REGIONREVISORERNA

RAPPORT NR 3/2020

IT-säkerhet i nätverksanslu-ten medicinteknisk utrust-ning

Region Stockholm

Regionrevisorerna

2020-11-26

Diarienummer
RK 2019-0082

Regionstyrelsen

Projektrapport 3/2020 IT-säkerhet i nätverksansluten medicinteknisk utrustning

Revisorerna i revisionsgrupp I beslutade vid sitt möte 2020-11-26 att överlämna rapporten till regionstyrelsen för yttrande senast 2021-03-16.

Revisorernas samlade bedömning är att regionstyrelsen har genomfört åtgärder för att stärka styrningen, kraven och ansvarsfördelningen kring IT-säkerhet för nätverksansluten medicinteknisk utrustning sedan revisionens förra granskning 2014. Trots detta kvarstår flera rekommendationer från 2014 och nya lämnas i och med denna granskning. Det är till exempel osäkert om nätverksansluten medicinteknisk utrustning, som sjukhusen har upphandlat och konfigurerat med avsteg från regionens gällande riktlinjer, upprätthåller en tillräcklig IT-säkerhetsnivå. Revisorerna anser också att uppföljningen av hur nämnder eller styrelser arbetar i praktiken kan förbättras.

Revisorerna vill särskilt ha regionstyrelsens svar på

- hur regionstyrelsen ska säkerställa att nätverksansluten medicinteknisk utrustning, som nämnder och bolag har konfigurerat med avsteg från regionens gällande riktlinjer, upprätthåller en tillräcklig IT-säkerhetsnivå.
- hur regionstyrelsen ska stärka uppföljningen av hur nämnder och bolag arbetar med IT-säkerhet kopplat till nätverksansluten medicinteknisk utrustning.
- hur regionstyrelsen säkerställer att krav i styrdokument och arbetssätt i regionen ökar antalet samordnade upphandlingar av medicinteknisk utrustning.

I övrigt hänvisar revisorerna till revisionskontorets rapport.

Paragrafen justeras omedelbart.

Kenneth Strömberg
ordförande

Anette Carlstedt
sekreterare

Region Stockholm
Regionrevisorerna
Box 22230
104 22 Stockholm

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

Säte: Stockholm
Org.nr: 232100-0016
www.sll.se

Besök oss: Hantverkargatan 25B, T-bana Rådhuset, se www.sl.se

Regionrevisorerna

2020-11-26

Diarienummer
RK 2019-0082

Nämnden för
Karolinska universitetssjukhuset

Projektrapport 3/2020 IT-säkerhet i nätverksansluten medicinteknisk utrustning

Revisorerna i revisionsgrupp II beslutade vid sitt möte 2020-11-26 att överlämna rapporten till nämnden för Karolinska universitetssjukhuset för kännedom och möjlighet till yttrande senast 2021-03-16.

Revisorernas samlade bedömning är att regionstyrelsen har genomfört åtgärder för att stärka styrningen, kraven och ansvarsfördelningen kring IT-säkerhet för nätverksansluten medicinteknisk utrustning sedan revisionens förra granskning 2014. Trots detta kvarstår flera rekommendationer från 2014 och nya lämnas i och med denna granskning. Det är till exempel osäkert om nätverksansluten medicinteknisk utrustning, som sjukhusen har upphandlat och konfigurerat med avsteg från regionens gällande riktlinjer, upprätthåller en tillräcklig IT-säkerhetsnivå. Revisorerna anser också att uppföljningen av hur nämnder eller styrelser arbetar i praktiken kan förbättras.

Revisorerna vill betona vikten av att Karolinska universitetssjukhuset aktivt samarbetar med SF IT i egenskap av driftsoperatör för att säkerställa sjukhusets säkerhet i nätverksansluten medicinteknisk utrustning.

I övrigt hänvisar revisorerna till revisionskontorets rapport.

Paragrafen justeras omedelbart.

Hans-Erik Salomonsson
Ordförande

Christina Holmqvist
Sekreterare

Region Stockholm
Regionrevisorerna
Box 22230
104 22 Stockholm

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

Säte: Stockholm
Org.nr: 232100-0016
www.sll.se

Besök oss: Hantverkargatan 25B, T-bana Rådhuset, se www.sl.se

Regionrevisorerna

2020-11-26

Diarienummer
RK 2019-0082

Styrelsen
Danderyds Sjukhus AB

Projektrapport 3/2020 IT-säkerhet i nätverksansluten medicinteknisk utrustning

Revisorerna i revisionsgrupp II beslutade vid sitt möte 2020-11-26 att överlämna rapporten till styrelsen för Danderyds Sjukhus AB för kännedom och möjlighet till yttrande senast 2021-03-16.

Revisorernas samlade bedömning är att regionstyrelsen har genomfört åtgärder för att stärka styrningen, kraven och ansvarsfördelningen kring IT-säkerhet för nätverksansluten medicinteknisk utrustning sedan revisionens förra granskning 2014. Trots detta kvarstår flera rekommendationer från 2014 och nya lämnas i och med denna granskning. Det är till exempel osäkert om nätverksansluten medicinteknisk utrustning, som sjukhusen har upphandlat och konfigurerat med avsteg från regionens gällande riktlinjer, upprätthåller en tillräcklig IT-säkerhetsnivå. Revisorerna anser också att uppföljningen av hur nämnder eller styrelser arbetar i praktiken kan förbättras.

Revisorerna vill betona vikten av att Danderyds Sjukhus AB aktivt samarbetar med SF IT i egenskap av driftsoperatör för att säkerställa sjukhusets säkerhet i nätverksansluten medicinteknisk utrustning.

I övrigt hänvisar revisorerna till revisionskontorets rapport.

Paragrafen justeras omedelbart.

Hans-Erik Salomonsson
ordförande

Christina Holmqvist
sekreterare

Region Stockholm
Regionrevisorerna
Box 22230
104 22 Stockholm

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

Säte: Stockholm
Org.nr: 232100-0016
www.sll.se

Besök oss: Hantverkargatan 25B, T-bana Rådhuset, se www.sl.se

Regionrevisorerna

2020-11-26

Diarienummer
RK 2019-0082

Fastighets- och servicenämnden

Projektrapport 3/2020
IT-säkerhet i nätverksansluten medicinteknisk utrustning

Revisorerna i revisorsgrupp III beslutade vid sitt möte 2020-11-26 att överlämna rapporten till fastighets- och servicenämnden för kännedom med möjlighet till yttrande senast 2021-03-16.

Revisorerna samlade bedömningen är att regionstyrelsen har genomfört åtgärder för att stärka styrningen, kraven och ansvarsfördelningen kring IT-säkerhet för nätverksansluten medicinteknisk utrustning sedan revisionens förra granskning 2014. Trots detta kvarstår flera rekommendationer från 2014 och nya lämnas i och med denna granskning. Det är till exempel osäkert om nätverksansluten medicinteknisk utrustning, som sjukhusen har upphandlat och konfigurerat med avsteg från regionens gällande riktlinjer, upprätthåller en tillräcklig IT-säkerhetsnivå. Revisorerna anser också att uppföljningen av hur nämnder eller styrelser arbetar i praktiken kan förbättras.

Revisorerna vill betona vikten av att SF IT aktivt samarbetar med regionens sjukhus i egenskap av driftsoperatör för att säkerställa sjukhusens säkerhet i nätverksansluten medicinteknisk utrustning.

I övrigt hänvisar revisorerna till revisionskontorets rapport.

Paragrafen justeras omedelbart.

Anders Lönn
ordförande

Christina Holmqvist
sekreterare

Region Stockholm
Regionrevisorerna
Box 22230
104 22 Stockholm

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

Säte: Stockholm
Org.nr: 232100-0016
www.sll.se

Besök oss: Hantverkargatan 25B, T-bana Rådhuset, se www.sl.se

Kort om rapporten

Medicinteknisk utrustning fyller en viktig funktion för att diagnostisera, behandla och lindra sjukdomar och skador. Nätverksansluten medicinteknisk utrustning integreras därför allt mer i arbetsprocesser och utgör en betydande del av de ekonomiska investeringarna inom hälso- och sjukvården. För att kunna ta tillvara de möjligheter som digitaliserad medicinteknisk utrustning ger, och samtidigt hantera risker som följer med uppkopplade enheter, rekommenderar revisionen regionstyrelsen att säkerställa att nätverksansluten medicinteknisk utrustning som har upphandlats och konfigurerats med avsteg från regionens gällande riktlinjer upprätthåller en tillräcklig it-säkerhetsnivå. Vidar bör regionstyelsen stärka uppföljningen av hur nämnder och bolag arbetar med it-säkerhet kopplat till nätverksansluten medicinteknisk utrustning.

1 Slutsatser och rekommendationer

Revisionen har låtit granska om regionen har tillräcklig styrning och intern kontroll för att motverka störningar som kan hota driftsäkerheten för medicinteknisk utrustning (MTU). Granskningen avser regionstyrelsen, fastighets- och servicenämnden (SF IT), styrelsen för Danderyd sjukhus samt nämnden för Karolinska universitetssjukhuset.

Granskningen har, under ledning av revisionskontoret, genomförts av konsult. Ansvarig projektledare vid revisionskontoret har varit Inger Sohlberg. Ansvarig konsult har varit Louise Tornhagen, PwC. Revisionen har nedan sammanfattat de slutsatser som kan dras och lämnar rekommendationer med anledning av granskningen. Konsultens iakttagelser och bedömningar framgår i bilaga.

Inledning

Medicinteknisk utrustning så som bildsystem, pacemakers, respiratorer m.m. fyller en viktig funktion för att diagnostisera, behandla och lindra sjukdomar och skador. MTU utgör en betydande del av de ekonomiska investeringarna inom hälso- och sjukvården. När MTU kopplas upp på nätverk och integreras med olika it-system uppkommer risker för intrång som kan medföra höga kostnader och orsaka patientrisker då utrustningen i vissa fall är livsuppehållande.

Revisionens samlade bedömning är att regionstyrelsen har genomfört åtgärder för att stärka styrningen, kraven och ansvarsfördelningen kring it-säkerhet för MTU, men att uppföljningen av hur nämnder eller styrelser i praktiken arbetar med detta inte är tillräcklig. Regionstyrelsen bör också försäkra sig om att nätverksansluten MTU, som sjukhusen har upphandlat och konfigurerat med avsteg från regionens gällande riktlinjer, upprätthåller en tillräcklig it-säkerhetsnivå.Samverkan mellan nätverksleverantören SF IT och akutsjukhusens medicintekniska avdelningar kan dessutom stärkas ytterligare, framför allt när det gäller upphandling och riskhanteringsarbetet.

Revisionen genomförde 2014 en liknande granskning.[1] Då framkom att ansvarsfördelningen mellan regionstyrelsens centrala it-funktion och akutsjukhusen var otydlig avseende it-säkerhet i nätverksansluten MTU. Granskningen visade att det fanns ett behov av att tydliggöra roller och ansvar på både central och lokal nivå och att den centrala styrningen behövde öka. Vidare bedömde revisionen att regelverket för it-säkerhet borde kompletteras med specifika krav för MTU och att det i samordnade underlag för gemensamma upphandlingar borde tydliggöras krav på it-säkerhet. Revisionen

[1] IT-säkerhet i nätverksansluten medicinteknisk utrustning, Rapport 2 2014.

konstaterar att rekommendationerna från 2014, trots vidtagna åtgärder, till stor del fortfarande är aktuella.[2]

Ansvarsfördelning och samverkan

Regionen har ett decentraliserat ansvar för it- och informationssäkerhet. Det innebär att respektive nämnd eller bolag är ansvarig för att hantera it-säkerheten av nätverksansluten MTU medan SF IT i sin roll som nätverksleverantör för daglig drift av nätverk levererar lösningar till sjukhusen. För nätverksansluten MTU är det därför väsentligt att det finns en tydlig ansvarsfördelning och fungerande samarbete mellan sjukhusens MT-avdelningar, SF IT och vårdverksamheten som kravställare på och användare av MTU och samtliga leverantörer av uppkopplad MTU. Otydliga ansvarsförhållanden eller avsaknad av väl fungerande samarbete ökar risken för incidenter som kan orsaka störningar inom vården.

Granskningen visar att regionstyrelsen sedan revisionens förra granskning 2014 har stärkt den centrala styrningen och ansvarsfördelningen av it-säkerhet för nätverksansluten MTU. Ett ledningssystem har implementerat för att tydliggöra ansvar, roller och gemensamma arbetssätt för informationssäkerhet. Därmed finns nu också utsedda informationssäkerhetssamordnare på samtliga bolag och förvaltningar.

Granskningen visar också att ansvarsfördelningen mellan SF IT och akutsjukhusens MT-avdelningar har tydliggjorts sedan 2014, med bl.a. tjänsteöverenskommelser och gränsdragningslistor. Trots dessa åtgärder är det revisionens bedömning att samverkan mellan SF IT och akutsjukhusens MT-avdelningar behöver utvecklas ytterligare och ske mer formaliserat och regelbundet. Samverkan bör i större utsträckning inkludera förebyggande aktiviteter. Exempelvis behöver MTU-upphandlingar som görs av respektive nämnd eller bolag på ett tydligare sätt involvera expertkunskap från SF IT för att stärka säkerheten i nätverksansluten MTU. Revisionen anser även att SF IT behöver ha en komplett bild över vilken medicinteknisk utrustning som är nätverksansluten för respektive bolag eller nämnd. Har inte SF IT en komplett bild av all utrustning försvåras deras möjligheter att förebygga och åtgärda problem eftersom liknande problem kan uppstå på andra sjukhus. Att SF IT har en samlad kunskap om befintlig utrustning har också ett värde inför framtida upphandlingar.

---

[2] Det gäller rekommendationerna 33533 – Regionstyrelsen bör säkerställa dels att krav i styrdokument och arbetssätt i regionen ökar antalet samordnade upphandlingar av MTU, 29097 - Regionstyrelsen bör stärka och tydliggöra ansvaret för IT-säkerhet kopplat till MTU på övergripande nivå och tydliggöra hur den organisatoriska samverkan mellan SF IT och akutsukhusens MT-avdelningar ska ske vad gäller säkerhetskrav samt 29096 - Regionsstyrelsen bör komplettera regelverket för informationssäkerhet med specifika krav för nätverksansluten MTU så att stöd finns för praktisk tillämpning i verksamheten för exempelvis anslutningsprocesser, uppdateringar och styrning av fjärråtkomst.

Samordnade upphandlingar ger bättre förutsättningar att ställa krav på it-säkerhet gentemot leverantörer av MTU. Antalet samordnade upphandlingar av MTU har också ökat sedan 2014. Under 2019 genomfördes 32 samordnade upphandlingar FSN:s upphandlingsavdelning. Vid upphandlingar av nätverksansluten MTU inkluderas numera dessutom it-säkerheten i större utsträckning. Men trots dessa åtgärder bedömer revisionen att det fortsatt finns ett behov av att se över vilka samordnade upphandlingar som ytterligare skulle kunna göras avseende MTU.

Efterlevnad av riktlinjer

Regionstyrelsen har det övergripande ansvaret för informationssäkerheten inom regionen. I det arbetet ingår att kontinuerligt följa upp informationssäkerhetsarbetet i nämnder eller bolag. Regionledningskontoret förvaltar policyer och riktlinjer, samordnar och följer upp förvaltningar och bolagens arbete inom informationssäkerhet. Varje nämnd och styrelse har ansvar för informationssäkerheten inom sina respektive verksamhetsområden och ska utifrån regionövergripande riktlinjer utarbeta egna verksamhetsnära styrdokument samt löpande följa upp informationssäkerheten och vidta åtgärder.

Revisionen bedömer att regionledningskontoret sedan 2014 har vidtagit flera åtgärder för att stärka styrning och uppföljning av informationssäkerhetsarbetet. Det finns en utarbetad och formaliserad process för nämndernas och bolagens generella arbete med informationssäkerhet. Processen utgör ett stöd för ledningar och verksamheter att genomföra egenkontroll, utvärdera och kontinuerligt förbättra informationssäkerheten. Ett it-stöd för informationssäkerhet har också implementerats som används vid anskaffning av utrustning, systemutvecklingsprojekt och underhåll av driftsatta system. Som komplement till policy och riktlinjer för informationssäkerhet finns dessutom en omfattande mängd stöddokument, men vissa av dem är utdaterade sedan mer än ett år tillbaka. Vid samordnad upphandling beaktas numera informationssäkerhet både i upphandlingsunderlag och genom att expertfunktioner inom it- och informationssäkerhet involveras.

De generella reglerna för informationssäkerhet ska även gälla för MTU och det finns därför inga centralt upprättade tillämpningsanvisningar specifikt avseende informationssäkerhet för MTU. Nätverksansluten MTU är dock mer komplex utifrån ett informations- och it-säkerhetsperspektiv, bland annat när det gäller hantering av leverantörernas uppdateringar. Sjukhusen upplever att det är svårt att få leverantörerna att följa regionens generella riktlinjer. I avsaknad av centralt utformade tillämpningsanvisningar får varje sjukhus hitta på egna lösningar för att åtgärda säkerhetsproblem kopplade till MTU. Regionledningskontoret bör därför överväga att ta fram tillämpningsanvisningar för MTU.

Granskningen visar att Karolinska universitetssjukhuset och Danderyds sjukhus har implementerat processen för informationssäkerhet och utformat

lokala tillämpningsanvisningar för informationssäkerhet utifrån regionens styrande och stödjande dokument. Granskningen visar också att sjukhusen i stor utsträckning arbetar utifrån det centralt framtagna ramverket för informationssäkerhet.

Revisionen bedömer dock att sjukhusens praktiska tillämpning av ramverket kan förbättras när det gäller informationssäkerheten som berör MTU specifikt. Sjukhusen kontrollerar inte heller efterlevnad av regelverket för redan installerad nätverksansluten MTU på ett systematiskt sätt. Revisionen bedömer därför att regionstyrelsen uppföljning av hur nämnder och bolag har tagit sig an arbetet med it-säkerhet kopplat till nätverksansluten MTU behöver stärkas.

Systematiskt säkerhetsarbete

Revisionen bedömer att det finns en väl genomarbetad och tydlig dokumenterad process för riskhantering av nätverksansluten MTU när det gäller ansvar och utformning. Enligt tillämpningsanvisningar för riskhantering, som dock inte är uppdaterade, ska riskanalyser bl.a. genomföras vid upphandling, ny- och vidareutveckling av it-system samt vid beslut om väsentliga nätverksförändringar. Det finns också riktlinjer för hur internkontrollarbetet ska utformas och återrapporteras. Akutsjukhusen som ingår i granskningen har tagit fram egna stöddokument för arbetet med riskhantering. Men det finns inga specifika centrala riktlinjer avseende riskanalyser för MTU, vilket gör att sjukhusen genomför dem på olika sätt.

Regionledningskontoret genomför analyser av olika it-säkerhetsrelaterade hot och händelser samt ger nämnder och bolag vägledning och rekommendationer kring dessa. Regionledningskontoret har också utarbetat stöd för incidentrapportering och sjukhusen som ingår i studien har rutiner för hur rapportering ska ske och hur ärenden ska eskaleras.

Däremot visar granskningen att samordningen av riskarbetet kan förbättras mellan sjukhusen, SF IT och regionledningskontoret. SF IT uppger att de inte alltid involveras i sjukhusens riskanalyser eller tar del av riskanalysernas resultat. Den funktion inom regionledningskontoret som genomför säkerhetstester på utvalda system i syfte att förebygga incidenter upplevs återkoppla resultaten från testerna alltför sällan (vartannat år).

Rekommendationer

- Regionstyrelsen bör säkerställa att nätverksansluten MTU, som har upphandlats och konfigurerats med avsteg från regionens gällande riktlinjer, upprätthåller en tillräcklig it-säkerhetsnivå.

- Regionstyrelsen bör stärka uppföljning av hur nämnder och bolag arbetar med it-säkerhet kopplat till nätverksansluten medicinteknisk utrustning.

Bilagor

Konsultrapport Granskning av IT-säkerhet i nätverksansluten medicinteknisk utrustning, PwC.

Vad gör regionrevisorerna?

Regionrevisorerna granskar den verksamhet som bedrivs av regionens 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 styrelser sammanfattar revisionskontoret den granskning som genomförts under det gångna året. Verksamhetsrevisionen redovisas löpande i projektrapporter. Publikationerna presenteras på regionrevisorernas webbsida på www.sll.se. Det går även att prenumerera på regionrevisorernas nyhetsbrev Nytt från regionrevisionen genom att anmäla intresse via e-postmeddelande till landstingsrevisorerna.rev@sll.se.

Region Stockholm

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
Org.nr: 232100-0016

Granskning av IT-säkerhet i nätverksansluten medicinteknisk utrustning

Region Stockholms revisorer

Oktober 2020

Louise Tornhagen
Hugo Horstmann
Anders Hägg

pwc

Revisionsrapport

Innehållsförteckning

Sammanfattning och slutsatser

Granskningen visar att Regionstyrelsen har **stärkt styrningen** och **ansvarsfördelningen** av IT-säkerhet av nätverksansluten medicinteknisk utrustning. Implementeringen av ledningssystemet är genomfört vilket bl.a. inkluderar att tillse att informationssäkerhetssamordnare utsetts på samtliga bolag/nämnder.

Antalet **samordnade upphandlingar** av medicinteknisk utrustning har ökat och IT- säkerhets-perspektivet har inkluderats i högre grad. Vi ser dock att det finns ett behov att se över vilka samordnade upphandlingar som kan göras ytterligare avseende MTU.

Ansvarsfördelningen mellan FSN som nätverksleverantör och akutsjukhusens MT-avdelningar tydliggörs med bl.a. tjänsteöverenskommelser och gränsdragningslistor. Vi menar dock att **samverkan** mellan SF IT och akutsjukhusens MT-avdelningar behöver utvecklas och ske regelbundet och formaliserat samt vara mer proaktiv. Som exempel kan nämnas upphandling av nätverksansluten medicinteknisk utrustning som genomförs av respektive akutsjukhus. Vi menar också att upphandlingar som görs av respektive nämnd/bolag tydligare bör involvera expertkunskap från SF IT. Vi ser även en brist i att SF IT **inte har en komplett bild** över vilken medicinteknisk utrustning som är nätverksansluten för respektive bolag/nämnd.

Avseende akutsjukhusens **tillämpning av riktlinjer och anvisningar** inom ramen för ledningssystemet för informationssäkerhet visar granskningen att det finns en **utarbetad och formaliserad process** detta. Compliance-processen har implementerats som ett stöd i detta arbete inom ramen för ledningssystemet. Vi ser dock att det är en brist att stöddokumenten inte längre är giltiga. I stort visar granskningen att både **Karolinska universitetssjukhuset** och **Danderyds sjukhus** arbetar utifrån det centralt framtagna ramverket för informationssäkerhet samt att de tagit fram egna stöddokument inom området.

Granskningen visar samtidigt på att det finns en rad **brister i den praktiska tillämpningen** av nuvarande process som potentiellt kan medföra risker för informationssäkerhet kopplat till MTU. Exempel på brister är svårigheter att ställa krav på leverantörer och att compliance-mätningar inte utförs systematiskt på redan installerad nätverksansluten MTU och resursbrist.

Vi bedömer vidare att det saknas en tillfredsställande **uppföljning** från regionledningskontoret av hur nämnd/bolag har tagit sig an arbetet med IT säkerhet kopplat till nätverksansluten MTU.

Avseende **riskhantering** är vår bedömning är att det finns en väl genomarbetad och tydligt dokumenterad process utifrån ansvar och utformning. Det finns en funktion, Region Stockholm CERT vid regionledningskontoret, som genomför analyser av olika IT-säkerhetsrelaterade hot och händelser samt ger nämnder och bolag vägledning och rekommendationer kring dessa. Riktlinjer anger vidare hur internkontrollarbetet ska vara utformat och återrapporteras. Båda akutsjukhusen har därtill tagit fram egna stöddokument för arbetet med riskhantering. Det finns även stöd gällande incidentrapportering från regionledningskontorets CERT-funktion och sjukhusen har rutiner för hur rapportering ska ske och ärenden eskaleras.

Detta till trots finns fortfarande utvecklingspotential i riskhanteringsarbetet avseende informationssäkerhet. Samordningen mellan nämnder/bolag och SF IT lyfts fram som ett problemområde även avseende riskhantering. Det saknas även en tydlig bild av hur **ärendehanteringen** är tänkt att fungera i regionen. Båda sjukhusen, och i synnerhet Danderyds sjukhus, påtalar en utvecklingspotential när det gäller systematiskt riskhanteringsarbete.

Utgångspunkt för granskningen

Motiv till granskningen

Medicinteknisk utrustning (MTU) fyller en viktig funktion för att diagnostisera, behandla och lindra sjukdomar och skador. MTU utgör en betydande del av de ekonomiska investeringarna inom hälso - och sjukvården. Införandet av ny teknik och processer såsom automatisering, artificiell intelligens och sakernas internet (IoT) sker i allt större utsträckning med uppkopplade enheter.

Medicinska informationssystem såsom journalsystem och andra IT- system är som regel att betrakta som medicintekniska produkter. Digitaliseringen av medicintekniska produkter och uppkopplade enheter benämns ofta som ”Internet of Things” medför många nya möjligheter, men ger också upphov till nya IT säkerhetsrisker. Trots all innovation som uppkommit genom tillväxten inom telemedicin och uppkopplade enheter så riskerar hälso-och sjukvården attacker som orsakat avsevärda störningar inom vården och som kan kostat stora belopp att ställa till rätta. Bildsystem, livsuppehållande system, pacemakers och defibrillatorer, och många andra uppkopplade enheter är alla tänkbara mål för attacker som riskerar påverka IT-säkerheten. Alla uppkopplade enheter kan påverkas. Utöver den traditionella service och underhållsarbetet behövs idag ett strukturerat arbete kring införande av MTU i nätverk enligt gällande standarder.

Region Stockholms revisorer genomförde 2014 en granskning av IT-säkerhet i nätverksansluten MTU. Vid denna granskning framkom bland annat följande:

- Ansvarsfördelningen mellan regionens centrala IT-funktion och akutsjukhusen ansågs vara otydlig avseende IT-säkerhet i nätverksansluten MTU.
- Behov av att tydliggöra roller och ansvar på både central och lokal nivå. Styrningen bedömdes vara beroende av informella processer och individuella insatser vilket leder till en ökad risk för IT-säkerheten i MTU.
- Det bedömdes också finnas ett ökat behov av central styrning.
- Regelverk för IT-säkerhet som kompletteras med specifika krav för MTU.
- Tydligare samordnat underlag för gemensamma upphandlingar där krav på IT-säkerhet tydligt bör framkomma.

Med anledning av ovanstående har regionens förtroendevalda revisorer beslutat att granska hur Region Stockholm arbetar för att hantera IT- säkerhet i nätverksansluten MTU, samt att följa upp det arbetet som genomförts sedan den tidigare granskningen.

Syfte och revisionsfråga

Syftet med granskningen är att bedöma om regionen har ändamålsenliga rutiner och system för att motverka störningar som kan hota driftsäkerheten för MTU.

Den övergripande revisionsfrågan för granskningen är följande:

Finns tillfredsställande styrning och kontroll av nätverksansluten MTU så att IT-säkerheten säkerställs?

Den övergripande revisionsfrågan har brutits ner i följande tre delfrågor:

A. Hur säkerställer regionstyrelsen tydlig ansvarsfördelning och effektiv samverkan vad gäller säkerhetskrav mellan FSN som nätverksleverantör och akutsjukhusens MT-avdelningar?
B. Hur säkerställer regionstyrelsen respektive akutsjukhusens MT-avdelningar att nätverksansluten MTU uppfyller krav i policyer och riktlinjer?

C. Finns ett systematiskt säkerhetsarbete inkl. riskanalyser gällande teknisk säkerhet och informationssäkerhet i nätverksansluten MTU såväl lokalt som centralt inom Region Stockholm?

Bedömningsgrunder

- Region Stockholms riktlinjer för informationssäkerhet, främst de delar som handlar om krav på informationshantering och nätverksansluten utrustning (fullmäktige 2013-03-19, LS 1112–1733 uppdatera 2018-05-25).
- Lag (1993:584) om medicintekniska produkter
- Socialstyrelsens föreskrifter (SOSFS 2008:1) om användning av medicintekniska produkter i hälso- och sjukvården
- Patientdatalagen
- HSLF-FS 2016:40
- Region Stockholm Budget 2020
- Region Stockholms upphandlingspolicy
- Reglementen för regionstyrelsen och övriga nämnder
- Övriga regioninterna styrdokument som rör granskningsområdet

Avgränsning

Granskningen har avgränsats till att omfatta:

- Regionstyrelsen
- Styrelsen för Danderyds sjukhus
- Nämnden karolinska universitetssjukhuset
- Fastighets- och servicenämndens verksamhet, FS IT

Metod

Granskningen har genomförts genom dokumentgranskning samt semistrukturerade intervjuer. Urval av intervjupersoner har skett i samråd med uppdragsgivaren. Totalt har 11 intervjuer genomförts enskilt eller i grupp. Av hänsyn till den rådande situationen med smittspridning av covid-19 under våren 2020 har samtliga intervjuer genomförts på distans genom videomöte eller telefonintervju.

- Informationssäkerhetschef, Region Stockholm
- Informationssäkerhetssamordnare, hälso- och sjukvårdsförvaltningen
- Upphandlingschef, serviceförvaltningen
- Avdelningschef och tekniker för infrastruktur och drift, SF IT
- Informationssäkerhetssamordnare, Karolinska universitetssjukhuset
- Informationssäkerhetssamordnare, Danderyds sjukhus
- Inköpschef, Karolinska universitetssjukhuset
- Inköpschef, Danderyds sjukhus
- IT-chef Karolinska universitetssjukhuset
- IT-chef, Danderyds sjukhus
- Medicinteknisk chef, Karolinska universitetssjukhuset
- Enhetschefer Medicinsk teknik, Danderyds sjukhus

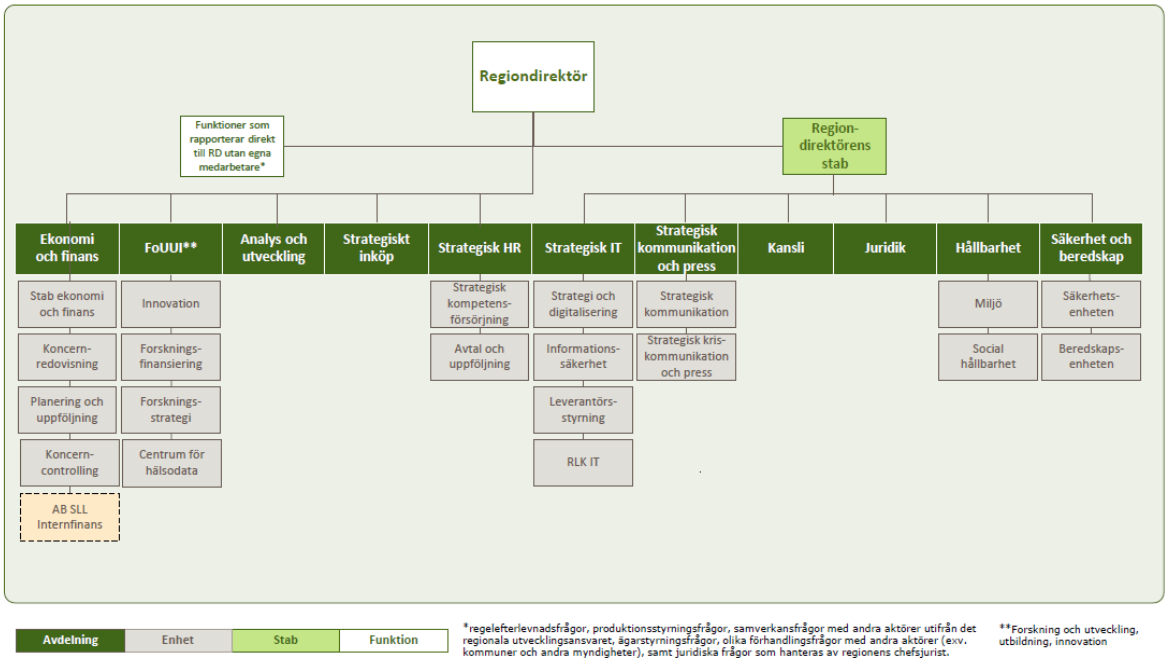
Samtliga intervjupersoner och uppgiftslämnare har haft möjlighet att sakgranska rapporten.

Organisering av IT säkerhet i nätverksansluten MTU

Regionstyrelsen ansvarar för att regionens policy och riktlinjer för säkerhet och informationssäkerhet utformas och hålls aktuella. Regionstyrelsen har även det övergripande ansvaret för säkerhet och informationssäkerhet inom regionen.

Strategisk IT Enheten förvaltar kraven i policy och riktlinjer och samordnar och följer upp förvaltningar och bolags arbete inom området. Enheten **informationssäkerhet** vid regionledningskontoret har i uppdrag att förvalta ledningssystemet, inklusive policy, riktlinjer och anvisningar.

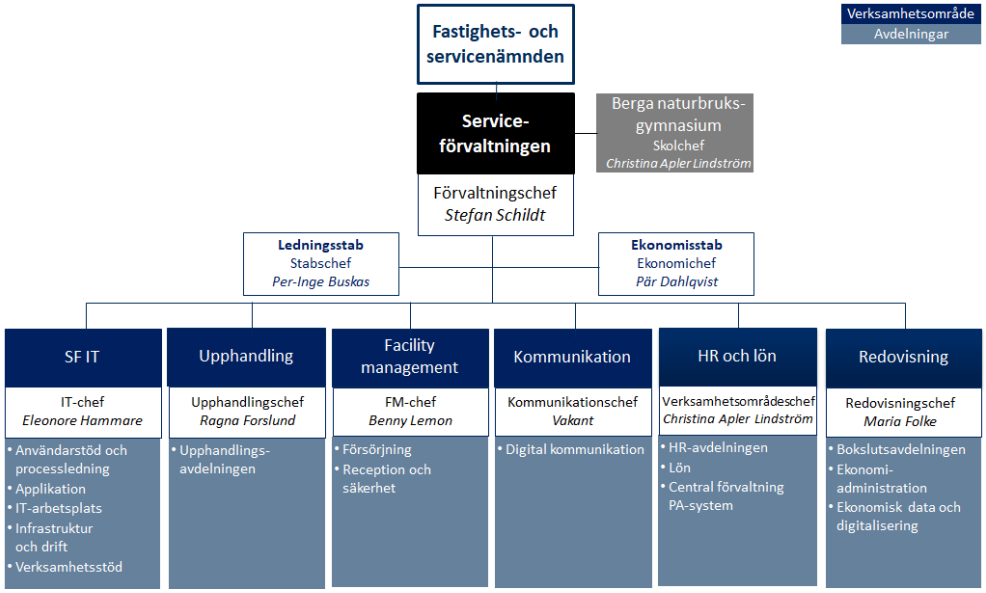
Figur 1: Organisationskarta regionledningskontoret.



Nämnder och bolag ska utifrån de regionövergripande riktlinjerna för informationssäkerhet utarbeta egna verksamhetsnära styrdokument i form av riktlinjer, anvisningar och instruktioner. Den som är chef är ansvarig för säkerheten inom den egna verksamheten. Varje nämnd och styrelse är ytterst ansvarig för informationssäkerheten inom sin förvaltning och bolag enligt Region Stockholms riktlinjer för informationssäkerhet. Det åligger 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.

Fastighets- och servicenämnden, FSN, (genom serviceförvaltningen) har regionfullmäktiges uppdrag att tillhandahålla koncerngemensamma servicetjänster till Region Stockholms nämnder och bolag. Från och med 2020 debiteras nämnder och bolag fullt ut för vad respektive tjänst kostar. **Serviceförvaltningen IT (SF IT)** är Region Stockholms gemensamma IT-organisation. Uppdraget, enligt reglemente, är att ”mot ersättning erbjuda nämnder och bolag tjänster inom internt producerad drift och förvaltning av it- och mt-tjänster, it-support och tjänster för samordning och koordinering av it-drift”.

Figur 2: Organisationskarta serviceförvaltningen under Fastighets- och servicenämnden.



A. Ansvarsfördelning och samverkan

Hur säkerställer regionstyrelsen tydlig ansvarsfördelning och effektiv samverkan vad gäller säkerhetskrav mellan FSN som nätverksleverantör och akutsjukhusens MT-avdelningar?

När medicintekniska system och IT-system kopplas samman uppkommer potentiella patientsäkerhetsrisker. Det finns en tradition av att MTU och IT hanteras i separata strukturer, även om gränsen blir allt mer flytande. Den största organisatoriska förändringen ligger därför i etablerandet av nya förvaltningsorganisationer, ofta i enlighet med modellen PM3, som då även inkluderar MTU. För att få en fungerande förvaltning behövs beslutsstrukturer och processer som underhåller relationen mellan berörda parter; verksamhet och IT/MT.

Det pågår organisationsförändringar på såväl Danderyds sjukhus som Karolinska universitetssjukhuset inom IT och enheterna för medicinsk teknik. **Danderyds sjukhus** genomförde vid årsskiftet 2019/20 en organisationsförändring som innebär att de teknikrelaterade områdena har lyfts ur den generella serviceorganisationen (SjukhusGemensam Service) till en egen avdelning under sjukhusledningen. I den nya avdelningen ingår MT, e-hälsa (IT), DS Innovation samt Lokal och Bygg. **Karolinska Universitetssjukhuset** kommunicerade den 2020-02-02 på sjukhusets intranät att Medicinsk vårdteknologi, MVT, slås samman med Stab IT med en gemensam chef. De intervjuade menar att det skapar förutsättningar att samverka mellan IT och MT på sjukhusnivå för att bland annat stärka säkerheten i nätverksansluten MTU samt effektivisera kostnader och resursåtgång.

På nationell nivå pågår ett arbete med **ordnat införande av MTU** likt den process som finns inom ramen för ordnat införande av läkemedel. Syftet är att regionerna på samma sätt som de samverkar när det gäller ordnat införande av nya läkemedel ska samarbeta kring ny medicinteknik. Arbetet har dock försenats i och med pågående pandemi, Covid-19. Region Stockholm är representerade i detta arbete genom såväl HSF som regionledningskontoret.

Iakttagelser

A.1 Övergripande ansvarsfördelning för IT-säkerhet

Region Stockholm har ett decentraliserat ansvar för IT-säkerhet. Varje nämnd och styrelse har, enligt informationssäkerhetspolicyn, 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. Det är dock inte tydligt hur man följer upp att nämnder/bolag tar sig an detta uppdrag. Det finns inte heller något samlat ansvar för IT- säkerhet av nätverksansluten MTU på en regionövergripande nivå.

Sedan granskningen 2014 har Region Stockholm implementerat ett ledningssystem för informationssäkerhet. Syftet är att stärka ansvar, roller samt att etablera ett gemensamt arbetssätt för informationssäkerhet, vilket beskrivs vidare under revisionsfråga B och C. I syfte att tydliggöra roller och ansvar ytterligare inom ramen för informationssäkerhet ska varje nämnd/bolag anmäla till regionledningskontoret vem som är informationssäkerhetssamordnare på respektive nämnd/bolag.

A.1.1 Samordningsinitiativ

Det pågår ett arbete som leds från regionledningskontoret i syfte att stärka it-styrningen och standardiseringen av it-miljö inom Region Stockholm. Utgångspunkten för arbetet med att stärka styrningen av it inom regionen beskrivs i ett regionstyrelseärende (LS2018-0197). Dialog med representanter för medicinsk teknik och ansvarig för kategoristyrningsarbetet uppges föras under hösten 2020.

Vissa av de intervjuade menar att regionens styrmodell behöver utvecklas för att säkerställa en tillfredsställande IT-säkerhet, bl a behöver ansvarsfördelningen tydliggöras. Vidare anges även att utveckling av säkra testmiljöer är nödvändigt för att kunna hantera accesser på korrekt sätt.

Det pågår ett arbete på regionledningskontoret med samordningsinitiativ för IT-säkerhet inom fyra områden. Förslag till uppdaterade styrande dokument för informationssäkerhet har tagits fram och remitterats till nämnder och bolag. De beskriver styrande principer, regler och krav på hur nämnder och bolag ska arbeta med informationssäkerhet. Arbetet finns sammanfattat i två remiss-PM.

I det ena ärendet föreslås en verksamhetsskyddspolicy som är tänkt att ersätta nuvarande informationssäkerhetspolicy och säkerhetspolicy. Syftet är att minska administrativ överbyggnad och detaljstyrning i möjligaste mån samt säkra en sammanhållen styrning. Det andra ärendet avser revidering av nuvarande riktlinjer för informationssäkerhet. Syftet är i likhet med förslag till verksamhetsskyddspolicy att minska detaljstyrning, t.ex. genom att ta bort bestämmelser om krav på lokala styrande dokument i de fall där sådana kan tas fram centralt.
Syftet är även att förenkla tillämpning och tolkning av riktlinjerna.

Sammanfattningsvis innehåller inte de remitterade förslagen på styrande dokument tydliga skrivningar rörande hur samverkan mellan nämnderna/bolagen å ena sidan och SF IT å andra sidan skulle kunna förbättras. Enligt intervjuer med informationssäkerhetschef på regionledningskontoret regleras ansvarsfördelningen framförallt i avtalet mellan regionstyrelsen och fastighets- och servicenämnden.

A.2 Upphandling av nätverksansluten MTU

Andelen samordnade upphandlingar genomförda av region Stockholms upphandlingsavdelning har ökat. I dessa samordnade upphandlingar har en utveckling skett avseende att inkludera IT-säkerhet kopplat till nätverksansluten MTU, vilket beskrivs fördjupat under revisionsfråga B.

Respektive nämnd/bolag har därtill egna inköpsavdelningar som genomför de upphandlingar av MTU som inte samordnas. Enligt de intervjuade sker ingen systematisk dialog med SF IT inför lokala upphandlingar av nätverksansluten MTU. Samma krav på informationssäkerhet ska dock ställas av regionens samtliga bolag och nämnder vid upphandlingar.

En utmaning som adresseras i intervju är att akutsjukhusen i regionen genomför liknande upphandlingar per sjukhus istället för att genomföra samordnade upphandlingar. Som exempel kan nämnas patientövervakningssystemet PAMS. SF IT menar att det kan innebära en risk för suboptimering och att viktig erfarenhet från liknande upphandlingar inte nyttjas. Intervjuade vid Karolinska universitetssjukhuset och Danderyds sjukhus anger att ambitionen är att SF IT ska vara med som tillfrågade experter vid anskaffning av nätverksansluten MTU.

A.3 Samverkan mellan SF IT och akutsjukhusen

För nätverksansluten MTU är det betydelsefullt att det finns en tydlig ansvarsfördelning och samverkan mellan SF IT som nätverksleverantör, akutsjukhusen som användare av den medicintekniska utrustningen (MT, IT och verksamheterna) och leverantörerna.
Vid granskningen som genomfördes av revisorerna 2014 framkom en otydlighet i ansvarsfördelningen avseende säkerhetskrav mellan SF IT och akutsjukhusen.

SF IT ansvarar i sin roll som nätverksleverantör för daglig drift av nätverk, levererar tjänster och lösningar till regionens verksamheter mot ersättning. Respektive nämnd/bolag är ansvarig för att hantera IT-säkerheten av nätverksansluten MTU. Samverkan regleras genom tjänsteöverenskommelser för nätverksansluten MTU. I tillägg till överenskommelserna finns dokumentation av gränssnitten. Enligt de intervjuade har detta tillkommit sedan den förra granskningen. Dokumentation av gränssnitt har tagits fram av SF-IT tillsammans med MVT under införandet av NKS. Dokumentationen hanteras som ett samarbete mellan SF-IT och respektive sjukhus enligt framtagen gränssnittprocess.

Dokumentet ska fyllas i av akutsjukhusen och beskriver hur ett nätverk ska designas för att vara säkert ur flera dimensioner och långsiktigt över tid. Vid implementering av nätverksansluten MTU får sjukhusen enligt intervju stöd av SF IT. Vi har inom ramen för granskningen tagit del av gränssnittsdokument för såväl Karolinska som Danderyds sjukhus.

Enligt intervjuerna med Karolinska ansvarar de fortfarande för en del av IT driften. Danderyds sjukhus uppger dock att de köper IT-tjänster till stor del av SF IT då sjukhusets egen IT-organisation är förhållandevis liten. SF IT tillhandahåller nätverk för MTU på Danderyds sjukhus.

Enligt intervju har informationssäkerhetssamordnare på Karolinska och Danderyd dialog med motsvarande funktion på SF IT vid behov. Under dessa möten diskuteras frågor med utgångspunkt i tjänsteöverenskommelsen.

A.3.1 SF IT:s överblick över nätverksansluten MTU

I regionens strategi för IT och digitalisering 2020–2023 anges att varje nämnd och bolag ska dokumentera vilken information som hanteras i verksamheten och vilket skyddsvärde informationen har. Enligt tidigare granskning har SF IT inte en komplett förteckning över sjukhusens nätverksanslutna MTU. Respektive sjukhus skulle säkerställa vilken MTU som fanns samt vilken som var kopplad till nätverk. SF IT:s överblick över sjukhusens nätverksanslutna MTU är oförändrad vid tiden för denna granskning. Respektive sjukhus har kontroll över vilken MTU som är nätverksansluten primärt genom inventariesystemet Medusa.

A.4 Bedömning revisionfråga A

Vi bedömer att Regionstyrelsen har genomfört ett antal åtgärder för att stärka styrning och ansvarsfördelning kring IT-säkerhet för MTU vilket inkluderar implementering av ledningssystem och att utse informationssäkerhetssamordnare på respektive nämnd/bolag. Därtill har antalet samordnade upphandlingar ökat och IT- säkerhetsperspektivet inkluderats i högre grad.

Vi bedömer dock att det saknas en uppföljning från regionledningskontoret av hur nämnd/bolag de facto tagit sig an arbetet med IT säkerhet kopplat till nätverksansluten MTU.

Vi menar vidare att samverkan mellan SF IT och akutsjukhusens MT-avdelningar behöver utvecklas och ske regelbundet och formaliserat samt vara mer proaktiv. Som exempel kan nämnas upphandling av nätverksansluten medicinteknisk utrustning som genomförs av respektive akutsjukhus.

Vi ser att det är en brist att SF IT inte har en komplett bild över vilken medicinteknisk utrustning som är nätverksansluten för respektive bolag/nämnd.

B. Efterlevnad av riktlinjer

Hur säkerställer regionstyrelsen respektive akutsjukhusens MT-avdelningar att nätverksansluten MTU uppfyller krav i policyer och riktlinjer?

I syfte att förhindra informationssäkerhetsincidenter och upprätthålla medicinsk viktig verksamhet behöver en region bedriva ett ändamålsenligt informationssäkerhetsarbete. Information som finns i regionen eller på akutsjukhusen ska klassas, rutiner och riktlinjer ska finnas på plats och arbetet ska regelbundet följas upp, och det kräver också ett säkerhetsmedvetande hos de som hanterar informationen på daglig basis. I syfte att tydliggöra detta finns det ett stort värde i att ha ett välfungerande implementerat ledningssystem för informationssäkerhet.

Iakttagelser

Av styrande dokument och intervjuer framgår det att Region Stockholm har en *Informationssäkerhetspolicy (*regionfullmäktige, 2013-03-19, LS 1112–1733 samt *Riktlinjer för informationssäkerhet (*regionfullmäktige, 2013-03-19, LS 2016–0646 som gäller för hela region Stockholm. Enligt intervjuer utgör regionens ISO-anpassade ledningssystem för informationssäkerhet av flera delar däribland principer, regler och krav som anges i policy/riktlinjer och är bindande för samtliga nämnder och bolag. Figur 3 illustrerar översiktligt hur compliance-processen ska bidra till systematiskt informationssäkerhetsarbete.

Figur 3: Compliance-processen inom ramen för regionens ledningssystem för informationssäkerhet.

Övriga delar i ledningssystemet för informationssäkerhet består av en handlingsplan för informationssäkerhet, riskhantering samt ett IT-baserat verktyg för systematiskt informationssäkerhetsarbetet, vilket inkluderar efterlevnadskontroll och uppföljning - Compliance Management (“compliance-verktyg”). Handlingsprogrammet för informationssäkerhet är upphävt i senaste budgeten. Enligt intervjuer med informationssäkerhetschef pågår det ett arbete med att ta fram en uppdaterad målbild.

Att ledningssystemet är grunden för Region Stockholms arbete inom informationssäkerhet framgår också av strategi för IT och digitalisering 2020–2023. Det pågår just nu ett arbete med att se över styrande dokument inom ramen för ledningssystemet.

B.1 Samverkansforum

Det framförs i intervju att Informationssäkerhetsrådet (ISR), bestående av informations-säkerhetssamordnare från respektive förvaltning/bolag och informationssäkerhetschefen, träffas varje månad för att följa upp ledningssystemet för informationssäkerhet. Det påtalas dock att rådet sällan diskuterar informationssäkerhet avseende MTU specifikt. Samverkan kring informationssäkerhet kopplat till MTU specifikt uppges vara mer lämpat för samverkansmöten

mellan vårdgivare. Därtill finns genom Region Stockholm CERT:s dialoger med nämnder, bolag och driftorganisationer.

B.2 Centralt stöd för kravställning av IT-säkerhet

B.2.1 Samordnade upphandlingar

Enligt Region Stockholms inköpspolicy ska nämnder och bolag verka för att en ökad andel upphandlingar genomförs som samordnade upphandlingar. Under 2019 genomfördes 32 stycken samordnade upphandlingar avseende MTU av Region Stockholms upphandlingsavdelning. I dessa har en utveckling skett med att inkludera IT-säkerhet av nätverksansluten MTU. Såväl informationssamordnare som experter inom IT-och informationssäkerhet ska finnas med vid kravställning. Upphandlingsunderlaget har utvecklats för att stödja regionens arbete inom detta område.

B.2.2 Centralt upprättade stöddokument

De regionövergripande generella kraven för informationssäkerhet ska i full utsträckning även gälla MTU. Det finns inga centralt upprättade tillämpningsanvisningar avseende informationssäkerhet specifikt för MTU. Regionstyrelsens förvaltning har upprättat en **vägledning för säkerställande av informationssäkerhet vid upphandling och avrop** (fastställd av informationssäkerhetschef 2018-11-01). Vägledningen var dock endast giltig till 2018-12-31. I denna rekommenderas att den upphandlande verksamheten i tidigt skede tar kontakt med informationssäkerhetssamordnare vid SF IT för att få stöd med analysen inför upphandling. En rad frågor avseende informationssäkerhet ska analyseras inför kravställan i upphandling. Vid kravställan ska kravdatabas användas som stöd.

I vägledningen för avtalsskrivning finns tre mallar för avtalsbilagor rörande informationssäkerhet - 1) hantering hos leverantör, 2) hantering hos region Stockholm (information hanteras i regionens it-system) samt 3) hantering hos region Stockholm (information hanteras i leverantörens it-system).

Regionledningskontoret har även upprättat en tillämpningsanvisning för complianceprocessen, **Compliance-process för systematiskt informationssäkerhetsarbete** (fastställd av regiondirektören 2016-03-22). I tillämpningsanvisningarna beskrivs compliance-processens delar, it-stöd och uppföljning.

Utöver denna tillämpningsanvisning har sju ytterligare tillämpningsanvisningar tagits fram med koppling till styrande dokument för informationssäkerhet, däribland:

- **Tillämpningsanvisning: Införande av ledningssystem för informationssäkerhet** (fastställd av regiondirektören 2016-01-14)
- **Tillämpningsanvisning: Hantering av informationstillgångar** (fastställd av regiondirektören 2016-01-14)
- **Tillämpningsanvisning: Riskhantering** (fastställd av regiondirektören 2016-01-14)

I likhet med vägledning för säkerställande av informationssäkerhet vid upphandling och avrop upphörde samtliga tillämpningsanvisningar vara giltiga 2018-12-31.

B.2.3 Compliance-processen och kravställan vid upphandling av MTU

Compliance-processen har skapats för att stödja ledningar och verksamheter i det kontinuerliga arbetet med att styra, genomföra egenkontroll, utvärdera och ständigt förbättra informationssäkerheten. Compliance-processen illustreras i tillämpningsanvisningarna med följande bild:

Figur 4: Complianceprocessens aktiviteter/steg.

Med Gap-analys avses en analys för att skapa en bild över en verksamhets eller ett it-systems informationssäkerhetsstatus i förhållande till regionens riktlinjer för informationssäkerhet. Det framgår vidare av tillämpningsanvisningarna att kravkataloger finns framtagna för tre nivåer som stöd i arbetet med informationssäkerhet - strategisk nivå, verksamhetsnivå och teknisk nivå. Kravkatalogen innehåller nivåanpassade frågor.

Compliance-portalen har implementerats av regionen som IT-stöd för egenkontroll och uppföljning av kravefterlevnad, frågeställningar som kan användas för leverantörens deklaration av efterlevnad avseende informationssäkerhet. I dokumentation över deklaration av informationssäkerhet via compliance-portalen som vi har tagit del av framgår att processen kan användas för 1) driftsatta system, för 2) systemutvecklingsprojekt och 3) vid anskaffning av nya system (upphandling/avrop). I dokumentationen framgår att frågorna är indelade i en rad kategorier däribland dokumentation av IT-miljö, riskhantering, autensiering, behörighetshantering och intrångsskydd.

I regionens riktlinjer för informationssäkerhet anges att anslutning av IT-utrustning som inte tillhandahållits av regionen utan av t.ex. leverantörer ska regleras i skriftligt avtal där det anges vilka säkerhetsåtgärder som ska vidtas för att skydda verksamhetens IT-miljö och informationstillgångar. Kraven på systemet ska tydligt framgå i kravspecifikationen och följas upp.

MTU upplevs vara komplext utifrån ett informations- och IT-säkerhetsperspektiv. Det uppges i intervjuer med både Karolinska universitetssjukhuset och Danderyds sjukhus vara svårt att ställa höga säkerhetskrav på sådan utrustning och att få leverantörer att möta regionens riktlinjer. Utmaningar beskrivs som branschspecifika för MTU vilket genererar svårigheter för leverantörer att uppfylla kraven och att akutsjukhusen måste hitta andra sätt att hantera dessa frågor. Enligt intervjuer med informationssäkerhetschef får ansvarig för upphandlingsprojekt istället undersöka hur regionen kan uppnå kraven på annat sätt så att skyddet upprätthålls. Upphandlande funktioner ska enligt intervjuer försöka utmana leverantörerna att på sikt leva upp till kraven i patientdatalagen och riktlinjer.

B.2.4 Informationssäkerhetsklassificering och systemkrav

I Region Stockholms informationssäkerhetspolicy anges att all information ska **klassificeras.** Enligt regionens riktlinjer för informationssäkerhet ska IT-systemet, innan det tas i drift, vara godkänt ur säkerhetssynpunkt av den för vars verksamhet systemet inrättas och vara informationssäkerhetsklassificerade enligt regionens klassificeringsmodell. Informations-säkerhetsklassningen uppges ha förenklats vilket enligt intervju gett goda resultat.

Region Stockholms riktlinjer för informationssäkerhet anger att **nätverk ska vara logiskt separerade**. De ska utformas så att det finns gränssnitt mot andra nätverk. Nätverk, dess komponenter och systemsamband ska vara dokumenterade.

Regionens riktlinjer för informationssäkerhet stipulerar vidare att **systemloggar** ska vara skyddade mot obehörig åtkomst och manipulation. De ska omfattas av fastställda rutiner för säkerhetskopiering och arkivering. Systematiska och regelbundna stickprovskontroller ska även göras av loggarna enligt fastställd rutin.

I tillämpningsanvisningen för informationstillgångar specificeras regionens modell för informationssäkerhetsklassificering. Modellen bygger på tre huvudsakliga informationssäkerhetsaspekter - konfidentialitet (information skyddas mot obehörig åtkomst), riktighet (information skyddas mot obehörig och avsiktlig förändring) och tillgänglighet (informationen ska kunna användas i förväntad utsträckning). En fyragradig bedömningsskala ska användas – ingen/försumbar, måttlig, betydande/allvarlig och mycket allvarlig/katastrofal.

Fastställd informationssäkerhetsklass styr utformningen av olika slag av säkerhetsåtgärder, exempelvis vilka säkerhetsfunktioner som ska finnas i IT-system.

I intervju framkommer att nätverksinfrastrukturen upplevs vara ett utmanande område, t.ex. segmentering av nätverk. Segmenterade nätverk innebär att kommunikationen är begränsad mellan de olika nätverk som systemen är kopplade till, vilket försvårar intrång. SF IT uppges inte involveras i tillräcklig utsträckning avseende nätverkssegmentering.

B.3 Central uppföljning av regionens krav på IT-säkerhet

Det åligger varje nämnd och styrelse att löpande följa upp informationssäkerheten och vidta tillräckliga åtgärder för att upprätthålla tillräcklig intern kontroll enligt regionens riktlinje för informationssäkerhet. I *vägledning för säkerställande av informationssäkerhet vid upphandling och avrop* föreskrivs att det är avtalsförvaltarens ansvar att säkerställa att uppföljning sker av hur leverantören lever upp till de krav som ställts på informationssäkerhet.

Ansvariga för en verksamhet eller ett IT-system ska genomföra egenkontroller i enlighet med compliance-processen. Informationssäkerhetssamordnare ska samordna detta arbete lokalt och rapportera till förvaltningschef/VD. Därutöver ska högsta ledning på bolag/nämnd minst en gång per år gå igenom verksamhetens ledningssystem för informationssäkerhet och föra dialog med verksamheten avseende genomgången enligt tillämpningsanvisning avseende införande av ledningssystem för informationssäkerhet. Enligt tillämpningsanvisning till ledningssystemet för informationssäkerhet har förvaltningschef/VD på respektive nämnd/bolag ansvar att årligen rapportera status avseende informationssäkerhet till nämnd/styrelse.

För **samordnade upphandlingar** ansvarar, enligt intervju, upphandlingsavdelningen på serviceförvaltning för den affärsmässiga uppföljningen av avtalets krav. Uppföljning från leveransperspektivet sker ofta av verksamheten som avropar och tar emot utrustningen.

Systemägarskapet kan ligga på regional eller lokal nivå (dvs på respektive sjukhus). Systemägaren ansvarar för skyddsnivån för den information som får användas i systemet samt identifiera och åtgärda avvikelser. Informationssäkerhetssamordnare ska agera stöd och följa upp detta arbete. Om samordnare behöver stöd kring analyser och att identifiera risk kontaktas regionledningskontoret.

Enligt regionens riktlinje för informationssäkerhet är det emellertid regionstyrelsen som har det övergripande ansvaret för att kontinuerlig uppföljning av informationssäkerhet görs. Efterlevnaden av regionens riktlinjer för informationssäkerhet ska årligen följas upp på en övergripande nivå genom informationssäkerhetsrådet och rapporteras till regiondirektören via informationssäkerhetschefen. Enligt intervju kan även regionledningskontoret vid behov utföra ytterligare uppföljningar under året. Det har dock framkommit att någon rapport avseende efterlevnad av informationssäkerhet inte upprättats för regionen som helhet under 2019. Detta förklaras med fullmäktiges uppdrag i budget 2020 att mål och indikatorer för informationssäkerhet ska arbetas om. Vi har tagit del av rapporten för 2018 som lämnades till regiondirektören av informationssäkerhetschefen. Värt att notera är att informationssäkerhet endast följs upp aggregerat på övergripande nivå utifrån ledningssystemets delar. Det finns inga särskilda uppgifter kring efterlevnad av informationssäkerhet för MTU och inte heller redovisning av enskilda bolag/nämnders efterlevnad av regionens informationssäkerhetsriktlinjer.

B.4 Karolinska universitetssjukhuset

B.4.1 Karolinskas forum för informationssäkerhet

Det finns ett strategiskt forum för informationssäkerhet på sjukhuset som går under benämningen Ledningsforum för informationssäkerhet. Det består av informationssäkerhets-samordnaren, sjukhusets dataskyddsombud och chefen för säkerhetsledningen.

Därtill finns ett taktiskt forum, Informationssäkerhetsforum. Det består av

informationssäkerhetssamordaren, sjukhusets dataskyddsombud samt informationssäkerhetskoordinatorer från alla sjukhusets verksamheter.

Det finns ingen representant från MT vid något av forumen. Det uppges vidare att Ledningsforum för informationssäkerhet är under omstart på grund av flertalet omorganisationer och avgångar.

B.4.2 Karolinskas stöddokument för informationssäkerhet

Karolinska har upprättat **Tillämpningsanvisningar för inköp och upphandling** (godkänt av t.f. ekonomidirektör 2020-09-04) som omfattar samtliga inköp/hyra/leasing som sjukhuset genomför. Karolinskas tillämpningsanvisningarna för inköp och upphandling beskriver bl.a. ansvarsfördelningen avseende inköp.

Karolinska har även upprättat **Tillämpningsanvisningar för informationssäkerhet** (beslutad av chef för information och IT-säkerhet, 2019-05-29). Tillämpningsanvisningarna är omfattande och inkluderar roller och ansvar, informationsklassificering, driftsäkerhet och utveckling och anskaffning av IT-system.

Vidare har sjukhuset en **checklista vid upphandling** samt en **mall för kravspecifikation** som inkluderar punkter rörande informationssäkerhet.

B.4.3 Karolinskas kravställning av IT-säkerhet vid upphandling av MTU

Karolinskas inköpsavdelning har under 2019 genomfört fyra annonserade upphandlingar och tre frivilliga förhandsinsyner för nätverksansluten MTU. I Karolinskas tillämpningsanvisningar för inköp och upphandling anges att sjukhusets inköpsavdelning hanterar inköp som inte verksamheterna själva kan avropa eller som måste föregås av upphandling. Vid upphandling som innebär att annan part ska behandla personuppgifter för sjukhusets räkning ska personuppgiftsbiträdesavtal (PUB-avtal) upprättas. Vidare anges att anskaffning av MTU alltid ska initieras av förvaltningarna inom Medicinsk Vårdteknologi. I intervju framgår att Karolinskas inköpsavdelning endast får hjälp av en person med kravställan av IT-säkerhet vilket uppges vara otillräckligt.

I Karolinska universitetssjukhusets upprättade checklista vid upphandling anges att handläggare vid upphandling ska stämma av informationstyp med sakkunniga och vid behov hänvisa verksamheten till informationssäkerhetsansvarig för klassning av informationen och komplettering av kravspecifikationen.

Karolinska har en mall för kravspecifikation av MTU i vilken det framgår en rad krav som ska uppfyllas vid upphandling, däribland:

- att programvara till upphandlad MTU ska uppfylla gällande regelverk för informationshantering av person/patientdata inom Karolinska/Region Stockholm.
- att uppdateringar med nya säkerhetspatchar eller servicepacks bör ske i samråd med kontaktpersoner på Medicinsk vårdteknologi och kliniken. Valideringsprocessen ska beskrivas av leverantören.
- att säkerhetsmeddelanden, servicemeddelanden, incidentrapporter, avvikelserapporter och motsvarande information med inverkan på säkerhet, risker, funktioner eller handhavande ska löpande vidarebefordras till MVT och klinisk kontaktperson på Karolinska.

Vidare gäller enligt uppgift att system som behandlar/transporterar sekretessbelagda/ skyddsvärda uppgifter ska ha en förmåga att kryptera trafik på adekvat nivå.

Av Karolinska universitetssjukhusets mall för kravspecifikation av MTU framgår vidare att för att kunna ställa och utvärdera IT-krav krävs att lokal IT-funktion ingår i sakkunniggruppen. Vidare framgår att komplett MTU inkl. mätdator/IT-system och legala tillbehörmaterial ska vara CE-märkt som ett system. Det uppges i intervju att MT-enheten har en egen IT-avdelning som har hand om en del av den dagliga driften och teknisk förvaltning av system kopplade till MTU.

Inköpsavdelningen sköter upphandling av MTU och vid behov inkluderas Medicinsk Vårdteknologi och SF IT. Utifrån resurs- och kompetenshänseende anser flera av de intervjuade det i dagsläget är nödvändigt att MT-tekniker på Karolinska säkerställer att IT-säkerhetskrav följs. Det uppges dock att dialog med SF IT kan förekomma vid upphandling av ny nätverksansluten MTU.

I intervju framförs att implementering av ISO 80001 som reglerar ansvarsfördelningen mellan aktörer som hanterar medicintekniska nätverk är ett viktigt led i att öka samordningen och därmed säkerheten i nätverksansluten MTU. Implementeringen av denna har ännu inte gjorts fullt ut inom regionen.

B.4.4 Karolinskas informationssäkerhetsklassningar

Avseende informationssäkerhetsklassificering anges i Karolinskas tillämpningsanvisningar för informationssäkerhet det ramverk som används utifrån den övergripande uppdelningen- tillgänglighet, riktighet och konfidentialitet. Verksamhet som driver upphandling ska göra en informationssäkerhetsklassificering och bedöma vad som är nödvändigt att inkludera i kravställan till leverantörer. I det arbetet kan informationssäkerhetssamordnare vara med som stöd.

B.4.5 Karolinskas uppföljning av regionens krav på IT-säkerhet

Vid intervju framförs att det är verksamheterna som följer upp parametrar i kravställan. I sjukhusets tillämpningsanvisningar för informationssäkerhet anges hur uppföljning av informationssäkerhet ska ske. Beskrivningen ligger i linje med centrala anvisningar.

Enligt uppgift görs i dagsläget inte compliance-mätning för efterlevnad av regelverket för redan installerad nätverksansluten MTU med systematik. Det uppges dock att det pågår ett förbättringsarbete för detta område.

B.5 Danderyds sjukhus

B.5.1 Danderyds stöddokument för informationssäkerhet

Det finns en av tjänstemän upprättad riktlinje för Danderyds Sjukhus, **Informationssäkerhett – Utveckling och anskaffning av it-system vid Danderyds sjukhus AB** (beslutad av informationssäkerhetssamordnare, 2016-11-25). Riktlinjen anges dock endast vara giltig till 2017-11-25. Syftet med riktlinjen är delvis att säkerställa att informationssäkerhet är en integrerad del av informationssystem över hela livscykeln. Målet är också att säkerställa att informationssäkerhet designas och införs inom utvecklingscykeln av informationssystem.

Sjukhuset har även upprättat **Informationssäkerhet - Uppföljning av efterlevnad vid Danderyds Sjukhus AB** (beslutad av informationssäkerhetssamordnare, 2017-12-18). Riktlinjens syfte är att ge en beskrivning av vikten av efterlevnad av kraven i ledningssystem för informationssäkerhet.

Vidare finns en upprättad riktlinje, **Informationssäkerhet – Riskhantering vid Danderyds Sjukhus AB** (beslutad av informationssäkerhetssamordnare 2017-12-18). Syftet med riktlinje är att sjukhuset på ett systematiskt sätt ska arbeta med riskanalys samt förebyggande åtgärder.

B.5.2 Danderyds kravställning av IT-säkerhet vid upphandling av MTU

I riktlinjen “Informationssäkerhet - Utveckling och anskaffning av it-system vid Danderyds Sjukhus AB” som dock inte längre är giltig anges att en instruktion och ett väldefinierat arbetssätt krävs när nya system eller utvecklade systemkomponenter implementeras från utvecklings- och testmiljön in i produktionsmiljön. Objektägaren/systemägaren för respektive it-system ansvarar för att kravställa avseende systemförvaltningen.

Sjukhusets inköpsstöd uppges genom ett upphandlingsverktyg ha flera mallar som används för att säkerställa att korrekta krav ställs. Samarbetet inom Danderyds sjukhus mellan upphandling och expertfunktioner upplevs fungera bra även om det

ibland kan vara tidskrävande att få hjälp av tillämpliga expertfunktioner.

I intervju framkommer delvis olika åsikter rörande SF IT:s involvering i upphandlingsarbetet. Vissa uppger att SF IT har ansvar för de IT-tunga delarna av kravställan och att man från sjukhuset kompletterar deras arbete. Andra menar att det finns en funktionsbrevlåda hos SF IT som kan användas men att det inte finns en utsedd kontaktperson från SF IT för att systematiskt bistå med IT-relaterade upphandlingar. Det upplevs finnas oklarheter gällande kostnadsfördelning då sjukhuset tar hjälp av centralt upphandlingsstöd och det har därför skett ett arbete för att bygga upp lokal kompetens. Samtidigt framförs att redundans och kompetenshöjning är en utmaning för ett välfungerande upphandlingsarbete när det gäller nätverksansluten MTU.

I intervju framförs att compliance-portalen används och att det säkerställs att leverantörer uppfyller krav. Informationssäkerhetssamordnaren ska vara involverad i upphandlingar som rör informationsklassade data.

Samordnad upphandling framförs vara ett sätt för att i större utsträckning få igenom säkerhetskrav mot leverantörer som har svårigheter att möta lagstiftningens och regionens informationssäkerhetskrav.

Vi har tagit del av ett dokumenterat exempel för upphandlad nätverksansluten MTU som genomgått compliance-processen.

B.5.3 Danderyds informationssäkerhetsklassningar

Informationsklassningar uppges göras i enlighet med regionens klassningsstandard. Klassningar görs i regel av verksamhetschef i dialog med informationssäkerhetsansvarig och MT-enheten på sjukhuset.

B.5.4 Danderyds uppföljning av regionens krav på IT-säkerhet

I informationssäkerhet - Uppföljning av efterlevnad vid Danderyds Sjukhus AB anges bl.a. att utformningen, driften och användningen av informationssystem ska genomgå årliga granskningar. Granskningar ska även genomföras då väsentliga händelser som påverkar informationssäkerheten inträffar. Informationssäkerhet ska enligt riktlinjerna säkerställas genom interna revisioner, compliance-processen och ledningens genomgång. Däremot utförs enligt uppgift inte systematisk compliance-mätning för efterlevnad av regelverket för redan installerad nätverksansluten MTU. I Danderyds Sjukhus AB:s verksamhetsberättelse 2019 anges att arbete med informationssäkerhet kontinuerligt följts upp under året, bl.a. som en del av internkontrollplanen och i de uppdrag som är ålagda sjukhuset.

Uppföljning av upphandlad MTU sker enligt intervju av MT-enheten på sjukhuset alternativt av informationssäkerhetssamordnaren. Det pågår ett utvecklingsarbete kring hur gränsdragningen kan förbättras avseende uppföljning mellan upphandling, MT-enheten och informationssäkerhetssamordnaren.

B.6 Bedömning revisionfråga B

Vår bedömning är att finns en utarbetad och formaliserad process för regionledningens och nämndernas/bolagens generella arbete med informationssäkerhet. Regionstyrelsen har genomfört en rad åtgärder för att stärka styrning och uppföljning och ledningssystemet för informationssäkerhet utgör grunden för detta och Compliance-processen ett stöd i detta arbete. Som komplement till policy och riktlinjer finns en omfattande mängd stöddokument. Det stöddokument vi har tagit del av är dock inte längre giltiga utan är utdaterade sedan mer än ett år tillbaka.

En utveckling har skett inom ramen för samordnad upphandling där informationssäkerhet beaktas både i upphandlingsunderlag och genom expertfunktioner inom IT- och informationssäkerhet.

I stort visar granskningen att både Karolinska universitetssjukhuset och Danderyds sjukhus arbetar utifrån de centralt framtagna ramverket för informationssäkerhet samt att de tagit fram egna stöddokument inom området.

Granskningen visar dock samtidigt på att det finns en rad brister i den praktiska tillämpningen av nuvarande process som potentiellt kan medföra risker för informationssäkerhet kopplat till MTU. Det föreligger svårigheter att ställa krav på leverantörer avseende fullständig efterlevnad av de regionövergripande kraven på informationssäkerhet. Granskningen har också visat att sjukhusen inte utför systematisk compliance-mätning av redan installerad nätverksansluten MTU. I flera av de genomförda intervjuerna framförs resursbrist som en orsak till brister i informationssäkerhetsarbetet.

C. Systematiskt säkerhetsarbete

Finns ett systematiskt säkerhetsarbete inkl. riskanalyser gällande teknisk säkerhet och informationssäkerhet i nätverksansluten MTU såväl lokalt som centralt inom Region Stockholm?

Iakttagelser

Enligt regionens informationssäkerhetspolicy ska nödvändiga åtgärder för att tillse rätt skydd föregås av återkommande risk- och sårbarhetsanalyser. Regionens riktlinjer för informationssäkerhet föreskriver att det ska finnas en dokumenterad beskrivning av IT-systems ändamål, säkerhetsklass och allmänna säkerhetsmål. Därtill ska hot-, risk- och sårbarhetsanalyser genomföras regelbundet, och innan viktiga förändringar genomförs. Vi har tagit del av tillämpningsanvisning riskhantering.

Utifrån dessa analyser ska lämpliga skyddsåtgärder vidtas för att fastställd skyddsnivå ska få avsedd effekt. Det ska finnas systemdokumentation för varje IT-system. Dokumentationen ska normalt bestå av system-, drift- och användardokumentation, och utformas enligt gällande förvaltningsstyrningsmodell.

C.1 Centralt stöd avseende risk- och sårbarhetsanalyser för MTU

Det finns inga specifika centrala riktlinjer avseende riskanalyser för MTU. Det är respektive bolag/nämnd som ansvarar för riskanalyser för informationssäkerhet inom ramen för sin verksamhet. Regionens informationssäkerhetspolicy stipulerar att återkommande risk- och sårbarhetsanalyser ska göras som grund för nödvändiga åtgärder avseende informationssäkerhet. Enligt de intervjuade har arbetet gått långsamt och inte implementerats fullt ut.

Enligt Region Stockholms riktlinjer för informationssäkerhet ska varje verksamhet för sina IT-system genomföra och dokumentera analyser avseende vilka hot, risker och sårbarheter som kan påverka verksamheten. Utifrån dessa analyser ska lämpliga säkerhetsskyddsåtgärder vidtas. Ett riskhanteringsbeslut ska fattas för varje risk och åtgärdsplan ska framtas om risken inte kan godtas. På regionens intranät uppges finnas information för bedömning av risker.

I den ej längre giltiga tillämpningsanvisningar för riskhantering anges att riskanalyser ska genomföras:

- Vid upphandling, ny- och vidareutveckling av it-system
- Inför beslut om väsentliga nätverksförändringar och -åtgärder

- För att hitta rätt ambitionsnivå i kontinuitetsplaner
- Då det annars är påkallat

I tillämpningsanvisning beskrivs regionens ramverk för att arbete med riskhantering gällande informationssäkerhet. Riskbedömning rekommenderas utgå från en fyra-gradig skala för sannolikhet och detsamma för konsekvens.

Enligt intervju arbetar regionledningskontoret med riskbedömningar och att identifiera hot och händelser som kan påverka informationssäkerheten på regionövergripande nivå Inom Regionledningskontoret finns Region Stockholm CERT (tidigare Region Stockholm SOC) som är regionens stödjande funktion inom it-säkerhet. Region Stockholm bevakar och analyserar fortlöpande cyberhoten och it-säkerhetsrelaterade incidenter och stödjer nämnder och bolag att upptäcka och hantera dessa. Detta sker genom råd och rekommendationer till utpekade kontaktytor i nämnder och bolag enligt uppgift. Uppföljning av rekommendationer kan ske av informationssäkerhetssamordnare på berörd nämnd eller bolag eller regionövergripande av regionledningskontoret.

SF IT uppger att det inte finns en stringens kring i vilken utsträckning de blir involverade avseende riskanalyser som sjukhusen gör. Ibland blir de kontaktade rörande ett pågående riskanalysarbete. Generellt framför de dock att de inte tar del av de riskanalyser som sjukhusen gör.

C.1.1 Pen-tester

Region Stockholm CERT vid regionledningskontoret genomför analyser av olika it-säkerhetsrelaterade hot och händelser och ger nämnder och bolag vägledning och rekommendationer kring dessa. Säkerhetstester genomförs på utvalda system i syfte att förebygga incidenter och resultaten delas med berörd nämnd/bolag. Enligt vissa av de intervjuade delas resultatet av CERT:s arbete dock endast vartannat år med sjukhusen vilket upplevs vara alltför sällan.

C.2 Regionens internkontrollarbete

Det framkommer i intervju att det inte är helt tydligt var olika IT-frågor för MTU ska hanteras. Från SF IT lyfts att samordningsproblem rörande IT-frågor kvarstår efter etableringen av serviceförvaltningen. Detta påtalas vara särskilt framträdande gällande MTU.

Det står föreskrivet i regionens riktlinjer för informationssäkerhet att samtliga ändringar ska kunna härledas till en ansvarig beställare. Rutiner ska fastställas för ändringshantering och testning och vara känd av berörda personer. Vid akuta ändringar ska dokumentation upprättas.

Vid problem med MTU kopplat till nätverket ska det felanmälas till SF IT vilket det finns en ärendehantering för. I intervju lyfts även att det kan finnas utrymme för tydligare fördelningsnycklar för kostnader som sjukhusen betalar för serviceförvaltningens arbete. Vidare lyfts i intervju att det skulle vara fördelaktigt med viss grundläggande IT-infrastruktur som inte finansieras av sjukhusen för att uppnå en grundläggande IT-säkerhet för regionen som helhet.

I de tjänsteöverenskommelser vi har tagit del av mellan sjukhus och SF IT finns angivet vilka kontaktvägar som ska användas vid anmälan av fel, leveransrelaterade frågor och avtalsinnehåll.

C.3.1 Incidentrapportering kopplat till nätverksansluten MTU

På regionens intranät finns information om IT-säkerhetsincidenter. CERT tillhandahåller råd och rekommendationer för att häva och /eller begränsa säkerhetsrelaterade incidenter genom att tillhandahåll expertkompetens, metoder och verktyg. Det anges att CERT prioriterar IT-säkerhetsincidenter utifrån direkt och potentiell påverkan på verksamheten utifrån fyra nivåer- från låg till kritisk. Prioriteringsnivåerna används av CERT för att prioritera hanteringstid och resurser för olika ärenden.

C.4 Karolinska universitetssjukhuset

C.4.1 Karolinskas arbete med risk- och sårbarhetsanalyser

I Karolinskas upprättade *Tillämpningsanvisningar för informationssäkerhet* anges att verksamheterna kontinuerligt ska genomföra riskanalyser för de informationstillgångar som är viktiga för verksamheten. Risker ska identifieras och bedömas utifrån konsekvens för sjukhuset om informationen inte är tillgängligt när det behövs (tillgänglighet), inte är korrekt (riktighet) eller om obehöriga fått tillgång till informationen (konfidentialitet) samt hur sannolikt det är att risken faktiskt uppstår. Konsekvens bedöms genom ett angivet ramverk utifrån olika parametrar (däribland patientsäkerhet) med fyra nivåer – lindrig, kännbar, allvarlig och katastrof. Sannolikhet bedöms genom ett ramverk med bakgrund om det upplevts tidigare och med vilken frekvens det tidigare har skett med fyra nivåer - mindre sannolikt, möjligt, sannolikt, mycket sannolikt. I tillämpningsanvisningarna finns även sju angivna uppgifter som ska ingå i varje dokumentation av en risk, t.ex. konsekvenser av risk och strategi för hantering av risk. Det anges att riskanalysverktyg och instruktioner finns tillgängligt på intranätet.

Det uppges i intervju att sjukhuset har upprättat egna rutiner och mallar för riskhantering av risker relaterat till MTU. Riskhantering ska utföras vid t.ex. egentillverkning, inför mjukvaruuppgradering/uppdatering av medicinteknisk produkt, driftsättning av eller förändringar i medicintekniska IT-system samt anslutning av medicinteknisk produkt mot nätverk.
PÅ MT finns, enligt uppgift, en riskhanteringsansvarig person som ansvarar för riskhanteringsprocessen enligt 14971 och 80001.

I intervju framförs att arbetet med ledningssystemet ISO 80001 inte kommit så långt som planerat. Generellt inom MT upplevs emellertid att det sker mycket arbetet med riskhantering och dokumentation av riskanalyser. Det ska i arbetet med informationssäkerhet även finnas dialog med sjukhusets informationssäkerhetssamordnare.

C.4.2 Karolinskas internkontrollplan 2020

I Karolinska universitetssjukhusets internkontrollplan 2020 bedöms följande områden omfatta en mycket hög risk (den högsta risk-nivån):

- begränsningar i dagens IT-systems funktionalitet och implementering
- bristande investeringsmedel för IT-utveckling
- brister i förvaltning avseende MTU riskerar att vi ej uppfyller lagstadgade EU-krav på hanteringen av MT

Vidare bedöms följande områden omfatta hög risk i sjukhusets internkontrollplan 2020 (näst högsta risk-nivån):

- nuvarande IT-struktur för informationsförsörjning på 1:a linjechefsnivå är ej tillräcklig
- brister i informationsspridning till alla nivåer kan leda till att regelefterlevnad ej uppnås

C.3.2 Karolinskas ärendehantering för nätverksansluten MTU

Enligt tillämpningsanvisningar för informationssäkerhet ska medarbetare rapportera avvikelser enligt anvisad rutin. Akuta IT-incidenter ska rapporteras till IT-driftorganisationen via exempelvis verksamheten IT-support. IT-incidenter som innebär en utrednings- eller åtgärdsfas ska enligt tillämpningsanvisningarna rapporteras till närmaste chef och till sjukhusets informationssäkerhetssamordnare.

Enligt intervju kontaktar MT-enheten incidentmanagers på SF IT och Karolinska IT beroende på incident. I intervju beskrivs att det finns en servicedesk på Karolinska som tar emot samtal om bl.a. incidenter. Om en incident eskalerar finns en eskaleringsordning med incidentmanagers som har ledningsfunktion att kalla in personal eller kalla in IT och chefsläkare. För några utvalda system finns även beredskapskedjor som är kontaktbara dygnet runt. Verksamhetschefer ska vidare säkerställa att det finns reservrutiner. Det finns även möjlighet att kontakta SF IT genom

de vanliga kontaktvägarna ifall ett problem uppstår. Under etableringen av Nya Karolinska sjukhuset (NKS) förekom en del utmaningar av systemmässig karaktär och då skedde, enligt intervju, mycket samverkan mellan MT-enheten, SF IT och Karolinska IT.

C.5 Danderyds sjukhus

C.5.1 Danderyds arbete med risk- och sårbarhetsanalyser

I den upprättad riktlinje, Informationssäkerhet – Riskhantering vid Danderyds sjukhus AB, Av riktlinjen framgår att informationssäkerhetssamordnaren ansvarar för att genomföra en hot-, risk- och sårbarhetsanalys inom informationssäkerhetsamordnaren minst en gång årligen. Riskbedömning samt eventuella förslag på riskbehandling ska dokumenteras. Vid vilka tillfällen riskanalyser ska genomföras följer regionledningskontorets tillämpningsanvisning för området. Processen för riskhantering ska ske genom följande steg:

1. Avgränsning (definiera analysobjektens omfattning)
2. Riskidentifiering (identifiera hot/risker/sårbarheter)
3. Riskanalys (analysera riskens omfattning)
4. Riskutvärdering och riskbehandling (analysera informationssäkerhetsriskens prioritet och behandling)
5. Effektutvärdering av åtgärder
6. Dokumentation, uppföljning och rapportering

Enligt riktlinjen ska risker delas in i strategiska risker, operativa risker, ekonomiska risker och compliance risker. Risker ska identifieras och bedömas utifrån konsekvens för sjukhuset samt hur sannolikt det är att risken faktiskt uppstår. Konsekvens bedöms genom ett angivet ramverk utifrån olika parametrar (däribland invånare/medarbetare och verksamhets/process) med fyra nivåer – ingen/försumbar, måttlig, betydande/allvarlig och mycket allvarlig/katastrof. Sannolikhet bedöms genom ett ramverk med bakgrund om det upplevts tidigare och med vilken frekvens det tidigare har skett med fyra nivåer - mycket liten sannolikhet, liten sannolikhet, stor sannolikhet och mycket stor sannolikhet.

I intervju beskrivs att riskanalyser görs men att det finns ett behov att arbeta mer med kvaliteten på riskstandarden, inte minst avseende MTU. För några år sedan påbörjades ett arbete för att införa riskhantering enligt ISO-80001 men som ännu inte har slutförts. Det har anställts en person som ska arbeta mer systematiskt med detta än som gjorts tidigare. Riskhanteringen utgår från dokument som Danderyds sjukhus själva har tagit fram.

C.5.2 Danderyds internkontrollplan 2020

Enligt upprättad riktlinje för riskhantering av informationssäkerhet sker eskalering av informationssäkerhetsrisker genom att informationssäkerhetssamordnaren lyfter risken/riskerna inom Sjukhusgemensam Service (SGS) ordinarie riskhanteringsarbete, Servicedirektören ansvarar för att informationssäkerhetsriskerna lyfts upp till den sjukhusövergripande interna kontrollplanenen. Sjukhusets ledningsgrupp ansvarar därefter för att värdera informationssäkerhetsriskerna utifrån riskfaktor och väsentlighet samt för att följa upp riskerna och säkerställa förebyggande arbete. I Danderyds sjukhus internkontrollplan 2020 bedöms följande områden omfatta en medelhög risk:

- Andelen implementerade säkerhetsåtgärder för informationssäkerhet understiger 50%

C.5.3 Danderyds ärendehantering för nätverksansluten MTU

Vid störningar eller incidenter används ett ärendehanteringssystem. Det uppges vara svårt att följa ärendet när det är registrerat. Det är en särskild funktion på Danderyds sjukhus som registrerar ärendet och följer upp det. Incidentrapportering eskaleras till regionledningskontorets CERT-funktion. Eventuella intrångsförsök ser däremot endast SF IT som äger nätverken. Enligt intervjuer med Danderyds sjukhus pågår det en upphandling av ett ärendehanteringssystem vid

tiden för granskningen

C.6 Bedömning revisionsfråga C

Vår bedömning är att det finns en väl genomarbetad och tydligt dokumenterad process för riskhantering av nätverksansluten MTU utifrån ansvar och utformning. Vidare finns en funktion, Region Stockholm CERT vid regionledningskontoret, som genomför analyser av olika it-säkerhetsrelaterade hot och händelser samt ger nämnder och bolag vägledning och rekommendationer kring dessa. CERT utför även penetrationstester för regionens nämnder och bolag. Riktlinjer anger hur internkontrollarbetet ska vara utformat och återrapporteras. Båda sjukhus har dessutom tagit fram egna stöddokument för arbetet med riskhantering.

Vidare finns stöd gällande incidentrapportering från regionledningskontorets CERT-funktion samt att sjukhusen har rutiner för hur det ska ske och eskaleras.

Dock lyfts samordningsproblematiken mellan nämnder/bolag och SF IT även avseende riskhantering. Det upplevs inte heller finnas en fullt tydlig bild hur ärendehanteringen är tänkt att fungera i regionen. Båda sjukhusen, och i synnerhet Danderyds sjukhus, påtalar en utvecklingspotential när det gäller systematiskt riskhanteringsarbete. Vissa av de intervjuade menar att CERT skulle kunna delge bolagen/nämnderna resultatet av sina analyser oftare. Det är även värt att notera skillnaden i riskområden i de båda sjukhusens internkontrollplaner avseende IT-säkerhet.

2020-10

Anders Hägg

Louise Tornhagen

av Regionrevisorerna för Region Stockholm enligt de villkor och under de förutsättningar som framgår av avtal från den 2020-02-26. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.