Region Västmanland

Regionens revisorer 2019-10-03

Hans Strandlund

Till
Regionstyrelsen för svar
Regionfullmäktige för kännedom

Uppföljning och fördjupad informationssäkerhetsgranskning

PwC har på uppdrag av Region Västmanlands revisorer genomfört en uppföljning och fördjupad granskning avseende regionens informationssäkerhetsarbete. Revisorerna har uppmärksammat vikten av ett systematiskt säkerhetsarbete för att säkerställa att medarbetare och patienters integritet skyddas då digitaliseringen ökar och regionens verksamheter blir mer och mer beroende av informationssystem. Granskningen har syftat till att besvara följande revisionsfråga: Bedriver regionstyrelsen ett ändamålsenligt arbete med informationssäkerhet och har tidigare identifierade brister åtgärdats?

Vi bedömer sammantaget att regionstyrelsen delvis uppfyller revisionsfrågan.

Ur rapportens bedömningar kan bland annat noteras att samtlig dokumentation som tillhandahållits är aktuell och giltig, dock har inte informationssäkerhetspolicyn uppdaterats utifrån tidigare granskningsrekommendationer. Ett ledningssystem för informationssäkerhet finns men det saknas fortfarande ett visst antal punkter från ISO/IEC27001 Annex A och det genomförs ingen uppföljning på huruvida verksamheterna efterlever riktlinjerna. Roller och ansvar inom informationssäkerhet är definierat och framgår i informationssäkerhetspolicyn, dock saknas det utöver detta ett tydligt ansvar för genomförande av säkerhetsåtgärder. Regionen har tagit fram processer för att utföra stickprov på behörigheter i patientjournalsystemet, dock har det inte genomförts några stickprov på behörigheterna. Processer, rutiner och verktyg är implementerade för att säkerställa att regionens medarbetare har rätt behörighetstilldelningar i patientjournalsystemet. Det har även utformats dokumentation kring behörighetstilldelning och åtkomst till patientuppgifter.

Utifrån våra iakttagelser bör nämnas att många åtgärder redan identifierats och eventuellt påbörjats av regionen avseende de utvecklingsområden som uppmärksammats i granskningen. Beaktat detta rekommenderar vi regionstyrelsen att uppmärksamma följande i kommande arbete gällande informationssäkerhet:

- Region Västmanland bör se över åtgärdsmålen i ISO/IEC 27001 för att säkerställa att regionen täcker samtliga för att i framtiden kunna vara certifieringsbara.
- Säkerställ att styrande dokument är reviderade med lämplig intervall samt att informationssäkerhetspolicyn och riktlinjerna följs upp regelbundet.
- Inför systematisk dokumentation av vilka informationssäkerhetsåtgärder som tillämpats i verksamheten.
- Specificera i den kommande verksamhetsplanen de aktiviteter som ska genomföras i syfte att främja en god säkerhetskultur.
- Ett fortsatt arbete gällande riktlinjerna generellt behöver ses över.
- Region Västmanland bör utforma metoder och riktlinjer kring incidenthantering och informationssäkerhet i upphandling.

Region Västmanlands revisorer Telefon: 010-212 61 18
c/o PwC
Box 885
721 23 VÄSTERÅS

Regionens revisorer 2019-10-03

Hans Strandlund

- Inkludera informationssäkerhetsarbetet i regionens framtida plan och budget.
- Specificera och kommunicera ut tydliga roller och ansvar för säkerhetsåtgärder i verksamheten.
- Ta fram styrdokument och processer för kravställning mot informationssäkerhetsarbetet.
- Gör e-utbildningen obligatoriskt för att säkerställa att alla medarbetare genomgår den. Se även till att ha regelbundna utbildningstillfällen och inte enbart vid nyanställning.
- Region Västmanland bör göra uppföljning av riskanalyser för behörighetstilldelning samt ta fram gallringsrutiner gällande behörighetssystemet. Regionen bör även se över kontinuerliga stickprov i patientjournalsystemet.
- Region Västmanlands lösenordspolicy bör stärkas.

Iakttagelser och bedömningar i sin helhet framgår i bifogad rapport. Revisorerna önskar svar från regionstyrelsen senast 2020-01-14.

FÖR REGIONENS REVISORER

Hans Strandlund
Ordförande Revisor

Region Västmanlands revisorer Telefon: 010-212 61 18
c/o PwC
Box 885
721 23 VÄSTERÅS

Uppföljning och fördjupad informationssäkerhets-granskning

Region Västmanland

pwc

Revisionsrapport

Innehållsförteckning

Sammanfattning

PwC har på uppdrag av Region Västmanlands revisorer genomfört en uppföljning och fördjupad granskning avseende regionens informationssäkerhetsarbete. Revisorerna har uppmärksammat vikten av ett systematiskt säkerhetsarbete för att säkerställa att medarbetare och patienters integritet skyddas då digitaliseringen ökar och regionens verksamheter blir mer och mer beroende av informationssystem. Granskningen har syftat till att besvara följande revisionsfråga:

Bedriver Regionstyrelsen ett ändamålsenligt arbete med informationssäkerhet och har tidigare identifierade brister åtgärdats?

Vi bedömer sammantaget att Region Västmanland **delvis uppfyller** revisionsfrågan. Den övergripande bedömningen grundar sig på en sammanvägd bedömning av granskade kontrollmål samt följande centrala iakttagelser och bedömningar:

Kontrollmål 1 – Har regionen aktuella och ändamålsenliga styrande dokument och riktlinjer inom informationssäkerhet som är implementerade i verksamheten?

Bedömning - Samtlig dokumentation som tillhandahållits är aktuell och giltig, dock har inte informationssäkerhetspolicyn uppdaterats utifrån tidigare gransknings rekommendationer. Regionen tillämpar ISO/IEC27001 Annex A, av dessa ca 140 aktiviteter har ca 130 genomförts. Detta sammantaget gör att PwC bedömer kontrollmålet som **delvis uppfyllt.**

Kontrollmål 2 – Fungerar regionens ledningssystem för informationssäkerhet ändamålsenligt?

Bedömning - Ett ledningssystem för informationssäkerhet finns men det saknas fortfarande ett visst antal punkter från ISO/IEC27001 Annex A och det genomförs ingen uppföljning på huruvida verksamheterna efterlever riktlinjerna. Detta sammantaget gör att vi bedömer kontrollmålet som **delvis uppfyllt**.

Kontrollmål 3 – Arbetar regionen ändamålsenligt med uppföljning kring efterlevnad av informationssäkerhet?

Bedömning - I enlighet med ledningssystemet ska råden göra uppföljning av genomförda analyser samt föreslå prioriteringar av åtgärder, dock har inte någon dokumentation som styrker genomförandet erhållits. Detta sammantaget gör att vi bedömer kontrollmålet som **delvis uppfyllt.**

Kontrollmål 4 – Finns det en tydlig organisation, roll och ansvarsfördelning kopplat till informationssäkerhet?

Bedömning - Roller och ansvar inom informationssäkerhet är definierat och framgår i informationssäkerhetspolicyn, dock saknas det utöver detta ett tydligt ansvar för genomförande av säkerhetsåtgärder. Sammantaget bedömer PwC kontrollmålet som **delvis uppfyllt.**

Kontrollmål 5 – Är kravställningen mot IT-organisationen ändamålsenlig?

Bedömning - Styrdokument för IT-säkerhet i drift och förvaltning existerar, dock finns det inga styrdokument eller processer gällande kravställning för informationssäkerhet. Med detta som bakgrund bedöms regionen **delvis uppfyllt** kontrollmålet.

Kontrollmål 6 – Arbetar regionen aktivt för att främja en god säkerhetskultur inom informationssäkerhetsområdet?

Bedömning - Främjandet av en god säkerhetskultur finns inte dokumenterat i en systematisk genomförandeplan. Det har tillhandahållits en verksamhetsplan för prioriterade fokusområden för 2019, dock är inte aktiviteter för genomförandet specificerat. Detta sammantaget gör att vi bedömer kontrollmålet som **delvis uppfyllt**.

Kontrollmål 7 – Är processer för att kontinuerligt utföra stickprov på behörigheterna i patientjournalsystemet implementerade?

Bedömning - Sammanfattningsvis har regionen tagit fram processer för att utföra stickprov på behörigheter i patientjournalsystemet, dock har det inte genomförts några stickprov på behörigheterna. Detta sammantaget gör att vi bedömer kontrollmålet som **inte uppfyllt.**

Kontrollmål 8 – Är erforderliga processer på plats för att säkerställa behörigheterna i patientjournalsystemet?

Bedömning - Processer, rutiner och verktyg är implementerade för att säkerställa att regionens medarbetare har rätt behörighetstilldelningar i patientjournalsystemet. Det har även utformats dokumentation kring behörighetstilldelning och åtkomst till patientuppgifter. Detta sammantaget gör att vi bedömer kontrollmålet som **uppfyllt.**

Kontrollmål 9 – Finns en god kontohantering implementerad?

Bedömning - Arbetet med kontohanteringen bör ses över utifrån ett säkerhetsperspektiv då flera konton utgör ett antal risker för regionen. Detta sammantaget gör att vi bedömer kontrollmålet som **inte uppfyllt.**

Kontrollmål 10 – Finns det en kontinuerlig rutin för att revidera regionens konton?

Bedömning - Stora delar av processerna för att revidera regionens konton är automatiserade, dock fungerar inte rutinen ändamålsenligt då det upptäcktes en hel del konton som inte bör existera. Detta sammantaget gör att vi bedömer kontrollmålet som **inte uppfyllt.**

1. Inledning

1.1 Bakgrund

Med hälso- och sjukvårdens digitalisering blir frågan om informationssäkerhet allt viktigare för att säkra patienternas integritet och säkerhet. Mellan 2016 - 2018 genomfördes ett flertal granskningar inom området där flera brister uppmärksammades:

- Fysisk säkerhet av verksamhetskritisk digital information (2015)
- Teknisk IT-granskning (2016)
- Granskning av informationssäkerhet (2017)
- Granskning av säkerhet i patientsystemet och hantering av patientjournaler (2018)

Vår tids nya teknik är digitalisering och den behöver användas i effektiviseringens syfte. Digitalisering är ett globalt fenomen och för landstingen och regionerna innebär det att allt fler aktiviteter inom verksamheterna i olika grad är beroende av informationssystem. Informationen ska inte bara vara tillgänglig utan lika viktigt är det att den håller rätt kvalitet och kan hanteras utan att känsliga uppgifter förändras eller sprids till obehöriga. Det medför att både informationen i sig och de system som används för att förvara och överföra informationen behöver skyddas. För att skapa ett informationssäkerhetsarbete som motsvarar verksamheternas behov ställs krav på organisatorisk styrning och kontroll.

Denna granskning är en uppföljning och fördjupning av delar från tidigare granskningar för att säkerställa hur väl de identifierade bristerna har åtgärdats samt hur informationssäkerhetsarbetet har utvecklats.

1.2 Syfte och Revisionsfråga

Revisorerna har med utgångspunkt i väsentlighet och risk beslutat att granska regionens fortsatta arbete med informationssäkerhet.

Den övergripande revisionsfrågan är:

Bedriver regionstyrelsen ett ändamålsenligt arbete med informationssäkerhet och har tidigare identifierade brister åtgärdats?

1.3 Revisionskriterier

Offentlighets- och sekretesslag (2009:400).

Myndigheten för samhällsskydd och beredskaps (MSB) föreskrifter om landstings och kommuners risk- och sårbarhetsanalyser (MSBFS 2015:4 & 2015:5).

Socialstyrelsens föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40).

Patientdatalag (2008:355).

Regionens regler, policys och riktlinjer motsvarande informationssäkerhet.

MSB Strategi för stärkt informationssäkerhet inom vård och omsorg.

1.4 Kontrollfrågor

- Har regionen har aktuella och ändamålsenliga styrande dokument och riktlinjer inom informationssäkerhet som är implementerade i verksamheten?
- Fungerar regionens ledningssystem för informationssäkerhet ändamålsenligt?
- Arbetar regionen arbetar ändamålsenligt med uppföljning kring efterlevnad av informationssäkerhet?
- Finns det en tydlig organisation, roll och ansvarsfördelning kopplad till informationssäkerhet?
- Är kravställningen mot IT-organisationen är ändamålsenlig?
- Arbetar regionen aktivt för att främja en god säkerhetskultur inom informationssäkerhetsområdet?
- Är processer för att kontinuerligt utföra stickprov på behörigheterna i patientjournalsystemet implementerade?
- Är erforderliga processer på plats för att säkerställa behörigheterna i patientjournalsystemet?
- Finns en god kontohantering finns implementerad?
- Finns det en kontinuerlig rutin för att revidera regionens konton?

1.5 Avgränsning

Granskningen kommer fokusera på identifierade brister i regionens informationssäkerhetsarbete. Uppföljning av tidigare kontrollmål kommer att vara utgångspunkten i granskningen.

1.6 Metod

- Granskning av relevant dokumentation så som policy och riktlinjer.
- Intervjuer med berörda delar av verksamheten samt stickprov. Granskningen omfattar intervjuer med informationssäkerhetssamordnare, systemägare och verksamhetschefer. Vid stickproverna intervjuade vi individer som arbetar i den dagliga verksamheten så som ansvariga chefer, tjänstemän och systemägare.
- En teknisk del av granskningen genomfördes genom PwC:s koncept Baseline Security Assessment. Denna granskningsdel genomfördes av PwC Data Analytics. De genomförde kontroller av kontohanteringen och inställningar som hämtats ut från Active Directory med hjälp av script.

2. Iakttagelser och bedömningar

2.1 Kontrollmål 1 – Styrandedokument och riktlinjer

Har regionen aktuella och ändamålsenliga styrande dokument och riktlinjer inom informationssäkerhet som är implementerade i verksamheten?

Iakttagelser

I tidigare granskning ”*Granskning av informationssäkerhet*” som genomfördes hos Region Västmanland framkom det att regionen hade tagit fram flertalet styrande dokument, se specifikation enligt bilaga 1. Utgångspunkten i Region Västmanlands ”*Informationssäkerhetspolicy*” (giltig från och med 2014-09-24) är att regionen ska bedriva ett systematiskt arbete med informationssäkerhet som bygger på riskanalyser. Vidare framgår det vilken inriktning regionen följer, vilket är ISO/IEC 27001. I tidigare granskning uppmärksammades det att regionens samtliga styrande dokument var aktuella och giltiga förutom informationssäkerhetspolicyn. I Region Västmanlands informationssäkerhetspolicy beskrivs tio principer som ska styra regionens arbete med informationssäkerhet. Vid tidigare granskningar uppmärksammandes det att av de tio principerna som nämns i policyn hade fem implementerats i riktlinjer. Dessa var riktlinjer för riskanalys, informationsklassning, informationssäkerhet för medarbetare, drift och förvaltning av IT-miljö och krav på spårbarhet för patientuppgifter. Gällande uppföljning av principerna som ska styra regionens arbete med informationssäkerhet har arbetet gått framåt. Inga riktlinjer har utformats, men vid upphandlingar avseende informationssäkerhet har stödmaterial publicerats för inköp i ledningssystemet som bland annat föreskriver riskanalyser och informationsklassning vid uppstart av upphandlingar. Någon riktlinje för incidenthantering har inte utformats men Centrum för digitalisering har dokumenterade rutiner för incidenthantering.

I denna granskning har fokus varit på stickprov ute i verksamheten för att identifiera att styrande dokument är implementerade. Enligt intervjusvar med medarbetarna framkom det att dokument som avser informationssäkerhet är svåra att hitta vilket kan resultera i att riktlinjerna inte alltid efterlevs.

Medarbetare i Region Västmanland är medvetna om dokumentet “*Informationssäkerhet för medarbetare*” (giltig från och med 2016-12-05) regionen har tagit fram, avseende samtliga medarbetare som använder regionens information i olika aspekter, inklusive uppdragstagare och externa leverantörer. Enligt dokumentet är det verksamhetschefens ansvar att se till att medarbetarna får den utbildning som krävs samt tillgång till tydlig information gällande informationssäkerhet. Vidare framgår det krav på medarbetarna gällande lösenordshantering och användning av IT-utrustning samt att användning av regionens internetbaserade tjänster såsom internet och e-post för privat bruk inte är tillåtet. Det finns även riktlinjer gällande hantering av patientuppgifter och ansvarsskyldighet för att medarbetare ska vara uppmärksamma när det kommer till inkommande e-post. Medarbetare är även medvetna om att de företräder regionen i alla sammanhang och bör beakta regionens värdegrund.

Bedömning

I tidigare granskning uppmärksammades det att regionens samtliga styrande dokument var aktuella och giltiga förutom informationssäkerhetspolicyn. Det framkom att hälften av principerna beskrivna i informationssäkerhetspolicyn hade täckning i riktlinjer, vilket granskningen visar även denna gång. Utöver detta fanns det enbart en riktlinje avseende åtkomst till patientuppgifter och inte en för annan känslig information. Vid tidigare granskning rekommenderades att dokumentet *”Informationssäkerhet för medarbetare”* skulle rubriceras som en instruktion och inte en riktlinje, detta har inte än åtgärdats. Enligt stickprov som genomfördes framkom att det inom verksamheterna existerar svårigheter med att hitta dokumentation avseende informationssäkerhet, vilket kan leda till ett gap i implementeringen. Därmed bedöms kontrollmålet **delvis uppfyllt.**

2.2 Kontrollmål 2 – Ledningssystem

Fungerar regionens ledningssystem för informationssäkerhet ändamålsenligt?

Iakttagelser

Det uppmärksammades i tidigare granskning att Region Västmanland utifrån verksamhetsplanen för informationssäkerhet från 2018 hade en målsättning att regionen ska vara certifieringsbar enligt SS-ISO/IEC27001. I den tidigare verksamhetsplanen saknades det en tidsplan och åtgärder för att införa informationssäkerhetsarbetet i enlighet med SS-ISO/IEC27001. Region Västmanland har fortsatt arbetet sedan tidigare granskning och utav samtliga aktiviteter i Annex A har informationssäkerhetssammordnaren bedömt att regionen uppfyller 130 av 140.

I verksamhetsplanen framgick det att det skulle tas fram ett flertal metoder och riktlinjer, samtliga är uppfyllda förutom följande:

- Framtagning av metod och riktlinjer kring incidenthantering
- Informationssäkerhet i upphandlingar

Det saknas en metod och riktlinjer kring incidenthantering i ledningssystemet men Centrum för digitalisering har dokumenterat rutiner. Vidare saknas det även metod och riktlinjer för informationssäkerhet i upphandlingar, men det har publicerats stödmaterial för inköp i ledningssystemet, som bland annat föreskriver riskanalyser och informationsklassning vid uppstart av upphandlingar.

Det finns ett IT-säkerhetsråd som sker en gång i månaden, då huvudansvariga inom drift och nätverk samlas för att diskutera den tekniska säkerheten. Vidare finns det ett informationssäkerhetsråd som sammanträder fem gånger om året med syftet att informera verksamheternas medarbetare gällande riktlinjer som ska efterlevas.

I dagsläget är det säkerhetsorganisationen som ansvarar för att skapa riktlinjerna där antingen regiondirektör eller hälso- och sjukdirektör skriver under. Det finns en process där det sker utskick av information via intranätet för att nå ut till regionens medarbetare, men enligt intervjusvar anses informationen vara svår att hitta då ledningssystemet innehåller mängder av dokumentation.

Bedömning

Regionens ledningssystem för informationssäkerhet fungerar delvis ändamålsenligt. Det saknas fortfarande ett visst antal punkter från ISO/IEC27001 Annex A, men är något som informationssäkerhetssamordnaren arbetar med. Det existerar i dagsläget riktlinjer för informationssäkerhet men enligt ett stickprov av medarbetare följer regionen inte upp efterlevnaden (se kontrollmål 3). Medarbetarna anser att det inte finns några tydliga roller och ansvar eller direktiv från ledningen på vad som måste göras (se kontrollmål 4). Sammanfattningsvis finns det utformade rutiner kring incidenthantering och publicerat stödmaterial i ledningssystemet för informationssäkerhet i upphandlingar. Medarbetarna inom regionen är medvetna om att ledningssystemet för informationssäkerhet existerar, dock anser de att direktiv från ledningen som avser riktlinjerna är bristande. Därmed bedömer vi att regionen **delvis uppfyller** kontrollmålet.

2.3 Kontrollmål 3 – Uppföljning och efterlevnad

Arbetar regionen ändamålsenligt med uppföljning kring efterlevnad av informationssäkerhet?

Iakttagelser

Enligt informationssäkerhetsamordnaren har regionen en internrevision som genomför uppföljningen kring regionens efterlevnad av informationssäkerhet och ställer krav mot verksamhetschefen. Dock genomför inte internrevisionen någon formell kontroll kring efterlevnaden av riktlinjer och dokumentation.

Region Västmanland har en bra styrning av informationssäkerhet inom verksamheterna, dock rapporteras endast vissa delar av internrevisionens resultat av uppföljning och efterlevnad till ledningen. Vidare finns det rutiner och instruktioner för loggranskning av vårdtillfällen och medarbetarna är medvetna om hur de skall hantera ett intrång eller en incident. Regionen använder riskbedömningsverktyget VIRA för att hålla sig uppdaterade om information kring informationssäkerhet samt hot och brott som påverkar omvärlden.

Bedömning

Internrevisionen rapporterar delvis medarbetarnas efterlevnad av informationssäkerhet till ledningen. I enlighet med ledningssystemet ska råden utföra uppföljningar av genomförda analyser samt föreslå prioriteringar av åtgärder, dock har det inte erhållits någon dokumentation som styrker dessa genomföranden. PwC har efterfrågat en systematisk genomförandeplan i förhållande till informationssäkerhetsarbetet, en sådan har inte tillhandahållits. Detta ligger till grund för bedömningen att regionen **delvis uppfyller** kontrollmålet.

2.4 Kontrollmål 4 – Roller och ansvar

Finns det en tydlig organisation, roll och ansvarsfördelning kopplat till informationssäkerhet?

Iakttagelser

I dokumentationen ”*Informationssäkerhet för medarbetare*” framgår det tydliga riktlinjer för hur medarbetarna ska hantera information på ett säkert sätt. Enligt intervjusvar uppmärksammas det att IT-avdelningens roller inom informationssäkerhet är tydligt definierade samt att respektive chef ansvarar för att medarbetarna har den rätta kunskapsnivån som krävs, dock finns det enbart en informationssäkerhetssamordnare till en stor organisation som ansvarar för samordning och utveckling av informationssäkerhetsarbetet.

I den tidigare granskningen rekommenderades att regionen skulle se över ansvaret för implementeringar av säkerhetsåtgärder. Enligt informationssäkerhetsamordnaren har en åtgärd skett och ansvaret för att ta fram säkerhetsåtgärder har tilldelats förvaltningsobjekten.

Vid en tidigare granskning önskade informationssäkerhetssamordnaren att ett informationssäkerhetsombud skulle finnas tillgängligt ute i verksamheterna för att stötta i informationssäkerhetsarbetet. Någon åtgärd har ännu inte utförts och efterlevnaden sker fortfarande inte ändamålsenligt. I intervjusvar framgår det att informationssäkerhet bör finnas med som en stående punkt på agendan i den dagliga verksamheten för att säkerställa att ämnet inte prioriteras bort under arbetsplatsträffar eller liknande.

Bedömning

Vår bedömning är att informationssäkerhetsarbetet är väldefinierat inom organisationen. Med detta som bakgrund bedöms Region Västmanland **uppfylla** kontrollmålet gällande en tydlig organisation, roll och ansvarsfördelning kopplat till informationssäkerhet.

2.5 Kontrollmål 5 – Kravställning

Är kravställningen mot IT-organisationen ändamålsenlig?

Iakttagelser

I intervjusvar uppmärksammas det att regionen för tillfället inte har styrdokument eller processer gällande kravställning som specifikt avser informationssäkerhet. Däremot finns det styrdokument för IT-säkerhet i drift och förvaltning. Dessa styrdokument kompletteras med lokala instruktioner och rutiner från Centrum för digitalisering. Det framkommer under intervju att Centrum för digitalisering samarbetar med informationssäkerhetsamordnaren som kravställer och som finns tillgänglig vid behov.

Bedömning

Styrdokument för IT-säkerhet i drift och förvaltning existerar, dock finns det inga riktlinjer eller processer gällande kravställning för informationssäkerhet. Med detta som bakgrund bedöms regionen **delvis uppfyllt** kontrollmålet.

2.6 Kontrollmål 6 – Säkerhetskultur

Arbetar regionen aktivt för att främja en god säkerhetskultur inom informationssäkerhetsområdet?

Iakttagelser

I dokumentet ”*Informationssäkerhet för medarbetare*” framgår det tydligt hur verksamhetens medarbetare ska hantera information i alla olika avseenden. Vidare framgår det i ”*Region Västmanlands Organisation för systematiskt säkerhetsarbete*” hur regionens säkerhetsorganisation ska arbeta för att skapa en struktur och kultur som stödjer styrning och uppföljning av regionens systematiska säkerhetsarbete.

I tidigare granskning framkom det att Region Västmanland hade ambitionen att ta fram obligatoriska utbildningar för medarbetarna. Sedan dess har regionen lanserat en e-utbildning för informationssäkerhet under 2018, som dock inte är obligatorisk. Enligt intervjusvar finns det inte tillräckligt med förutsättningar att fokusera på riktlinjer eller utbildning gällande informationssäkerhet då vikten av fokus ligger på ens egna arbetsuppgifter. Det framkommer även i intervjusvar att utbildning inom informationssäkerhet är prioriterat för de nyanställda och inte medarbetarna som under en längre tid har arbetat inom regionen.

Verksamhetschefer försöker genomföra utbildningen under arbetsplatsträffar (APT) för att säkerställa att medarbetarna tar del av informationen, dock minskar utfallet av antalet genomförda tillfällen på grund av att e-utbildningen inte är obligatorisk, detta är något som informationssäkerhetssamordnaren vill ändra på.

I dokumentet *”Region Västmanlands organisation för systematiskt säkerhetsarbete”* specificeras att Kris- och katastrofmedicinska rådet ska ta fram planering för utbildning och övningar utifrån inventering av utbildningsbehov avseende fortbildning och kompetensutveckling inom området. Medarbetare har under det föregående året genomfört en GDPR-utbildning. Enligt intervjusvar planerar Centrum för digitalisering gemensamt med informationssäkerhetsamordnaren en utbildning i form av övningar, där medarbetarna får lära sig att hantera riktiga attacker.

I regionens verksamhetsplan *”Verksamhetsplan Informationssäkerhet 2019”* framgår det att under 2019 kommer ytterligare insatser gällande informationssäkerhet införas. I enlighet med verksamhetsplanen ska även arbetet med GDPR och NIS fortsätta samt följas upp. Ett ytterligare fokusområde som ska ses över under slutet av 2019 är civilt försvar/robusta IT-relaterade tjänster som omfattas av lagstiftning för att säkerställa att de uppfyller kraven.

Bedömning

Det finns en medvetenhet när det kommer till säkerhetskulturen vilket underlättar arbetet gällande informationssäkerhet i Region Västmanland och under året som gått har aktiviteter genomförts för att höja medvetenheten ytterligare. En ny informationssäkerhetsutbildning lanserades under 2018 och medarbetare utbildades i GDPR. Utformandet av utbildning gällande attacker är även under bearbetning vilket kommer underlätta informationssäkerhetsarbetet.

Främjandet av en god säkerhetskultur specificeras i intervjusvar men det är inte dokumenterat i en systematisk genomförandeplan. Det har tillhandahållits en verksamhetsplan för prioriterade fokusområden för 2019, dock är inte aktiviteter för genomförandet specificerat. Vidare fortsätter arbetet med GDPR, NIS och civilt försvar inom regionen. Därmed bedöms Region Västmanland **delvis uppfylla** kontrollmålet gällande ett aktivt arbete för att främja en god säkerhetskultur inom informationssäkerhetsområdet.

2.7 Kontrollmål 7 – Stickprov i patientjournalsystemet

Är processen för att kontinuerligt utföra stickprov på behörigheterna i patientjournalsystemet implementerade?

Iakttagelser

I den tidigare granskningen som genomfördes uppmärksammades att det inte fanns någon process för att kontinuerligt utföra stickprov på behörigheterna i patientjournalsystemet. Enligt intervjusvar har regionen ett verktyg för att kunna göra uppföljningar av utdelade behörigheter i patientjournalsystemet. Verktyget har även kompletterats av riktlinjer med tvingande regler för att kvartalsvis göra uppföljning av samtliga utdelade behörigheter, dock har inga stickprov i patientjournalsystemet genomförts enligt verksamhetscheferna.

Bedömning

Sammanfattningsvis har regionen tagit fram och implementerat processer för att utföra stickprov på behörigheter i patientjournalsystemet, dock har inga sådana genomförts. Detta sammantaget gör att PwC bedömer kontrollmålet som **inte uppfyllt**.

2.8 Kontrollmål 8 – Behörighetsprocesser

Är erforderliga processer på plats för att säkerställa behörigheterna i patientjournalsystemet?

Iakttagelser

Vid tidigare granskning fanns det ingen praktisk tillämpbar metod för att genomföra stickprov på behörigheter i patientjournalsystemet dock var detta ett pågående arbete. Enligt *“Journalföring och behandling av personuppgifter i hälso- och sjukvården”* ska vårdgivaren ansvara för rutiner av ändringar och regelbundet följa upp behörigheter i patientjournalsystemet som ska vara uppdaterade oavsett nyanställning, byte av eller vid avslutad tjänst.

Sedan tidigare granskning har regionen utformat dokumentet *”Beställning av Cosmicbehörigheter i HSA-Användarmanual”* där det framgår att tilldelning av behörigheter ska ske utifrån medarbetarens yrkesroll i verksamheten. Objektägare har tillsammans med verksamheten definierat grundbehörigheter utifrån arbetsbeskrivningar. Vidare framgår det i dokumentet *”Tilldelning av behörigheter i journalsystem m.m.”* tydligt att användare tilldelas behörigheter i journalsystemet i enlighet med deras yrkesroll. På uppdrag av verksamhetschefen ansvarar HSA-redaktören för att rätt behörigheter beställs och återfinns i *“Matris över innehåll i grundbehörigheter Cosmic”.*

HSA-redaktören ansvarar för att:

- Beställa Cosmicbehörighet samt diverse uthopp i HSA, vilket utfärdas av respektive förvaltning.
- Cosmicbehörigheter avbeställs när en person slutar.
- Lägga till/ta bort medarbetaruppdrag för personer och kontrollera vilka som har medarbetaruppdrag på den aktuella enheten och se till att det är korrekt.

I dokumentationen *”Åtkomst till patientuppgifter i journal”* framgår de behörigheter som medarbetarna har till patientjournalerna. Vid behov av dessa ska en analys genomföras för att undvika risken att medarbetarna får högre behörigheter än vad som framgår i arbetsbeskrivningen.

I tidigare granskning ”*Granskning av säkerhet i patientsystem och hantering av journaler*” från 2018 arbetade regionen med att utveckla en rapport i DUVA som definierar medarbetarnas behörigheter. Sedan denna granskning har informationssäkerhetsamordnaren slutfört denna rapport som är ett verktyg för verksamhetscheferna att kunna kontrollera och säkerhetsställa behörigheter för respektive medarbetare.

I intervjusvar framkommer det att grupperingen Förvaltningen för Elektroniska journaler har upprättat instruktioner som verksamheterna ska följa för att säkerställa att användare har rätt behörigheter. Därefter har varje klinik med verksamhetschef en skyldighet att upprätta egna rutiner och kontrollfunktioner så att behörighetssättningen är och förblir korrekt i patientjournalsystemet. Det uppmärksammades i intervjusvar med verksamheten att synen på upprättandet av egna rutiner och kontrollfunktioner skiljer sig beroende på vilken klinik det gäller. Några kliniker har upprättat kompletterande rutiner och kontrollfunktioner medan andra ser att instruktionen som Förvaltningen för Elektroniska journaler utformat är tillräckliga. Ingen dokumentation från klinikerna har anskaffats för att styrka eventuella kompletterande rutiner eller kontrollfunktioner utöver de som Förvaltningen för Elektroniska journaler tillhandahållits.

Bedömning

Processer, rutiner och verktyg är implementerade för att säkerställa att medarbetare har rätt behörighetstilldelningar i patientjournalsystemet. Det har även utformats

dokumentation kring behörighetstilldelning och åtkomst till patientuppgifter. Verktyget som arbetats fram gör det möjligt att skapa rapporter som ska användas som underlag för verksamhetschefer för att kontrollera och säkerställa behörighetstilldelning för respektive medarbetare. Därmed bedöms Regionen **uppfylla** kontrollmålet.

2.9 Kontrollmål 9 – Kontohantering

Finns en god kontohantering finns implementerad?

Iakttagelser

I tidigare granskning uppmärksammades det att det saknades loggning och spårbarhet på otillåtet förändrade villkor samt automatiserade processer för monitorering och inventering av administrativa konton. Utifrån denna uppföljning av granskning som genomförs avseende regionens kontohantering går det att utläsa att det fortfarande finns aktiva konton med administrationsrättigheter som försvårar spårbarheten och ansvaret. Vidare saknas det fortfarande automatiserade processer för att kartlägga regionens administrativa konton.

Utifrån den tekniska granskningen ”Baseline Security Assessment” som genomfördes på plats hos Region Västmanland den 8 maj 2019 gällande kontohantering, kunde PwC fastställa att säkerhetsinställningarna för lösenord bör utvärderas. Sårbarheter har upptäckts och återkoppling om detta har förmedlats till regionen för hantering.

Bedömning

Analysen som genomfördes hos Region Västmanland visar att arbetet med kontohanteringen bör ses över utifrån ett säkerhetsperspektiv då flera konton utgör ett antal risker för regionen. Därmed bedöms regionen **inte uppfylla** kontrollmålet.

2.10 Kontrollmål 10 – Rutin för revidering av konton

Finns det en kontinuerlig rutin för att revidera regionens konton?

Iakttagelser

Vid den tidigare granskningen som genomfördes saknades det automatiserade processer för att kontrollera livslängden av regionens konton. Dessa innefattade om utloggning efter en viss inaktivitet skedde, om loggning av åtkomst till låsta konton saknades och om det existerade en övervakning av huruvida användarkonton användes utanför det vanliga användarbeteendet.

Resultatet från uppföljningsgranskningen visade på att rutinen för att revidera regionens konton är i stora delar automatiserad då de styrs utifrån personalsystemet och HSA-katalogen. Region Västmanland följer HSA regelverket Inera och för manuellt upplagda användare har HSA-redaktörerna i verksamheten ansvaret för att kvartalsvis stämma av att dessa användare är korrekta. Påminnelse avseende användare skickas ut från den centrala förvaltningen. Utveckling pågår för att i framtiden underlätta arbetet för HSA-redaktörer när det kommer till avstämning och uppföljning av konton.

När det gäller användare såsom konsulter eller leverantörer som läggs upp direkt i AD, är rutinen att dessa är tidsbegränsade och ansvarig chef behöver aktivt förlänga dessa konton.

Bedömning

Region Västmanland har automatiserat stora delar av processerna för att revidera regionens konton. Det finns en rutin för revidering av konton men den fungerar inte ändamålsenligt eftersom kontrollmål 9 uppvisar att det finns konton som inte bör existera, därför bedömer PwC att regionen **inte uppfyller** kontrollmålet.

3. Revisionell bedömning

Revisorerna i Region Västmanland har givit PwC i uppdrag att genomföra en uppföljning och fördjupad granskning avseende Regionens informationssäkerhetsarbete.

Den övergripande revisionsfrågan är:

Bedriver Regionstyrelsen ett ändamålsenligt arbete med informationssäkerhet och har tidigare identifierade brister åtgärdats?

För att Region Västmanland ska bli lyckosamma i sitt systematiska säkerhetsarbete krävs det en tydlig verksamhetsplan gällande informationssäkerhetsarbetet i regionen. Detta för att säkerställa en god säkerhetskultur men även fokus på behörighetstilldelningen i de olika verksamhetssystemen.

Den fördjupade granskningen av informationssäkerhetsarbetet visar att Region Västmanland arbetar aktivt med frågorna som gäller informationssäkerhet och IT-säkerhet. Informationssäkerhetsarbetet är dock inte med i planen eller budgeten för 2019-2021. Det finns en plan för 2019 för arbetet med Informationssäkerhet i regionen men den saknar aktiviteter för utförandet. Vi bedömer därför att regionen **delvis uppfyller** revisionsfrågan.

3.1 Rekommendationer

Utifrån våra iakttagelser bör nämnas att många åtgärder redan identifierats och eventuellt påbörjats av regionen avseende de utvecklingsområden som uppmärksammats i granskningen. Beaktat detta rekommenderar vi Regionstyrelsen att uppmärksamma följande i kommande arbete gällande informationssäkerhet:

- Region Västmanland bör se över åtgärdsmålen i ISO/IEC 27001 för att säkerställa att regionen täcker samtliga för att i framtiden kunna vara certifieringsbara.
- Säkerställ att styrande dokument är reviderade med lämplig intervall samt att informationssäkerhetspolicyn och riktlinjerna följs upp regelbundet.
- Inför systematisk dokumentation av vilka informationssäkerhetsåtgärder som tillämpats i verksamheten.
- Specificera i den kommande verksamhetsplanen de aktiviteter som ska genomföras i syfte att främja en god säkerhetskultur.
- Ett fortsatt arbete gällande riktlinjerna generellt behöver ses över.
- Region Västmanland bör utforma metoder och riktlinjer kring incidenthantering och informationssäkerhet i upphandling.
- Inkludera informationssäkerhetsarbetet i regionens framtida plan och budget.
- Specificera och kommunicera ut tydliga roller och ansvar för säkerhetsåtgärder i verksamheten.
- Ta fram styrdokument och processer för kravställning mot informationssäkerhetsarbetet.

- Gör e-utbildningen obligatoriskt för att säkerställa att alla medarbetare genomgår den. Se även till att ha regelbundna utbildningstillfällen och inte enbart vid nyanställning.
- Region Västmanland bör göra uppföljning av riskanalyser för behörighetstilldelning samt ta fram gallringsrutiner gällande behörighetssystemet. Regionen bör även se över kontinuerliga stickprov i patientjournalsystemet.
- Region Västmanlands lösenordspolicy bör stärkas.

4. Bilagor

Informationssäkerhetspolicy (Fastställd av Landstingsfullmäktige 2014-09-24)

Verksamhetsplan Informationssäkerhet 2019 – Region Västmanlands systematiska säkerhetsorganisation (antagits 2019, godkänd av Michael Patricksson)

Verksamhetsplan Informationssäkerhet 2019– Region Västmanlands systematiska säkerhetsorganisation (antagits 2019, godkänd Michael Patricksson)

Region Västmanlands Organisation för systematiskt säkerhetsarbete (antagits 2017-05-24, godkänd Jan Hallberg, administrativ direktör)

Riktlinje för riskanalys informationssäkerhet (antagits 2017-08-28, godkänd Jan Hallberg, administrativ direktör)

Riktlinje loggranskning (antagits 2019-02-12, godkänd Jan Hallberg, administrativ direktör)

Riktlinje åtkomst till patientuppgifter i journal (antagits 2018-01-15, fastställd av Landstingsstyrelsen)

Riktlinje för informationsklassning (giltig från 2017-08-28, godkänd Jan Hallberg)

Riktlinjer informationssäkerhet för medarbetare (antagits 2016-12-05, godkänd Anders Åhlund, Regiondirektör)

Riktlinje utlämnande av journalhandlingar, kopplar mkt till PUL (antagits 2016-03-15, utfärdat Åsa Ternström, landstingsjurist, godkänd Jan Hallberg)

Riktlinje sekretess och tystnadsplikt, kopplar lite till PUL, offentlighets- och sekretesslagen (antagits 2017-08-29, godkänd Jan Hallberg)

Beställning av Cosmicbehörigheter i HSA- Användarmanual (antagits 2018-03-02, godkänd Pernilla Hansson)

Matris över innehåll i grundbehörigheter Cosmic (antagits 2018-03-01)

2019-10-03

Tobias Bjöörn
Uppdragsledare

Catharina Ankre
Projektledare
