Granskning av informationssäkerhet

Region Värmland

Oktober 2019

Linus Owman
Mattias Lööf
Fredrika Jönander

pwc

Revisionsrapport

Innehållsförteckning

Sammanfattning

PwC har på uppdrag av Region Värmlands förtroendevalda revisorer granskat regionens informationssäkerhet. Syftet är att granska om Regionstyrelsen tillsett att regionens informationssäkerhet (inkl. IT-säkerhet) är ändamålsenlig. I granskningen ingår även en uppföljning av förstudien avseende ”IT-säkerhet” från 2015. Revisionsfrågorna har varit:

- Har Regionstyrelsen säkerställt en styrning (exempelvis genom beslut och riktlinjer, budgetmedel) och uppföljning som ger en ändamålsenlig informationssäkerhet? Detta särskilt mot bakgrund av regionbildningen (bland annat ny organisation, nya system, nya verksamheter).

- Har Regionstyrelsen vidtagit åtgärder med anledning av de brister och de förbättringsförslag som framfördes i förstudien 2015 samt har åtgärder vidtagits i enlighet med det svar som dåvarande landstingsstyrelsen tillställde revisorerna?

- Om granskningen påvisar brister, vilka rekommendationer ges?

Efter genomförd granskning bedömer vi att Regionstyrelsen **till viss del** har uppfyllt kontrollmålen. Sammantaget bedöms regionen arbeta med informationssäkerhet, men det finns tydliga förbättringsmöjligheter för att fullt ut nå ett tillfredsställande och ändamålsenligt arbete. Vi lämnar ett antal rekommendationer för att säkerställa ett fortsatt effektivt arbete med informationssäkerhet inom regionen.

PwC:s bedömning som svar på revisionsfrågorna är att Regionstyrelsen **inte helt** har säkerställt en styrning och uppföljning som ger en ändamålsenlig informationssäkerhet. Grunden till denna bedömning är den nuvarande avsaknaden av regelbunden revision, granskning och uppdatering av styrande dokumentation, avsaknaden av dokumentation för vissa väsentliga informationssäkerhetsprocesser samt bristande uppföljning och rapportering kring informationssäkerhetshändelser och incidenter till Regionstyrelsen.

PwC bedömer även att Regionstyrelsen **inte helt** har vidtagit åtgärder med anledning av de brister och förbättringsförslag som framfördes i förstudien 2015. Denna bedömning bygger på den iakttagna avsaknaden på både systematisk informationsklassning av samtliga system, samt regelbundet och dokumenterat utförande av riskanalyser, vilket är åtgärder som rekommenderades av förstudien. Den ovan nämnda punkten kring brister med styrningen och dokumentation påvisar således att det fortfarande finns ett förbättringsarbete som regionen bör utföra.

Rekommendationer

Utifrån våra iakttagelser bör nämnas att flertalet åtgärder identifierats av Region Värmland och eventuellt redan påbörjats avseende de förbättringsområden som uppmärksammats i granskningen. Beaktat detta rekommenderar vi Regionstyrelsen att uppmärksamma följande i framtida arbete avseende informationssäkerhet:

Människor och processer:

- ➢ Dokumentera huvudsakliga informationssäkerhetsprocesser. Säkerställ och tydliggör roller, ansvar och mandat.
- ➢ Säkerställ att samtlig dokumentation är uppdaterad och giltig.
- ➢ Säkerställ att informationssäkerhetspolicyn ses över och revideras med lämpliga intervall samt att riktlinjerna följs upp med regelbundenhet. Dessutom bör riktlinjerna revideras så att det tydligt framgår ansvarig för vidare uppdatering.
- ➢ Identifiera och definiera mätbara mål för samtliga åtgärdsmål i syfte att följa upp dessa kontinuerligt. Därtill bör regionen slutföra omsättningen av principerna beskrivna i informationssäkerhetspolicyn till riktlinjer.
- ➢ Etablera en obligatorisk informationssäkerhetsutbildning för samtliga anställda i Region Värmland. Säkerställ att utbildningar och övningar för att utveckla och säkerställa kompetens om informationssäkerhet genomförs regelbundet.
- ➢ Specificera i den kommande verksamhetsplanen de aktiviteter som ska genomföras i syfte att främja en god säkerhetskultur. Regionen bör även genomföra systematiska uppföljningar av utbildningsverksamheten.
- ➢ Formalisera utvärderingsarbetet efter en inträffad incident för att säkerställa att åtgärder genomförs för att förhindra att liknande incidenter inträffar igen.
- ➢ Minska personberoendet för att säkerställa att verksamheter kan fortlöpa vid ett eventuellt personalbortfall.
- ➢ Med hänsyn till den nya lagstiftningen inom säkerhetsskydd från april 2019 bör Region Värmland genomföra en djupare analys av regionens kritiska informationstillgångar för Sveriges säkerhet.

Teknik:

- ➢ Undersök möjligheten till att införskaffa en SIEM-lösning som aggregerar säkerhetsloggar från väsentliga nätverkspunkter och skapar relevanta alerter.
- ➢ Implementera behörighetstilldelning och behörighetsgrupper som baseras på i förväg bestämda roller.
- ➢ Automatisera sårbarhetsskanning så att det genomförs på regelbunden basis och dokumentera processen.
- ➢ Utöka den geografiska spridningen på regionens serverhallar för att säkerställa redundans, det vill säga information som upprepar redan etablerad information för att säkra informationen.

1. Inledning

1.1 Bakgrund

Under det senaste årtiondet har en snabb utveckling inom datakommunikation och teknik ägt rum. Digitaliseringen påverkar många olika delar av samhället, exempelvis har IT gått från att stödja affärsprocesser till att driva verksamheter. Detta medför att det är viktigt att identifiera och adressera cyberhot och risker. Allt fler allvarliga cybersäkerhetsincidenter har drabbat såväl privat som offentlig sektor de senaste åren. En gemensam beståndsdel i flera av de allvarligaste händelserna är information som på ett eller annat sätt kommit obehörig tillhanda, antingen genom bristande rutiner och hantering eller genom yttre påverkan, och i vissa fall en kombination av båda dessa. I det moderna samhället har så gott som all brottslighet en IT-koppling. I *Informationssäkerhet – trender 2015* skriver Myndigheten för samhällsskydd och beredskap (MSB) att *”Informationssäkerhet kommer framöver att allt mera betraktas som en fråga om att skydda hela samhället och dess välstånd snarare än bara teknik.”*. Att regionens informationssäkerhet är essentiell för ett välfungerande samhälle råder det inget tvivel om.

Som ett led i att förhindra cybersäkerhetsincidenter och upprätthålla samhällsviktig verksamhet behöver en region bedriva ett ändamålsenligt informationssäkerhetsarbete. Information som finns i regionen skall klassas, rutiner och riktlinjer ska finnas på plats och arbetet ska regelbundet följas upp. Detta kräver också ett säkerhetsmedvetande hos dem som hanterar informationen på daglig basis. Informationssäkerhet regleras inte i en sammanhållande lag utan genom bestämmelser i flera olika regelverk. Det finns även i lagstiftning, föreskrifter och rekommendationer inom hälso- och sjukvård etc.

Informationssäkerhet innebär en rutin och/eller process som tillämpas för att skydda information och mildra informationsrisker. En sådan process har som syfte att säkerställa att *konfidentialiteten*, *integriteten*, och *tillgängligheten* av information inte röjs. För att åstadkomma detta kan flera säkerhetsåtgärder tillämpas. Dessa säkerhetsåtgärder kan huvudsakligen sägas falla inom tre kategorier; administrativa, tekniska, och åtgärder som riktar sig till att skapa en säkerhetskultur anpassad till att skydda information. Ändamålsenlig och uppdaterad dokumentation är således väsentlig för att samtliga informationssäkerhetsåtgärder ska kunna tillämpas och efterföljas (se även 2.1).

Mot bakgrund av detta har PwC på uppdrag av Region Värmlands förtroendevalda revisorer genomfört en granskning av regionens informationssäkerhet. Målet med granskningen är, utöver besvarandet av revisionsfrågorna, att ge Region Värmland en nulägesbild beträffande dess informations- och cybersäkerhetsförmåga kopplad till människor, processer och teknik. Nulägesbilden inbegriper aspekter såsom styrkor, förbättringsområden samt övergripande rekommendationer som regionen kan beakta som första steg i riktningen mot att arbeta proaktivt med informations- och cybersäkerhetsfrågor. Nulägesbilden ställs även i relation till tidigare genomförd granskning *“Förstudie IT-säkerhet”* (2015), och utmynnar i ett antal rekommendationer för regionens fortsatta arbete med informationssäkerhet. Nulägesbilden, vilken bilägggs

denna rapport som ett arbetsmaterial kan med fördel ansvändas av regionens IT- och informationssäkerhetsansvariga för att på ett konkret sätt driva förbättringsåtgärderna vidare inom regionen.

1.2 Syfte och Revisionsfrågor

Granskningen har haft som syfte att besvara följande revisionsfrågor:

- Har Regionstyrelsen säkerställt en styrning (exempelvis genom beslut och riktlinjer, budgetmedel) och uppföljning som ger en ändamålsenlig informationssäkerhet? Detta särskilt mot bakgrund av regionbildningen (bland annat ny organisation, nya system, nya verksamheter).

- Har Regionstyrelsen vidtagit åtgärder med anledning av de brister och de förbättringsförslag som framfördes i förstudien 2015 samt har åtgärder vidtagits i enlighet med det svar som dåvarande landstingsstyrelsen tillställde revisorerna?

- Om granskningen påvisar brister, vilka rekommendationer ges?

Utifrån revisionsfrågorna ovan har tre stycken kontrollmål brutits ut för att konkret kunna värdera, mäta och besvara revisionsfrågorna.

1.3 Kontrollmål

- Regionen har ändamålsenlig och uppdaterad dokumentation på plats för arbetet med informationssäkerhet.

- Regionen säkerställer styrning och uppföljning av dess informationssäkerhet på ett ändamålsenligt sätt.

- Regionen har vidtagit åtgärder med anledning av bristerna i förstudien från 2015 och med anledning av regionbildningen 2019.

1.4 Avgränsning

Granskningen avgränsas till att gälla informationssäkerhet inom Region Värmland 2019 samt uppföljning av den förstudie som genomfördes 2015.

1.5 Metod

Granskningen har genomförts med hjälp av ramverket NIST Cyber Security Framework. Ramverket, vilket utvärderar en organisations förmåga att genomföra handlingar kopplade till de fem domänerna: *Identifiera, Skydda, Upptäcka, Respondera* och *Återställa* utifrån ett resurs-, rutin- och teknikperspektiv. Varje område innehåller ett antal kontrollmål vars grad av uppfyllnad poängsätts på en skala från 1 till 5. Ramverket har anpassats efter Region Värmlands förutsättningar och verksamhet. PwC har utvärderat Region Värmlands mognadsgrad beträffande följande funktioner:

Identifiera:, Området täcker Region Värmlands förmåga att identifiera kritiska informationstillgångar och data, det nuvarande läget för styrning och övergripande riskhantering när det kommer till cybersäkerhet. Som ett led i detta har PwC bland annat sett till processer kopplade till riskhantering samt klassificering av tillgångar.

Skydda: Området fokuserar på Region Värmlands nuvarande tillstånd när det kommer till att skydda regionens information samt att avskräcka från hot. Denna kategori inbegriper även förmågan att hantera behörighetskonton samt säkerhet kopplad till data.

Upptäcka: Området inkluderar bland annat Region Värmlands förmåga att övervaka IT- och säkerhetsrelaterade händelser. Detta medför bland annat möjlighet till nätverks-övervakning, samt sökning efter skadlig kod och sårbarheter.

Respondera: Området täcker Region Värmlands rutiner för åtgärdsplanering och aktiviteter kopplade till interna och externa intressenter vid en eventuell incident. Denna förmåga inkluderar bland annat forensik (kriminalteknik) och incidenthantering.

Återställa: Området relaterar till Region Värmlands processer för kontinuitetshantering och förmågor relaterade till resiliens och återhämtning efter hantering av incidenter. Kommunikation och publika relationer (PR) inkluderas även i denna kategori.

Granskningen baserar sig på tre kvalitativa workshops tillsammans med nyckelfunktioner inom Region Värmland. Arbetet med IT- och informationssäkerhet hos Region Värmland genomförs till största del av Region-IT och informationshanteringsenheten samt det nyinrättade informationssäkerhetsrådet. Region Värmlamnd har ombetts att, utifrån granskningsområdet identifiera relevanta personer för intervjuerna. Dessa personer har sammantaget gedigen kunskap om, samt erfarenhet av, verksamheten och dess informations- och cybersäkerhet. Informationen har sedan värderats och på så sätt har en mognadsgrad kunnat tas fram. Vidare har granskningen inkluderat analys och genomläsning av rutiner, policyer och strategier. Granskningen genomfördes under augusti och september 2019. Den dokumentation som PwC tagit del av återfinns som bilaga. Intervjuer inom ramen för granskningen har genomförts med:

- Hälso-och sjukvårdsdirektör
- Biträdande HR-chef
- Redovisningschef
- IT-säkerhetsansvarig
- Arkivarie, Informationssäkerhetssamordnare
- Informationssäkerhetssamordnare
- Säkerhetschef och beredskapschef
- Regionstyrelsens ordförande
- Regionstyrelsens vice ordförande
- Regionstyrelsens andra vice ordförande
- Medicinskt ledningsansvarig/Cosmic patientjournalsystem

2. Övergripande resultat - NIST

2.1 Inledning

NIST cybersäkerhetsramverk omfattar en riskbaserad sammanställning av riktlinjer som syftar till att hjälpa organisationer att identifiera, genomföra och förbättra säkerhetspraxis och skapa ett gemensamt språk för intern och extern kommunikation av säkerhetsproblem. Ramverket är en reiterativ process utformad för att utvecklas i synkronisering med förändringar när det kommer till säkerhetshot, processer och lösningar. Detta innebär i klartext att givet den konsekventa metodologin kan mätningen återupprepas för att kartlägga hur organisationen förflyttat sig i mognadsgrad.

Ramverket tillhandahåller en utvärdering av mekanismer som möjliggör för verksamheten att bestämma dess nuvarande cybersäkerhetsförmåga, sätta individuella mål och etablera en plan för åtgärder och upprätthållandet av cybersäkerhetsprogram. Detta innebär att resultatet nedan kan användas som utgångspunkt för ett systematiskt handlingsprogram framåt. Nivåerna varierar mellan 1 till 5, där 1 indikerar att medvetenheten om risker är låg, medan 5 indikerar att processer och program har etablerats och blivit väl implementerade i verksamheten. Organisationer rekommenderas att sträva mot att uppnå minst nivå 3 eller 4.

Begreppet cybersäkerhet som används utav NIST ramverket omfattar både informationssäkerhet och IT-säkerhet. Ramverket bygger på en indelning utifrån tre dimensioner - människor, processer, och tekniska verktyg - och berör därmed säkerhetskontroller som är administrativa, tekniska och kulturella. De fem funktioner som ramverket granskar täcker därmed in samtliga informationssäkerhetsprocesser.

2.2 Resultat NIST

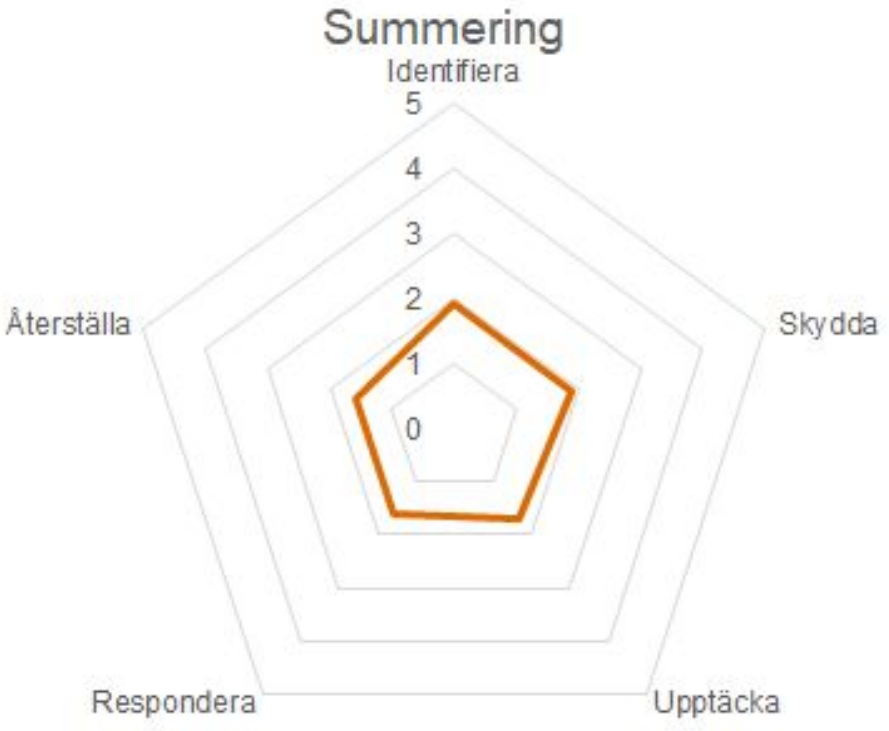
Det har utifrån en informationsinsamling, som bygger på dokumentationsgranskning och intervjuer, framkommit att det finns utrymme för förbättring när det kommer till regionstyrelsens styrning och uppföljning av informationssäkerhetsarbetet. De främsta bristerna berör Region Värmlands avsaknad av dokumenterade processer och ansvarsroller gällande ett flertal informations- och cyberssäkerhetsområden. PwC har noterat att Regionen ofta utför flera viktiga processer och rutiner inom informationssäkerhet, men att dessa utförs utan systematik.

PwC anser dock att Region Värmland har goda förståelser och rutiner kring informations- och cybersäkerhet när det kommer till verksamhetskritiska system som exempelvis Cosmic. Detta anses vara en avspegling av verksamhetens mognadsförståelse kring regionens roll som leverantör av samhällsviktiga tjänster. Region Värmland har till viss del genomfört övningar inom ramen för krisberedskap för att öva roller och ansvar kopplat till detta, dock inte kopplat till informations- eller cybersäkerhet.

Granskningen av Region Värmlands informationssäkerhet visar att det finns en hög medvetenhet om vikten av informations- och cybersäkerhet, både i det operativa och det strategiska arbetet. Det område som påvisar störst brister är avsaknaden av

formaliserade och strukturerade rutiner och processer, vilket främst visar sig genom avsaknad av aktuell och uppdaterad dokumentation som faktiskt används i Region Värmlands arbete. Vidare genomförs varken utbildning eller övning i en ändamålsenlig utsträckning och det saknas strukturerade rutiner och processer för kontroll och uppföljning.

Givet att Region Värmland är en leverantör av samhällskritiska tjänster, och givet att organisationer i allmänhet bör sträva efter nivå 3 eller 4, får regionens resultat inom de fem domänerna anses vara lågt. För mer detaljer kring respektive domän och bedömningen därvav, se bilagt arbetsmaterial *"Informationssäkerhetsgranskning Region Värmland"*.



Identifiera: 1,9
Respondera: 1,7
Skydda: 1,9
Återställa: 1,6
Upptäcka: 1,7

3. Iakttagelser och bedömningar

3.1 Kontrollmål 1: Regionen har ändamålsenlig och uppdaterad dokumentation på plats för arbetet med informationssäkerhet.

3.1.1 Inledning

Region Värmland har ändamålsenlig dokumentation inom vissa områden, men det saknas processer för regelbunden revision och uppdatering av dessa. Region Värmland har exempelvis en tydligt definierad *Strategi för Nätsegmentering* som fastställer en strategisk inriktning för tekniska nätverkssäkerhetsåtgärder, en viktig teknisk säkerhetsåtgärd som bidrar till att konfidentialitet, tillgänglighet och integritet inte röjs. Vidare använder regionen dokumenthanteringssystemet Platina och Vida/Canea One. Det finns även en dokumentationshierarki, som dock inte fungerar ändamålsenligt till följd av brist på samt ogiltiga dokument.

3.1.2 Iakttagelser

Utifrån PwC:s granskning har det framkommit att ett *systematiskt och kontinuerligt* uppdateringsarbete kring dokumentationen på IT- och informationssäkerhetsområdet ännu inte är på plats. Region Värmland har även endast en begränsad mängd dokumentation på plats för flera områden som berör informationssäkerhet. Regionen saknar väsentlig formell dokumentation för att styra sitt IT- och informations-säkerhetsarbete på en strategisk nivå som förankrar arbetet med Regionens centrala roll som leverantör av samhällsviktiga tjänster. Exempelvis saknas det en IT-säkerhetsstrategi, fastän ett sådant dokument efterfrågas av den övergripande *Säkerhetsstrategi för Landstingen Värmland*. Utöver detta har PwC iakttagit att det saknas en formell och dokumenterad process för att revidera och uppdatera dokumentation på en regelbunden basis. Informationssäkerhetspolicyn från 2012 förlängdes senast i augusti 2017 till 2018-12-31 (LK/171766). Sedan dess har den inte förlängts eller uppdaterats. Även dokumentation underordnad Informations-säkerhetspolicyn saknar regelbunden revision och uppdatering. PwC har dessutom iakttagit en otydlighet kring huruvida nuvarande dokumentation hör samman med varandra då många dokument saknar hänvisningar till övrig dokumentation.

PwC har även iakttagit att flera väsentliga informationssäkerhetsprocesser saknar dokumentation, antingen i form av processbeskrivningar, rutiner eller instruktioner, vilket kan kopplas till avsaknaden av en tydligt tillämpad dokumentationsstruktur. Nedanstående bild visar en vanligt förekommande struktur på en dokumentationshierarki inom ett ledningssystem för informationssäkerhet:

Figur 1: Exempel på dokumentationshierarki inom ett Ledningssystem för informations-säkerhet

PwC har iakttagit att Regionen har delar av denna dokumentationsstruktur på plats, med flera beskrivna instruktioner och rutiner, exempelvis *Reservrutiner vid driftstopp el, vatten, IT*. I flera fall finns det tydliga kopplingar mellan rutiner och riktlinjer. Regionen använder digitala verktyg som *Platina* och *Vida/Canea One* för att organisera dokumentationen.

Under intervjuer framkom att Region Värmland har som ambition att arbeta framåt i enlighet med ett ledningssystem för informationssäkerhet (ISO 27000), vilket bl.a. enligt intervjuer avspeglar sig i den dokumentation som är under utarbetning. Inom ett ledningssystem för informationssäkerhet bör den strategiska inriktningen för ett informationssäkerhetsarbete fastställas av en strategi och policy. En sådan strategi eller policy för informationssäkerhet bör ge en tydlig förklaring till syftet med ett gediget informationssäkerhetsarbete och bör även förstärkas av en underordnad standard som beskriver samtliga processer som informationssäkerhet omfattar. En sådan standard bör ge en inriktning för, och en beteckning av, samtliga processer som ska utföras och bör även hänvisa till underordnade dokument (processbeskrivningar och rutiner) som beskriver vem som ansvarar för utförandet av underordnade aktiviteter och hur det ska utföras. Processbeskrivningar bör i sin tur omfatta samtliga informationssäkerhets-åtgärder; administrativa, tekniska, och dem som riktar sig mot att skapa säkerhetskultur.

Med hänsyn till ovan har PwC iakttagit att Regionen saknar dokumentation för flera processer med bäring på ett strukturerat informationssäkerhetsarbete. Avseende exempelvis *riskhantering* (som berör informationssäkerhet), har PwC noterat att det saknas formell dokumentation. De processer som utförs inom riskhantering är varken dokumenterade eller formaliserade. Detta fastän den informationssäkerhetspolicy som antagits 2012 benämner riskhantering och riskbedömning som en huvudsaklig komponent i samband med informationsklassning. Det saknas även dokumentation som

fastställer en regionens riskaptit eller risktolerans som eventuella riskhanteringsåtgärder kan hänvisa till.

Utifrån intervjuer kan det konstateras att utkast till nya styrande dokument för informationssäkerhet, vilka ska beslutas under hösten, håller på att tas fram. Tidigare informationssäkerhetsdokumentation har använts som beslutsunderlag för Regionstyrelsen, men utöver de styrande dokumentens existens involveras inte Regionstyrelsen i regionens informationssäkerhetsarbete.

PwC har dock noterat att Region Värmland har dokumentation på plats för verksamhetskritiska system som Cosmic. Patientjournalsystemet har tydligt definierade återställningsplaner. Det finns även reservrutiner för IT som beskriver processer för avbrottsplanering och hur drift av kritiska system ska säkerställas. Inom området incidenthantering finns det även dokumenterade eskalerings- och delegationsordningar kring hur medarbetare ska agera under händelser.

3.1.3 Bedömning

Utifrån iakttagelser från dokumentationsgranskning och intervjuer är PwC:s bedömning att kontrollmålet **delvis uppfylls**.

Bedömningen är grundad i avsaknaden av regelbunden revision, granskning och uppdatering av samtlig dokumentation, iakttagelsen att vissa processer saknar dokumentation, samt i iakttagelsen att det saknas ett strukturerat ledningsarbete som samordnar samtlig väsentlig dokumentation. Detta speglas av den varierande förekomsten av dokumentation för informationssäkerhetsprocesser.

3.2 Kontrollmål 2: Regionen säkerställer styrning och uppföljning av dess informationssäkerhet på ett ändamålsenligt sätt.

3.2.1 Inledning

Utöver tydlig, beslutad och kommunicerad dokumentation kräver ett gediget informationssäkerhetsarbete även tydliga processer och rutiner för att säkerställa styrning och ändamålsenlig uppföljning. En strukturerad uppföljning och rapportering av resultat och efterlevnad av styrande dokument är en förutsättning för att styrelse och nämnder ska kunna följa upp och utvärdera förvaltningarnas uppdrag och verksamheternas arbete. Uppföljning är viktig för att regionens invånare ska få en inblick i verksamheten och säkerställa att offentliga medel används effektivt.

Region Värmland har nyligen genomfört en omorganisering som har direkt bäring på Regionstyrelsens förmåga att utöva adekvat styrning över IT- och informations-säkerhetsfrågorna, vilken innebär att Region-IT organisatoriskt numera ligger direkt under Regiondirektören. Detta innebär att det finns ett formellt utpekat ansvar för dessa frågor i organisationen.

Regionen har även ett Informationssäkerhetsråd som träffas minst en gång i kvartalet, och inkluderar flera nyckelpersoner med bäring på regionens informationssäkerhet.

Sedan ett antal år tillbaka använder regionen sig av PM3-modellen, vilket är en förvaltningsmodell.

3.2.2 Iakttagelser

Det tidigare landstinget Värmland saknade ett formellt strukturerat arbete utifrån ISO 27000-standarden och informationssäkerhetsfrågor tenderade att konstant omprövas. Det framåtsyftande arbetet med bl.a. omarbetad dokumentation har som ambition att vara i linje med ISO27000. Vid intervjuer framkommer att det generellt sett saknas central styrning i Region Värmland, vilket även identifieras som en sårbarhet och svaghet i regionen. Det framkommer under intervjuerna med både strategiska och operativa funktioner att det saknas en gemensam förståelse för nuläge, respektive önskat läge, gällande informationssäkerhet. Under intervjuer konstateras att det saknas bestämmelser och riktlinjer från Regionsstyrelsen respektive ledning avseende efterlevnad av säkerhetsbestämmelser och grundläggande inställningar och krav.

Det saknas rutiner för uppföljning av Region Värmlands framtagna och beslutade dokumentation på samtliga nivåer. Det framgår av intervjusvar att erfarenhetsåterföring och utvärderingar inte genomförs i önskad utsträckning. Vidare saknas det även rutiner för uppföljning för att säkerställa att identifierade förbättringar implementeras i verksamheten.

Under intervjuer framkommer det att finns en tydlig avsaknad av dokumenterade processer och ansvarsroller gällande ett flertal informations- och cyberssäkerhets-områden. Ett flertal viktiga processer och rutiner inom informationssäkerhet utförs *ad hoc* till följd av brist på styrning. Exempelvis saknas det en dedikerad grupp som endast arbetar och styr *asset management* (dvs tillgångshantering på hårdvarusidan). Att tillägga är dock att Region Värmland, som tidigare nämnt, under ett antal år använt sig av styr- och samverkansmodellen PM3 som används för förvaltning och verksamhetsutveckling i stort. Uppföljningen av aktiviteter och genomförda projekt sker dock inte kontinuerligt i verksamheterna i enlighet med PM3-modellen. Vid intervjutillfällen uppkom att ett återkommande problem anses vara att styrningen blir lidande till följd av att det inte finns några objektägare i regionens högsta ledningsgrupper.

Ansvaret för dokumentationen ligger hos området dokumentationen berör, exempelvis ansvarar IT-säkerhet för dokumentation gällande IT-säkerhet. Därmed finns det ett tydligt ägarskap inom tjänstemannaorganisation för dokumentation och processer kring informationssäkerhetsstyrning i form av framtagning av styrdokument, policys, riktlinjer och instruktioner. Det framkommer under intervjuer att det finns ett ansvar förankrat inom organisationen gällande just dokumentationen, men att kontinuerlig revidering av styrande dokumentation samtidigt betraktas som ett förbättringsområde.

Det kan konstateras att Region Värmland inte arbetar aktivt med rutiner och processer med syfte att fortsätta utveckla och stärka processen med arbetet kring efterlevnad av informationssäkerhet. Ett sådant arbete skulle inludera regelbunden revision och uppdatering av styrande dokument. I dokumentet *“Säkerhetsstrategi för Landstinget i Värmland”* från 2018 framgår att styrning och ledning inom säkerhetsområdet ska bli tydligare och effektivare genom framtagning av ett antal styrdokument,

informationssäkerhet inkluderat. Vidare framgår i samma dokument att informationssäkerhetssamordnare årligen ska rapportera till landstingsstyrelsen vilka skyddsåtgärder som behöver vidtas och som har genomförts avseende informationssäkerhetsområdet. Uppföljning av tidigare genomförda riskanalyser och informationsklassningar har dock inte genomförts.

Ytterligare ett exempel berör regionens arbete med datasäkerhet i förhållande till ett livscykelperspektiv, vilket innebär att titta på processer, verksamheter och rutiner ur ett helhetsperspektiv. Under intervjuer har det framkommit att regionen arbetar med livscykelprogram när det kommer till information som lagras, med planer för gallring och bevarande av information i förhållande till en livscykel. Däremot saknas det rutiner för en dataklassning i enlighet med ett livscykelsperspektiv samt protokoll kring eventuella beslut som tas utifrån ett sådant perspektiv, exempelvis dokumenterade utföranden av gallring. Det saknas även dokumentation kring vissa incidenthanteringsprocesser som till exempel förteckningar på tidigare incidenter och definierade incidentalerter. PwC har även iakttagit en avsaknad av uttalade responsstrategier för incidenter som har inträffat. Däremot har PwC tagit del av dokumentation avseende avvikelsehantering och incidentrapportering.

Region Värmlands rapporteringsvägar vid händelse av en incident beskrivs som otydliga. Det framkommer att Regionstyrelsen är otydlig i sin styrning gällande vilken sorts information som efterfrågas vid inträffade händelser, i vilka forum samt i vilken form. Detta kan exemplifieras genom att Regionstyrelsen aldrig kallat Region Värmlands IT-chef till Regionstyrelsens möten i syfte att erhålla avrapporteringar (inte heller efter genomförd omorganisation, 1 september 2019). Region Värmland formulerar årligen en skriftlig rapport om status på informationssäkerhet. Utöver det efterfrågats inga regelbundna rapporteringar från Regionstyrelsen, varken i muntlig eller skriftlig form.

Inom vissa områden finns dock en tydliggjord rollfördelning, där RKKB (regional katastrof- och krisberedskap) inkluderas. Det är en strategisk gruppering som aktiveras vid större händelser (även informationssäkerhetrelaterade) och ser bland annat över informationssäkerhet i förhållande till de tjänster som levereras inom regionen. Enligt intervjusvar finns lista på funktioner samt ersättare för gruppen.

Då omorganiseringen av Region-IT:s nya placering infördes så sent som den 1 september 2019 har dock ännu inga former för hur ofta återrapportering sker, eller vilka frågor som en sådan återrapportering ska innehålla, formaliserats. Det pågår även en rad olika insatser och projekt inom ramen för dessa verksamheter, däremot framkommer det att detta görs *ad hoc* och utan delegation från Regionstyrelsen.

3.2.3 Bedömning

Utifrån iakttagelser från dokumentationsgranskning och intervjuer är PwC:s bedömning att kontrollmålet är **delvis uppfyllt**.

När det gäller den generella bilden av Regionstyrelsens förmåga att styra och leda verksamheten, med bäring på IT- och informationssäkerhet, är bilden vi får att den hittills inte varit ändamålsenlig. Regionen saknar i stora delar ett *systematiskt* arbete med IT- och informationssäkerhet. *Detta är dock inte detsamma som att säga att arbete relaterat*

till dessa frågor inte bedrivs. Regionen har både en IT-avdelning (Region-IT) vilken numera sorterar direkt under RD, och regionen har likaså ett informationssäkerhetsråd, vilket innebär att det finns ett utpekat ansvar för dessa frågor i organisationen. Det pågår även en rad olika insatser och projekt inom ramen för dessa verksamheter.

Enligt vår bedömning saknas är nuläget *för det första* att det saknas en formaliserad systematik i hur arbetet bedrivs. *För det andra* saknas det en helhetsbild av vad som genomförs. Organisationen går inte i takt inte i alla delar vad gäller systematiken kring riskanalyser, informationsklassning och stödjande och styrande dokumentation, vilka alla utgör viktiga byggstenar i ett systematiskt IT- och informationssäkerhetsarbete.

Beträffande huruvida det överhuvudtaget är möjligt att skaffa sig en helhetsbild av vad verksamheten totalt sett gör för insatser inom IT- och informationssäkerhetsområdet är beskrivningen att IT-chefen kan lägga en del av pusslet och att den informationssäkerhetsansvariga (på informationshanteringsenheten) kan lägga en annan del, men att ingen äger helheten. Detta resulterar i ett fragmenterat IT- och informationssäkerhetsarbete.

Givet att Regionstyrelsen hittills inte regelbundet och med systematik efterfrågat återrapportering inom IT- och informationssäkerhetsområdet innebär detta vidare att inte heller Regionstyrelsen kan sägas besitta den helhetsbild som krävs för att styra, leda eller ge direktiv gällande informationssäkerhetsarbetet. Denna situation accentueras *för det tredje* ytterligare av avsaknaden av formaliserad och uppdaterad dokumentation av väsentliga styrdokument såsom IT- och informationssäkerhetsstrategier. Det är inte klart huruvida avsaknaden av vissa centrala styrdokument har lett till att styrsignalerna varit svaga, eller om de svaga signalerna lett till att vissa styrande dokument inte kommit på plats.

Regionens självbild i arbetet med IT- och informationssäkerhet, särskilt såsom den kommunicerats till revisorerna från dåvarande Landstingsstyrelsen, är att regionen presterar väl och ibland på en högre nivå än andra jämförbara regioner. Detta framkom både i Landstingsstyrelsens skrivelse från 2016 (LK/161169) samt i intervjuer med representanter från den administrativa ledningen. I och med resultatet av denna granskning kan denna självbild behöva justeras något, utan att ta udden av alla de goda initiativ och åtgärder som genomförs, just på grund av bristen på systematik i arbetet.

Den organisatoriska flytten av IT-säkerhet innebär att IT-frågorna nu fått ett helt annat strategiskt fokus och att kanalen till Regiondirektören (och via denne rapporteringen till Regionstyrelsen) är öppen på ett helt annat sätt än tidigare. I praktiken innebär detta att förutsättningarna nu finns på plats för en förändring i positiv riktning, och det kan finnas anledning att återkomma till just detta gränssnitt i kommande granskningar.

Sammanfattningsvis kan man säga att det genomförs arbetsinsatser inom både IT- och informationssäkerhet, men att den formella och systematiska sidan av detta arbete hittills tyngs av brister i form av tydliga rapporteringsvägar (framför allt på strategisk nivå), avsaknad av dokumentation, och delvis av avsaknad av riskanalyser och informationsklassning, vilket innebär att helheten uteblir.

3.3 Kontrollmål 3: Regionen har vidtagit åtgärder med anledning av bristerna i förstudien från 2015 och med anledning av regionbildningen 2019.

3.3.1 Inledning

Förstudien från 2015[1] benämnde flera brister inom IT- och informationssäkerhets-området. Bristerna listas nedan:

- Styrdokumenten (policydokument och därtill hörande tillämpningsföreskrifter) behöver förtydligas, uppdateras och kompletteras för att fortsatt bilda verkningsfull grund för bland annat vad som kan kallas IT-säkerhet.
- En väsentlig aktivitet i uppdateringen av styrdokumenten är att utföra analyser, få informationen klassad och tydliggöra för verksamhetens chefer att de har det yttersta praktiska ansvaret för informationssäkerheten. Landstingsstyrelsen har att inse att detta även innebär återkommande utbildning av och/eller information till alla delar av verksamheten.
- Landstingsstyrelsen kan förbättra och tydligt ange hur de vill få arbetet med informationssäkerheten rapporterad till sig. I samband med detta kommer det att underlätta för praktiskt ansvariga om styrelsen också anger på vilket sätt denna rapportering kommer att nå medborgarna.
- Det finns motiv för revisionen att fortsättningsvis på olika sätt omfatta informationssäkerhet i kommande granskningar.

Som framkommit under iakttagelserna för kontrollmål 1 och 2 kan det konstateras att det endast finns ett begränsat antal styrdokument för informationssäkerhet på plats. Vidare konstateras att det fortfarande saknas systematisk och kontinuerlig revidering av dokumentation för IT- och informationssäkerhet. En ny riktlinje för informationssäkerhet i Region Värmland är påbörjad och kommer enligt intervjuade uppskattningsvis beslutas under hösten 2019. Den påbörjade riktlinjen kommer att slå fast hur organisation, roller och ansvar för informationssäkerhet på en övergripande nivå ska utformas i regionen och kommer vidare att vara en del av Region Värmlands ledningssystem för informationssäkerhet.

3.3.2 Iakttagelser

Den tidigare informationssäkerhetspolicyn för Region Värmland skapades 2012 samt förlängdes 2017. Giltighetstiden för förlängningen ut 2018-12-31, vilket innebär att det under granskningens gång inte funnits någon aktuell, giltig eller beslutad informations-säkerhetspolicy på plats.

Utifrån intervjuer har det framkommit att regionen inte har slutfört den påbörjade systematiska klassningen av sina informationstillgångar. I det svar till revisorerna som dåvarande Landstingsstyrelsen avgav i samband med 2015 års förstudie av IT-säkerhet,

[1] Landstinget i Värmland *Förstudie IT-säkerhet,* KPMG

har ett sådant arbete påbörjats inom ramen för förvaltningsmodellen PM3. Klassificering av IT-system med avseende på informationssäkerhet genomförs av regionen men samtliga verksamhetssystem har inte klassats utifrån informationssäkerhetskrav. Enligt intervju med IT-chef har Regionens arbete i samband med införandet av GDPR inneburit att frågan om klassning av personuppgifter kom upp på agendan. Däremot har någon systematisk genomgång av övriga informationsklasser inte genomförts mer än sporadiskt. Dock har Regionen visat en förståelse för känslig och skyddsvärd information, exempelvis patientjournalsystemet Cosmic (ett verksamhetskritiskt system) som anses innehålla information i högsta säkerhetsklass. Det saknas dokumentation i form av exempelvis instruktioner för informationsklassning i regionen. Däremot finns rutiner och processer på plats för riskanalys i samband med upphandlingar och i samband med införandet av nya system.

Avseende åtgärder vidtagna med anledning av regionbildningen som genomfördes 1 januari 2019 så har nya verksamheter, bland annat kollektivtrafik och folkhögskolor, tillkommit. Från ett IT-perspektiv är Region Värmland i skrivande stund i färd med att kartlägga de system och tjänster som tillförts verksamheten. Det framkommer i intervjuer att det finns misstanke om att flertalet system kan komma att vara verksamhetskritiska, exempelvis systemstödet inom kollektivtrafiken, men detta har ännu inte klargjorts.

Som konstaterats i iakttagelserna under kontrollmål 2 noteras att någon särskild rapportering om status på IT-säkerheten ännu inte efterfrågas av Regionstyrelsen. I dokumentet *Svar på revisionsrapport om IT-säkerhet* (LK/161169) framgår att informationssäkerhetsincidenter och IT-säkerhetsincidenter sammanställs i en årlig informationssäkerhetsrapport. Det sker dock ingen löpande rapportering, utöver den årliga rapporteringen, om informationssäkerhet till Regionstyrelsen i dagsläget.

Utöver detta har det, enligt intervjusvar, varit många andra frågor inom regionen som haft en högre prioritet i det förändringsarbete som regionbildningen innebar, exempelvis frågor kring ekonomi, redovisning, personalfrågor och inrymmandet av nya verksamheter. I detta har IT- och informationssäkerhetsfrågorna fått stå tillbaka. Det har inte skett någon ytterligare medelstilldelning till IT i samband med regionbildningen.

3.3.3 Bedömning

Utifrån iakttagelser från dokumentationsgranskning och intervjuer är PwC:s bedömning att kontrollmålet **delvis uppfylls**.

Bedömningen är grundad i avsaknaden på regelbunden revision, granskning och uppdatering av samtlig dokumentation samt att vissa processer saknar dokumentation. Det saknas giltig och beslutad dokumentation inom ett flertal områden, däribland informationssäkerhet inkluderat. Att Regionstyrelsen endast efterfrågar en rapportering årligen resulterar i att medvetenheten om informationssäkerhet inte kan säkerställas.

De positiva effekterna av de riskanalyser som genomförs i samband med upphandlingar uteblir om riskanalyserna inte kan sättas i relation till regionens totala riskkarta, vilken i nuläget åtminstone delvis saknas. Detta grundar sig i att det förekommer

riskbedömningar på bredare front, exempelvis inom Region Värmlands hälso- och sjukvårdsverksamhet.

Bristen på systematisk informationsklassning resulterar i svårigheter för regionen att skapa en helhetsbild av hur IT- och informationssäkerhetsarbetet ska bedrivas för att adressera och minimera de risker som olika informationsklasser innebär. Samma sak gäller för ett systematiskt arbete med risker kopplat till IT- och informationssäkerhet.

4. Revisionell bedömning

De övergripande revisionsfrågorna för aktuell informationssäkerhetsgranskning är följande:

- *Har Regionstyrelsen säkerställt en styrning (exempelvis genom beslut och riktlinjer, budgetmedel) och uppföljning som ger en ändamålsenlig informationssäkerhet? Detta särskilt mot bakgrund av regionbildningen (bland annat ny organisation, nya system, nya verksamheter).*

PwC:s bedömning är att Regionstyrelsen **inte helt** har säkerställt en styrning och uppföljning som ger en ändamålsenlig informationssäkerhet. Grunden till denna bedömning är den nuvarande avsaknaden av regelbunden revision, granskning och uppdatering av styrande dokumentation, avsaknaden av dokumentation för vissa väsentliga informationssäkerhetsprocesser, samt bristande kontinuerlig uppföljning och rapportering kring informationssäkerhetshändelser och incidenter till Regionstyrelsen.

- *Har Regionstyrelsen vidtagit åtgärder med anledning av de brister och de förbättringsförslag som framfördes i förstudien 2015 samt har åtgärder vidtagits i enlighet med det svar som dåvarande landstingsstyrelsen tillställde revisorerna?*

PwC bedömer även att Regionstyrelsen **inte helt** har vidtagit och kommit i mål med åtgärder med anledning av de brister och förbättringsförslag som framfördes i förstudien 2015. Denna bedömning bygger på den iakttagna avsaknaden av både systematisk informationsklassning av samtliga system samt regelbundna och dokumenterade riskanalyser, vilket är åtgärder som rekommenderades av förstudien. Den ovan nämnda punkten kring brister med styrningen och dokumentation påvisar således att det fortfarande finns ett förbättringsarbete som regionen bör utföra.

- *Om granskningen påvisar brister, vilka rekommendationer ges?*

Med hänvisning till de brister som identifierats följer här nedan en förteckning på rekommendationer som regionen bör ta i åtgärd. Revisionsfrågorna besvaras vidare utifrån följande formulerade kontrollmål:

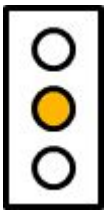
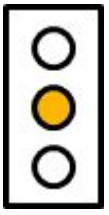
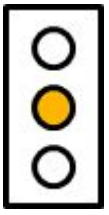
1. Regionen har ändamålsenlig och uppdaterad dokumentation på plats för arbetet med informationssäkerhet.

2. Regionen säkerställer styrning och uppföljning av dess informationssäkerhet på ett ändamålsenligt sätt.

3. Regionen har vidtagit åtgärder med anledning av bristerna i förstudien från 2015 och med anledning av regionbildningen 2019.

Rekommendationer återges därefter.

4.1 Bedömningar mot kontrollmål

Kontrollmål	Kommentar	
Kontrollmål 1: Regionen har ändamålsenlig och uppdaterad dokumentation på plats för arbetet med informationssäk erhet.	**Delvis uppfyllt** Bedömningen är grundad i avsaknaden av regelbunden revision, granskning och uppdatering av samtlig dokumentation samt att vissa processer saknar dokumentation.	
Kontrollmål 2: Regionen säkerställer styrning och uppföljning av dess informationssäk erhet på ett ändamålsenligt sätt.	**Delvis uppfyllt** Bedömningen grundar sig i bristen på involvering från Regionstyrelsen avseende informationssäker-het samt avsaknad av kontroll och uppföljning av dokumentation, pågående arbete och inträffade händelser.	
Kontrollmål 3: Regionen har vidtagit åtgärder med anledning av bristerna i förstudien från 2015 och med anledning av regionbildningen 2019.	**Delvis uppfyllt** Bedömningen grundar sig i att flertalet åtgärder påbörjats, men att majoriteten ännu inte slutförts samt att många ännu inte initierats.	

Rekommendationer

Människor och processer:

- Dokumentera huvudsakliga informationssäkerhetsprocesser. Säkerställ och tydliggör roller, ansvar och mandat.
- Säkerställ att samtlig dokumentation är uppdaterad och giltig.
- Säkerställ att informationssäkerhetspolicyn ses över och revideras med lämpliga intervall samt att riktlinjerna följs upp med regelbundenhet. Dessutom bör riktlinjerna revideras så att det tydligt framgår ansvarig för vidare uppdatering.
- Identifiera och definiera mätbara mål för samtliga åtgärdsmål i syfte att följa upp dessa kontinuerligt. Därtill bör regionen slutföra omsättningen av principerna beskrivna i informationssäkerhetspolicyn till riktlinjer.
- Etablera en obligatorisk informationssäkerhetsutbildning för samtliga anställda i Region Värmland. Säkerställ att utbildningar och övningar för att utveckla och säkerställa kompetens om informationssäkerhet genomförs regelbundet.
- Specificera i den kommande verksamhetsplanen de aktiviteter som ska genomföras i syfte att främja en god säkerhetskultur. Regionen bör även genomföra systematiska uppföljningar av utbildningsverksamheten.
- Formalisera utvärderingsarbetet efter en inträffad incident för att säkerställa att åtgärder genomförs för att förhindra att liknande incidenter inträffar igen.
- Minska personberoendet för att säkerställa att verksamheter kan fortlöpa vid ett eventuellt personalbortfall.
- Med hänsyn till den nya lagstiftningen inom säkerhetsskydd från april 2019 bör Region Värmland genomföra en djupare analys av regionens kritiska informationstillgångar för Sveriges säkerhet.

Teknik:

- Undersök möjligheten till att införskaffa en SIEM-lösning som aggregerar säkerhetsloggar från väsentliga nätverkspunkter och skapar relevanta alerter.
- Implementera behörighetstilldelning och behörighetsgrupper som baseras på i förväg bestämda roller.
- Automatisera sårbarhetsskanning så att det genomförs på regelbunden basis och dokumentera processen.
- Utöka den geografiska spridningen på regionens serverhallar för att säkerställa redundans.

Bilaga

Dokumentationslista

- AVDS (karta)
- AVDS Reporting Methodology - High Accuracy and Consolidation
- Benefits and Features for AVDS Vulnerability Management Solutions
- Information, utrustning och nätverk
- IT-utrymmen
- Publikt nät
- Molntjänster inom RV
- Organisationsskiss med verksamhetsområden
- Organisationsskiss övergripande
- Ny Informationssäkerhetspolicy
- Förstudie IT-säkerhet Rapport KPMG
- Hantering av Office 365 som molntjänst
- Informationssäkerhet i Region Värmland
- IT-säkerhetsregelverk
- Strategi för nätsegmentering
- Förlängning av giltighetstid för informationssäkerhetspolicy
- Säkerhetspolicy för Region Värmland
- Säkerhetsstrategi för Landstinget i Värmland
- RUTIN FÖR INFORMATIONSSPRIDNING VID STÖRRE DRIFTSTÖRNING
- Verksamhetsanalys avbrottsplanering
- Åtkomst till medarbetares konto
- Säkerhet vid planerad stängning av lokaler
- Rapportera informationssäkerhetsincidenter
- Kommunikationsfunktion i lokal särskild sjukvårdsledning
- Kommunikationsfunktion i regional särskild sjukvårdsledning
- Kriskommunikationsplan
- Logghantering vårdinformationssystem
- Avbrottsplanering
- Tillträde lokaler
- Skalskydd och larm
- Reservrutiner vid driftstopp el, vatten, IT
- Reservrutin vid driftstopp eller driftstörningar i Cosmic
- Svar på revisionsrapport om IT-säkerhet

2019-10-15

Maria Jäger

Linus Owman

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av Region Värmland enligt de villkor och under de förutsättningar som framgår av projektplan från den 24 oktober 2018. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.