IT-säkerhet

Revisionsrapport

Region Västernorrland

KPMG AB

2017-12-13

Antal sidor 20

Antal bilagor 3

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Document classification: KPMG Confidential

Region Västernorrland
IT-säkerhet
Revisionsrapport
2017-12-13

Innehållsförteckning

© 2017 KPMG AB. All rights reserved.

Document classification KPMG Confidential

1. Sammanfattning

1.1 Allmänt

Landsting och regioner är beroende av IT-stöd för sin verksamhet. Att information, som är viktig för verksamheten, kan identifieras och få lämpligt skydd är således väsentligt. Brister i IT-säkerhet kan leda till obehörig åtkomst samt att spårbarhet och tillgänglighet inte kan tillgodoses. Vi har av revisorerna i landstinget i Västernorrland (LVN) haft som uppdrag att utföra en granskning avseende IT-säkerhet.

Från vår granskning vill vi särskilt framhålla att:

- Styrelsen behöver säkerställa att det finns moderna, konkreta och väl kända styrmedel för IT-säkerheten. Att organisera informationssäkerhetsarbetet och ansvaret för IT-säkerheten i två olika ansvarsområden underlättar inte en effektiv hantering. Särskilt som det inte finns uttalat och dokumenterat hur det praktiskt ska åstadkommas. En väsentlig aktivitet i uppdateringen av styrdokumenten är att utföra analyser[1], få informationen klassad och tydliggöra för verksamhetens chefer att de har det yttersta praktiska ansvaret för informationssäkerheten och därmed vilken IT-säkerhet som kommer att behövas. Detta innebär ett behov av återkommande utbildning av och information till alla delar av verksamheten.

- Vi anser det oroande att anpassningen till nya förordningar, författningar och direktiv (bland annat dataskyddsförordningen, GDPR) inte kommit längre än vad som framkommer vid våra intervjuer. Verksamheten som bedrivs framför allt inom sjukvården omfattas i stor utsträckning och det är kort om tid för att få till stånd alla nödvändiga anpassningar. Eftersom styrningen av informationssäkerheten inte bedöms som utvecklad i en ändamålsenlig omfattning så ger det heller inget stöd för hur anpassningsarbetet ska bedrivas.

- Vi saknar att styrelsen genom åren inte säkerställt efterlevnaden av informationssäkerheten så att det påverkat hur internkontrollen inriktats och hanterats. Vi menar även att styrelsens uppfattning om efterlevnaden av informationssäkerheten ska framgå av centrala dokument som patientsäkerhetsberättelser och årsredovisningar.

- Vi anser att med underlag av våra iakttagelser det finns motiv för revisionen att fortsättningsvis på olika sätt omfatta informationssäkerhet i kommande granskningar.

[1] Verksamhetsanalys, riskanalys och en GAP-analys.

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved

Document classification: KPMG Confidential

1.2 Bedömning utifrån revisionsfrågorna

Vi bedömer att styrelsen:

- Inte tillsett att det vid granskningstillfället finns aktuella styrande dokument i en omfattning och konkretisering som tydliggör alla de krav som ställs på hur arbetet med informationssäkerhet, och därmed IT-säkerhet, ska bedrivas.
- Inte tillsett att det finns ett genomtänkt och därmed strukturerat arbete för att säkerställa en IT-säkerhet som kan bedömas vara tillräcklig för de utmaningar som väntar med början under 2018. Förmågan att leverera den IT-säkerhet som bedöms som nödvändig måste utgå från de informationssäkerhetsbehov som verksamheterna identifierar.
- Inte har former för att säkerställa efterlevnaden av informationssäkerhet och därmed IT-säkerheten.

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved

Document classification: KPMG Confidential

2. Bakgrund

Revisorerna skriver i underlaget för denna granskning att: *”Landsting och regioner är beroende av IT-stöd för sin verksamhet. Att information, som är viktig för verksamheten, kan identifieras och få lämpligt skydd är således väsentligt. Brister i IT-säkerhet kan leda till obehörig åtkomst samt att spårbarhet och tillgänglighet inte kan tillgodoses. Informationssekretess samt informationens riktighet är även viktiga att säkerställa. Styrelsen ansvarar för de informationssystem som stödjer landstingets verksamhet.”*

Vi har av revisorerna i Landstinget i Västernorrland (LVN) haft som uppdrag att utföra en granskning avseende IT-säkerhet som landstingets revisorer aktualiserat i sin revisionsplan för 2017.

2.1 Syfte och revisionsfrågor

Syftet med granskningen har varit att ge revisorerna svar på följande huvudsakliga revisionsfrågor:

- Har styrelsen tillsett att det finns aktuella styrande dokument, såsom policy och riktlinjer för IT-säkerhet som tydliggör vilka krav som ställs och hur arbetet ska bedrivas?
- Har styrelsen tillsett att det finns ett strukturerat arbete för att säkerställa en tillräcklig IT-säkerhet?
- Finns former för att säkerställa efterlevnaden?

2.2 Avgränsning

Vi har i vår granskning tagit fasta på att det i revisionsplanen för 2017 anges att granskningens inriktning ska ha ett övergripande perspektiv.

2.3 Revisionskriterier

Revisionskriterierna för denna granskning har utgjorts av de styrande dokument (policy, riktlinjer, anvisningar och instruktioner) som landstinget upprättat och formellt antagit vad gäller informationssäkerhet och då särskilt det som styr IT-säkerheten. Vi har även bett om att få ta del av underlaget till de styrande dokumenten i form av analyser (t ex risk- och konsekvensanalyser) samt resultatet av utförda interna revisioner och genomförda internkontroller. Våra bedömningar av styrande dokument vilar på standarderna i ISO/IEC 27000-serien.

2.4 Ansvarig nämnd

Granskningen avser regionstyrelsen[2].

[2] I fortsättningen av rapporten, förutom i bilagorna, benämner vi landstingsstyrelsen och regionstyrelsen som styrelsen. Efter samma princip använder vi fullmäktige för både landstingsfullmäktige och regionfullmäktige.

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved

Document classification: KPMG Confidential

2.5 Granskningsansvarig

Granskningen har utförts av Lars Anteskog vid KPMG: s avdelning för offentlig sektor. Rapporten är granskad av kvalitetsansvarig för uppdraget Andreas Endrédi. Rapporten har även varit överlämnad till administrativ direktör samt FUI-direktören vilka har samordnat faktagranskningen.

2.6 Metod

Granskningen har genomförts genom:

- Dokumentstudier av formellt fastställda styrande dokument.
- Förekommande underlag till de styrande dokumenten och tjänstemannainitiativ för styrning och kontroll.
- Studier av styrelsens internkontrolldokument och rapportering om IT-säkerhet.
- Intervjuer med informationssäkerhetsamordnaren, tillförordnad[3] IT-säkerhetsansvarig, IT-chef, Chefen för administration och juridik, administrativ direktör samt FUI-direktören. Vi har även fått underlag från och intervjuat samordnaren för internkontrollarbetet.

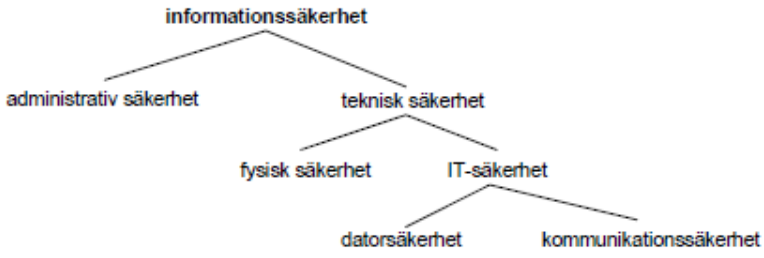
3. Resultat av granskningen

Iakttagelser och kommentarer redovisas i avsnitt nedan i den ordning revisionens frågor framgår av avsnitt ovan.

3.1 IT-säkerhet i förhållande till informationssäkerhet

Granskningen är inriktad mot IT-säkerhet. Följande beskrivning redogör för begreppen informationssäkerhet och IT-säkerhet. Det utifrån det av fullmäktige beslutade informationssäkerhetspolicy. Av policyn framgår att: *”Landstingets informationssäkerhetsarbete ska bedrivas i enlighet med standarden SS-ISO/IEC 27000.”*

Av standarderna i 27000 serien kan utläsas att IT-säkerhet är underordnad informationssäkerheten. Placeringen innebär att beslut om IT-säkerhet styrs av de beslut som tas av system och/eller objektägare som tillämpar det LIS[4] som styrelsen beslutat ska vara en del av LVN: s samlade ledningssystem. Med teknisk säkerhet menas de tekniska lösningar som förvarar och skyddar information. Mer om SS ISO/IEC 27000, 27000-serien och LIS i avsnitt nedan.



[3] Enligt uppgift gäller förordnande från juni 2016 till decembers utgång 2017.
[4] Ledningssystem för informationssäkerhet.

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved

Document classification: KPMG Confidential

3.2 LVN: s organisation för informations- och IT-säkerhet

För att skapa en grund för våra svar på revisionsfrågorna behöver organisationen där ansvaret för informations- och därmed IT-säkerheten i LVN beskrivas.

Informationssäkerheten sorterar under den administrativa direktören. Där har chefen för administration och juridik en (1) informationssäkerhetssamordnare att tillgå för det operativa arbetet. Det är en samordning utan i styrdokument angivet ansvar och mandat för att driva informationssäkerhetsarbetet och säkerställa organisationens förståelse och efterlevnad av den informationssäkerhet som beslutats.

IT-säkerheten sorterar under FUI-direktören. Där har IT-chefen via sin enhet Arkitektur och Metodstöd en (1) IT-säkerhetsansvarig till sitt förfogande. En dag i veckan har hen tillgång till en extern konsult som stöd i sitt arbete. FUI-direktören ansvarar även för den medicintekniska sidan av LVN: s verksamhet.

Kommentarer till 3.1 och 3.2

Uppdelningen av ansvaret så som redovisat är såvitt vi förstår en kvarleva från beslut flera år tillbaka i tiden. Ansvarsfördelningen har gällt de senaste åren och har vad vi erfar inte varit föremål för analys och utredning även när landstinget övergått till att fortsatt fungera som en region. Innevarande organisation har vad vi bedömer inte den gynnsammaste effekten på ett ändamålsenligt informationssäkerhetsarbete och därmed IT-säkerheten. Särskilt inte om formellt beslutad inriktning mot standard och ledningssystem fortsatt ska gälla. Rådande fördelning av ansvar rimmar inte med antagen policy och riktlinjer och gör det onödigt motsägelsefullt när informationssäkerhet och därmed IT-säkerhet ska ledas, utvecklas, kommuniceras och sist men inte minst kontrolleras.

Vi rekommenderar att en översyn görs av hur informationssäkerhetsarbetet övergripande ska styras och utvecklas och därmed påverka hur IT-säkerheten ska utformas. Ny teknik, nya lagar och nya utmaningar gör att uppdraget och ansvaret måste vara tydligt definierat så att informationssäkerhetsarbetet optimalt uppnår sitt syfte. Vi anser det därmed nödvändigt med en tydligare (uppdaterad) vägledning för hur den övergripande informationssäkerheten ska organiseras så att den stödjer de anställda och innebär trygghet för medborgarna.

3.3 Styrande dokument för IT-säkerheten

3.3.1 Informationssäkerhetspolicy

Informationssäkerhetspolicyn med diarienummer 08LS5946 är kortfattad och har gällt utan revidering i snart tio år. Antagen av fullmäktige 2008-06-25 redovisas följande*: "Avsikten med denna policy är att skydda landstingets informationstillgångar och skapa förtroende för att landstinget hanterar medborgares information på ett tryggt sätt."* Avslutningsvis framgår att: *"Landstingsstyrelsen fastställer riktlinjer för hur arbetet ska bedrivas."* I snart sju år är detta den enda riktlinjen vi kan finna ha formellt beslutats inom *"Ledningsystem, informationssäkerhet".* Först omkring årsskiftet 2017 tillkommer det till LIS ytterligare en riktlinje och fyra rutiner/regler.

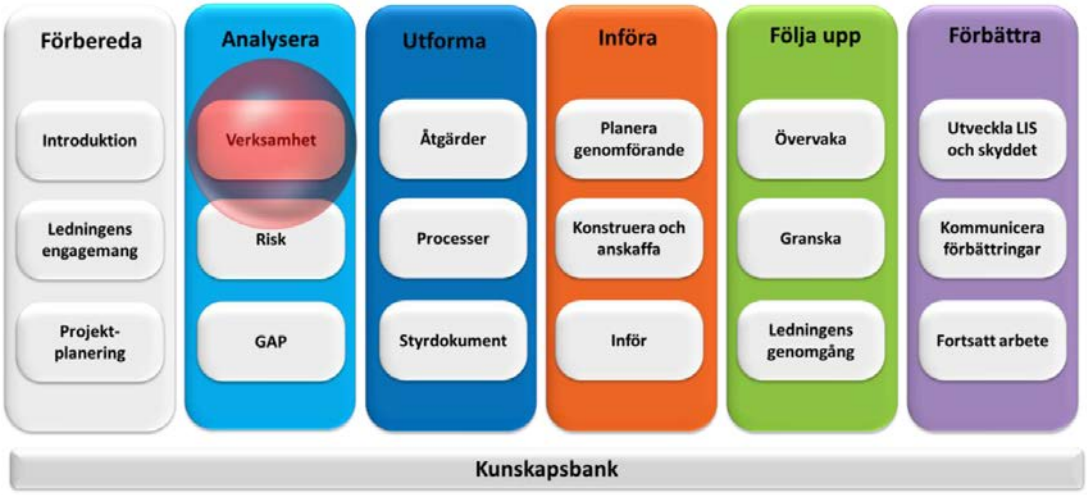
© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved

Document classification: KPMG Confidential

Kommentarer

Att kortfattat ange att: *”Landstingets informationssäkerhetsarbete ska bedrivas i enlighet med standarden SS-ISO/IEC 27000”* och sedan upprepa exakt samma text en gång till i *”Ledningsystem, informationssäkerhet”* ger ett otydligt och därmed oklart budskap om målsättningen med informationssäkerhetsarbetet. Det finns ett behov av att utveckla och förtydliga målet med informationssäkerhet. SS-ISO/IEC 27000 är endast standarden för *”Ledningssystem för informationssäkerhet – Översikt och terminologi”*. För att det ska bli ett konkret informationssäkerhetsarbete och därmed även ändamålsenlig anpassning av IT-säkerheten behöver fler standarder antas.

Lämpligtvis anges då i ett uppdaterat policydokument att informationssäkerhetsarbetet ska bedrivas enligt standarder i 27000-serien[5] och för att möta kraven i GDPR[6] kanske även tillämpliga standarder i 29000-serien[7]. Resultatet av de analyser som vanligtvis utförs när ett LIS tillämpas ger rimligen vägledning om vilka standarder som kan bli aktuella att först introducera.



Bilden är hämtad från MSB[8]: s metodstöd för LIS

Fullmäktige bör även ta ett beslut om informationssäkerhetsarbetet enligt 27000-serien ska certifieras eller inte.

[5] Överväg att i ett första steg anta SS-ISO/IEC 27001 Ledningssystem för informationssäkerhet – Krav, SS-ISO/IEC 27002 Riktlinjer för styrning av informationssäkerhet, SS-ISO/IEC 27003 Vägledning för införande av ledningssystem för informationssäkerhet, SS-ISO/IEC 27004 Vägledning för mätning av informationssäkerhet och SS-ISO/IEC 27005 Riskhantering för informationssäkerhet.
[6] GDPR utläses General Data Protection Regulation. På svenska Dataskyddsförordningen, EU-förordningen som gäller som svensk lag från 25 maj 2018.
[7] 29134 Privacy impact assessment och 29151 Code of practice for personally identifiable information protection.
[8] Myndigheten för samhällsskydd och beredskap.

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved

Document classification: KPMG Confidential

3.3.2 Ledningssystem, informationssäkerhet

Rubricerade dokument anges i beslutet från styrelsen 2010-10-12 vara en riktlinje. Från dokumentet som inte reviderats sedan beslutet hämtar vi följande från inledningen: *”Vi är helt beroende av information för att vi skall lyckas med vårt professionella uppdrag. Informationen skall vara korrekt och den skall vara tillgänglig för dem som har rätt till den. Information gör det möjligt för oss att upprätthålla patientsäkerhet, konkurrenskraft, kontrollera kassaflöden, följa gällande lagar och att ha ett gott anseende som en tillförlitlig organisation*”. Vidare står att läsa: *”Vi måste ha i åtanke att informationssäkerhet till den absolut största delen (70-80 %), handlar om vårt eget beteende. Endast 20-30 procent är tekniska frågor.”* Inledningen avslutas med: *”Detta dokument visar de grundläggande kraven för detta ledningssystem. Hur detta ska gå till beskrivs i efterföljande styrdokument.”*

Kommentarer

Styrelsen kan utifrån de styrande dokument som introducerats i verksamheten från 2010 och fram till årsskiftet 2017 inte bedömas ha uppnått sina intentioner om en ändamålsenlig informationssäkerhet tillika IT-säkerhet. Eftersom det saknas en stor mängd konkretiseringar i form av styrdokument för verksamheten att känna till, leva efter och för styrelsen att tillse att de efterlevs. Detta förhållande har inte hindrat att det ändå, ibland utan hänvisning till LIS, av både fullmäktige och styrelse beslutats om styrdokument avseende informationssäkerhet och därmed påverkat utformningen av IT-säkerheten. Mer om styrdokumenten i avsnitt nedan. Endast utifrån det faktum att konkret styrande dokument inte i nämnvärd grad införts genom åren finns det skäl för styrelsen att ta ett fastare kunskapsorienterat och kommunikativt grepp om säkerheten för sina informationstillgångar.

3.3.3 Styrande dokument i övrigt

Vi har från IT-säkerhetsansvarig och informationssäkerhetssamordnaren erhållit dokument som enligt deras uppfattning helt eller delvis är att betrakta som styrande för informationssäkerheten och i förlängningen IT-säkerheten. I bilaga 1 redovisas dessa inklusive de två som avhandlats ovan. Dokumenten är sådana som beslutats i politiska instanser, antagits i anslutning till LIS men även angivits fastställda på annat sätt.

En genomgång av dokumenten visar på följande:

- Inte alla erhållna dokument är att betrakta som styrande.
- Det saknas dokumenterad koppling till informationssäkerhetspolicyn och LIS för flera av dokumenten.
- Flera dokument saknar eller har otydlig anknytning till den IT-säkerhet som granskningen är avgränsad till.
- Vi bedömer det som osäkert om flera av dokumenten är giltiga i förhållande till fastställarens mandat.
- Datering saknas på flera dokument. Med ledning av dateringen är flera av dem inte heller längre giltiga.
- Några är ålderstigna och vi bedömer att det finns risk för att de leder till felaktig styrning.

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved

Document classification: KPMG Confidential

- Några gäller endast för en del av verksamheten.

Kommentarer

Vi bedömer att styrelsens ambitioner med styrande dokument från 2010 har, och rimligen har haft, för svag verkansgrad på informationssäkerheten. Det kan rimligtvis inte accepteras att ansvaret för informationssäkerheten endast vilar på enskildas initiativ, vilja och kunskap. När nu regionen förfogar över bedömt kunnig och engagerad personal är det av vikt att de formellt organiseras tillsammans med tydliga och enhetliga instruktioner om hur styrningen ska dokumenteras, kommuniceras och efterlevas.

Vi bedömer därför att styrelsen ***inte*** tillsett att det vid granskningstillfället finns aktuella styrande dokument i en omfattning och konkretisering som tydliggör alla de krav som ställs på hur arbetet med informationssäkerhet, och därmed IT-säkerhet, ska bedrivas.

3.4 Arbetet med IT-säkerhet

Vi har i avsnitt ovan konstaterat brister i styrdokumenten och vi ser ingen tydlig anvisning om hur arbete med IT-säkerhet ska organiseras och bedrivas. Vi har ovan redogjort för och kommenterat hur ansvaret för informationssäkerhet i förhållande till IT-säkerhet vid granskningstillfället är organiserat. För att få en övergripande praktisk insikt om hur arbetet ändå bedrivs så har vi i intervjudelen av vår granskning inriktat oss mot att få en sådan beskrivning. De sex funktioner som anges i avsnitt ovan har fått sig tillsänt ett ramverk av frågor innan intervjutillfället. Frågorna redovisas i bilaga 2 till denna rapport. Nedan följer våra sammanvägda iakttagelser och kommentarer från intervjuerna.

Ansvaret för IT-säkerheten (även förhållandet till ansvaret för informationssäkerheten) är inte definierat och dokumenterat för merparten av de intervjuade. Tillförordnad IT-säkerhetsansvarig har av IT-chefen fått sin rollbeskrivning. Trots det övergripande ansvaret för IT-säkerheten har ansvariga för informationssäkerheten inte några särskilda resurser för denna del. IT-säkerhetsansvarig har ingen egen budget för sitt arbete. Som en funktion inom IT-avdelningen finns för 2017 avsatt 600 000 kronor av vilka en konsult förbrukar två tredjedelar av beloppet. IT-chefen bedömer att inom det ansvar han anser sig ha för IT-säkerheten så har han de resurser som behövs. Generellt behöver dock IT-avdelningen ett tillskott av ytterligare personal för att säkerställa detta över tid.

Angående rapportering: IT-chef lämnade en delårsrapport 2016 vars IT-säkerhetsinnehåll inte lämnade något avtryck i den årsredovisning som senare upprättats. Informationssäkerhetssamordnaren har svarat på politikers frågor med anledningen av vad som rapporterats om Transportstyrelsen. I övrigt uppger de intervjuade att något krav eller önskemål om rapportering i någon form inte nått dem. Ingen av dem har heller på eget initiativ rapporterat något om IT-säkerhet till någon. Tjänsteskrivelsen som svar till politiken är protokollförd utan att följdfrågor ställts. Frågor från externa parter inskränker sig till att lokal media ställt frågor om virusangrepp och hanteringen av olegitimerad personal.

Angående organisationen: De intervjuade har inte tillgång till någon dokumentation som redovisar varför informationssäkerhetsarbetet organiserats med skilda ansvarsområden. Inför bildandet av regionen har vad vi förstår inga analyser, förstudier eller utredningar gjorts. Det uppges inte finnas några minnesanteckningar, protokoll och

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved

Document classification: KPMG Confidential

beslut som behandlar frågan. Befintlig landstingsorganisation har, förefaller det, utan justeringar och anpassningar blivit regionens organisation för övergripande informationssäkerhet. De intervjuade uppfattar heller inte att någon ny organisation efterfrågats från något håll. Däremot framgår det av de intervjuade att en sådan behövs.

Angående hur arbetet bedrivits: Det finns inte någon dokumentation som redovisar hur det operativa arbetet (t ex arbets-, utvecklings- och kontrollplaner) och ansvaret för IT-säkerheten inom rådande organisation är fördelat. Informationssäkerhetssamordnaren samarbetar informellt med IT-säkerhetsansvarig. På den översta ansvarsnivån förekommer vad vi förstår ingen samordning av hur IT-säkerheten ska anpassas utifrån verksamhetens informationssäkerhetskrav. Rådande situation kan ses som ett resultat av att det inte finns fastställda strategier för informations- likaväl som IT-säkerhetsarbetet. Vi uppfattar att årliga verksamhetsplaner inte avhandlat området med någon större tydlighet genom åren. Det långsiktiga arbetet verkar ha gått i stå och ersatts av en utveckling som drivs av ett fåtal tjänstemän på den operativa nivån. I och med det diskuteras inte framtidsfrågor som att anta fler standarder än ISO 27000 och om informationssäkerhetsarbetet vinner på att certifieras eller inte. Enstaka röster anser dock att detta ändå måste ske för att styra hur informationssäkerheten ska kunna hanteras med kvalitet.

Angående kontroll: Ingen av de intervjuade uppger sig någonsin ha varit involverade i någon riskanalys för internkontrollen något år. Mer om internkontroll i avsnitt nedan.

Angående de ekonomiska och personella resurserna: Ansvariga för IT-säkerheten anser sig ha de resurser de behöver. Det i förhållande till hur de själva uppfattar att de ska utföra sitt uppdrag. Informationssäkerhetssidan med det övergripande ansvaret uppger att de behöver ökade resurser för alla delar av sitt ansvar.

Angående anpassning till kommande direktiv och förordningar: När vi sammanfattar intervjusvaren så framträder en bild av att kunskapen varierar om vad statusen är för anpassningen till GDPR, Dataskyddslagen[9] och NIS-direktivet [10].

Medvetenhet verkar dock finnas. En signal som vi fått är att sedan mitten av oktober förekommer inget konkret arbete. Andra uppgifter anger att en (1) externkonsult finns på plats. Någon projektplan finns inte att redovisa för oss men möten i syfte att något behöver göras och görs uppges ha förekommit. Om representanter för politiken deltar i dessa samtal är oklart. Huruvida det finns en budget för arbetet är okänt vid våra intervjutillfällen. En konkret fråga i ämnet har ställts av den patientetiska nämnden: Hur

[9] Dataskyddslagen SOU 2017:19 redovisar de nationella anpassningar som behöver utföras inom den svenska rätten till följd av GDPR. Lagen är tänkt att utgöra ett generellt komplement och ska även kompletteras med sektorsspecifika författningar. Bland flera kan nämnas Patientdatalagen (2008:355), Läkemedelslagen (2015:315), Lagen (2005:258) om läkemedelsförteckning och Lagen (2006:496) om blodsäkerhet.

[10] "The directive on security of Network and Information Systems". EU-kommissionen överlämnade den 7 februari 2013 ett direktivförslag om åtgärder för att säkerställa en hög gemensam nivå av nät- och informationssäkerhet i hela EU. Regeringen utsåg 2016-03-13 en utredare med uppdrag att föreslå hur NIS-direktivet ska genomföras i svensk rätt (SOU 2017:36). Direktivet påverkar bland annat hälso- och sjukvården genom IVO (Inspektionen för vård och omsorg) och föreslås träda i kraft 2018-03-10. Det är MSB (Myndigheten för samhällsskydd och beredskap som ska upprätta en förteckning avseende vilka tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet (samhällsviktiga tjänster) för varje sektor.

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved

Document classification: KPMG Confidential

säkras underleverantörer? Det har i granskningen inte framkommit vilka svar som lämnats.

Har IT-säkerhetsincidenter[11] inträffat under 2017: Inte alls enligt de intervjuade med reservation för hur ett telefoniavbrott under året skulle ha klassificerats enligt NIS-direktivet.

Varierande svar har lämnats på vår fråga: *"Vilken eventuell tydlig/konkret styrning avseende IT-säkerhet (informationssäkerhet) saknar du eventuellt från styrelsen?"* Vi får svar att det inte saknas någon ytterligare/kompletterande styrning. Det är tjänstemännens ansvar att lyckas bättre är ett svar. Från annat håll anges att ett tydligare engagemang och intresse anses behövas och det tillsammans med en tydligare organisation. Allmänt efterfrågas formellt fastställda strategier och från någon särskilt vad gäller molntjänster. En specifik önskan är att innebörd och innehåll av IT-säkerheten behöver konkretiseras.

Saknade de intervjuade någon revisionsfråga: Svaren varierar även här. Vi får svar som; Inget specifikt om IT-säkerhet. Fått med det mesta. Det måste finnas fler styrande dokument för verksamheten totalt. Certifiering är av intresse. Varför granskas inte informationssäkerheten?

Kommentarer

Vi anser det oroande att anpassningen till nya förordningar, författningar och direktiv inte kommit längre än vad som framkommer av intervjusvaren. Verksamheten som bedrivs framför allt inom sjukvården omfattas i stor utsträckning och det är kort om tid för att få till stånd alla nödvändiga anpassningar. Eftersom styrningen av informationssäkerheten inte bedöms som utvecklad i en ändamålsenlig omfattning så har ansvariga heller inget stöd av detta i anpassningsarbetet.

Utifrån intervjusvaren har vi fått ytterligare underlag till att rekommendera styrelsen att förbättra möjligheten att utveckla styrningen av informationssäkerheten för att nå till den konkreta tillämpning som vid granskningstillfället saknas. Ska antagen policy och riktlinje från 2008 och 2010 fortfarande gälla så behövs en organisation som är anpassad till dokumentens utfästelser. Med dagens uppdelning på två olika ansvarsområden blir det nödvändiga strategiarbetet mer komplicerat än det behöver vara.

Som svar på revisionsfrågan: Vi anser att styrelsen inte tillsett att det finns ett genomtänkt och därmed strukturerat arbete för att säkerställa en IT-säkerhet som kan bedömas vara tillräcklig för de utmaningar som väntar med början under 2018. Förmågan att leverera den IT-säkerhet som bedöms som nödvändig måste utgå från de informationssäkerhetsbehov som verksamheterna identifierar.

[11] Enligt MSB inrymmer begreppet IT-incident tekniskt orienterade säkerhetsincidenter och informationssäkerhetsaspekter. IT-incident kan då vara: Störning i mjuk- eller hårdvara, störning i driftmiljö, informationsförlust eller informationsläckage, informationsförvanskning, hindrad tillgång till information, säkerhetsbrist i en produkt, angrepp, handhavandefel, oönskad eller oplanerad störning i kritisk infrastruktur eller annan plötslig oförutsedd händelse som lett till skada.

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved

Document classification: KPMG Confidential

3.5 Efterlevnad av IT-säkerheten

3.5.1 Internkontroll

Vi noterar i ”Riskanalys Regionstyrelsen 2017” två så kallade riskidentiteter (av sammanlagt 34 stycken) båda benämnda *”IT-säkerhet”*. De beskrivs och riskvärderas enligt följande:

- *”Saknar tillgång till kritisk information i rätt tid samt tillförlitlighet i informationen.”* Befintlig åtgärd redovisas som: *”Säkerhetsansvarig finns. Outsourcing är genomförd med tydliga krav på säkerhet.”* Som styrande dokument anges *”Avtal med leverantör.”* Riskvärdering för hur effektivt hanteringen är anges som medel. Riskvärdering avseende påverkan på verksamheten anges även den till medel. Bedömd sannolikhet med att risken för påverkan inträffar är angiven till *”möjlig*”. Riskidentiteten togs ***inte*** med i 2017 års internkontrollplan.
- *”Avvikelse mot fastställda kravspecifikationer inom IT-säkerhet. Driftavbrott. Ej tillgång till kritisk information.”* Befintlig åtgärd beskrivs: *”Tillgång intranät. IT-supportportal. IT självservice. Förvaltningsmodell. Information. Utbildningar. Stödfunktioner.”* Som styrande dokument anges *”Kravspecifikationer.”* Riskvärdering för hur effektivt hanteringen är anges inte. Riskvärdering avseende påverkan på verksamheten anges till medel. Bedömd sannolikhet med att risken för påverkan inträffar redovisas som *”möjlig*”. Riskidentiteten togs ***inte*** med i 2017 års internkontrollplan.

Vad vi förstår av samordningsfunktionen för internkontrollarbetet så har arbetet med riskanalyser generellt sett *”inte varit så utvecklat”* inom landstinget. Det har inte funnits ett gemensamt arbetssätt, *”en strukturerad modell”*. Av det följer att det förekommer att det inte finns *”dokumentation alls av processen/analysen”*.

Att riskidentiteterna för IT-säkerhet finns i analysen för 2017 uppges bero på att det: *”I oktober 2015 fanns ett par risker kopplat till IT med i det exempel som presenterades för stabscheferna inom kansliet, inklusive IT-chefen.”* Fortsatt uppges att: *”Alla chefer fick i uppdrag att återkomma med ett par uppdaterade risker. Utifrån det, så bestämdes att IT skulle komma med i 2016 års plan för uppföljning av intern kontroll.”* I *”Delårsrapport om uppföljning av intern kontroll 2016, Landstingets Kansli”* bilaga 8a daterad 2017-01-31 redogörs för resultatet. Vi återger hela texten i vår bilaga 3 och redogör för våra iakttagelser med att:

- Landstingets kansli genomförde en stickprovsgenomgång av tre kravspecifikationer i IT-avtal. Granskningen visade på skillnader i landstingets kravställning avseende IT-säkerhet. Effekten av iakttagelserna blev att en riktlinje ”Hantering av tillgångar” fastställdes. Praktiskt innebar det att informationsklassning skulle genomföras. Rutin för informationsklassning skulle skapas och verktyget KLASSA[12] användas. Vi noterar att det resulterat i att styrdokument avseende informationsklassning upprättats.

[12] Informationsklassning är en metod som hjälper verksamheten att välja rätt åtgärder som skyddar informationen. För att förenkla kommuners, landstings och regioners genomförande av informationsklassningen har SKL tagit fram verktyget KLASSA. Verktyget kan användas både i det praktiska arbetet med förvaltning av enskilda verksamhetssystem och i det systematiska kvalitetsarbetet på övergripande nivå.

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved

Document classification: KPMG Confidential

- Det uppges ha genomförts två stycken interna revisioner. Av vad, vem, varför och resultatet är inte redovisat. Så är även fallet med denna inledda granskning av efterlevnad av kravspecifikation inom IT-säkerhet hos en av landstingets leverantör av IT-system.
- En nulägesanalys inom IT-säkerhet genomfördes hösten 2016 efter vilken det skapats en handlingsplan. Kopplingen till informationssäkerhet tas inte upp däremot finns noteringar om att kontakt tagits med informationssäkerhetssamordnaren vad gäller upprättande av förslag till en riktlinje.
- *”Utbildning i IT-säkerhet har genomförts för all personal inom IT för att öka kunskapen och säkerställa att styrande dokument som berör IT-säkerhet är kända.”*
- Det konstateras finnas ett behov av att: *”Säkerställa att kravspecifikationer inför upphandling/avtal av IT-system uppfyller lagar, landstingets regelverk samt dataskyddsförordningen som träder i kraft 25 maj 2018.”*

Till analysresultatet för 2017 uppges att både tjänstemän och politiker har medverkat. Det finns ingen underliggande dokumentation till varför riskidentiteterna upprepades från föregående års analys och varför riskvärderingen blev den som har angetts. Varför riskvärderingen 2017 inte kvalificerade riskidentiteterna till interkontrollplanen finns det heller ingen dokumentation som förklarar. Det senare vare sig som en komplettering eller ett tillägg till delårsrapportens iakttagelser och åtgärder för 2016.

3.5.2 Landstinget om IT-säkerhet i offentliga dokument

Årsredovisning för 2015 och 2016 samt *”Kvalitets- och patientsäkerhetsberättelse*[13] *2016”* redovisar ingenting om IT-säkerhet. Vi kan inte heller iaktta att informationssäkerhet redovisats i dokumenten.

Kommentarer till 3.5.1 och 3.5.2

Internkontrollen avseende IT-säkerheten har omfattat exakt samma två riskidentiteter tre år i rad[14]och ingen underliggande dokumentation finns att ta del av som redovisar motivet till detta. Till detta ska läggas att ingen av de intervjuade uppger att de deltagit i riskanalysen.

Ska styrelsen kunna uppge att internkontrollarbetet är väl anpassat till de risker som finns i hanteringen av sin informationstillgångar måste kontrollarbetet utvecklas och dokumenteras. Vi anser att arbetet ska lyftas till nivån att det är informationssäkerheten som ska säkerställas. Som rekommendation använder vi texten från styrelsens styrdokument för LIS: *”Vi är helt beroende av information för att vi skall lyckas med vårt professionella uppdrag”*. Vi bedömer att ett omtag i internkontrollarbetet är nödvändigt för att kunna leva upp till fortsättningen av texten: *”Information gör det möjligt för oss att*

[13] Enligt SOSFS 2011:9 7 kap. 3 § ska patientsäkerhetsberättelsen ha en sådan detaljeringsgrad att det går att bedöma hur det systematiska patientsäkerhetsarbetet har bedrivits i verksamhetens olika delar, och att informationsbehovet hos externa intressenter tillgodoses. Sveriges kommuner och landsting påminner i sin mall för ändamålet att från 2017-03-01 enligt HSLF-FS 2016:40, 7 kap. 1§ *”Journalföring och behandling av personuppgifter i hälso- och sjukvården”* (tidigare enligt SOSFS 2008:14) ska det beskrivas hur verksamheten arbetat (analyserat, kontrollerat, utvecklat etc.) med informationssäkerhet.
[14] När dokumentation inhämtats har vi även erhållet *”Intern kontroll - Riskanalys inför 2018”.*

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved

Document classification: KPMG Confidential

upprätthålla patientsäkerhet, konkurrenskraft, kontrollera kassaflöden, följa gällande lagar och att ha ett gott anseende som en tillförlitlig organisation". Denna utfästelse anser vi även ska komma till uttryck i årsredovisningar och patientsäkerhetsberättelser kommande år.

Vi bedömer att styrelsen kan och ska vara noggrann med att säkerställa och kommunicera att informationssäkerheten och därmed IT-säkerheten efterlevs som det är beslutat. När styrelsen inte nämner informations- och/eller IT-säkerhet i årsredovisningar öppnas det för tvivel på att det finns etablerade former för att säkerställa efterlevnad av det som beslutats. Det intrycket understryks av att det inte nämns något om informationssäkerhet i den senaste patientsäkerhetsberättelsen. Vi bedömer därför att styrelsen inte har former för att säkerställa efterlevnaden av informationssäkerhet och därmed IT-säkerheten.

Datum enligt ovan

KPMG AB

Lars Anteskog

Projektansvarig

Detta dokument med bilagor har upprättats enbart för i dokumentet angiven uppdragsgivare och är baserat på det särskilda uppdrag som är avtalat mellan KPMG AB och uppdragsgivaren. KPMG AB tar inte ansvar för om andra än uppdragsgivaren använder dokumentet och informationen i dokumentet. Informationen i dokumentet kan bara garanteras vara aktuell vid tidpunkten för publicerandet av detta dokument. Huruvida detta dokument ska anses vara allmän handling hos mottagaren regleras i offentlighets- och sekretesslagen samt i tryckfrihetsförordningen.

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved

Document classification: KPMG Confidential

Region Västernorrland
IT-säkerhet
Bilaga 1 – Styrande dokument
2017-12-13

Inledning

Nedan redovisade styrande dokument är tillhandahållna i olika och ibland samma omfattning av revisionsdirektören, IT-säkerhetsansvarig och informationssäkerhetssamordnaren.

Förklaring till rubrikerna

- Filnamn = Eftersom alla dokumenten är erhållna elektroniskt så redovisas här filens namn med undantag av ”Synkronisering av kalender, kontakter mm11227.doc” som har kortats på grund av platsbrist.
- Typ är vår kategorisering utifrån vad vi kan utläsa av dokumentet. P = Policy, PR = Protokoll, R = Riktlinje och RR = Rutin/Regel
- Infosäk = Vi har angivit J om vi bedömt att detta dokument i sin utformning och sitt innehåll i någon omfattning styr informationssäkerheten.
- IT-säk = Vi har angivit J om vi bedömt att detta dokument i sin utformning och sitt innehåll i någon omfattning styr IT-säkerheten.
- Beslut = Om en instans anges ha tagit beslut om styrdokumentet har vi markerat: LF = Landstingsfullmäktige, LS = Landstingsstyrelsen, HS = Hälso- och sjukvårdsnämnden och LIS = När det i dokumentet hänvisas till ledningssystem för informationssäkerhet.
- Fastställd = När beslutsinstans saknats har vi markerat med P där vi funnit ett personnamn som fastställare av dokumentet.
- Verksamhet = Vi markerar med ett J där det av dokumentet framgår att det gäller för landstinget gemensamt.
- Gäller from = Här anger vi det senaste av de datum som redovisas som från och med eller reviderat. Saknar dokumentet datum lämnas fältet tomt.
- Gället tom = Här anger vi det datum som redovisas giltigt till och med. Saknar dokumentet datum lämnas fältet tomt.

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved

Document classification: KPMG Confidential

Region Västernorrland
IT-säkerhet
Bilaga 1 – Styrande dokument
2017-12-13

Filnamn	*Typ*	*Info säk*	*IT-säk*	*Be-slut*	*Fast-ställd*	*Verk-sam-het*	*Gäller from*	*Gäller tom*
10749 Regel för funktionsbrevlådor, resurser och distributionslistor.doc	RR	J	J		P	J		
123392_Diarieföring och ärendehantering.doc	R	J		LS		J	2014-10-27	
25522_E-postsignatur.doc	R	J		LS		J	2014-10-09	
72390_Namnsättning och format på e-postadresser.doc	R	J	J		P	J	2015-03-30	2017-03-30
73602_Godkända mottagare för säker e-post.doc	RR	J	J		P	J	2015-05-13	2017-05-13
81654_Hemkataloger och e-postkonton.doc	R	J	J		P	J	2013-05-31	2017-05-31
91377_Godkänd mobila enheter för synkronisering.doc	R	J	J		P	J	2013-05-31	2017-05-31
Användning av e-post 110762.doc	RR	J	J		P	J	2014-05-15	2018-05-15
Avgifter för kopior av allmänna handlingar_13LS1104.doc	R	J		LF		J		
Behandling av personuppgifter 189615.doc	R	J		LS		J	2010-10-11	
Behörighetstilldelning vårdsystem (73775).doc	R	J		LS		J	2012-10-11	
Diarieföring och ärendehantering (123392).doc	R	J		LS		J	2014-10-17	
E-post med patientinformation 73601.doc	R	J			P	J	2015-04-08	2017-10-08
Fimtecknare LVN - Beslut enligt Landstingsstyrelsens protokoll den 16 december 2014.pdf	PR	N		LS		J	2016-06-14	
Handläggning vid misstanke om dataintrång (176655).doc	RR	J	J		P	J	2016-02-03	2017-08-03
Hantering av tillgångar 231696.doc	R	J	J	LIS	P	N	2016-11-21	2018-05-21
Informationsklassning - verktyget KLASSA.docx	RR	J		LIS		J	2017-02-02	
Informationsklassning - modell.docx	RR	J		LIS		J	2017-02-17	
Informationssäkerhetspolicy.doc	P	J		LF		J	2008-06-25	
Intern revision Oktav(129217) .doc	RR	J			P	N		
Kravbild, befintliga systems uppfyllande av patientdatalagen(34821).DOC	R	J			P	J		
Krisberedskap och allmän säkerhet i Landstinget Västernorrland (92653).doc	P	J	J	LF		J	2013-10-30	
Kvalitetssäkra rutiner och processer 42277.doc	RR	J	J		P	N	2017-05-08	2018-11-08
Ledningssystem informationssäkerhet.doc	R	J	J	LS		J	2010-10-12	
Ljud- och bildupptagning i landstingets lokaler - 234581.doc	R	J		HS		N	2014-12-19	
Loggkontroll 147630.doc	RR	J			P	J	2016-05-19	2017-11-19

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved

Document classification: KPMG Confidential

Region Västernorrland
IT-säkerhet
Bilaga 1 – Styrande dokument
2017-12-13

Filnamn	*Typ*	*Info säk*	*IT-säk*	*Be-slut*	*Fast-ställd*	*Verk-sam-het*	*Gäller from*	*Gäller tom*
Mobiltelefoni 71106.doc	RR	J	J		P	J	2016-10-17	2018-04-17
Policy för internettjänster.pdf	P	J	J	LS		J	2002-08-28	
RAPS - SITHS 178762.doc	R	J			P	J	2015-10-13	2018-10-13
Rilktlinjer för säkerhets- och krisberedskapsarbetet i Landstinget Västernorrland (92657).doc	R	J	J	LS		J	2013-11-12	
Rutin för kontroll av loggar inom Folktandvården(t.o.m. 2016-09-30).doc	RR	J			P	N	2015-03-13	2016-09-30
Signering inom hälso- och sjukvården(32462).DOC	R	J			P	J	2012-04-19	2014-04-19
Spårbarhet 36273.doc	R	J		LS		J	2011-04-04	2010-10-12
Synkronisering av kalender, kontakter mm11227.doc	RR	J	J		P	J	2012-05-28	2017-11-28
Systemdokumentation 231947.doc	RR	J	J	LIS	P	N	2016-11-22	2018-05-22
Systemförteckning 235331.doc	RR	J	J	LIS	P	N	2016-11-21	2018-05-21
Utlämnande av journalhandling (158248).doc	R	J			P	J	2015-05-13	2017-05-13

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved

Document classification: KPMG Confidential

Region Västernorrland
IT-säkerhet
Bilaga 2 – Intervjufrågor
2017-12-13

Följande frågekomplex användes vid intervjuerna.

1. Hur är ditt ansvar för IT-säkerheten definierat och dokumenterat?
2. Vem har definierat och dokumenterat ditt ansvar för IT-säkerheten?
3. Vilka resurser (ekonomiska och personella) har du till ditt förfogande för att utveckla, utbilda, säkerställa samt kontrollera efterlevnad av IT-säkerheten?
4. Vem/Vilka har muntligen och/eller skriftligen inom landstinget efterfrågat rapportering om IT-säkerheten i någon och/eller några omfattningar?
5. Till vem/vilka har du efter och/eller utan anmodan inom landstinget lämnat muntliga och/eller skriftliga rapporter till omfattande IT-säkerhet?
6. Vilka reaktioner har du fått *inom* landstinget på eventuellt lämnade skriftliga rapporter omfattande IT-säkerhet?
7. Vilka reaktioner har du fått *utom* landstinget på eventuellt lämnade skriftliga rapporter omfattande IT-säkerhet?
8. Vilken dokumentation (analyser, förstudier, utredningar, minnesanteckningar, protokoll, beslut etc.) finns som redovisar valet av att placera IT-säkerheten under FOI och den överordnade informationssäkerheten i den administrativa delen av verksamheten?
9. Finns det någon dokumentation som redovisar hur det operativa arbetet (t ex arbets-, utvecklings- och kontrollplaner) och ansvaret för IT-säkerheten inom rådande organisation är fördelat?
10. Vilka eventuella planer finns för att utveckla arbetet med informationssäkerheten och därmed IT-säkerheten? T ex Anta fler standarder än ISO 27000, certifiera verksamheten för ett antal standarder i 27000-serien eller alternativt föreslå någon annan metod för att säkerställa ändamålsenlig informationssäkerhet/IT-säkerhet?
11. I vilken omfattning har du medverkat i riskanalysen för internkontrollen för *2017* där riskidentiteten är benämnd IT-säkerhet?
12. I vilken omfattning har du medverkat i riskanalysen för internkontrollen för *2018* där riskidentiteten är benämnd IT-säkerhet?
13. Är de ekonomiska och personella resurserna du/ni har till förfogande tillräckliga för att utveckla, utbilda, säkerställa samt kontrollera efterlevnad av IT-säkerheten?
14. Har du/ni alla de resurser ni bedömer er behöva för att säkerställa efterlevnad av dataskyddsförordningen, dataskyddslagen och NIS-direktivet under 2018?
15. Vilken eventuell tydlig/konkret styrning avseende IT-säkerhet (informationssäkerhet) saknar du eventuellt från Landstings-/Regionstyrelsen?
16. Har det under 2017 inträffat någon eller några verksamhetsstörande incidenter som föranletts helt eller delvis av brister i IT-säkerheten?
17. Om incidenter inträffat hur har de rapporterats till styrelsen och berörda myndigheter?
18. Anser du att det saknas någon fråga ovan för att ge revisionen svar på de tre frågorna: *Har styrelsen tillsett att det finns ett strukturerat arbete för att säkerställa en tillräcklig IT-säkerhet? Har styrelsen tillsett att det finns aktuella styrande dokument, såsom policy och riktlinjer för IT-säkerhet som tydliggör vilka krav som ställs och hur arbetet ska bedrivas? Finns former för att säkerställa efterlevnaden?*

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved

Document classification: KPMG Confidential

Region Västernorrland
IT-säkerhet
Bilaga 3 – Delårsrapport om uppföljning av intern kontroll 2016, Landstingets Kansli bilaga 8a
2017-12-13

IT-säkerhet

Efterlevnad av fastställda kravspecifikationer inom IT-säkerhet:
Innehåller IT-avtalen tillräckliga säkerhetskrav?
Levereras den säkerhet som enligt avtalen ska finnas?
Besvaras av Landstingets kansli, genom stickprovsgenomgång av IT-avtal.

Stickprovsgenomgång av 3 st. kravspecifikationer i IT-avtal visar på skillnader i landstingets kravställning av IT-säkerhet. Riktlinjen ”Hantering av tillgångar” är därefter fastställd som innebär att informationsklassning ska genomföras. Rutin för informationsklassning kommer att skapas, där SKL:s verktyg Klassa ska användas som också visar upphandlingskrav. I de tre kontrollerade avtalen finns beskrivet att landstinget har möjlighet att kontrollera att överenskomna säkerhetskrav uppfylls.

Det är genomfört 2 st. interna revisioner.

Det är inlett en granskning av efterlevnad av kravspecifikation inom IT-säkerhet hos en av landstingets leverantör av IT-system.

Det är genomfört en nulägesanalys inom IT-säkerhet hösten 2016 samt skapat en handlingsplan utifrån den.

Utbildning i IT-säkerhet har genomförts för all personal inom IT för att öka kunskapen och säkerställa att styrande dokument som berör IT-säkerhet är kända.

Det finns behov av att säkerställa att kravspecifikationer inför upphandling/avtal av IT-system uppfyller lagar, landstingets regelverk samt dataskyddsförordningen som träder i kraft 25 maj 2018.

© 2017 KPMG AB, a Swedish limited liability company and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved

Document classification: KPMG Confidential