamt ska implementeras i landstingets förvaltningars och bolags verksamheter.

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 11 mars 2016
Landstingsrevisorernas projektrapport nr 9/2015, Ledningssystem för informationssäkerhet – arbetet med genomförande

Torbjörn Rosdahl

Daniel Forslund

Carl Rydingstam

Landstingsstyrelsens förvaltning
Direktör Strategisk IT i SLL

TJÄNSTEUTLÅTANDE
2016-03-11

LS 2016-0192

Handläggare:
Vesna Lucassi

Landstingsstyrelsen

Ankom
Stockholms läns landsting
2016 -03- 11
Dnr LS 2016-0192
Rotel VII

Yttrande över landstingsrevisorernas projektrapport nr 9/2015, Ledningssystem för informationssäkerhet - arbetet med genomförande

Ärendebeskrivning

Landstingsrevisorerna i revisorsgrupp II har lämnat projektrapport 9/2015, Ledningssystem för informationssäkerhet – arbetet med genomförande för yttrande.

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 11 mars 2016
Landstingsrevisorernas projektrapport nr 9/2015, Ledningssystem för informationssäkerhet – arbetet med genomförande

Förslag till beslut

Landstingsstyrelsen föreslås besluta

att avge yttrande till landstingsrevisorerna över landstingsrevisorernas projektrapport 9/2015, Ledningssystem för informationssäkerhet – arbetet med genomförande, enligt landstingsdirektörens tjänsteutlåtande.

Förvaltningens förslag och motivering

Sammanfattning
Landstingsrevisorerna samlade bedömning vid granskningen år 2015 är att det återstår arbete innan landstinget har nått en tillfredsställande nivå i implementeringen av ledningssystemet för informationssäkerhet, s.k. LIS. Revisorerna pekar på allvaret i detta och framhåller till landstingsstyrelsen att det är angeläget att tempot i införandet av ledningssystemet för informationssäkerhet ökar, både på central och på lokal nivå.

Landstingsstyrelsens förvaltning anser att landstingsrevisorernas rapport i allt väsentligt ger en rättvisande bild av situationen vid revisionstillfället. Arbetet med att inarbeta revisorernas rekommendationer har till stor del

redan påbörjats och kommer att intensifieras ytterligare i enlighet med rekommendationerna. Inom förvaltningen pågår ett flertal aktiviteter för att påskynda breddinförandet av landstingets ledningssystem för informationssäkerhet, däribland implementering av en för landstinget ny process för systematiskt informationssäkerhetsarbete, den så kallade compliance-processen. Ledningssystem börjar byggas upp inom verksamheterna i landstinget, och genom att arbeta målmedvetet utifrån det nya handlingsprogrammet för informationssäkerhet för åren 2016-2020 kommer informationssäkerhetsarbetet att intensifieras.

Bakgrund
Landstingsrevisorerna har granskat implementeringen av landstingets ledningssystem för informationssäkerhet. Granskningen genomfördes under år 2015 i form av dokumentstudier och intervjuer hos hälso- och sjukvårdsförvaltningen, Karolinska universitetssjukhuset, Stockholms läns sjukvårdsområde (SLSO) och Södersjukhuset samt genom intervjuer med landstingets informationssäkerhetschef vid landstingsstyrelsens förvaltning.

Den övergripande revisionsfrågan i granskningen var:

- Genomförs implementeringen av ledningssystemet för informationssäkerhet inom landstinget på ett sådant sätt att väsentliga risker inom området omhändertas?

Den övergripande revisionsfrågan bröts ner i delfrågor: Finns dokumenterade riskanalyser med tillhörande handlingsplaner på central och lokal nivå? Har informationsägare utsetts och informationssäkerhets-klassificering genomförts för viktiga informationstillgångar på lokal nivå? Är landstingsstyrelsens uppföljning tillräcklig för att ge underlag för beslut om åtgärder för att säkerställa god informationssäkerhet?

Granskningen hade ett särskilt fokus på förvaltningschefs/vd:s ansvar och informationssäkerhetssamordnarens roll i samband med implementering av ledningssystem för informationssäkerhet, s.k. LIS, på lokal nivå.

I projektrapporten konstaterar landstingsrevisorerna brister inom granskade områden. Landstingsrevisorernas samlade bedömning är att det återstår mycket arbete innan landstinget har nått en tillfredsställande nivå i implementeringen av ledningssystemet för informationssäkerhet.

Landstingsstyrelsen ges i rapporten följande rekommendationer:

- Prioritera arbetet med att införa compliance-processen i landstingets verksamheter för att påskynda det systematiska informationssäkerhets-arbetet.
- Prioritera arbetet med framtagande och beslut av tillämpnings-anvisningar, så att välgrundade och avvägda skyddsåtgärder kan vidtas.
- Säkerställa att ansvar och roller för informationssäkerhet implemen-teras i FOA-organisationen (landstingets förvaltningsstyrningsmodell enligt pm3).
- Följa upp hur informationssäkerhet säkerställs hos privata utförare inom vården.

Härutöver ges även hälso- och sjukvårdsnämnden och SLSO särskilda rekommendationer i syfte att stärka informationssäkerheten.

Överväganden
Landstingsfullmäktige och landstingsstyrelsen har fastställt policy och riktlinjer för informationssäkerhet inom Stockholms läns landsting, LS 1112-1733. Enligt policyn ska informationssäkerhetsarbetet styras genom landstingets ledningssystem för informationssäkerhet. Varje nämnd/styrelse har ansvar för informationssäkerheten inom sitt verksamhetsområde och ska årligen planlägga och löpande följa upp informationssäkerheten. Förvaltningschef/vd ansvarar för att all informationshantering sker enligt fastställda styrdokument. Landstingsstyrelsen har det övergripande ansvaret för samordning och uppföljning av informationssäkerheten inom landstinget.

Revisorerna konstaterar att förvaltningar och bolag har påbörjat implementering av ledningssystemet, LIS, i sina verksamheter, men att omfattningen av införandet skiljer sig i betydande utsträckning mellan verksamheterna. Den samlade bedömningen är att det återstår mycket arbete innan landstinget har nått en tillfredsställande nivå i implementeringen av ledningssystemet för informationssäkerhet.

Revisorerna pekar på allvaret i detta och på konsekvenserna om riskanalyser och informationsklassificering inte genomförs i tillräcklig utsträckning. Brister i detta avseende kan leda till att kontroller för att förebygga och upptäcka fel uteblir eller är otillräckliga och till att utvecklingen av fientliga it-relaterade hot (attacker, it-brott, spionage, kränkningar, etc.) inte i tillräcklig grad pareras med skyddsåtgärder.

Ny compliance-process för informationssäkerhetsarbete
Landstingsstyrelsens förvaltning har redan tidigare identifierat behovet av att öka tempot i införandet av ledningssystemet för informationssäkerhet, både på central och på lokal nivå. För att stärka styrningen av informationssäkerheten och påskynda implementeringen ytterligare har förvaltningen tagit fram en för landstinget ny och anpassad process för systematiskt informationssäkerhetsarbete, compliance-processen. Compliance-processen utgår från landstingets policy och riktlinjer för informationssäkerhet och stödjer såväl ledningar som verksamheter i det kontinuerliga arbetet med att styra, egenkontrollera, utvärdera och ständigt förbättra informationssäkerheten. Den ger vidare stöd för hur verksamheter bör arbeta med uppföljning inom området.

Insatser kommer att genomföras, för att förvaltningar och bolag inom landstinget ska implementera compliance-processen skyndsamt i sina verksamheter. Ett förslag på en ny tillämpningsanvisning för ändamålet har tagits fram och behandlas för närvarande i landstingets informationssäkerhetsråd som består av utsedda informationssäkerhetssamordnare från respektive förvaltning och bolag. Landstingsstyrelsens förvaltning kommer under år 2016 även att tillhandahålla utbildning och praktiskt stöd till förvaltningar och bolag för att stödja den lokala implementeringen av compliance-processen.

Insatser för att belysa ansvarsfrågan
Landstingsrevisorerna konstaterar vidare att informationssäkerhet inte i tillräcklig utsträckning är en ledningsfråga som hanteras av verksamheternas förvaltningschefer/vd:ar. En tillämpningsanvisning gällande LIS-införande fastställdes i januari 2016 och skickades till landstingets förvaltningar och bolag. I denna finns beskrivning på hur landstingets ledningssystem för informationssäkerhet, LIS, ska införas och förvaltas på lokal nivå samt hur ledningens genomgång ska genomföras. Riktade utbildningsinsatser har genomförts och ytterligare insatser kommer att genomföras för att belysa ansvarsfrågan.

Årlig uppföljning av regelefterlevnad
Från och med år 2015 genomför landstingsstyrelsens förvaltning årliga systematiska uppföljningar av förvaltningars och bolags efterlevnad av övergripande informationssäkerhetskrav i riktlinjerna för informationssäkerhet enligt compliance-processen. Direktkontakt tas med specifika förvaltningar och bolag utifrån analysresultaten. Syftet är att de förvaltnings- och bolagsspecifika återkopplingarna ska bidra till att påskynda det systematiska informationssäkerhetsarbetet på lokal nivå.

Handlingsprogram för informationssäkerhet
Ett handlingsprogram för informationssäkerhet för Stockholms läns landsting har tagits fram för åren 2016-2020. Handlingsprogrammet ska ligga till grund för och styra förvaltningars och bolags lokala handlingsplaner. Genom handlingsprogram samordnas förvaltningars och bolags arbeten och ambitionsnivån för informationssäkerhetsarbetet i landstinget höjs.

Övriga insatser
Förvaltningen önskar framhålla att det – trots att implementeringen visserligen ännu inte nått en tillfredsställande införandenivå – för närvarande pågår flera aktiviteter på både central och lokal nivå som syftar till att påskynda införandetempot och det systematiska informationssäkerhetsarbetet inom landstinget. Ledningssystem börjar byggas upp inom verksamheterna i landstinget, och genom att arbeta målmedvetet utifrån det nya handlingsprogrammet för informationssäkerhet kommer informationssäkerhetsarbetet att intensifieras. Förutom redan nämnda aktiviteter ges ytterligare exempel nedan:

- De fem mest grundläggande tillämpningsanvisningarna för informationssäkerhet beslutades av landstingsdirektören i januari 2016. Arbete pågår med att ta fram ytterligare tillämpningsanvisningar. Likaså pågår arbete med att ta fram en landstingsgemensam klassificeringsmodell för bedömning av skadeverkan och prioritering av informationssäkerhetsincidenter.
- Landstingsrevisorerna konstaterar att arbetet med de initiala tillämpningsanvisningarna försenades till följd av bland annat förankringsarbete och hantering av oförutsedda händelser och att detta påverkat informationssäkerhetsarbetet på lokal nivå. Landstingsstyrelsens förvaltning bekräftar denna försening. Strukturen och processen för tillämpningsanvisningar är från och med år 2016 fastställd. Löptiden att ta fram nya tillämpningsanvisningar bedöms därmed nu vara avsevärt förkortad. Härutöver ses för närvarande organisationen och styrningen över i syfte att ta höjd för oförutsedda händelser och motverka förseningar.
- Förvaltningen kommer att fortsätta stödja landstingets FOA-organisation både i arbetet med rollbeskrivningar liksom med utbildningsinsatser och egenkontroller enligt compliance-processen.
- En dialog förs med Take Care-förvaltningen i syfte att stödja objektets informationssäkerhetsarbete.
- Förvaltningen kommer att föra en särskild dialog med hälso- och sjukvårdsförvaltningen gällande uppföljning av hur informationssäkerhet säkerställs hos privata utförare inom vården.

Avslutning
Sammanfattningsvis delar förvaltningen projektrapportens samlade bedömning att arbete återstår innan landstinget har nått en tillfredsställande nivå i implementeringen av ledningssystemet för informationssäkerhet, LIS. Syftet är dock att de aktiviteter som pågår ska leda till att arbetet med att bygga ledningssystemet för informationssäkerhet prioriteras av förvaltningar och bolag. Underlaget i landstingsrevisorernas projektrapport nr 9/15 kommer att utgöra en viktig del i förvaltningens fortsatta arbete inom området. Arbetet med att inarbeta revisorernas rekommendationer har till stor del påbörjats och kommer att intensifieras ytterligare i enlighet med rekommendationerna.

Ekonomiska konsekvenser av beslutet

Det uppstår inga ekonomiska konsekvenser av beslutet. Kostnaderna för ovan beskrivna aktiviteter ryms inom ordinarie budget.

Miljökonsekvenser av beslutet

I enlighet med landstingets Miljöpolitiska program 2012-2016 har hänsyn till miljön beaktats och slutsatsen är att det inte är relevant med en miljökonsekvensbedömning i detta ärende.

Toivo Heinsoo
Landstingsdirektör

Anders Nyström
Direktör Strategisk IT i SLL

PROJEKTRAPPORT NR 9/2015

Ledningssystem för informationssäkerhet

- arbetet med genomförande

Landstingsrevisorerna
STOCKHOLMS LÄNS LANDSTING

Vad gör Landstingsrevisorerna?

Landstingsrevisorerna granskar den verksamhet som bedrivs av landstingets nämnder och bolagsstyrelser. Revisionsuppdraget är det största inom kommunal verksamhet.

Att vara revisor är ett förtroendeuppdrag vars syfte är att med oberoende, saklighet och integritet främja, granska och bedöma verksamheten. Den övergripande uppgiften för revisorerna är att granska hur nämnder och styrelser tar sitt ansvar. De förtroendevalda revisorerna är fullmäktiges och ytterst medborgarnas instrument för den demokratiska kontrollen. De har därmed en viktig funktion i den lokala självstyrelsen.

Ledamöter i nämnder och styrelser ansvarar inför fullmäktige för hur de själva, anställda och uppdragstagare genomför verksamheten. I ansvaret ingår att genomföra en ändamålsenlig verksamhet utifrån fullmäktiges mål, beslut och riktlinjer samt de föreskrifter som gäller för verksamheten, på ett ekonomiskt tillfredsställande sätt och med en tillräcklig intern kontroll samt att upprätta rättvisande räkenskaper.

I årsrapporter för nämnder och bolag sammanfattar revisionskontoret den granskning som genomförts under det gångna året. Verksamhetsrevisionen redovisas löpande i projektrapporter. Publikationerna finns på Landstingsrevisorernas hemsida www.sll.se/rev. De kan också beställas från revisionskontoret. Det går även att prenumerera på Landstingsrevisorernas nyhetsbrev Nytt från landstingsrevisionen genom att anmäla intresse via e-postmeddelande till landstingsrevisorerna@rev.sll.se

Landstingsrevisorerna
STOCKHOLMS LÄNS LANDSTING

2016-02-02 RK 201504-0039

Landstingsstyrelsen

Projektrapport 9/2015
Ledningssystem för informationssäkerhet
- arbetet med genomförande

Revisorerna i revisorsgrupp I beslutade 2016-02-02 att överlämna rapporten till landstingsstyrelsen för yttrande senast 2016-05-13.

Revisorernas samlade bedömning är att det återstår mycket arbete innan landstinget har nått en tillfredsställande nivå i implementeringen av ledningssystem för informationssäkerhet.

Revisorerna vill till landstingsstyrelsen särskilt framhålla att det är angeläget att tempot i införandet av ledningssystemet för informationssäkerhet ökar, både på central och på lokal nivå, så att landstingsstyrelsen kan vidta välgrundade och avvägda skyddsåtgärder som bygger på verksamheternas riskanalyser och handlingsplaner.

I övrigt hänvisar revisorerna till revisionskontorets rapport.

Paragrafen förklarades omedelbart justerad.

Kenneth Strömberg
Ordförande

Christina Holmqvist
Sekreterare

Landstingsrevisorerna
Box 22230
104 22 Stockholm

Telefon: 08-737 25 00
Fax: 08-737 53 50
E-post: landstingsrevisorerna@rev.sll.se

Säte: Stockholm
Org.nr: 23 21 00 - 0016
www.sll.se/rev

Besöksadress: Hantverkargatan 25 B. T-bana Rådhuset

Landstingsrevisorerna
STOCKHOLMS LÄNS LANDSTING

2016-02-02 RK 201504-0039

Hälso- och sjukvårdsnämnden
Stockholms läns sjukvårdsområde
Södersjukhuset AB

Projektrapport 9/2015
Ledningssystem för informationssäkerhet
- arbetet med genomförande

Revisorerna i revisorsgrupp II beslutade 2016-02-02 att överlämna rapporten till hälso- och sjukvårdsnämnden och Stockholms läns sjukvårdsområde för yttrande samt till Södersjukhuset AB för möjlighet till yttrande senast 2016-05-13.

Revisorernas samlade bedömning är att det återstår mycket arbete innan landstinget har nått en tillfredsställande nivå i införande och tillämpning av systemet för att garantera informationssäkerhet. Detta är i sig allvarligt då så mycket av landstingets verksamhet är beroende av tillförlitlig information.

Revisorerna vill till hälso- och sjukvårdsnämnden och Stockholms läns sjukvårdsområde särskilt framhålla vikten av att rapportering sker till respektive verksamhets förvaltiningschef i enlighet med fastställda styrdokument för informationssäkerhet i syfte att stärka informationssäkerheten.

I övrigt hänvisar revisorerna till revisionskontorets rapport.

Paragrafen förklarades omedelbart justerad.

Hans-Erik Salomonsson
Ordförande

Rikard Lindqvist
Sekreterare

Landstingsrevisorerna
Box 22230
104 22 Stockholm

Telefon: 08-737 25 00
Fax: 08-737 53 50
E-post: landstingsrevisorerna@rev.sll.se

Säte: Stockholm
Org.nr: 23 21 00 - 0016
www.sll.se/rev

Besöksadress: Hantverkargatan 25 B. T-bana Rådhuset

INNEHÅLL

1 SLUTSATSER OCH REKOMMENDATIONER 4

2 UTGÅNGSPUNKTER FÖR GRANSKNINGEN 6

2.1 Motiv till granskningen 6
2.2 Revisionsfråga 6
2.3 Avgränsning 7
2.4 Bedömningsgrunder 7
2.5 Metod 7

3 LEDNINGSSYSTEM FÖR INFORMATIONSSÄKERHET – ORGANISATION OCH ANSVAR 7

4 IMPLEMENTERING AV LEDNINGSSYSTEM FÖR INFORMATIONSSÄKERHET 8

4.1 Organisation, riskanalyser och handlingsplaner 8
4.2 Informationsägare och informationsklassning 13
4.3 Landstingsstyrelsens uppföljning 14

1 Slutsatser och rekommendationer

Informationssäkerhetsarbetet i landstinget är väsentligt för att hantera risker och för att skyddsåtgärder ska kunna vidtas. Enligt policy och riktlinjer fastställda av fullmäktige ska informationssäkerhetsarbetet styras genom landstingets ledningssystem för informationssäkerhet (LIS). Revisionen har granskat i vilken utsträckning ledningssystemet har implementerats inom Stockholms läns landsting (SLL). Granskningen avser om implementeringen inom utvalda verksamheter genomförs på ett sådant sätt att väsentliga risker inom området omhändertas.

En process för systematiskt informationssäkerhetsarbete med tillhörande IT-baserat verktyg, Compliance-portalen, har utvecklats av landstingsstyrelsens förvaltning i syfte att ge stöd till verksamheterna och för att på central nivå ge underlag för uppföljning avlandstingets arbete med informationssäkerhet. Granskningen visar att verksamheterna har påbörjat användandet av verktyget. Omfattningen av införandet, framför allt när det gäller genomförda riskanalyser och informationssäkerhetsklassningar skiljer sig dock i betydande utsträckning mellan verksamheterna.

Granskningen har också visat att informationssäkerhet inte i tillräcklig utsträckning är en ledningsfråga som hanteras av verksamheternas förvaltningschefer/vd:ar, vilket påverkar landstingets systematiska informationssäkerhetsarbete. Detta gäller särskilt HSN och SLSO där rapporteringen till förvaltningschef av status för arbetet med implementering av LIS behöver utvecklas i enlighet med styrdokumenten för informationssäkerhet. Vidare visar granskningen att arbetet med införande av LIS fortfarande är i ett inledande skede. Det saknas systematik i arbetet med riskanalyser och riskhantering vilket kan innebära att väsentliga risker inom området inte omhändertas fullt ut vid de granskade objekten.

Ansvar och roller för informationssäkerhet som beskrivs i landstingets styrande dokument för området är tydliga. Enligt landstingets riktlinjer är ansvaret för informationssäkerheten kopplat till det delegerade verksamhetsansvaret. Detta är dock fortfarande inte i tillräcklig utsträckning implementerat i landstingets nya FOA-organisation (förvaltningsstyrningsmodell enligt pm3). Några huvudsakliga roller och ansvar har förtydligats i FOA-organisationens rollbeskrivningar, men ansvar och ansvarsfördelning behöver tydliggöras ytterligare, exempelvis mellan informationsägare och objektägare. Otydliga beskrivningar kan försvåra informationssäkerhetsarbetet, t.ex. när det gäller tolkningen av ansvar för informationssäkerheten och riskanalyser. Granskningen har också visat på otydligheter vad gäller ansvarsfördelningen mellan landstingsgemensam FOA-organisation och lokal FOA-förvaltning och hur landstingsgemensamma beslut/åtgärder förmedlas och tillämpas lokalt. En otydlig ansvarsfördelning riskerar att påverka effektiviteten i ledningssystemet för informationssäkerhet och därmed landstingsstyrelsens underlag för uppföljning och analys av landstingets informationssäkerhet.

Granskningen visar vidare att det saknas en landstingsgemensam terminologi inom informationssäkerhet, som även rör arbetet med riskanalyser. Gransk-

ningen har även visat att när information överförs till andra system inom landstinget är det inte tydligt vem som blir informationsägare.

Arbetet med framtagande och beslut av tillämpningsanvisningar har försenats i drygt ett år. Det är angeläget att tempot i införandet av ledningssystemet för informationssäkerhet ökar, både på central och på lokal nivå, så att landstingsstyrelsen kan vidta välgrundade och avvägda skyddsåtgärder som bygger på verksamheternas riskanalyser och handlingsplaner. Det saknas även central landstingsövergripande styrning och uppföljning av förhållningssätt gentemot privata utförare inom vården vad gäller informationssäkerhet. Revisionens samlade bedömning är att det återstår mycket arbete innan landstinget har nått en tillfredsställande nivå i implementeringen av LIS.

Rekommendationer

- Landstingstyrelsen bör
    - prioritera arbetet med att införa compliance-processen i landstingets verksamheter för att påskynda det systematiska informationssäkerhetsarbetet.
    - prioritera arbetet med framtagande och beslut av tillämpningsanvisningar, så att välgrundade och avvägda skyddsåtgärder kan vidtas.
    - säkerställa att ansvar och roller för informationssäkerhet implementeras i FOA-organisationen (landstingets förvaltningsstyrningsmodell enligt pm3).
    - följa upp hur informationssäkerhet säkerställs hos privata utförare inom vården.
- Hälso- och sjukvårdsnämnden bör, i syfte att stärka informationssäkerheten, säkerställa att rapportering sker till ledningen i enlighet med fastställda styrdokument för informationssäkerhet.
- Stockholms läns sjukvårdsområde bör, i syfte att stärka informationssäkerheten, säkerställa att rapportering sker till ledningen i enlighet med fastställda styrdokument för informationssäkerhet.

2 Utgångspunkter för granskningen

2.1 Motiv till granskningen

Landstingsfullmäktige och landstingsstyrelsen har fastställt policy och riktlinjer för informationssäkerhet inom Stockholms läns landsting (SLL)[1]. Enligt policyn ska informationssäkerhetsarbetet styras genom landstingets ledningssystem för informationssäkerhet[2]. Grunden i landstingets ISO[3]-anpassade ledningssystem för informationssäkerhet utgörs av policy, riktlinjer och tillämpningsanvisningar. En process för informationssäkerhetsarbete, Compliance-processen, och ett tillhörande IT-baserat verktyg[4] har tagits fram i syfte att stödja ett systematiskt informationssäkerhetsarbete, centralt såväl som lokalt.

Revisionen granskade i slutet av 2014 landstingets ledningssystem för informationssäkerhet (LIS). Granskningen visade att landstingets policy och riktlinjer för informationssäkerhet anpassats till gällande standard, men att införandet av LIS hade försenats. Ett fåtal tillämpningsanvisningar var framtagna och revisionen konstaterade att förseningen hade påverkat förutsättningarna för det lokala informationssäkerhetsarbetet. Det fanns även behov av att tydliggöra hur och när uppföljning av status för det lokala informationssäkerhetsarbetet vid nämnder och styrelser ska rapporteras till landstingsstyrelsen. Revisionen konstaterade att landstingsstyrelsen inte hade följt upp verksamheternas informationssäkerhet på det sätt riktlinjerna förutsätter.

Att riskanalyser och informationsklassning inte genomförs i tillräcklig utsträckning kan leda till att kontroller för att förebygga och upptäcka fel saknas eller är otillräckliga. Den snabba utvecklingen inom IT-området innebär dessutom att samhället sannolikt utsätts för risker som ännu inte är kända. Såväl nationella som internationella bedömare[5] anser att utvecklingen av fientliga IT-relaterade hot (attacker, IT-brott, spionage, kränkningar, etc.) går fortare än samhällets utveckling av skyddsåtgärder. Brister kan också leda till ett minskat förtroende för offentliga och privata aktörer som tillhandahåller viktiga tjänster för landstingets räkning.

Revisionen bedömer sammanfattningsvis att risknivån är fortsatt hög inom informationssäkerhetsområdet och årets granskning av implementeringen av ledningssystemet har därför fokuserats på landstingsstyrelsens uppföljning, analys och införande av ledningssystemet för informationssäkerhet.

2.2 Revisionsfråga

Övergripande revisionsfråga:
Genomförs implementeringen av ledningssystemet för informationssäkerhet inom landstinget på ett sådant sätt att väsentliga risker inom området omhändertas?

Revisionsfrågan är därefter nedbruten i tre delar:

A Finns dokumenterade riskanalyser med tillhörande handlingsplaner på central och lokal nivå?

[1] LS 1112-1733.
[2] Informationssäkerhetspolicy inom Stockholms läns landsting, LS 1112 – 1733, sid 4
[3] Internationella standardiseringsorganisationen, är ett internationellt standardiseringsorgan, representerat av nationella standardiseringsinstitutioner
[4] IT-verktyget Compliance-portalen, metod- och dokumentationsstöd för ledningssystemet.
[5] Bl.a. MSB:s trendrapport, FRA:s trendrapport och Swedish National Audit Office; Country Papers on Topic 2 Cyber Security.)

B Har informationsägare utsetts och säkerhetsklassning gjorts för viktiga informationstillgångar på lokal nivå?

C Är landstingsstyrelsens uppföljning tillräcklig för att ge underlag för beslut om åtgärder för att säkerställa en god informationssäkerhet?

2.3 Avgränsning

Granskningen kommer att ligga till grund för ansvarsprövningen av landstingsstyrelsen, Södersjukhuset AB (SÖS), Karolinska universitetssjukhuset (Karolinska), Stockholms läns sjukvårdsområde (SLSO) och hälso- och sjukvårdsnämnen (HSN). Granskningen har ett särskilt fokus på förvaltningschef/vd:s ansvar och informationssäkerhetssamordnarens roll i samband med implementering av LIS[6]. Revisionen har översiktligt granskat vilken status det grundläggande informationssäkerhetsarbetet har på ovan nämnda enheter inom landstinget.

2.4 Bedömningsgrunder

Landstingsfullmäktiges policy respektive riktlinjer för informationssäkerhet med fokus på följande områden:

- Landstingsstyrelsen har det övergripande ansvaret för samordning och uppföljning av informationssäkerheten inom landstinget.
- Följsamheten till landstingets riktlinjer för informationssäkerhet ska årligen följas upp på en övergripande nivå genom informationssäkerhetsrådet och rapporteras till landstingsdirektören via informationssäkerhetschefen.
- Varje nämnd och styrelse ansvarar för att löpande följa upp informationssäkerheten och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll.

2.5 Metod

Granskningen har genomförts i form av dokumentstudier och intervjuer. Intervjuerna har genomförts hos HSN, Karolinska, SLSO och SÖS. För dessa verksamheter har även utfallet från Compliance-portalen granskats. På landstingsstyrelsens förvaltning genomfördes intervjuer med landstingets informationssäkerhetschef.

3 Ledningssystem för informationssäkerhet – organisation och ansvar

Enligt landstingets policy och riktlinjer för informationssäkerhet ska landstinget bedriva ett systematiskt säkerhetsarbete i syfte att skydda landstingets information. Varje nämnd/styrelse har ansvar för informationssäkerheten inom sitt verksamhetsområde och ska årligen planlägga och löpande följa upp informationsarbetet. Förvaltningschef/vd ansvarar för att all informationshantering sker enligt fastställda styrdokument och ska bland annat utse en informationssäkerhetssamordnare som rapporterar informationssäkerhetsarbetet till förvaltningschef/vd.

Landstinget har inrättat ett informationssäkerhetsråd (ISR) där informationssäkerhetssamordnarna från landstingets förvaltningar/bolag samverkar för att övergripande främja, stödja, samordna och följa upp landstingets informations-

[6] Ledningssystem för informationssäkerhet.

säkerhetsarbete. Rådet leds av landstingets informationssäkerhetschef som organisatoriskt tillhör landstingsstyrelsens förvaltning (LSF).

Regelverket[7] anger att det för varje viktig informationstillgång ska utses en informationsägare som bl.a. ansvarar för att klassificera informationen, se till att riskanalyser genomförs och ställa de säkerhetskrav som krävs för en säker informationshantering. Landstingsstyrelsen fattade 2015-11-03 beslut[8] avseende översyn av roller, ansvar och beslutsmandat så att tydliga beslutskedjor kan etableras för IT-säkerhetsåtgärder och hantering av IT-säkerhetsrelaterade incidenter[8]. incidenter och avvikelser som rör informationssäkerhet bör hanteras och rapporteras inom ramen för de processer och rutiner som redan finns, det vill säga i enlighet med gällande krisberedskapsplan samt i enlighet med övrig avvikelsehantering.

Av landstingets riktlinjer för informationssäkerhet framgår att varje verksamhet ska genomföra och dokumentera analyser av vilka hot, risker och sårbarheter som kan påverka verksamheten och utifrån dessa analyser vidta lämpliga säkerhetsåtgärder. Informationsägaren ska se till att riskanalyser genomförs och att samordning av riskanalyser sker med andra informationsägare när behov finns för det. Regelverket säger också att alla anställda inom landstinget måste genomgå en grundläggande informationssäkerhetsutbildning, exempelvis DISA[9].

En väsentlig byggsten i landstingets ledningssystem för informationssäkerhet utgörs en ny process för informationssäkerhet, Compliance-processen, samt ett tillhörande it-system kallat Compliance-portalen. Verktyget är ett system för dokumentation, uppföljning och kontroll av informationssäkerhetsarbetet, centralt såväl som lokalt för landstinget. Systemet ger stöd för upprättande av handlingsplan, avvikelseanalys och även för riskbedömning och informationsklassificering. Se vidare avsnitt 4.3 nedan.

4 Implementering av ledningssystem för informationssäkerhet

4.1 Organisation, riskanalyser och handlingsplaner

Iakttagelser

Karolinska Universitetssjukhuset

På Karolinska finns en handlingsplan för verksamheten som även omfattar arbetet med informationssäkerhet. Verksamhetsanpassade styrande dokument för informationssäkerhet i form av riktlinjer och policy har tagits fram med utgångspunkt från de landstingsövergripande styrdokumenten. Karolinska har arbetat utifrån de tillämpningsanvisningar för implementering av LIS som landstinget centralt hittills har tagit fram.

Karolinska arbetar med Compliance-portalen och är landstingets pilot när det gäller införandet av Compliance-processen på flera organisationsnivåer, t.ex. division och klinik. I verktyget har flera enheter inom Karolinska deklarerat och riskbedömt arbetet utifrån ett informationssäkerhetsperspektiv. Karolinska framhåller att det finns många fördelar med verktyget och pekar framförallt på

[7] LS 1112-1733 Policy och riktlinjer för informationssäkerhet.
[8] LS 1404-0548
[9] Datorstödd informationssäkerhetsutbildning för användare.

möjligheten till systematisk uppföljning av informationssäkerhetsarbetet. Utifrån riskanalyser som Karolinska har genomfört i verktyget har handlingsplaner med åtgärder tagits fram. Uppföljning sker i Karolinskas ledningsforum för informationssäkerhet och med de lokala informationssäkerhetskoordinatorerna. Samverkan sker även mellan landstingets informationssäkerhetsråd och med SLL:s informationssäkerhetschef och SLL IT. Ramverk finns för uppföljning av avtal, juridiska krav och kontroll av externa leverantörer och frågorna diskuteras även i den gemensamma policygruppen för TakeCare.

Karolinskas lokala FOA-organisation[10] anser att ansvarsfördelningen fortfarande är otydlig när det gäller informationssäkerhetsarbetet. Detta gäller exempelvis ansvaret mellan den landstingsgemensamma FOA-organisationen och Karolinskas lokala FOA-förvaltning samt hur beslut/åtgärder i den gemensamma FOA-organisationen ska förmedlas och tillämpas lokalt på Karolinska. Man framhåller vidare att kraven på informationssäkerhet även behöver efterlevas i större utsträckning i systemutvecklingsprocesserna. Karolinska arbetar med sammanhållen journalföring och anser att medvetenheten och mognadsgraden när det gäller patientdatahantering är hög. Karolinska genomför kontinuerligt utbildningar inom området. Efter de senaste årens omfattande störningar i patientjournalsystemet TakeCare var Karolinska delaktig i arbetet med att ta fram en handlingsplan med åtgärder för att minska risken för att liknande störningar inträffar igen. Handlingsplanen inriktades på vårdinformationens tillgänglighet och åtkomst till systemet och majoriteten av åtgärderna är i dagsläget implementerade. På Karolinska finns det kontinuitetsplaner och återstartsplaner för merparten av systemen.

Karolinska reumatologen - pilotklinik

Reumatologkliniken på Karolinska är en pilotklinik för implementering av LIS. Det finns en handlingsplan för införandet och kliniken har deklarerat sin verksamhet och genomfört en riskanalys i Compliance-portalen. Riskanalysen visade att kliniken behöver identifiera vilka system som finns inom verksamheten och utifrån det arbeta med handlingsplanens åtgärder. Kliniken har genomfört DISA-utbildning för ett flertal medarbetare. Informationssäkerhetsfrågor har tagits upp på ledningsgruppens agenda och avrapportering sker med jämna mellanrum.

Informationssäkerhetsområdet har diskuterats på arbetsplatsträffar. Under diskussionerna har det bland annat framkommit att medarbetare ibland sparar patientinformation på gemensamma lagringsytor/kataloger. För ett år sedan kontrollerades behörigheterna i TakeCare. Då framkom det att behörighetsförändringarna inte fungerar tillräckligt bra i samband med att personal byter verksamhet (t.ex. sjukhus) inom landstinget. Detta innebär bl.a. att personer som tidigare har arbetat på Karolinska har kvar behörigheterna i TakeCare fast de nu arbetar i annan verksamhet inom SLL. Reumatologkliniken har en ambition att under 2016 ta fram en lokal behörighetstilldelningsrutin.

SLSO

SLSO har en lokal handlingsplan för implementering av LIS som inom kort ska fastställas av ledningen. Den lokala handlingsplanen tar upp centrala områden som bl.a. tillsättning av roller och stödjande/styrande dokumentation. Det finns dessutom fastställda anpassade lokala riktlinjer och en policy som bygger på de landstingsövergripande. Det saknas etablerade kommunikations- och rapporteringsvägar mellan informationssäkerhetssamordnaren och förvaltningschefen.

[10] Förvaltningsobjektarkitektur inom landstingets modell för förvaltningsstyrning (enligt pm³).

SLSO framhåller samarbete och tydlighet inom landstinget som framgångsfaktorer för det egna arbetet. Informationssäkerhetssamordnaren deltar på informationssäkerhetsrådets månadsmöten och är även delaktig i de arbetsgrupper som tillsatts av informationssäkerhetsrådet. Informationssäkerhetssamordnaren deltar även i den gemensamma policygruppen för TakeCare.

SLSO är i startskedet av implementeringen av Compliance-processen i den egna verksamheten och har genomfört den inledande deklarationen. Ambitionen är att starta upp ett pilotarbete där implementeringen av LIS ska testas för verksamheten. SLSO har även haft stöd av Trafikförvaltningen, som redan har implementerat processen och har flerårig erfarenhet av att arbeta utifrån denna. Den viktigaste frågan är nu att identifiera en lämplig pilotklinik och att kliniken kan få centralt stöd på samma sätt som Karolinskas pilotklinik har haft. Compliance-portalen bedöms vara en framtida hjälp för SLSO när det gäller uppföljning och central återkoppling av LIS-införandet. Riskanalyser av informationssäkerhet genomförs inte systematiskt i dagsläget.

När SLSO anlitar externa leverantörer upprättas PUB[11]-avtal för dessa. SLSO efterfrågar en central landstingsövergripande styrning och uppföljning av informationssäkerhetskrav gentemot externa leverantörer.

SLSO verksamhetsstöd eHälsa

Verksamhetsstöd eHälsa inom SLSO kommer dagligen i kontakt med risker som rör informationssäkerhetsområdet, det kan t.ex. handla om allt från att användare har problem med e-tjänstekort till användares hantering av patientinformation. Ett annat exempel är avvikelsehanteringen i landstings gemensamma IT-stöd för avvikelserapportering, Händelsevis, t.ex. vid fel på ordination av läkemedel i TakeCare. Det finns framtagna rutiner för överlämnande av patientinformation till tredje part såsom försäkringsbolag, myndigheter och organisationer. Intervjuad personal vid eHälsa känner inte till att det finns en hantering vad gäller informationssäkerhetsavvikelser och har därför arbetat med avvikelsehantering inom detta område. Ibland genomförs riskanalyser i samband med projektarbete även om det idag saknas rutin för detta. Verksamhetsstöd eHälsa känner inte till Compliance-portalen.

HSN

HSN följer SLL:s ledningssystem för informationssäkerhet men har inte anpassat de landstingsövergripande riktlinjerna till sin verksamhet, utan istället beslutat om identiska riktlinjer. När det gäller SLL:s informationssäkerhetspolicy kommer förvaltningen enligt uppgift inom kort att göra anpassningar till HSN:s verksamhet. Det finns en informationssäkerhetssamordnare som deltar i landstingets informationssäkerhetsråd. Informationssäkerhetssamordnaren rapporterar inte direkt till förvaltningschefen. HSN har nu fastställt en handlingsplan för det kommande arbetet med informationssäkerhet och implementering av LIS. Någon uppföljning är inte genomförd ännu. Handlingsplanen innehåller fyra prioriterade områden; styrande dokument, organisation av informationssäkerhetsarbetet, kunskapsspridning och förvaltningsetablering (informationsklassning, riskanalys mm). HSN har genom deklarationen i Compliance-portalen identifierat avvikelser men ännu inte vidtagit några skyddsåtgärder. HSN har varit delaktiga i arbetet med utformningen av Compliance-portalen och ser fördelar med verktyget, men efterfrågar en centralt framtagen utbildning för verktygets användningsområde.

[11] Personuppgiftsbiträdesavtal

Arbetet med riskanalyser skiljer sig inom HSN. Riskanalyser som delvis berört informationssäkerhetsområdet har genomförts för grupper av likartade system. Det finns dock vissa brister vad gäller dokumentation och uppföljning av riskanalyserna. Vad det gäller styrning och uppföljning av avtal och kontroll av externa leverantörer gällande informationssäkerhet så varierar detta och förvaltningen efterfrågar en central tillämpningsanvisning för detta område.

Informationssäkerhetsutbildningen DISA har genomförts av samtliga på avdelningen E-hälsa och strategisk IT, och ska fortsätta enligt plan med resterande avdelningar. Avdelningen anser att det finns mycket kunskap om informationssäkerhet inom HSN. Utmaningen är att samla den och få igång ett systematiskt arbete.

HSN utvecklingsavdelningen

Utvecklingsavdelningen på HSN menar att de har ett högt informationssäkerhetsmedvetande och känner till de styrande dokumenten och landstingets arbete med informationssäkerhet. Avdelningen anser att arbetet med informationssäkerhet måste vara flexibelt och det måste finnas utrymme för undantag. Många inom HSN sparar information på de lagringsytor som är tillgängliga för alla. Vilket i sin tur leder till att information blir tillgänglig för obehöriga. Avdelningen har infört skyddsåtgärder vad det gäller extern åtkomst till information. Att öka utbildningsgraden är det viktigaste enligt avdelningen, men DISA-utbildningen är inte genomförd.

Södersjukhuset

SÖS har ett regelverk för informationssäkerhet sedan 2013. Informationssäkerhetssamordnaren arbetar med att nå ut med information avseende arbetet med informationssäkerhet och deltar i landstingets informationssäkerhetsråd. Det finns arbetsplaner för implementeringen av LIS. Informationssäkerhetssamordnaren har möjlighet att rapportera till vd och deltar kontinuerligt på ledningens genomgång. SÖS har deklarerat arbetet med informationssäkerhet i Compliance-portalen och kommer under 2016 påbörja arbetet med att följa upp informationssäkerhetsarbetet i verktyget.

Vad gäller uppföljning av avtal, juridiska krav och kontroll av externa leverantörer så arbetar SÖS med detta, men inte på ett systematiskt sätt. Riskanalyser används ofta i samband med genomförande av projekt och i förändringsarbete. Däremot inte utifrån ett informationssäkerhetsperspektiv. SÖS har inte genomfört en övergripande riskanalys utifrån ett informationssäkerhetsperspektiv i Compliance-portalen. Detta finns dock med i handlingsplanen för 2016, liksom arbete med åtgärdsplan utifrån identifierade risker. Uppfattningen är att riskanalyserna i nuläget fokuserar på tillgänglighet, men inte på konfidentialitet[12]. På SÖS finns det ett antal metoder att genomföra riskanalyser på och det leder till förvirring och osäkerhet. SÖS anser att det borde finnas en landstingsgemensam terminologi inom informationssäkerhet som hanterar begreppsförvirringen, bland annat för arbetet med riskanalyser.

SÖS Verksamhetsområde Bild

På Verksamhetsområde Bild kommer de anställda dagligen i kontakt med informationssäkerhetsfrågor kopplat till patientsäkerhet. Utbildningsgraden inom informationssäkerhetsområdet varierar på avdelningen. Avdelningen känner till att de ska genomföra DISA-utbildningen, men inte hur eller när. Då avvikelser uppstår i arbetet rapporteras det i avvikelsesystemet Händelsevis, men avdel-

[12] Konfidentialitet innebär information inte görs tillgänglig eller avslöjas för obehöriga personer, enheter eller processer.

ningen saknar återkoppling när det gäller hantering av inträffade avvikelser. Personalen på Verksamhetsområde Bild är inte delaktiga i några riskanalyser, granskningar eller uppföljningar inom informationssäkerhetsområdet. Personalen känner inte heller till att det finns en organisation på SÖS som arbetar med informationssäkerhet. Verksamhetsområde Bild har uttalade rutiner för hur de ska arbeta när det är driftsstörningar.

Revisionens bedömning
Karolinska är drivande i arbetet med implementering av LIS inom landstinget och informationssäkerhetssamordnaren har en central roll i flera landstingsövergripande grupperingar. Karolinska har etablerat arbetet med riskanalyser och arbetar systematiskt med handlingsplaner. Revisionen bedömer dock att informationssäkerhetsarbetet på Karolinska hittills inte i tillräcklig utsträckning lyfts upp till sjukhusledningen och att det systematiska informationssäkerhetsarbetet är alltför personberoende. En rapportering till ledningen är enligt uppgift beslutad och kommer att genomföras.

Revisionens bedömning är att Karolinska bör förtydliga ansvarsfördelningen av informationssäkerhetsarbetet ytterligare. Detta gäller t.ex. ansvaret mellan landstingsgemensamma FOA-organisationen och Karolinskas lokala FOA-förvaltning samt hur landstingsgemensamma beslut/åtgärder ska förmedlas och tillämpas lokalt på Karolinska. Revisionen anser att det arbete som startats vid reumatologen på Karolinska bör tas tillvara och återkopplas till övriga kliniker så att piloterfarenheter och goda exempel sprids i verksamheten.

SLSO har centralt påbörjat sitt arbete med informationssäkerhet, men fortfarande saknas systematik och de har inte etablerat former och rutiner för rapportering till ledningen. SLSO har deklarerat status för informationssäkerhetsarbetet i Compliance-portalen. Däremot har inte några riskanalyser genomförts i verktyget vilket är viktigt att snarast påbörja då utfallet ska ligga till grund för det fortsatta arbetet på SLSO med implementering av LIS och genomförande av handlingsplan. Arbetet med att införa Compliance-processen har inte påbörjats när det gäller verksamheterna. Granskningen visade t.ex. att verksamhetsstöd eHälsa ännu inte känner till Compliance-portalen.

Revisionen bedömer att HSN behöver utveckla en sammanhållen styrning av arbetet med riskanalyser. Det saknas en systematisk rapportering av status för arbetet med implementering av LIS till förvaltningschefen. Det finns flera olika modeller för riskanalys inom förvaltningen och det är viktigt att förvaltningen säkerställer att informationssäkerhetsperspektivet beaktas i samtliga riskanalyser.

Även SÖS har påbörjat sitt informationssäkerhetsarbete. Det är viktigt att SÖS genomför en sjukhusövergripande riskanalys och tar fram en åtgärdsplan utifrån identifierade risker i enlighet med sin handlingsplan. Revisionen bedömer att informationssäkerhetssamordnaren på SÖS arbetar med att säkerställa grunderna för implementering av LIS.

De granskade objekten följer i varierande grad upp informationssäkerheten hos privata utförare. Revisionen menar att landstingsstyrelsen bör följa upp hur informationssäkerheten hos privata utförare säkerställs.

4.2 Informationsägare och informationsklassning

Iakttagelser

Karolinska

På Karolinska är roller som informationssäkerhetssamordnare och informationssäkerhetskoordinatorer tillsatta. Ansvaret för klassningen av information och rollen informationsägare ingår i det delegerade verksamhetsansvaret på Karolinska och informationssäkerhetssamordnaren och koordinatorerna utgör ett stöd till verksamhetsansvariga på sjukhuset. Karolinska har arbetat med införandet av landstingets förvaltningsstyrningsmodell för sina IT-system som bygger på pm3[13] modellen. Karolinska anser dock att förvaltningsmodellen inte harmoniserar med LIS då modellen inte tydliggör ansvar för informationssäkerhet. Historiskt har systemägarskapet varit förknippat med informationsägarskap. På Karolinska är det nu objektägaren/verksamhetschefen som är informationsägare, men det är fortfarande oklart vilket ansvar som rollen omfattar. Karolinska efterlyser att rollen informationsägare förtydligas centralt för att kunna tillämpas på ett likartat sätt i alla verksamheter.

SLSO

SLSO har inte hanterat frågan avseende harmonisering av förvaltningsmodellen pm3 till det styrande regelverket för informationssäkerhet. Det finns uttalade informationsägare när det gäller patientinformation. Inom SLSO är det verksamhetschefen för den verksamhet som skapat informationen som är informationsägare. SLSO har genomfört en informationsklassning för respektive system, men denna är inte fastställd. När information överförs/förflyttas till andra system inom landstinget är det inte tydligt vem som blir informationsägare. Ett exempel är GVR (Gemensamt Vårdregister) som HSF förvaltar och som används av flera enheter i landstinget. SLSO upplever även att informationsägarskapet blir otydligt då patientinformation förflyttas exempelvis från patientjournalsystemet till ekonomisystemet. För systemen TakeCare och Obstetrix finns det kontinuitetsplaner och återstartsplaner.

SLSO verksamhetsstöd eHälsa

Verksamhetsstöd eHälsa på SLSO anser att informationsägarskapet är tydligt och varje resultatenhet har en verksamhetschef som är informationsägare. Det saknas dock kunskap om pågående arbete med informationsklassificering. Verksamhetsstöd eHälsa känner till att det finns kontinuitetsplan för TakeCare, för övriga system är det oklart om någon plan finns framtagen. Avdelningen upplever att det finns otydligheter mellan förvaltningsmodellens roller och ansvar och informationssäkerhetsorganisationen inom landstinget.

HSN

HSN arbetar enligt förvaltningsmodellen pm3, men saknar stöd från central nivå av arbetet både med modellen generellt men också vad avser FOA-organisationens roller och kopplingen till informationssäkerhet. Däremot noteras att roller är tydligt uttalade i LIS. HSN har inte utsedda informationsägare för varje informationstillgång och har inte heller klassificerat all information. Då information ska överlämnas till extern part finns det framtagna rutiner och hjälp att tillgå. Däremot saknas detta vid utbyte av information mellan system inom landstinget. Det förekommer driftsavbrott och det finns framtagna rutiner för hur förvaltningen ska hantera kontinuitet vid dessa tillfällen, men rutinerna är inte framtagna utifrån informationsklassificering.

[13] pm3 är en förvaltnings- och portföljstyrningsmodell. Modellen är idag den mest använda modellen för förvaltningsstyrning i Sverige.

SÖS

Informationsklassning har genomförts för de viktigaste verksamhetssystemen på SÖS. För dessa finns det utsedda informationsägare. Tillämpningsanvisning har använts i arbetet med informationsklassificering av systemen. Det finns fastställda krav på tillgänglighet för de informationsklassificerade systemen, men det är oklart om det finns kontinuitetsplaner och återstartsplaner för alla dessa system. För systemen RIS och PACS som används vid Verksamhetsområde Bild finns kontinuitetsplaner. Avvikelser hanteras dagligen i röntgensystemen PACS och RIS samt i patientjournalsystemet TakeCare. Dessa rapporteras och eskaleras i avvikelsesystemet Händelsevis. Det finns ingen naturlig samverkan mellan informationssäkerhetssamordnaren och avvikelserapporteringen.

Revisionens bedömning
Karolinska har etablerat arbetet med informationsklassning och arbetar systematiskt med Compliance-portalen.

SLSO har informationsklassificerat systemen, men klassningarna är inte fastställd av ledningen vilket kan innebära risk för att relevanta skyddsåtgärder inte vidtas. Informationsägare har utsetts när det gäller patientinformation men ännu inte för samtliga väsentliga informationstillgångar.

På HSN har informationsklassificering genomförts för vissa informationstillgångar, men inte för alla och det finns inte heller utsedda informationsägare för samtliga väsentliga informationstillgångar. Ledningen behöver säkerställa att implementeringen av LIS genomförs utifrån handlingsplanen med stöd av Compliance-portalen.

Revisionen bedömer att arbetet med informationsklassning är etablerat på SÖS och att planen att informationsklassificera system och utse ansvariga roller i samband med anskaffning följer riktlinjerna för informationssäkerhet.

4.3 Landstingsstyrelsens uppföljning

Iakttagelser
Under våren 2015 skedde en inrapportering i Compliance-portalen från samtliga verksamheter i landstinget till landstingsstyrelsens förvaltning (LSF) när det gäller följsamheten till landstingets styrande dokument för informationssäkerhet. Under hösten har förvaltningen arbetat med att ta fram en analysrapport som bygger på denna inrapportering. Analysrapporten visar i stort att det systematiska informationssäkerhetsarbetet har kommit olika långt i olika verksamheter.

Arbetet med tillämpningsanvisningarna (TA) för beslut av landstingsdirektören har försenats över ett år. Arbetet med förankring, utbildning och omskrivningar har tagit lång tid. De fem viktigaste TA beslutades av landstingsdirektören den 14 januari 2016. Under 2016 kommer både informationssäkerhetspolicyn och riktlinjerna för informationssäkerhet att revideras dels med anledning av justeringar i TA och beslut rörande mandat, dels med anledning av ändringar i standarden för informationssäkerhet ISO-27000-serien.

Arbete pågår med framtagande av process för incidenthantering. En utredning av roller och ansvar har genomförts som beskriver hantering av IT-

säkerhetsrelaterade incidenter[14], och beslutades av Innovationsberedningen [15]2015-10-15, se vidare kapitel 3. Det pågår även ett arbete med att bygga upp en rapportering av status på informationssäkerheten till landstingsstyrelsen. Den omfattar både ledningens genomgång och framtagande av målstruktur som LS ska besluta om. Därefter kommer ett arbete med att operationalisera målen att ske.

Arbete med en dokumenterad riskbedömning på central nivå pågår. LSF kommer att göra en GAP-analys[16] och riskbedömning på förvaltningar/bolag. Tidigare arbetade LSF med kvalitativa övergripande bedömningar, men nu kommer arbetet ske kvantitativt med stöd av Compliance-portalen.

Det finns en arbetsversion av en central handlingsplan 2016-2020 för Stockholms läns landsting. När den centrala planen är antagen, troligen av landstingsstyrelsen under första kvartalet 2016, ska lokala handlingsplaner på förvaltningar/bolag tas fram. I handlingsprogrammet framgår vision, mål, delmål och resultatmål inklusive indikatorer.

Enligt landstingets riktlinjer är ansvaret för informationssäkerheten kopplat till det delegerade verksamhetsansvaret. Stöd från centralt håll avseende informationssäkerhetsarbetet inom landstingets FOA-organisation specifikt sker enligt LSF på två sätt: stöd till FOA-organisationens objektfamiljstyrgrupper samt stöd till landstingets informationssäkerhetsorganisation. Följande aktiviteter är genomförda: dialog och utbildningsinsatser med FOA-organisationen objektfamiljstyrgrupper, översättning och förtydliganden av roller i FOA-organisationens rollbeskrivningar utifrån ett urval av vad som finns i riktlinjerna samt utbildningsinsatser i informationssäkerhetsrådet.

Granskningen visar att det saknas tillfredsställande rutiner för behörighetsförändringar i TakeCare i samband med att personal byter verksamhet inom samma förvaltning/bolag (främst sjukhusen). Granskningen visar att det saknas tillfredsställande rutiner för behörighetsförändringar i TakeCare i samband med att personal byter verksamhet inom samma förvaltning/bolag (främst sjukhusen). Revisionen noterar dock att LSF för närvarande har en dialog med TC-förvaltningen kring krav. Det finns en funktion i TakeCare som gör det möjligt för medarbetare att ha olika roller med olika behörigheter på olika ställen men den funktionen har inte landstinget i sin installation av systemet.

Revisionens bedömning
Granskningen visar att förvaltningar och bolag har påbörjat implementering av Compliance-processen i sina verksamheter, samt arbetar i verktyget Compliance-portalen under förenklade former, men att det skiljer sig i vilken omfattning verksamheterna genomför riskanalyser och informationssäkerhetsklassning. Granskningen har visat att informationssäkerhet inte i tillräcklig utsträckning hanteras av verksamheternas högsta operativa ledningsnivå vilket kan försvåra det systematiska informationssäkerhetsarbetet i landstinget. Det är därför angeläget att tempot på införandet av LIS ökar, på både central och lokal

[14] LS 1404-0548
[15] Beredning under landstingsstyrelsen som bereder frågor om landstingets arbete med innovation, strategiska utvecklingen av landstingets IT-tjänster, teknisk infrastruktur, medicinteknik, informationssäkerhet, eHälsofrågor och utvecklingen av patientnära tjänster.
[16] Wikipedia: Målet med gapanalysen är att identifiera gapet mellan den nuvarande och den optimala fördelningen av insatser. Detta ger insikt om inom vilka områden som det finns rum för förbättring.

nivå så att landstingsstyrelsen kan vidta välgrundade och avvägda skyddsåtgärder som bygger på verksamheternas riskanalyser och handlingsplaner. Arbetet med framtagande och beslut av tillämpningsanvisningar har blivit försenat i drygt ett år. Revisionens samlade bedömning är att det återstår mycket arbete innan landstinget har nått en tillfredsställande nivå i implementeringen av LIS.

Trots att ett flertal aktiviteter genomförts som adresserar problemen i ansvar och roller vad gäller informationssäkerhetsarbetet mellan LIS och FOA-organisationen är revisionens bedömning att ytterligare riktade insatser behövs. Revisionen anser det viktigt att översyn sker av kontrollpunkter/ställda frågor i Compliance-portalen utifrån de erfarenheter den första rapporteringen gett. Det är t.ex. otydligt om hela eller delar av verksamheten ska ingå i svaren. Revisionen anser vidare att det pågående arbetet med rapportering av status på informationssäkerheten till landstingsstyrelsen (LS) är viktig för styrningen av informationssäkerhetsarbetet och att rapporteringen bör påbörjas snarast.

Kort om rapporten

Revisionen har granskat i vilken utsträckning ledningssystemet har implementerats inom Stockholms läns landsting. Granskningen visar att verksamheterna har påbörjat arbetet i den fastställda processen för informationssäkerhetsarbete och användandet av ledningssystemet. Omfattningen av genomförd riskanalys och informationssäkerhetsklassning skiljer sig dock i betydande utsträckning mellan verksamheterna. Revisionens samlade bedömning är att det återstår mycket arbete innan landstinget har nått en tillfredsställande nivå i implementeringen av ledningssystemet.

Landstingsrevisorerna
STOCKHOLMS LÄNS LANDSTING

Postadress: Box 22230, 104 22 Stockholm
Besöksadress: Hantverkargatan 25 B (T-bana Rådhuset)

Telefon: 08-737 25 00
E-post: landstingsrevisorerna@rev.sll.se **Hemsida:** www.sll.se/rev

Org.nr: 232100-0016