Stockholms läns landsting

Landstingsrådsberedningen

SKRIVELSE
2015-05-27

LS 2015-0344

Landstingsstyrelsen

Yttrande över landstingsrevisorernas projektrapport nr 14/2014, Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll?

Föredragande landstingsråd: Daniel Forslund

Ärendebeskrivning

Landstingsrevisorerna i revisorsgrupp I har översänt projektrapport 14/2014, Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll? för yttrande.

Förslag till beslut

Landstingsrådsberedningen föreslår landstingsstyrelsen besluta

att lämna yttrande över landstingsrevisorernas projektrapport 14/2014, *Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll?* enligt landstingsdirektörens tjänsteutlåtande.

Landstingsrådsberedningens motivering

Landstingsrevisorerna har granskat om ledningssystemet för informationssäkerhet ger förutsättningar för landstingsstyrelsen att säkerställa en tillräcklig styrning och intern kontroll inom området. Revisorernas bedömning är att arbete kvarstår i implementeringen av ledningssystemet, men att en tillräcklig kontroll kan ske när ledningssystemet är komplett och på plats. Landstingsstyrelsen ges ett antal rekommendationer kring den pågående implementeringen av ledningssystemet med stödjande tillämpningsanvisningar och uppföljningssystem.

Landstingsstyrelsen delar flera av landstingsrevisorernas synpunkter och konstaterar att arbetet på dessa områden pågår inom landstingets förvaltningar och att det i vissa delar redan är genomfört.

Landstinget ska vara väl förberett i händelse av en kris och effektivt kunna hantera och förebygga informationssäkerhetsincidenter. Ett arbete pågår för att se över organisation och resurser för de strategiska informationssäkerhetsfrågorna.

Beslutsunderlag

Arbetsutskottets protokollsutdrag den 5 maj 2015
Innovationsberedningens protokollsutdrag den 28 april 2015
Landstingsdirektörens tjänsteutlåtande den 9 april 2014
Landstingsrevisorernas projektrapport nr 14/2014, Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll?

Torbjörn Rosdahl

Daniel Forslund

Carl Rydingstam

§ 50

Yttrande Landstingsrevisorernas projektrapport 14/2014 - Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll?

LS 2015-0344

Ärendebeskrivning

Landstingsrevisorerna i revisorsgrupp I har översänt projektrapport 14/2014, Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll? för yttrande.

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 9 april 2014.
Landstingsrevisorernas projektrapport nr 14/2014, Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll?
Protokoll från Innovationsberedningen 28 april 2015.

Arbetsutskottets beslut

Arbetsutskottet beslutar föreslå landstingsstyrelsen besluta

att avlämna yttrande över landstingsrevisorernas projektrapport 14/2014, Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll? enligt landstingsdirektörens tjänsteutlåtande.

Beslutsexpediering:
Landstingsstyrelsen
Akt

§ 25
Landstingsrevisorernas projektrapport 14/2014 – Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll?

LS 2015-0344

Ärendebeskrivning

Landstingsrevisorerna i revisorsgrupp I har översänt projektrapport 14/2014, Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll? för yttrande.

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 9 april 2014
Landstingsrevisorernas projektrapport nr 14/2014, Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll?

Förslag och yrkande

Vid sammanträdet föreligger följande förslag
Landstingsdirektörens tjänsteutlåtande den 9 april 2014

Innovationsberedningens beslut

Innovationsberedningen föreslår arbetsutskottet föreslå landstingsstyrelsen besluta

att avlämna yttrande över landstingsrevisorernas projektrapport 14/2014, Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll? enligt landstingsdirektörens tjänsteutlåtande.

Beslutsexpediering:
Landstingsstyrelsens arbetsutskott
Akt

Landstingsstyrelsens förvaltning
Direktören strategisk IT

TJÄNSTEUTLÅTANDE
2015-04-09

LS 2015-0344

Handläggare:
Vesna Lucassi

Ankom
Stockholms läns landsting
2015 -04- 14
Dnr LS 2015-0344
Rotel VII

Landstingsstyrelsens
innovationsberedning

Yttrande över landstingsrevisorernas projektrapport nr 14/2014, Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll?

Ärendebeskrivning

Landstingsrevisorerna i revisorsgrupp I har översänt projektrapport 14/2014, Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll? för yttrande.

Beslutsunderlag

Landstingsdirektörens tjänsteutlåtande den 9 april 2014
Landstingsrevisorernas projektrapport nr 14/2014, Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll?

Förslag till beslut

Innovationsberedningen föreslår arbetsutskottet föreslå landstingsstyrelsen besluta

att lämna yttrande över landstingsrevisorernas projektrapport 14/2014, Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll? enligt landstingsdirektörens tjänsteutlåtande.

Förvaltningens förslag och motivering

Sammanfattning
Landstingsrevisorerna konstaterar vid revisionstillfället år 2014 att landstingets ledningssystem för informationssäkerhet, när det är på plats, kan skapa förutsättningar för landstingsstyrelsen att ha en tillräcklig intern kontroll inom området, men framhåller samtidigt vikten av att införandet inte bör försenas ytterligare. Landstingsstyrelsens förvaltning anser att revisonens rapport i huvudsak ger en rättvisande bild av situationen vid revisionstillfället. Arbete pågår med de aktiviteter som är nödvändiga för

införandet. En första mätning av förvaltningars och bolags informationssäkerhet genomfördes i början av år 2015.

Bakgrund
Landstingsstyrelsen och landstingsfullmäktige har fastställt policy och riktlinjer för informationssäkerhet inom Stockholms läns landsting. Informationssäkerhetsarbetet styrs genom landstingets ledningssystem för informationssäkerhet. Den pågående implementeringen av ledningssystemet med stödjande tillämpningsanvisningar och uppföljningssystem är viktiga förutsättningar för ett systematiskt informationssäkerhetsarbete inom landstinget samt för landstingsstyrelsens uppföljning och samordning inom området.

Revisionen har granskat om ledningssystemet ger landstingsstyrelsen förutsättningar att samordna och följa upp statusen på informationssäkerheten inom landstinget i syfte att stärka den interna kontrollen inom området. Granskningen har fokuserats på administrativ informationssäkerhet samt på landstingsstyrelsens ansvar i informationssäkerhetsarbetet. Den övergripande revisionsfrågan för granskningen var:

- Ger ledningssystemet för informationssäkerhet förutsättningar för landstingsstyrelsen att säkerställa en tillräcklig styrning och intern kontroll inom området?

Den sammanfattande bedömningen från granskningen är att ledningssystemet för informationssäkerhet, när det är komplett och på plats, kan skapa förutsättningar för landstingsstyrelsen att ha en tillräcklig intern kontroll inom området. Revisionen konstaterar samtidigt att arbete kvarstår i implementeringen av ledningssystemet. Landstingsstyrelsen ges i rapporten följande rekommendationer:

- Landstingsstyrelsen bör säkerställa implementeringen av ett ledningssystem för informationssäkerhet genom att snarast färdigställa arbetet med tillämpningsanvisningar samt det så kallade compliance-verktyget.
- Landstingsstyrelsen bör tydliggöra hur och när uppföljningen av status för det lokala informationssäkerhetsarbetet vid nämnder och styrelser ska ske och hur och när resultatet från dessa uppföljningar ska återrapporteras.
- Landstingsstyrelsen behöver säkerställa att nämnder och styrelser följer upp de krav som ställs på informationssäkerhet även när det gäller privata utförare som anlitas för att utföra kärnverksamhet för landstingets räkning.

Förvaltningen delar i stort revisorernas problembild och slutsatser, men önskar även framföra några kommentarer och synpunkter.

Övervägande
Informationssäkerhet är idag en stor utmaning. Den höga förändringstakten inom IT-området och behovet av exponering mot internet gör att hotbilden ständigt förändras. En tydlig styrning och uppföljning av informationssäkerhetsarbetet inom landstinget är därför en nödvändighet. Ett aktivt informationssäkerhetsarbete är viktigt inte bara ur ett kvalitetsperspektiv. Det är dessutom en framgångsfaktor i det förebyggande arbetet med att förhindra oönskade händelser och hantera informationssäkerhetsincidenter.

Grunden i landstingets ISO-anpassade ledningssystem för informationssäkerhet utgörs av policy och riktlinjer. Revisionens granskning visar att de styrande dokumenten är anpassade till gällande standard, ISO/IEC 27000-serien. Revisionen påtalar samtidigt vikten av att landstingsstyrelsens planerade harmonisering till den nya reviderade ISO-standarden, ISO/IEC 27000:14, sker skyndsamt. Förvaltningen instämmer i detta men önskar samtidigt framhålla att arbete pågår i landstingets förvaltningar och bolag med att implementera ledningssystemet på lokal nivå. Det är viktigt att harmoniseringen till den nya ISO-standarden inte stör det pågående arbetet i allt för stor utsträckning.

Övriga delar i ledningssystemet för informationssäkerhet utgörs av till riktlinjerna tillhörande tillämpningsanvisningar, handlingsplan för informationssäkerhet samt ett IT-baserat verktyg för systematiskt informationssäkerhetsarbete, vilket inkluderar efterlevnadskontroll och uppföljning

Revisionen konstaterade vid revisionstillfället att arbetet med riktlinjerna och de tillhörande tillämpningsanvisningarna är försenat och bör färdigställas snarast. Arbete med ta fram dessa pågår inom förvaltningen. Prioriterade tillämpningsanvisningar är granskade i informationssäkerhetsrådet där förvaltningars och bolags informationssäkerhetssamordnare deltar, och är nu innehållsmässigt färdiga för att skickas ut på remiss till förvaltningar och bolag.

En väsentlig byggsten i landstingets ledningssystem för informationssäkerhet utgörs av ett så kallat compliance-verktyg. Det är ett IT-baserat och behörighetsstyrt system för uppföljning och kontroll av informationssäkerhetsarbetet, centralt såväl som lokalt inom landstinget. Under

granskningstillfället var etableringen och tillgängliggörandet av IT-stödet till nämnder och styrelser ännu inte driftsatt.

Revisionen konstaterade därför att införandet av ett systematiskt informationssäkerhetsarbete inom landstinget försenats. Förvaltningen önskar påtala att det landstingsövergripande IT-stödet, så kallade Compliance-portalen, nu är infört. En första mätning av förvaltningars och bolags informationssäkerhetsarbete är genomförd. Analyser pågår för närvarande och resultatet kommer att återrapporteras till landstingsstyrelsen under år 2015.

Landstingsrevisorerna konstaterar vidare att det ännu inte finns någon dokumenterad beskrivning av hur resultaten i Compliance-portalen ska bearbetas, värderas och återkopplas till landstingsstyrelsen. Förvaltningen önskar i sammanhanget framhålla att en beskrivning av hur resultaten ska hanteras nu är framtagen, och stöd för överskådliga sammanställningar och rapporter finns i verktyget. Beskrivning och stöd kommer sannolikt att utvecklas med tiden allteftersom mätningar blir gjorda. Någon ytterligare dokumenterad beskrivning av detta har inte planerats.

För att säkerställa uppföljning inom informationssäkerhetsområdet har landstingsfullmäktige beslutat om ett nytt målområde med en övergripande indikator från och med år 2014. Målområdet benämns "Säkra processer - Säkerhetsarbetet ska bedrivas på ett systematiskt sätt" och en indikator är definierad som är direkt kopplad till arbetet med införandet av ledningssystemet för informationssäkerhet. Indikatorn följs upp årligen via bokslut. Uppföljningen på lokal nivå kommer att ske årligen enligt i förväg fastställt årshjul. Landstingsstyrelsens förvaltning har analyserat förvaltningarnas och bolagens rapporteringar för år 2014.

Rapportering av sammanställda resultat, såväl avseende delmålet Säkra processer som Compliance-resultaten, kommer att ske årligen.

Revisionens tredje och sista rekommendation är att landstingsstyrelsen behöver säkerställa att nämnder och styrelser följer upp de krav som ställs på informationssäkerhet även när det gäller privata utförare som anlitas för att utföra kärnverksamhet för landstingets räkning. Landstingets policy för informationssäkerhet gäller för samtliga privata utförare som arbetar på uppdrag av landstingets förvaltningar och bolag. Compliance-portalen ger förutsättningar för förvaltningar och bolag att följa upp om privata utförare uppfyller policyn. Mätning av denna aktivitet kommer att ske genom den årliga uppföljningen av den lokala nivån.

Utöver de tre rekommendationerna önskar landstingsförvaltningen nedan kommentera ett par andra punkter i rapporten.

Revisorerna konstaterar att ansvar och roller beskrivs på lite olika sätt i de styrande informationssäkerhetsdokumenten och i landstingets förvaltningsstyrningsmodell enligt pm3. I landstingets policy och riktlinjer för informationssäkerhet är rollen systemägare definierad. Beskrivningarna och benämningarna i landstingets riktlinjer för informationssäkerhet är generella och valda oberoende av vilken förvaltningsstyrningsmodell som nyttjas. Systemägarrollen motsvaras av flera roller i den nu gällande förvaltningsstyrningsmodellen. Ansvaret för rollen systemägare enligt riktlinjerna för informationssäkerhet ska återfinnas i de roller som finns i förvaltningsstyrningsmodellen. En dialog förs med ansvariga för förvaltningsstyrningsmodellen för att säkerställa att ansvaret täcks in.

Revisionen konstaterar avslutningsvis att sammanställnings- och analysarbetet, liksom arbetet med implementering och förvaltning av ledningssystemet i stort, bedöms vara omfattande och tidskrävande. Revisionen bedömer att det är oklart om det finns tillräckliga resurser på central nivå att administrera denna uppgift över tid. Det bedöms även vara oklart om det finns förutsättningar att tillhandahålla tillräckligt centralt stöd för informationssäkerhetssamordnarna, både vad gäller Compliance-verktyget och allmänt stöd gällande ledningssystemet i sig.

Landstingsstyrelsens förvaltning delar denna bedömning. Landstingsdirektören har fått i uppdrag att utarbeta och fastställa en organisation för förvaltningen som säkerställer genomförandet av landstingsstyrelsens beslut och uppdrag. Styrningen ska bli mer effektiv för att de visioner och mål som anges i budgeten om framtidens vård och en förbättrad kollektivtrafik ska kunna bli verklighet. Informationssäkerhetsområdet behöver stärkas, och styrningen och samordningen av informationssäkerhetsarbetet i landstinget utvecklas ytterligare. Mot denna bakgrund pågår arbete med att se över organisation och resurser för de strategiska informationssäkerhetsfrågorna.

Förvaltningen önskar avslutningsvis framhålla att landstingsrevisorernas iakttagelser och bedömningar kommer att beaktas i arbetet med att utveckla processerna för att fullgöra landstingsstyrelsens uppdrag.

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

Vesna Lucassi
Avdelningschef

PROJEKTRAPPORT NR 14/2014

Ankom
Stockholms läns landsting
2015 -02- 25
Dnr LS 2015-0344

Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll?

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. Landstingsrevisorerna omfattar både de förtroendevalda revisorerna och revisionskontoret.

Att vara revisor är ett förtroendeuppdrag vars syfte är att med oberoende, sakligt 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

Revisorsgrupp I

2015-02-19

Diarienummer:
RK 201409-0055

Landstingsstyrelsen

Projektrapport 14/2014
Ledningssystem för informationssäkerhet, förutsättningar för en god intern kontroll?

Revisorerna i revisorsgrupp I beslutade 2015-02-19 att överlämna rapporten till landstingsstyrelsen för yttrande senast 2015-05-22.

Revisorernas samlade bedömning är att landstingets ledningssystem för informationssäkerhet, när det är komplett och på plats, kan skapa förutsättningar för landstingsstyrelsen att ha en tillräcklig intern kontroll inom området. Införandet av ledningssystemet har försenats med cirka ett år. Granskningen visar att förseningen har påverkat förutsättningarna dels för det lokala informationssäkerhetsarbetet, dels för landstingsstyrelsen att på central nivå kunna följa upp verksamheternas informationssäkerhet som landstingsfullmäktiges riktlinjer för informationssäkerhet förutsätter.

Revisorerna vill till landstingsstyrelsen särskilt framhålla vikten av att implementeringen av ledningssystemet inte försenas ytterligare. Vidare menar revisionen att landstingsstyrelsen bör tydliggöra hur och när uppföljningen av status för det lokala informationssäkerhetsarbetet vid nämnder och styrelser ska ske och hur och när resultatet från dessa uppföljningar ska återrapporteras till landstingsstyrelsen. Landstingsstyrelsen bör även säkerställa att ansvaret för informationssäkerhet förtydligas i landstingets förvaltningsstyrningsmodell. Avslutningsvis vill revisionen framhålla vikten av att landstingsstyrelsen säkerställer att nämnder och styrelser följer de krav som ställs på informationssäkerhet även när det gäller privata utförare som anlitas för att utföra kärnverksamhet för landstingets räkning.

I övrigt hänvisar revisorerna till revisionskontorets rapport.

Paragrafen justerades omedelbart.

Kenneth Strömberg
ordförande

Agneta Fohlström
sekreterare

Landstingsrevisorerna
Box 22230
104 22 Stockholm

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

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

Besök oss: Hantverkargatan 25 B. T-bana Rådhuset

INNEHÅLL

1 SAMMANFATTNING OCH SLUTSATSER 4

2 UTGÅNGSPUNKTER FÖR GRANSKNINGEN 6

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

3 LEDNINGSSYSTEM FÖR INFORMATIONSSÄKERHET 7

3.1 Revisionens bedömning 9

4 ÖVERENSSTÄMMELSE MELLAN GÄLLANDE STANDARD OCH LANDSTINGETS POLICY OCH RIKTLINJER 9

4.1 Revisionens bedömning 10

5 ORGANISATION, ROLLER OCH ANSVAR 11

5.1 Revisionens bedömning 13

6 UPPFÖLJNING MED HJÄLP AV COMPLIANCE-VERKTYGET 14

6.1 Revisionens bedömning 15

1 Sammanfattning och slutsatser

Revisionen har granskat styrning och samordning av informationssäkerhetsarbetet i Stockholms läns landsting (SLL) utifrån landstingsstyrelsens övergripande ansvar. Granskningen syftar till att utreda om landstingets ledningssystem för informationssäkerhet ger landstingsstyrelsen förutsättningar för att säkerställa en tillräcklig styrning och intern kontroll inom området samt om det harmoniserar med tillämplig standard för informationssäkerhet, ISO 27000.

Granskningen visar att landstingets policy och riktlinjer för informationssäkerhet är anpassade till gällande standard och ger en tydlig beskrivning av roller och organisatoriskt ansvar för informationssäkerhetsfrågorna i landstinget.

Ansvar och roller beskrivs dock på lite olika sätt i de styrande informationssäkerhetsdokumenten och i landstingets förvaltningsstyrningsmodell (som baseras förvaltningsstyrningsmodellen pm3). Det kan medföra risk för begreppsförvirring, vilket kan leda till olika tolkningar som försvårar informationssäkerhetsarbetet. Landstingsstyrelsen bör säkerställa att ansvaret för informationssäkerheten förtydligas i landstingets förvaltningsstyrningsmodell.

Revisionen menar att det är viktigt att landstingsstyrelsens planerade harmonisering till den nya reviderade ISO-standarden sker skyndsamt och att styrdokumenten ensas så att de ger samma bild.

Policy och riktlinjer beslutades av landstingsfullmäktige under 2013, medan landstingsstyrelsens tillämpningsanvisningar för informationssäkerhetsarbetet ännu inte är klara. Landstingets handlingsplan för informationssäkerhet har inte uppdaterats sedan 2012. Enligt gällande policy ska handlingsplanen aktualiseras och beslutas årligen.

Den femte komponenten i landstingets ledningssystem är s.k. Compliance Management, för vilket ett tillhörande IT-baserat verktyg, compliance-verktyget, har tagits fram. Syftet med IT-stödet är att stödja processen för det systematiska informationssäkerhetsarbetet, centralt såväl som lokalt. Etableringen och tillgängliggörandet av IT-stödet till nämnder och styrelser har påbörjats, men är försenat. Införandet av ett systematiskt informationssäkerhetsarbete inom landstinget är därmed försenat med cirka ett år. Revisionen bedömer att förseningen har påverkat förutsättningarna för det lokala informationssäkerhetsarbetet, där några förvaltningar och bolag arbetat i egna spår medan andra har avvaktat.

Landstingsstyrelsen har visserligen i samband med årsrapporten för 2014, följt upp förvaltningars och bolags informationssäkerhet via ett för landstinget nytt målområde, "Säkra processer", men förseningen av compliance-verktyget har inneburit att landstingsstyrelsen på central nivå inte kunnat följa upp verksamheternas informationssäkerhet på det sätt riktlinjerna förutsätter. När verktyget väl är implementerat bör det dock, enligt revisionens bedömning, kunna ge landstingsstyrelsen stöd i detta arbete. För att säkerställa en god intern styrning och kontroll inom landstinget bör det dock tydligt framgå, i exempelvis till-

lämpningsanvisningar och/eller i planeringsprocesser, hur och när uppföljningen av status för det lokala informationssäkerhetsarbetet vid nämnder och styrelser ska ske, och hur och när resultatet från dessa uppföljningar ska återrapporteras till landstingsstyrelsen.

Landstingets nämnder och styrelser har ett eget ansvar för informationssäkerheten inom sina respektive verksamhetsområden. Landstingets decentraliserade organisation medför att informationssäkerheten därmed vilar på respektive förvaltnings eller bolags egen förmåga och resurser att driva det lokala informationssäkerhetsarbetet utifrån de centrala styrdokumenten. Granskningen visar att nämndernas och styrelsernas informationssäkerhetsarbete behöver förstärkas. Enligt enkätsvaren från informationssäkerhetssamordnarna har endast ett fåtal av nämnderna och styrelserna implementerat ett lokalt ledningssystem för informationssäkerhet. Vidare uppger endast en minoritet att organisationen klassificerat sina informationstillgångar och ett fåtal har utsett informationsägare. Detta försvårar det systematiska informationssäkerhetsarbetet för hela landstinget. Mot den bakgrunden bedömer revisionen att landstingsstyrelsen, med sitt övergripande ansvar, bör utveckla styrning och samordning av informationssäkerhetsarbetet i landstinget ytterligare.

Revisionen menar att det är viktigt att landstingsstyrelsen säkerställer att nämnder och styrelser följer de krav som ställs på informationssäkerhet även när det gäller privata utförare som anlitas för att utföra kärnverksamhet för landstingets räkning. Det saknas i dagsläget en systematik i såväl kravställande som uppföljning av dessa. Det kan leda till att skyddet av känsliga informationstillgångar äventyras i samband med informationsöverföringar mellan olika juridiska personer.

Den sammanfattande bedömningen från granskningen är att ledningssystemet för informationssäkerhet, när det är komplett och på plats, kan skapa förutsättningar för landstingsstyrelsen att ha en tillrecklig intern kontroll inom området. Granskningen visar dock att det finns en del arbete som kvarstår i implementeringen av ledningssystemet.

Rekommendationer

- Landstingsstyrelsen bör säkerställa implementeringen av ett ledningssystem för informationssäkerhet genom att snarast färdigställa arbetet med tillämpningsanvisningar samt det s.k. compliance-verktyget.

- Landstingsstyrelsen bör tydliggöra hur och när uppföljningen av status för det lokala informationssäkerhetsarbetet vid nämnder och styrelser ska ske och hur och när resultatet från dessa uppföljningar ska återrapporteras.

- Landstingsstyrelsen behöver säkerställa att nämnder och styrelser följer upp de krav som ställs på informationssäkerhet även när det gäller privata utförare som anlitas för att utföra kärnverksamhet för landstingets räkning.

2 Utgångspunkter för granskningen

2.1 Motiv till granskningen

Landstingsstyrelsen och landstingsfullmäktige 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-anpassade ledningssystem för informationssäkerhet utgörs av policy, riktlinjer och tillämpningsanvisningar. Policy och riktlinjer är fastställda medan tillämpningsanvisningarna är under utarbetning. Övriga delar i ledningssystemet för informationssäkerhet utgörs av en handlingsplan för informationssäkerhet samt ett IT-baserat verktyg för systematiskt informationssäkerhetsarbete, vilket inkluderar efterlevnadskontroll och uppföljning ("compliance-verktyg").

Den pågående implementeringen av ett ledningssystem med tillämpningsanvisningar och uppföljningssystem är en viktig förutsättning för ett systematiskt informationssäkerhetsarbete inom landstinget samt för landstingsstyrelsens uppföljning och samordning. Mot denna bakgrund har revisionen granskat om ledningssystemet ger landstingsstyrelsen förutsättningar att samordna och följa upp statusen på informationssäkerheten inom landstinget i syfte att stärka den interna kontrollen inom området. Granskningen har i första hand fokuserats på administrativ informationssäkerhet, särskilt inom områdena övergripande regelverk, organisation, metoder och kontroll.

2.2 Revisionsfråga

Den övergripande revisionsfrågan för granskningen har varit:

Ger ledningssystemet för informationssäkerhet förutsättningar för landstingsstyrelsen att säkerställa en tillräcklig styrning och intern kontroll inom området?

Den övergripande revisionsfrågan har brutits ner i följande två delfrågor:

1. Hur ger organisationen inom informationssäkerhetsområdet förutsättningar för landstingsstyrelsen att samordna, styra och följa upp informationssäkerhetsarbetet i landstinget?

2. Hur är landstingets policy och riktlinjer för informationssäkerhet harmoniserat med tillämplig standard inom området för att därigenom skapar förutsättningar för tillräcklig intern kontroll.[3]

2.3 Avgränsning

Granskningen har inriktats mot landstingsstyrelsens ansvar i informationssäkerhetsarbetet och syftar inte till att bedöma om informationssäkerheten är tillräcklig inom landstingets olika förvaltningar och bolag.

---

[1] LS 2013-03-05, LF 2013-03-19
[2] Informationssäkerhetspolicy inom Stockholms läns landsting, LS 1112 – 1733, sid 4
[3] Ledningssystem för informationssäkerhet, ISO 27001:2014.

Granskningen har översiktligt omfattat den fjärdedel av de centrala tillämpningsanvisningar som granskats av informationssäkerhetssamordnarna och som kommer att skickas på remiss inom landstingets verksamheter.

2.4 Bedömningsgrunder

- SLL:s Informationssäkerhetspolicy (fullmäktige 2013-03-19, LS 1112-1733).
- SLL:s Riktlinjer för informationssäkerhet landsting, (fullmäktige 2013-03-19, LS 1112-1733).
- Ledningssystem för informationssäkerhet - Krav, ISO/IEC 27001:2014.
- Riktlinjer för informationssäkerhetsåtgärder, ISO/IEC 27002:2014.

2.5 Metod

Granskningen har genomförts i form av dokumentstudier och intervjuer. De olika styrande dokumenten i landstingets ledningssystem för informationssäkerhet har granskats mot gällande standard inom området, ISO 27001:2014 och 27002:2014. Dessutom har revisionen granskat compliance-verktygets funktionalitet och överensstämmelse med policy och riktlinjer, samt mot gällande standarder. Revisionen har intervjuat landstingets informationssäkerhetschef, biträdande förvaltningschef samt informationssäkerhetssamordnare vid Folktandvården i Stockholm AB, Karolinska Universitetssjukhuset och Stockholms läns sjukvårdsområde (SLSO). Intervjuerna har kompletterats med en enkät till landstingets samtliga informationssäkerhetssamordnare för att ge en mer täckande bild över situationen. Svarsfrekvensen på enkäten var 87,5 procent.

3 Ledningssystem för informationssäkerhet

Landstingsstyrelsens förvaltning har tagit fram en genomförandeplan gällande implementering av ledningssystemet för informationssäkerhet. Planen är indelad i fyra faser, och ambitionen enligt landstingsstyrelsens förvaltning är att dessa faser ska införas och/eller påbörjas inom landstingets samtliga bolag och förvaltningar under år 2015 och 2016.

Enligt *informationssäkerhetspolicyn* ska landstinget bedriva ett systematiskt informationssäkerhetsarbete i syfte att skydda informationen inom verksamheten. Skyddet ska vara anpassat till skyddsvärde, risk och lagkrav för att därigenom möjliggöra för landstingets verksamheter att uppnå sina mål. Policyn gäller för landstingets samtliga nämnder, bolagsstyrelser och stiftelser. Enligt policyn gäller den även för privata utförare när de arbetar för landstinget.

Syftet med *landstingets riktlinjer för informationssäkerhet* är att konkretisera informationssäkerhetspolicyn och på ett mer handgripligt sätt beskriva hur informationssäkerhetsarbetet ska bedrivas i landstinget. Enligt policyn ansvarar landstingsstyrelsen för "...samordningen av informationssäkerhetsarbetet i landstinget", medan riktlinjerna anger att landstingsstyrelsen har ansvar för "...samordning och uppföljning av informationssäkerheten och har därmed det övergripande ansvaret för informationssäkerheten inom landstinget." Enligt intervjuer med ansvariga tjänstemän vid landstingsstyrelsens förvaltning är det den bredare ansvarsbeskrivningen i riktlinjerna som är den gällande.

Tillämpningsanvisningarna, som är under utarbetande, ska ge konkret vägledning när det gäller informationssäkerhet för alla förvaltningar och bolag. Implementeringen av tillämpningsanvisningarna har förskjutits med upp mot ett år och planeras därför ske etappvis under våren 2015 efter det att de beslutats av landstingsdirektören. För närvarande finns remissutgåvor för en fjärdedel av de anvisningar som ska tas fram. Totalt kommer det att finnas ett tjugotal tillämpningsanvisningar när arbetet är klart.

Flera informationssäkerhetssamordnare har i enkätsvar och intervjuer fört fram farhågor kring den försenade tidsplanen för beslut och implementering av tillämpningsanvisningarna. Det framförs att implementeringen av lokala system för informationssäkerhet på nämnder och styrelser har stannat upp i väntan på de centrala tillämpningsanvisningarna. En del samordnare framhåller dock att det är viktigt att tid ges för att arbeta igenom tillämpningsanvisningarna ordentligt.

Handlingsplan för informationssäkerhetsarbete i landstinget syftar till att styra landstingets övergripande informationssäkerhetsarbete på kort sikt. Enligt policyn ska det årligen fastställas en övergripande handlingsplan för informationssäkerhetsarbetet i landstinget. Det saknas dock en gällande handlingsplan för 2014. Den senaste handlingsplanen är från 2012 och gäller för åren 2012 och 2013.

En väsentlig byggsten i landstingets ledningssystem för informationssäkerhet utgörs av ett så kallat *compliance-verktyg.* Det är ett IT-baserat och behörighetsstyrt system för uppföljning och kontroll av informationssäkerhetsarbetet, centralt såväl som lokalt inom landstinget. Kraven i centrala och lokala styrdokument läggs in i systemet som kravkataloger och systemet ger stöd för handlingsplan, avvikelseanalys och uppföljning genom indikatorer. Stöd ges även för riskbedömning och informationsklassificering. Verktyget har utvecklats i två versioner, ett för internt bruk inom landstinget och ett för externt bruk, för uppföljning av till exempel upphandlade entreprenörer liksom vid nya upphandlingar. Det senare har ännu inte driftsatts. Landstingets förvaltningar och bolag kommer, enligt uppgift, att börja använda verktyget under våren 2015.

Merparten av landstingets informationssäkerhetssamordnare anser, enligt enkät och intervjusvar, att landstinget har relevanta och samstämmiga centrala styrdokument inom informationssäkerhetsområdet. Utifrån genomförda intervjuer och av revisionens egna iakttagelser framkommer det dock att rollerna som anges i landstingets förvaltningsstyrningsmodell och som baseras på pm3[4] inte är harmonierade med rollerna som anges i de centrala styrdokumenten för informationssäkerhet. Som exempel kan nämnas att begreppet informationsägare inte finns i landstingets nya förvaltningsstyrningsmodell, vilket innebär risk för att rollen inte får legitimitet och att arbetet inom informationssäkerhetsområdet därigenom kan försvåras..

[4] pm3 är en förvaltningsstyrningsmodell vars syfte är att organisera förvaltningsverksamhet så att den kan bedrivas på ett affärsmässigt sätt. Med hjälp av pm3 fastställs bland annat beslutsmandat, beslutsfora, ansvarsroller samt prioriterings- och uppföljningsprinciper.

3.1 Revisionens bedömning

Implementeringen av ledningssystemet för informationssäkerhet inom landstinget har försenats med cirka ett år. Bedömningen är dock att när det är komplett och på plats, kan det skapa förutsättningar för landstingsstyrelsen att ha en god intern kontroll inom området. Revisionen vill emellertid betona vikten av att tillämpningsanvisningarna inte försenas ytterligare då det påverkar förutsättningarna för både det lokala informationssäkerhetsarbetet och för landstingsstyrelsen att på central nivå följa upp informationssäkerheten vid landstingets nämnder och styrelser.

Revisionen noterar vidare att landstingsstyrelsen snarast behöver besluta om en aktualiserad handlingsplan för informationssäkerhet.

Revisionen menar att landstingets ansvar för informationssäkerhet behöver förtydligas i landstingets förvaltningsstyrningsmodell baserad på pm3. När det exempelvis gäller samstämmighet mellan roller och ansvar i de styrande dokumenten visavi landstingets nuvarande förvaltningsstyrningsmodell, menar revisionen att det är viktigt att en harmonisering mellan förvaltningsstyrningsmodellen och de styrande dokumenten inom informationssäkerhetsområdet sker skyndsamt för att minska risken för begreppsförvirring och för att inte minska legitimitet i ansvar och roller inom informationssäkerhetsområdet.

4 Överensstämmelse mellan gällande standard och landstingets policy och riktlinjer

Revisionen har granskat hur landstingets policy och riktlinjer för informationssäkerhet harmoniserar med tillämplig standard inom området och därigenom skapar förutsättningar för intern kontroll. Den internationella standarden för informationssäkerhet benämns ISO 27000-serien. Standardens olika delar syftar till att ge förutsättningar för ett systematiskt och effektivt arbetssätt för organisationer som strävar efter förbättrad intern kontroll och styrning av informationssäkerheten. Standarden har två inledande delar, ISO 27001 samt ISO 27002, båda reviderade 2013 och utgivna i svensk översättning 2014. Den första delen anger de krav verksamheter bör följa för att införa, underhålla och förbättra ett ledningssystem för informationssäkerhet och den andra ger vägledning när kraven ska införas.

Landstingsfullmäktige har, i enlighet med standarden, som högsta ledning i landstinget, beslutat om en informationssäkerhetspolicy för att beskriva organisationens syn på sina mål för informationssäkerheten. Enligt standarden bör informationssäkerhetspolicyn innehålla uppgifter om:

a) definition av informationssäkerhet samt mål och principer som styr all verksamhet som är relaterad till informationssäkerhet
b) tilldelning till definierade roller och av allmänna och särskilda ansvar för hantering av informationssäkerhet
c) processer för att hantera avvikelser och undantag

Granskningen visar att landstingets policy och/eller riktlinjer hanterar punkterna ovan.

Enligt COSO-modellen[5] definieras intern kontroll som en övergripande process där organisationens ägare, ledning och personal samverkar i syfte att uppnå:

- ändamålsenlig och kostnadseffektiv verksamhet
- tillförlitlig rapportering och information om verksamheten
- efterlevnad av tillämpliga lagar, föreskrifter, riktlinjer

ISO-standarden för informationssäkerhet har en likartad uppbyggnad, struktur och syfte som COSO-modellen. Granskningen visar att landstingets policy och riktlinjer för informationssäkerhet har samma struktur och huvudsakliga innehåll som den vägledande ISO-standarden. Standarden nämns också som utgångspunkt för landstingets arbete i de fastställda riktlinjerna[6]. I enlighet med standarden anger policyn att informationssäkerhet ingår som en viktig del i landstingets övergripande arbete med intern styrning och kontroll samt riskhantering. I de styrande dokumenten beskrivs roller och ansvar för informationssäkerheten inom landstingets verksamheter. Vikten av att styra och följa upp externa leverantörers informationssäkerhet beskrivs i de styrande dokumenten i enlighet med standarden.

Det enda område där det råder viss otydlighet i kopplingen mot standardens krav gäller kontroll av efterlevnad av juridiska och avtalsmässiga krav, teknisk efterlevnad samt kontroll av externa leverantörer. Landstingets styrande dokument innehåller för detta område övergripande information om vad som gäller för efterlevnad på central nivå och förvaltningarnas och bolagens ansvar för uppgifterna, men det framgår inte hur dessa krav rent faktiskt ska hanteras på lokal nivå. Av intervjuerna med landstingsstyrelsens förvaltning framkom att det i nuläget inte är planerat att ta fram någon särskild tillämpningsanvisning för hur efterlevnaden av dessa tre områdena ska genomföras.

Den styrande dokumentationen för landstinget är fastställd under våren 2013 och därmed inte fullt ut anpassad till senaste utgåvan av standarden som har reviderats något med bland annat vägledningstexter. Under intervjuerna med landstingsstyrelsens förvaltning framkom att policy och riktlinjer kommer att revideras under våren 2015 och därefter föreslås fastställas på nytt av landstingsfullmäktige respektive av landstingsstyrelsen för att informationen i dessa ska motsvara förändringarna i standarden.

4.1 Revisionens bedömning

Granskningen visar att landstingets styrdokument och arbete med informationssäkerhet är förankrat i standarden för informationssäkerhet liksom COSO-ramverket för intern styrning och kontroll. Mot denna bakgrund bedömer revisionen att ledningssystemet skapar förutsättningar för landstingsstyrelsen att ha en god intern kontroll inom området. Det finns emellertid behov att utveckla tillämpningsanvisningar för de områden där det ställs tydliga krav i standarden

[5] COSO (*Committee of Sponsoring Organizations of the Treadway Commission*).är ett ramverk för att utvärdera ett företags interna kontroll. Beskrivningen av COSO modellen kommer från: PwC (Anders Haglund, Jan Sturesson och Roland Svensson), 2005: Intern kontroll – En del av verksamhets- och ekonomistyrningen

[6] SLL:s Riktlinjer för informationssäkerhet landsting, (fullmäktige 2013-03-19, LS 1112-1733), sid 2

men där det i dagsläget inte är tydligt hur styrning och uppföljning av efterlevnad på lokal nivå bör ske. I det pågående arbetet med att ta fram tillämpningsanvisningar bör landstingsstyrelsen säkerställa att efterlevnadskraven för dessa områden täcks in i någon tillämpningsanvisning.

5 Organisation, roller och ansvar

Landstinget har ett decentraliserat ansvar för informationssäkerhetsarbetet. Nedan beskrivs de olika funktionerna inom landstinget som har ett direkt ansvar inom informationssäkerhetsområdet, samt deras viktigaste ansvarsområden.

Enligt landstingets *reglemente för styrelser och nämnder* från december 2014[7] åligger det landstingsstyrelsen "...att ansvara för landstingets samordnade IT-verksamhet och övergripande frågor om informationssäkerhet..." Det innebär en förändring jämfört med tidigare gällande reglemente, som inte innehöll någon skrivning om landstingsstyrelsens ansvar inom informationssäkerhetsområdet.

För att säkerställa uppföljning inom informationssäkerhetsområdet har landstingsfullmäktige beslutat om ett nytt målområde med en övergripande indikator från och med 2014. Målområdet benämns "Säkra processer – Säkerhetsarbetet ska bedrivas på ett systematiskt sätt" och indikatorn är definierad till "Andel av landstingets förvaltningar och bolag som infört metoder och verktyg för systematiskt arbete". Indikatorn är nedbruten i två delar, dels informationssäkerhet, dels säkerhet. Således är indikatorn direkt kopplad till arbetet med införandet av ledningssystemet för informationssäkerhet och framskridandet kommer att följas upp årligen.

Av policyn framkommer att *landstingsfullmäktige* beslutar om informationssäkerhetspolicyn och att *landstingsstyrelsen* har ansvar för att policy likväl som riktlinjer för informationssäkerhet utarbetas och hålls aktuella. Vidare fastställer policyn att *landstingsstyrelsen* dels har ansvar för samordningen av informationssäkerhetsarbetet i landstinget, dels att årligen fastställa en övergripande handlingsplan för informationssäkerhetsarbetet. Som framgår tidigare i rapporten så är den senaste handlingsplanen från 2012.

Landstingsdirektören har styrelsens uppdrag att sörja för att informationssäkerhetsarbetet bedrivs så effektivt som möjligt. Enligt policyn har landstingsdirektören även ansvaret för att övergripande tillämpningsanvisningar inom området utarbetas och hålls aktuella i enlighet med policy och riktlinjer. Som framgått ovan så finns det ännu inte några beslutade landstingsövergripande tillämpningsanvisningar för landstinget.

Inom landstingsstyrelsens förvaltning har *informationssäkerhetschefen* det operativa ansvaret för att förvalta landstingets ledningssystem för informationssäkerhet. Informationssäkerhetschefens arbete omfattar därmed informations-

[7] Stockholms läns landsting, Arbetsordningar, reglementen och delegationsordning, december 2014

säkerhetsfrågor på en övergripande och strategisk nivå för hela landstinget. I ansvaret ingår omvärldsbevakning, samordning, att vara sammankallande i landstingets informationssäkerhetsråd samt att inhämta information om och rapportera informationssäkerhetsläget i landstinget som ett led i uppföljningen av informationssäkerheten. Informationssäkerhetschefen samverkar och leder arbetet på lokal nivå genom Informationssäkerhetsrådet (ISR).

Varje *nämnd och styrelse* har, enligt policyn, ansvar för informationssäkerheten inom sina respektive verksamhetsområden. Det åligger även varje nämnd och styrelse att årligen planlägga och löpande följa upp informationssäkerheten och i övrigt vidta de åtgärder som krävs för att uppnå och upprätthålla tillräcklig intern kontroll. Enligt landstingets informationssäkerhetspolicy ska varje nämnd och styrelse ta fram egna, verksamhetsnära styrdokument för informationssäkerhet som utgår från de centrala styrdokumenten. Av enkätsvaren framkommer det att endast ett fåtal av landstingets verksamheter har lokala styrdokument på plats. Vissa av dessa anger som skäl att de centrala tillämpningsanvisningarna inväntas innan man avser att slutföra arbetet med att ta fram egna styrdokument.

Enligt riktlinjerna ska informationstillgångar klassificeras och informationsägare utses vid landstingets förvaltningar och bolag. Ungefär en tredjedel av samordnarna uppger i enkäten att det inte har utsetts några informationsägare vid deras bolag och/eller förvaltningar, medan en tredjedel uppger att så delvis har skett. Viktiga informationstillgångar klassificeras sällan utifrån informationsägarnas krav, det är enbart två som svarar att så sker fullt ut. Orsaken är enligt de intervjuade att informationsägare inte har blivit utsedda, eller att de utsedda informationsägarna sällan känner till vilket ansvar som ligger i rollen. Det framkommer även av intervjuerna att det råder en osäkerhet kring huruvida en beslutad informationsklassning ska följa med i de fall som informationen lämnas över till, eller tas emot från en annan organisatorisk enhet.

Policyn gäller för samtliga privata utförare som arbetar på uppdrag av landstingets förvaltningar och bolag. Detta ska, enligt policyn, regleras genom avtal med respektive leverantör. I enkätsvaren anger 65 procent av de tillfrågade samordnarna att det inte framkommer, alternativt endast framkommer i ett fåtal av verksamheternas avtal med de privata utförarna, att policyn även gäller dem. För en av verksamheterna anges att det framkommer i samtliga avtal. Drygt 60 procent svarar att bolagen och förvaltningarna inte genomför uppföljning av om leverantörerna följer landstingets informationssäkerhetspolicy. Några gör det för ett fåtal leverantörer men ingen gör det för samtliga avtal. Ingen av de tillfrågade känner till något fall där landstinget från centralt håll genomfört någon uppföljning av hur bolag och förvaltningar följer upp gentemot leverantörerna.

Varje förvaltning och bolag ska utse en *informationssäkerhetssamordnare* som ska ansvara för att samordna och följa upp respektive organisations informationssäkerhetsarbete. Granskningen visar att det är stora skillnader i hur långt landstingets nämnder och styrelser har kommit i sitt lokala informationssäkerhetsarbete beroende på skiftande lokala förutsättningar. Av enkätsvaren framkommer att en majoritet av de tillfrågade anser sig ha en tillräcklig kompetens och erfarenhet för att sköta sina arbetsuppgifter inom informationssäkerhetsom-

rådet lokalt ute på bolag och förvaltningar. Samtidigt menar nästan hälften av de tillfrågade att de saknar tillräckligt mandat och/eller resurser för att sköta sitt arbete inom området i önskvärd grad.

Av enkätsvaren framkommer att ingen av informationssamordnarna uppfattar landstingets informationssäkerhetsorganisation som otydlig. En femtedel anser dock att det inte är tydligt hur informationssäkerheten styrs inom landstinget. Cirka 70 procent anser att samordning och samverkan är tillräcklig inom området, och 30 procent anser den otillräcklig. Flera av de intervjuade menar att landstingets IT-leverantörer, såväl externa som den interna leverantören SLL IT, behöver involveras mer i informationssäkerhetsarbetet. Detta gäller till exempel säkerhetsaspekter kopplad till teknisk drift och teknisk förvaltning av system.

Informationssäkerhetsrådet (ISR) består av informationssäkerhetssamordnarna från landstingets förvaltningar och bolag. Rådets uppgift är, enligt policyn, att främja, stödja samordna och följa upp landstingets informationssäkerhetsarbete på ett övergripande plan. Samtliga informationssäkerhetssamordnare som svarat på enkäten uppger att de deltar regelbundet på informationssäkerhetsrådets möten. De flesta anser även att det som avhandlas på mötena är adekvat. Flera menar dock att det finns betydande skillnader vad gäller förutsättningarna, framförallt vad gäller tid, för de olika informationssäkerhetssamordnarna att bedriva informationssäkerhetsarbete i de egna verksamheterna. Detta leder till skillnader i engagemang och påverkar mötenas kvalitet. Det framförs även att mötena har lite för mycket karaktären av informationsmöte, vilket går ut över dialogen mellan deltagarna. Hälften anser att mötena, bland annat av tidsbrist, inte berör viktiga frågeställningar som till exempel infrastrukturfrågor, säker kommunikation (krypterad e-post) och säkra molntjänster.

5.1 Revisionens bedömning

Revisionen bedömer att de styrande dokumenten i ledningssystemet, policy och riktlinjer för informationssäkerhet, ger en tydlig och övergripande beskrivning av roller och organisatoriskt ansvar för informationssäkerheten i landstinget, såväl centralt som lokalt, i enlighet med den gällande standarden inom området. Det kvarstår emellertid en del arbete för att ledningssystemet ska kunna anses vara implementerat fullt ut. Behov finns bland annat av att landstingsstyrelsen tydliggör hur uppföljning ska ske på lokal och från central nivå. I arbetet med att utveckla tillämpningsanvisningar bör även beaktas hur den tekniska informationssäkerheten ska hanteras, likväl som hur landstingets IT-leverantörer ska involveras mer systematiskt i informationssäkerhetsarbetet.

Landstingets nämnder och styrelser har ett eget ansvar för informationssäkerheten inom sina respektive verksamhetsområden. Granskningen visar att nämndernas och styrelsernas informationssäkerhetsarbete behöver förstärkas. Enligt enkätsvaren från informationssäkerhetssamordnarna har endast ett fåtal av nämnderna och styrelserna implementerat ett lokalt ledningssystem för informationssäkerhet. Vidare uppger endast en minoritet att organisationen klassificerat sina informationstillgångar och ett fåtal har utsett informationsägare. Detta försvårar det systematiska informationssäkerhetsarbetet för hela landstinget. Mot den bakgrunden bedömer revisionen att landstingsstyrelsen, med

sitt övergripande ansvar, bör stärka styrningen och samordningen av informationssäkerhetsarbetet i landstinget ytterligare.

Revisionen menar att det är viktigt att landstingsstyrelsen säkerställer att landstingets informationssäkerhetskrav även följs av de privata utförare som anlitas för att utföra kärnverksamhet för landstingets räkning. Det saknas i dagsläget en systematik i såväl kravställande som uppföljning av dessa. Det kan leda till att skyddet av känsliga informationstillgångar äventyras i samband med informationsöverföringar mellan olika juridiska personer.

Landstingets decentraliserade organisation medför att stort ansvar vilar på respektive förvaltnings eller bolags egen förmåga och resurser att driva det lokala informationssäkerhetsarbetet utifrån de centrala styrdokumenten.

6 Uppföljning med hjälp av compliance-verktyget

I både COSO-modellen för intern kontroll och i ISO-standarden för informationssäkerhet är uppföljning av efterlevnad en viktig komponent. Revisionen har granskat det IT-baserade compliance-verktyget som finns framtaget men som ännu inte är implementerat fullt ut. Det är tänkt att utgöra det huvudsakliga stödet för landstingsstyrelsen att styra och följa upp informationssäkerhetsarbetet på lokal nivå i landstingets verksamheter, men även för övriga nämnder och styrelser att följa upp det egna arbetet på lokal nivå. Granskningen har genomförts i syfte att se om verktyget kan ge landstingsstyrelsen tillräckliga förutsättningar för att följa upp nämndernas och styrelsernas lokala informationssäkerhetsarbete i enlighet med landstingsstyrelsens uppföljningsansvar inom området.

Compliance-verktyget är uppbyggt kring deklarationer/självvärderingar i form av mätpunkter/frågor som har sin förankring i landstingets policy och riktlinjer för informationssäkerhet. Syftet är att är frågorna ska besvaras av alla förvaltningar och bolag med stöd av respektive informationssäkerhetssamordnare. De svar som genereras ska sedan ge landstinget centralt en bild av statusen på det lokala informationssäkerhetsarbete som bedrivs vid landstingets förvaltningar och bolag.

De båda ISO-standarderna, 27001 och 27002, innehåller en stor mängd detaljerade krav på informationssäkerhet och det finns en ännu större mängd möjliga sätt att implementera och beskriva hur dessa krav har hanterats i en viss verksamhet. Syftet med compliance-verktyget är att underlätta för och strukturera kravställning liksom inrapportering och bearbetning av verksamheternas lokala informationssäkerhetsarbete på central landstingsnivå.

Revisionens genomgång av verktyget har motsvarat den genomgång som respektive förvaltning och bolag ska genomföra under 2015. Frågeställningarna, d.v.s. mätpunkterna, är bland annat fokuserade på lokala policyer och riktlinjer samt på om handlingsplaner är framtagna för informationssäkerhetsarbetet vid respektive förvaltning och bolag. I verktyget finns även stöd för respektive förvaltning eller bolag att genomföra och dokumentera riskbedömningar utifrån

identifierade avvikelser, och på så vis ge underlag för det egna förbättringsarbetet.

Av genomförda intervjuer med landstingsstyrelsens förvaltning framgår att målsättningen med verktyget är att det ska vara högsta ledningen för landstingets verktyg för systematiskt informationssäkerhetsarbete, d.v.s. utgöra ett stöd för uppföljning om landstinget, dess bolag och förvaltningar eller delar av dessa har tillfredställande system och rutiner för uppföljning och kontroll av informationssäkerheten. Målsättningen är även att det ska vara ett stöd för nämnder och styrelser att styra och följa upp den egna verksamheten gällande informationssäkerhet.

Målsättningen på sikt är, enligt intervjuerna, även att landstinget ska kunna använda compliance-verktyget som underlag till kravspecifikation vid upphandling av externa resurser och utförare.

Genomgången av verktyget har visat att dess struktur och uppbyggnad motsvarar innehållet i landstingets riktlinjer och policy för informationssäkerhet. De översiktliga testerna har också visat att det med hjälp av verktyget är möjligt att kvalitetssäkra och jämföra information från olika förvaltningar och bolag på ett överskådligt sätt. Under intervjuerna framkom det dock att det ännu inte finns någon dokumenterad beskrivning av hur själva uppgiften att bearbeta, värdera och återkoppla resultat till landstingsstyrelsen, likväl som tillbaka till nämnder och styrelser, ska bedrivas. Av genomförda intervjuer framgår det att detta arbete åtminstone till en början kommer att ske under ledning av landstingets informationssäkerhetschef.

6.1 Revisionens bedömning

Det compliance-verktyg som tagits fram och håller på att implementeras kommer enligt revisionens bedömning kunna ge landstingsstyrelsen stöd i att styra och följa upp det lokala informationssäkerhetsarbetet vid landstingets nämnder och styrelser. Compliance-verktyget bedöms ge förutsättningar för att underlätta insamling och bearbetning av verksamheternas informationssäkerhetsarbete och därmed skapa förutsättningar för ett strukturerat förbättringsarbete och en förbättrad intern kontroll av statusen på landstingets informationssäkerhet via indikatorer. Fortsatta utbildningsinsatser och stöd gällande implementering av verktyget bedöms vara framgångsfaktorer i detta sammanhang.

För att säkerställa att landstingsstyrelsen ska kunna ha en god intern kontroll inom området är det dock viktigt att landstingsstyrelsen ser till att arbetet med uppföljning på central nivå formaliseras så att det framgår hur och när uppföljningen av status för det lokala informationssäkerhetsarbetet vid nämnder och styrelser ska ske och hur och när resultatet från uppföljningen ska förmedlas till landstingsstyrelsen.

Sammanställnings- och analysarbetet, liksom arbetet med implementering och förvaltning av ledningssystemet i stort, bedöms vara omfattande och tidskrävande, och revisionen bedömer att det i dagsläget oklart om det finns tillräckliga resurser på central nivå att administrera denna uppgift över tid. Det bedöms även vara oklart om det finns förutsättningar att tillhandahålla tillräckligt

centralt stöd för informationssäkerhetssamordnarna, både vad gäller verktyget och allmänt stöd gällande ledningssystemet i sig.

Kort om rapporten

Revisionen har granskat styrning och samordning av informationssäkerhetsarbetet i landstinget utifrån landstingsstyrelsens övergripande ansvar. Den sammanfattande bedömningen från granskningen är att landstingets ledningssystem för informationssäkerhet, när det är komplett och på plats, kan skapa förutsättningar för landstingsstyrelsen att ha en tillräcklig intern kontroll inom området. Granskningen visar dock att införandet av ledningssystemet har försenats och att det finns en del arbete som kvarstår inför 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 **Fax:** 08-737 53 50
E-post: landstingsrevisorerna@rev.sll.se **Hemsida:** www.sll.se/rev

Org.nr: 232100-0016