Uppföljning av 2019 års granskning av IT-säkerhet

Redovisningsrevision 2022

Region Skåne

Region Skåne
Uppföljning av 2019 års granskning av IT-säkerhet

2023-02-16

Innehållsförteckning

1 Sammanfattning

KPMG har på uppdrag av Region Skånes revisorer följt upp synpunkter och rekommendationer från granskningen *”IT-säkerhet med inriktning på system som har betydelse för intern kontroll inom redovisningen”, 2019*. Granskningen var inriktad mot de för verksamheten betydelsefulla centrala ekonomi-och personalsystemen Raindance och Personec P, men inkluderade också regionens arbete med IT säkerhet, informationssäkerhet och dataskydd.

I det följande sammanfattas de mest väsentliga iakttagelserna från denna uppföljning:

Vi har noterat att det i samband med Dataskyddsförordningens ikraftträdande (maj 2018) utfördes kartläggning/registerföring av känsliga informationsslag lokalt vid regionens olika förvaltningar. Kartläggningen, liksom efterföljande arbete med klassificering, riskanalys, beslut om skyddsåtgärder samt lokalt införda skyddsåtgärder, dokumenterades utan gemensam struktur vid de olika förvaltningarna. Arbetet har därför inte kunnat sammanställas eller följas upp centralt. Av denna anledning finns osäkerhet med avseende på det genomförda arbetets omfattning och kvalitet. Exempel på noterat kvarvarande arbete är att endast 1/3 av region Skånes befintliga system hittills klassificerats.

Enligt beslutat ”*årshjul*” har central funktion för informationssäkerhet inom regionen efterfrågat information om det lokala arbetet för att kunna sammanställa aktuell status. Lokalt varierande svarsfrekvens, svarskvalitet, har medfört att detta inte varit möjligt.

Beslut har nu fattats om att införa ett gemensamt systemstöd (*iFacts*) och därmed enhetlig struktur, för att dokumentera genomfört arbete. Införandet av systemet planeras ske under 2023.

Vår rekommendation är att prioritera införandet av detta systemstöd för att möjliggöra uppföljning på central nivå. Härigenom skapas underlag för beslutsinstanser att rikta åtgärder där detta behövs.

Vi rekommenderar regionen att fastställa ”Key Performance Indicators” (KPI:er) som omfattar hela arbetsprocessen för informationssäkerhet (*Bild 1, pkt 9.1.5*), samt att besluta om regelbunden uppföljning och rapportering utifrån dessa. Dessutom bör uppföljningen ske mot respektive operativ enhet inom regionen, dels för att göra det möjligt att mer effektivt rikta åtgärder, men också för att undanröja eventuella otydligheter med avseende på ansvarsfördelningen för att genomföra arbetet med informationssäkerhet.

Nedan följer övriga noteringar/rekommendationer till Regionstyrelsen i punktform. För bättre insikt om bakgrundsförhållanden rekommenderas genomläsning av hela rapporten. Hänvisning till respektive punkt i rapporten anges inom parentes. Vi rekommenderar att

- externa parters leverans granskas av oberoende part för att säkerställa att leveransen utförs enligt avtal (*9.1.1*)
- inställningarna för autentisering via lösenord av användare i Raindance förstärks (*9.1.1*)
- tillämpad periodicitet av inaktivitet i Raindance (24 månader), för att inaktivera användarkonto bör kortas (*9.1.1*)
- regionen utvecklar gemensamma krav på autentisering via lösenord utifrån resultatet av respektive systems klassificeringsnivå *(9.1.1*)
- rutin som gör det möjligt att säkerställa alla användares aktualitet i Raindance bör införas. (*9.1.3*)
- rutin införs för att möjliggöra kontroll av aktiviteter som utförs av användare med höga behörigheter i Raindance (*9.1.3*)

— gruppkonton inte används, eftersom det förhindrar möjligheten att konstatera att endast behörig åtkomst till känsliga informationsslag förekommit (9.1.4).

2 Bakgrund

KPMG har på uppdrag av Region Skånes revisorer följt upp synpunkter och rekommendationer från granskningen under 2019 av ”IT-säkerhet med inriktning på system som har betydelse för intern kontroll inom redovisningen”. Av denna anledning har granskningen inriktats mot de centrala ekonomi- och personalsystemen Raindance och Personec P, båda av stor betydelse för regionens verksamhet.

Utgångspunkt för den under 2019 genomförda granskningen var för området relevanta styrande dokument, vilket inte enbart begränsades till aspekter utifrån IT-säkerhet (enligt granskningens rubricering), utan även aspekter på regionens arbete med informationssäkerhet. Regionens arbete utifrån Dataskyddsförordningen (2018:218) berördes också. Eftersom begreppet informationssäkerhet i allt större utsträckning numera används som ett samlingsbegrepp där såväl dataskydd som IT-säkerhet ingår, sker denna uppföljning även med denna utgångspunkt.

3 Syfte/revisionsfrågor

Det övergripande syftet med denna granskning är att följa upp regionens åtgärder utifrån rekommendationer enligt granskningen från 2019.

Därtill kommer ett utökat fokus att riktas mot att användares rättigheter i Raindance på ett lämpligt sätt begränsats till respektive användares eget ansvarsområde.

4 Avgränsning

Uppdraget är en uppföljning av den tidigare granskningen varför den avgränsats till att granska system som hanterar stora transaktionsvolymer i avsikt att säkerställa en korrekt redovisning. IT-miljön för granskningen har därmed begränsats till att inkludera systemen Raindance och Personec P, i enlighet med den tidigare granskningen.

5 Revisionskriterier

De revisionskriterier som låg till grund för granskningen 2019 var enligt följande:

— Gällande lagstiftning inom området (förordning (2018:1175) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS)

— Relevanta styrdokument

— Relevanta delar från användandet av ISO 27001:2013

Dessa kriterier ligger därför också till grund för denna uppföljning.

6 Ansvarig nämnd

Granskningen avser regionstyrelsen.

7 Metod

Uppdraget har utförts genom intervjuer med följande personer inom Region Skåne:

— Jeanette Johansson, Enhetschef IT stöd HR, Koncernkontoret

- Sara Persson, Controller, Verksamhetsansvarig Affärssystem, Koncernstab Inköp & Ekonomistyrning
- Helene Löwgren, t f Informationssäkerhetschef, Koncernkontoret
- Evelina Cederholm, Dataskyddsombud, Koncernkontoret
- Peter Back – Processledare för redovisning och bokslut, Koncernkontoret
- Ola Blixt, Verksamhetsspecialist Raindance, Gemensam Service, Regionservice
- Martin Hanqvist, Systemansvarig Raindance, Digitalisering IT och MT
- Peter Feldt, IT-säkerhetsansvarig, Digitalisering IT och MT

Granskningen av användares åtkomst i Raindance ”utanför eget område” har bland annat inriktats mot aktiva användarkonton, dess aktualitet (”senast login”) samt de ”företag” som tilldelade rättigheter avser i förhållande till respektive användares ”huvudföretag”. Dessutom har vi granskat hur beslutad ”Segregation of Duty” (SoD) stöds utifrån hur användares rättigheter i Raindance tilldelats.

Vi har därutöver erhållit ett antal styrande dokument vilka granskats som utgångspunkt för respektive granskningsområde. I de fall styrande dokument använts vid granskningen framgår detta vid respektive avsnitt nedan.

8 Projektorganisation

Granskningen har genomförts av Jan-Inge Hedin från KPMG under januari – februari 2023.

9 Granskning

9.1 Inledning

Aktuell status för rapporterade noteringar och rekommendationer framgår nedan inom områdena ”Raindance”, ”Personec P”, ”Resultatet av analys av användares rättigheter utanför eget område i Raindance”, ”IT säkerhet” samt ”Informationssäkerhet”. I stort följer detta strukturen från granskningen 2019.

För att inte tynga rapporten i onödan har vi valt att utelämna granskningspunkter med mindre betydelse och där inga rekommendationer lämnats.

9.1.1 Raindance

- Med avseende på rekommendationen om formellt avtal med CGI (leverantör av Raindance) med avseende på dess **leverans,** noterades redan 2019 att detta fanns.
  - *Status:* Det kan noteras att CGI:s rutiner för leverans inte granskats av oberoende part. En sådan bör utföras utifrån någon av förekommande globala standards. Syftet med en sådan granskning är att säkerställa att Region Skåne inte har oönskade/okända risker i sin verksamhet. Sådan granskning rekommenderas.
- Granskningen 2019 visade på förekomsten av anonyma **gruppkonton** i strid mot styrande dokument.
  - *Status:* Avseende analys av förekomst av gruppkonton hänvisas till punkt 9.1.3.
- Granskningen 2019 visade svagheter i rutinerna för att säkerställa att **användares rättigheter uppdateras** tidsenligt.

- *Status:* Nytt regelverk har fastställts, ”*Rutiner och riktlinjer för hantering av behörigheter i Raindance”* (2022-05-04). För effektivitet är detta beroende av att ansvariga chefer i tid informerar behörighetsadministrationen om anställds arbets- och ansvarsförändring. Eftersom detta inte alltid fungerar bör förvaltningarnas rutiner stärkas i detta avseende. Enligt regelverket skall användarkonto inaktiveras efter 24 månaders inaktivitet. Vi rekommenderar att en betydligt kortare periodicitet för inaktivering tillämpas. IAM-projektet (Identity Access Management), varigenom automatisering bedöms kunna ske, har ännu inte införts.
- Se vidare vid resultatet av vår fördjupade granskning av användarkontons aktualitet (Pkt 9.1.3).

— Granskningen 2019 visade behov av att stärka rutinen för **autentisering** (identifiering) vid inloggning i Raindance.

- *Status:* SSO (Single-Sign-On mot nätverket) har ännu inte implementerats för användare i Raindance. Det betyder att systemfunktioner i Raindance för inställning av krav på lösenord (teckenlängd, komplexitet mm) gäller.
- De aktuella inställningarna är väldigt svaga: *Teckenlängd: 6, Ej komplexitet, Bytesfrekvens 90 annars inaktivering efter 180*.
- Regionen saknar beslut om generella krav för autentisering via lösenord. Sådana krav bör utvecklas som utgångspunkt för olika klassificeringsnivåer vid klassificering utifrån systems behov av ”konfidentialitet”.
- Aktuell situation för Raindance, med svaga lösenordskrav samt stor möjlighet att gissa lösenord, skapar oönskade risker för obehörig åtkomst och därmed förknippade risker för redovisningen. Vi rekommenderar regionen att tillämpa betydligt starkare krav.

— Granskningen 2019 visade på behov att säkerställa efterlevnad av den årliga rutinen som avser godkännande av **rolluppsättningen** i Raindance. Dessutom planerades ett nytt specifikt kompetensområde för behörigheter, attester och beställare.

- *Status:* Årlig inventering, för att säkerställa tilldelade behörigheter samt attesträtter, sker numera. Angivet kompetensområde är uppstartat. Omorganisationer kan, enligt intervju, förklara viss tidsmässig tröghet i erforderliga behörighetsjusteringar. Beslut om oönskade kombinationer av rättigheter (”Segregation av Duties”, SoD) omfattar kombinationen att ”*Registrera leverantör*”, ”*Hantera betalning*” samt ”*Tilldela attesträtt*”. Resultatet av fördjupad analys av behörighetsfördelning framgår vid avsnitt 9.1.3.

— Vid granskningen 2019 rekommenderades regionen att stärka rutinerna för ändringshantering.

- *Status:* Systemstödet ”Ritz” (ServiceNow) har införts för ändringshantering samtidigt som rutinerna för processen har uppdaterats. Enligt intervjuer har detta medfört stora förbättringar.

9.1.2 Personec P

— Vid granskningen 2019 noterades användningen av gruppkonton i strid mot gällande föreskrifter.

- *Status:* Det förekommer numera inte gruppkonton i Personec P.

— Vid granskningen 2019 rekommenderades regionen att införa en automatisk kontroll för borttag av behörigheter då anställd avslutar sin anställning. Vidare rekommenderades en uppföljningskontroll av behörighetsgenomgångar. Samordning planerades ske med IAM projektet för att på sikt automatisera kontrollerna.

- *Status:* Automatiserade rutiner har ännu inte införts. Däremot framgår att rutin för behörighetskontroll har införts och tillämpas regelbundet.

- Vid granskningen 2019 rekommenderades regionen att införa SSO vid inloggning. Det fanns olika inloggningsförfarande för olika roller. SSO används för vissa roller (vanlig medarbetare) medan chef och löneadministration använder sina systemkonton.
  - *Status:* Generell inloggning via SSO har ännu inte införts. Däremot kommer rutin med generell inloggning till Personec via SSO tillsammans med personliga SITHS-kort att testas inom kort.

9.1.3 Analys av användares rättigheter ”utanför eget område” i Raindance

Vi har beställt och erhållit uppgifter om användarkonton, rättigheter samt företagstillhörigheter i Raindance per 2023-01-18. Informationen har sammanställts i nedan tabeller.

Användarkonton i Raindance	
- Totalt antal användarkonton	24 522
- Antal Spärrade	3 231
- Antal inaktiverade ("G99")	11 796
- Antal aktiva (ej spärr, ej "G99")	**9 495**
- Varav saknar datum för "senast inlog"	2 217
- Varav utan rätt till något företag (”0”)	2 014
- Varav inaktiva> 24 mån	1 084
- Varav inaktiv> 90 dagar	2 027
- Varav "Lösen går ut" <”Senast inlog"	183

Tabell 1.

Noteringar

- Ett stort antal användarkonton saknar datum för ”Senast inloggning”
  - 51 av dessa är användare i CGI vilka eventuellt använder ett alternativt sätt för inloggning varigenom datum inte framgår.
  - Avsaknad av datum för resterande användare är osäker, men enligt intervju kan anledningen vara att de aldrig använts.
- Mängden användare med datum för senast inloggning> 24 månader (respektive 90 dagar) visar på förekomsten av en stor andel inaktiva användare där konton ändå är aktiva.
- Förekomsten av konton med datum för ”Lösen går ut” före ”Senast inlog” är ologisk, eftersom signalen om ”Lösen går ut” borde släckts om lösen uppdaterats. Vi har därför bortsett från uppgiften om ”Lösen går ut”.

Användare med rätt att "Registrera ny leverantör" och "Registrera attesträtt" (G16) samt "Hantera faktura" (G24)	
- Antal användare med rätt att "Hantera faktura" (G24)	28
- Varav rättighet till "samtliga företag" ("-1")	28
- Varav med rätt att "Registrera ny leverantör" eller "Registrera attesträtt" (G16)	0
- Antal användare med rätt att "Registrera ny leverantör" eller "Registrera attesträtt" (G16)	5
- Varav rättighet till "samtliga företag" ("-1")	5
- Varav med rättighet att "Hantera faktura" (G24)	0

Tabell 2.

Noteringar

— Grupperna G24 respektive G16 används för att ”Hantera faktura”, ”Registrera ny leverantör” och ”Registrera attesträtt”. Vår uppföljning visar (*Tabell 2*) att användare i dessa grupper har separerats på ett sätt som följer SoD beslutet.

— Samtliga användarkonton i de aktuella grupperna har möjlighet att utföra tilldelade uppgifter i samtliga företag enligt inställningen ”-1”. Exempel på anledning till att inte användare kopplas till enbart ”eget företag”, är omorganisationer där verksamheter byter företagstillhörighet.

Övriga användare med behörighet att "Registrera ny leverantör" (40RG), "Registrera attesträtt" (37MSP) samt "Hantera faktura" (33LR)	
- Antal användare med rätt att "Hantera faktura" utanför gruppen G24 (33LR)	136
- Varav rättighet till "samtliga företag" ("-1")	109
- Varav utan rätt till något företag ("0")	21
- Varav med rätt till enstaka företag	6
- Varav med rättighet att "Registrera attesträtt" (37 MSP)	81
- Varav användare i gruppen GR0 (samtliga CGI-användare)	56
- Varav användare i grupperna GR1 eller GR2 (systemförvaltare)	8
- Varav användare utan grupptillhörighet (->)	17
- Varav användare från CGI	11
- Varav gruppkonton (Se nedan)	4
- Varav individuella användare från Region Skåne	2
- Varav med rättighet att "Registrera ny leverantör" (40RG)	80
- Dessa användare fördelas som ovan (33LR och 37MSP)	

Tabell 3.

Noteringar

— Förutom CGI (GR0) och systemförvaltarna (GR1, GR2) har två individuella användare i Region Skåne behörighet att såväl ”Hantera faktura” som att ”Registrera attesträtt” och ”Registrera ny leverantör”. Vid intervju framkom att *”dessa två kom upp i senaste inventeringen men eftersom det varit oklart vem som ska skriva på avslut av deras behörighet är det inte gjort, men kommer att göras nu”*.

— Gruppkonton har senast varit aktiva enligt följande:

- System manager 2020-09-30
- Testgrupp 2007-04-12
- Centralen 2013-10-03
- Logica Kundsupport 2014-05-26

Användarkonton med starka rättigheter (Adminrättigheter)	
- Antal användarkonton som tillhör CGI	68
- Varav i grupp GR0 (Högsta rättighetsnivå i Raindance)	56
- Varav saknar grupptillhörighet (->)	11
- Varav i grupp GR1	1
- Varav saknar datum "Senast inlog"	56
- Varav med datum för "Senast inlog”> 24 mån	9
- Antal användarkonton med rättigheter i GR1 och GR2 (egna användare)	8

Tabell 4.

Noteringar

- En stor andel av CGI:s användarkonton har inte aktuella datum för ”senast inlog” (där detta framgår). Rättigheterna ”GR0” är högre än GR1 och GR2. Denna nivå har endast CGI användare.
- Eftersom det för flera av CGI:s användare saknas datum för ”senast inlog” kan inte Region Skånes systemförvaltare bedöma aktualiteten för CGI:s användarkonton. I syfte att säkerställa att CGI-användare är aktuella har särskild rutin (intern kontroll) överenskommits mellan parterna.

9.1.3.1 Samlade bedömningar och rekommendationer

Ambitionen vid granskningen av användares rättigheter ”utanför eget område” var att verifiera om användare inom en verksamhet har möjlighet att påverka andra verksamheters redovisning. Komplex behörighetsstruktur samt förekommande omorganisationer (till exempel flytt av verksamheter mellan ”företag” i Raindance) har medfört att tilldelningen av rättigheter i Raindance ofta inkluderar samtliga ”företag” (”-1”). Eftersom inställningen ”-1” ger användare åtkomst till samtliga företag är inte rättigheterna begränsade till specifikt ansvarsområde (företag) varför vår granskningsambition inte varit möjlig att fullfölja.

Regionens arbete för att undvika olämpliga kombinationer av rättigheter (SoD) begränsas till hanteringen av leverantörsfakturor. Vi har analyserat efterlevnaden av detta beslut (separering av rättighet att ”Hantera faktura” från rättigheterna att ”Registrera ny leverantör” samt ”Hantera attesträtt”). Resultatet visar att dessa rättigheter separerats helt i enlighet med SoD- beslutet för ”vanliga” användare. Däremot har, av naturliga skäl, användare med höga behörigheter stora möjligheter att även påverka operativt varför andra kontroller av dess aktiviteter här bör införas.

Som framgår av Tabell 4 förekommer ett stort antal konton med höga behörigheter. Dels omfattar detta 68 användarkonton från CGI, dels 9 ”egna” användarkonton (systemförvaltare). Enligt noteringar från riskbedömning av Raindance planerar regionen att under 2023 införa rutin för loggning av externa användarkonton av identifieringssyfte. Vi rekommendera regionen att också införa rutin för loggning av aktiviteter utförda av användarkonton med höga behörigheter. Detta för att ge möjlighet att kontrollera att endast användare med operativt ansvar påverkar verksamheternas löpande operativa verksamhet.

Region Skåne har anledning att minst anlägga samma begränsning avseende aktualitet och rättighetsnivå för externa användarkonton som för egna användare. Eftersom de flesta CGI användare tillämpar metod för inloggning som inte skapar datumstämpel vid inloggning, har det via vår analys inte varit möjligt att verifiera aktualiteten för de flesta av dessa användare. Däremot förekommer 9 CGI användare (Tabell 4) där datum för senaste aktivitet> 24 månader.

Som tidigare noterats rekommenderas regionen att tillämpa en betydligt kortare period (f n 24 månader) av inaktivitet för inaktivering. Detta kommer att minska risken för obehörigt användande av aktiva konton som inte används. Analysen visar (Tabell 1) förekomsten av en stor mängd konton som varit inaktiva under lång tid. Tabellen visar att det också förekommer konton som varit inaktiva under längre tid är 24 månader men som fortfarande är aktiva.

9.1.4 IT säkerhet

Vi har sammanställt noteringar och rekommendationer med avseende på IT säkerhet från granskningen 2019 enligt nedan och följt upp utvecklingen sedan dess med regionens IT säkerhetssamordnare enligt nedan.

- Vid granskningen 2019 noterades förekomsten av gruppkonton i kombination med kraftfulla behörigheter i system. Detta bör undvikas eftersom det begränsar spårbarheten vid eventuella förändringar av kritiska data.

- *Status:* Det förekommer drygt 6 000 **gruppkonton**, bland annat G-konton som används i vårdens verksamheter. Det tillkommer nya regelbundet. Därav kvarstår vår rekommendation att begränsa användningen av gruppkonton, bland annat eftersom det då inte är möjligt att säkerställa att all åtkomst till kritiska data är behörig. I de situationer användningen beror på att flera användare delar samma dator rekommenderas användaridentiteten säkerställas genom autentisering vid byte av användare.

— Vid granskningen 2019 noterades att behörighetsadministrationen sker med långa handläggningstider vilket riskerar obehörighet tills ändringen genomförts.

- *Status:* Det är sällsynt med avsteg från reglerad handläggningstid på 15 minuter då behörighetsadministrationen hanteras av extern part. Uppläggning av nya konton sker via Microsoft Identity Manager (MIM).

— Vid granskningen 2019 rekommenderades att fortsätta införandet av Single Sign On (SSO) för samtliga funktioner inom ekonomistyrning.

- *Status:* Single Sign On är ännu inte aktiverat. Detta ställer ökade krav exempelvis på att de olika systemen har tillräckligt stöd för robust autentisering, men också att dessa möjligheter utnyttjas (Se exempel på avsteg vid punkt 9.1.1).

— Vid granskningen 2019 rekommenderades förbättringar kring såväl ändringshantering som incidenthantering. Bland annat rekommenderades användningen av ett systemstöd för att stödja en effektiv process, transparens och uppföljningsmöjligheter. Dessutom rekommenderades bättre rapportering kring incidenter, efterlevnad av krav samt hantering av risker för att säkerställa som stöd för ett mer ändamålsenligt arbete med informationssäkerhet.

- *Status:* Systemet ServiceNow (RITZ) används numera för såväl ändrings-, som incidenthantering. Man är väldigt nöjd med hur detta systemstöd fungerar.

— Vid granskningen 2019 rekommenderades regionen att genomföra klassificering som förutsättning för en korrekt kravbild som underlag för uppdatering av SLA gentemot CGI, Tieto och Visma.

- *Status:* Uppskattningsvis 1/3 av befintliga system har hittills klassificerats, varför man har en stor andel system kvar att klassificera. Däremot sker klassificering alltid för kravställande vid anskaffning av nya system.

— Vid granskningen 2019 rekommenderades regionen införa årlig omvärldsbedömning av faktorer som påverkar arbetet med IT-säkerhet och informationssäkerhet och uppdatera styrande dokument regelbundet. Områden som cyberbrottslighet bör ingå här.

- *Status:* Numera utförs årlig omvärldsbevakning. Cyberskydd och cyberbrottlighet ingår i denna bevakning.

— Vid granskningen 2019 rekommenderades regionen införa en sammanhållen riskfunktion som ett stöd till de enskilda förvaltningarna för att hantera och följa upp arbetet med IT-säkerhet/informationssäkerhet.

- *Status:* Vid informationsklassning och riskanalys av system medverkar numera samlad kompetens för informationssäkerhet, dataskydd och IT säkerhet.

— Vid granskningen 2019 rekommenderades utvecklingen av kontinuitetsplaner för att säkerställa driften av IT system utifrån krav på tillgänglighet. Sådana kontinuitetsplaner saknades till stor del. Manuella rutiner fanns men endast för vissa delar av processen.

- *Status:* Ansvaret för detta ligger hos koncernkontoret. På förvaltningen IT/MT finns kontinuitetsplaner för denna verksamhet. För Personec P finns ”i ***HR Fönster”*** en kontinuitetsplan som revideras årligen i samarbete mellan system- och verksamhetsansvarig. För 2022 beställdes av Tieto en scenarioplanering för återläsning av Personec P vid ett totalhaveri, men detta fick tyvärr prioriteras ned varför det inte

genomfördes. Ny plan för detta finns för 2023. För Raindance har avtal om leverans tecknats med CGI (Service Level Agreement, SLA). Regionen har utvecklat alternativa rutiner för att ändå kunna hantera funktionerna ”beställningar” och ”betalningar” vid längre avbrott.

— Vid granskningen 2019 framkom att ingen riskbedömning med avseende på cyberattacker genomförts. Det finns kontrollsystem för virusdetektering, sårbarhetsscanning och analys av onormala trafikmönster. Penetrationstester genomfördes vid införandet av nya system men inte löpande. Sammantaget skapade detta en osäkerhet kring förmågan att säkerställa en korrekt redovisning.
  - *Status:* Numera sker riskbedömning där Cyber Security ingår. Penetrationstester genomförs också regelmässigt.

— Vid granskningen 2019 framkom att det saknades en särskilt beslutad budget för att ha möjlighet att utveckla och bedriva ett systematiskt arbete för IT- och informationssäkerhet.
  - *Status:* Ny enhet för ”IT Säkerhet” har skapats vilken har egen budget. Enheten består av sex personer samt, för närvarande, tre konsulter för att komma i kapp med ”skulden” av informationsklassificering för befintliga system. Enheten har därmed kompetens inom Cybersäkerhet/IT säkerhet, informationssäkerhet, dataskydd samt riskanalysledning.

9.1.5 Informationssäkerhet

9.1.5.1 Inledning

Informationssäkerhet används numera oftast som samlingsbegrepp för aktiviteter, kontroller och systembaserade inställningar, vars syfte är att skydda hanteringen av känsliga informationsslag. Detta inkluderar då exempelvis skydd av personuppgifter (enligt Dataskyddsförordningen) och systembaserade inställningar.

Lämpliga skyddsåtgärder bestäms utifrån klassificering av behandlingar/processer där känsliga informationsslag eller kritiska systemfunktioner används. Syftet med klassificering är att bestämma ”känslighetsgrad” utifrån säkerhetsegenskaperna ”*Tillgänglighet”, ”Konfidentialitet” och ”Riktighet” (spårbarhet)*.

Det yttersta syftet med informationssäkerhet är således att uppnå en situation där **alla** behandlingar/processer som inkluderar känsliga informationsslag, eller för verksamheten kritiska systemfunktioner, utförs med **tillämpning** av beslutat skydd.

För en bättre struktur beskrivs regionens status, med noteringar och rekommendationer, här utifrån de processdelar som erfordras för att uppnå eftersträvat syfte med informationssäkerhet (se bild 1).

Bild 1.

9.1.5.2 Kartläggning/registerföring av känsliga informationsslag

I samband med Dataskyddsförordningens ikraftträdande (maj 2018) utförde regionens förvaltningar lokal kartläggning/registerföring av känsliga informationsslag samt dess koppling till behandlingar. Eftersom detta arbete saknade enhetlig struktur, bland annat avseende dokumentationsform, har det hittills inte varit möjligt att åstadkomma någon central

kartläggning/uppföljning för att säkerställa att detta arbete utförts för alla delar av regionens verksamheter. Detta gäller också huruvida analoga kritiska informationsslag inkluderades i denna kartläggning.

Syftet med införandet av systemstöd *(iFacts)* är att säkerställa enhetlighet och att tillämpad struktur skapar möjlighet till uppföljning i detta avseende. Detta inkluderar kopplingen mellan förekomsten av kritiska informationsslag och de behandlingar där dessa används. Planer finns att införa systemstödet under 2023.

Vi rekommenderar att regionen prioriterar införandet av beslutat systemstöd för att säkerställa enhetlighet och gemensam struktur för kartläggning/registerföring av känsliga informationsslag. Detta är viktigt för möjligheten att uppnå ett rimligt skydd av dess hantering.

9.1.5.3 Klassificering och riskanalys

Regionen saknar central förteckning över genomförda informationsklassificeringar, riskbedömningar och konsekvensbedömningar. Planen är att med hjälp av systemet *iFacts* ha möjlighet att skapa en sådan förteckning.

Regionen har regelverk som stöd för förvaltningarnas arbete med klassificering och riskanalys (*”Instruktion för informationsklassificering”, ”Klassificera informationstillgångar”, ”Mall - Konsekvensbedömning avseende dataskydd (DPIA)”*, *”Riskanalys Informationssäkerhet”* med flera dokument).

Som tidigare noterats sker klassificering och riskbedömning vid nyanskaffning av system, men däremot har endast cirka 1/3 av befintliga system hittills klassificerats och riskbedömts.

Eftersom momenten klassificering och riskbedömning är en förutsättning för möjligheten att besluta om och tillämpa rimliga skyddsåtgärder, är det vår rekommendation att genomföra detta arbete med prioritet.

9.1.5.4 Skyddsåtgärder

Beslut om skyddsåtgärder behöver dokumenteras på ett uppföljningsbart sätt för att säkerställa tillämpningen vid behandlingar där känsliga informationsslag ingår. Regionen saknar centrala förteckningar över hittills beslutade skyddsåtgärder, varför uppföljningar av tillämpningen inom regionen inte är möjlig. Det är viktigt att skapa möjligheter att dels följa upp om beslut om lämpligt skydd fattats, dels att dessa beslut kunnat fullföljas (så kallade GAP-analyser).

Vår rekommendation är att tillse att beslutat systemstöd skall ges en struktur som säkerställer möjligheten till uppföljning av att beslutade skyddsåtgärder faktiskt tillämpas inom alla delar av verksamheten.

9.1.5.5 Uppföljning och rapportering

Förvaltningarna ansvarar för att följa upp sitt eget arbete med informationssäkerhet (”Instruktion för tillämpning av riktlinje för informationssäkerhet”). Dessutom framgår detaljerade anvisningar genom ”Årshjulen för informationssäkerhet och dataskydd”. Det har beslutats att uppföljning skall ske med rapportering till såväl förvaltningsledning som centralt inom regionen.

Uppföljning och rapportering är förutsättningen för att beslutande instanser skall ha möjlighet att besluta om förstärkande åtgärder där detta behövs. Eftersom central uppföljning saknas har inte förutsättningar för sådana åtgärder funnits.

Central funktion för informationssäkerhet har, enligt ”årshjulet”, efterfrågat underlag från förvaltningarna för att ha möjlighet att skapa en tillförlitlig bild av arbetets omfattning. Enligt uppgift har variation i förvaltningarnas svarsfrekvens och kvalitet inte möjliggjort att en sådan bild kunnat sammanställas.

För att ha möjlighet att utveckla en meningsfull uppföljning/rapportering är det vår rekommendation att besluta om mätbara KPI:er (”Key Performance Indicators”) som representerar samtliga moment i processen för informationssäkerhet (Bild 1). Dessa KPI:er bör ligga till grund för uppföljningar.

Uppföljning bör ske konkret mot regionens operativa verksamheter för att tydligt spegla beslutad ansvarsfördelning. Otydlighet i detta avseende kan bidra till oönskad nedprioritering av det lokala arbetet med informationssäkerhet.

Uppföljning rekommenderas ske oberoende i förhållande till inblandade organisatoriska delar av regionen.

9.1.5.6 Iterativ process

För att säkerställa aktualitet rekommenderas bedömningar, klassificeringar, skyddsbeslut osv att uppdateras regelbundet. Allt eftersom verksamhet och omvärld förändras skapas samtidigt nya förutsättningar för de beslut om skydd som tidigare fattats.

Enligt intervjuer utförs detta inte i dagsläget, vilket delvis kan bero på att delar av processen ännu inte slutförts.

2023-02-16

KPMG AB

Jan-Inge Hedin

Senior Manager