Uppföljning av 2022 års granskning av informationssäkerhet – med fördjupning mot systemen Raindance och Personec P

Del av räkenskapsrevisionen 2023

Region Skåne

KPMG AB

2024-03-27

Antal sidor: 8

Region Skåne
Uppföljning av 2022 års granskning av informationssäkerhet – med fördjupning mot systemen

2024-03-27

Innehållsförteckning

1 Sammanfattning

KPMG har på uppdrag av Region Skånes revisorer följt upp noteringar från *”KPMG Granskningsrapport IT säkerhet 2022*”. Granskningen från 2022 var samtidigt en uppföljning av rapporten *”IT-säkerhet med inriktning på system som har betydelse för intern kontroll inom redovisningen”* från 2019. Dessa båda ursprungliga granskningar inkluderade översiktligt regionens arbete med informationssäkerhet (inklusive dataskydd och IT säkerhet).

Eftersom granskningarna utgör en del av respektive års redovisningsrevision har de centrala ekonomi- och personalsystemen Raindance och Personec P varit centrala.

I det följande sammanfattas våra mest väsentliga iakttagelser.

Enligt av regionen fastställd instruktion *”Riktlinjer för informationssäkerhet”* (2017-12-07), är *”en stor del av den information som behandlas känslig och värdefull”.* Därför skall informationen **skyddas** så att endast behöriga får tillgång till den (***K****onfidentialitet*), att den är korrekt och inte är manipulerad eller förstörd (***R****iktighet*) och att den finns när den behövs (***T****illgänglighet*). Genom **KRT**-analyser skall klassificerings- eller risknivå bedömas vid regionens samtliga behandlingar (processer) som utgångspunkt för att bedöma behovet av skyddsåtgärder. Enligt ”*Instruktion för riskhantering avseende informationstillgångar*” skall oacceptabel risknivå (”Mycket hög”) reduceras genom tillämpning av ändamålsenliga **skyddsåtgärder**.

Vid behandlingar (processer) inom regionen används **informationstillgångar** med olika känslighet eller värde för verksamheten. Dessa kan bestå av känsliga **informationsslag** (exempelvis journaler, personuppgifter) eller **systemfunktioner** som tillför värde för verksamheten och/eller som alltid måste vara tillgängliga. Beroende på grad och typ av känslighet kan skyddsåtgärder (exempelvis kryptering, stark autentisering, loggning, spegling av servermiljö eller andra kontroller av varierande slag) användas. Eftersom regionen saknar en gemensam **kravdatabas,** med koppling mellan klassificeringsgrad och krav, behöver skyddsåtgärd bestämmas unikt vid varje analys. Detta medför ett ökat personberoende.

Syftet med informationssäkerhet är således att säkerställa att behandlingar/processer hanteras med **tillämpning** av beslutade krav, eller skyddsåtgärder. Först när detta kan konstateras har syftet uppnåtts. Regelbundna **uppföljningar** bör utföras och utformas utifrån detta syfte. Rapport bör sammanställas till beslutande instans för att skapa möjlighet att säkerställa syftet.

Resultatet av vår granskning visar att det ännu återstår ett stort arbete innan ovan beskrivet syfte med regionens arbete med informationssäkerhet har uppnåtts. De centrala ekonomi- samt personalsystemen (Raindance och Personec P) ingår **inte** bland de system som hittills har klassificerats/riskanalyserats. Detta skapar en osäkerhet för graden av effektivitet i kontrollmiljön för de processer som stöds av dessa system. Utifrån våra rekommendationer från föregående års granskningar har endast ett fåtal åtgärdats.

Tilläggas bör att arbete pågår för att implementera en ny version av Raindance (drift planerad till januari 2025) samt att detta arbete (enligt intervju) inkluderar klassificering/riskanalys.

Utgångspunkt för **hittills genomförda** klassificeringar/riskanalyser har varit regionens system och inte behandlingar (processer) där känsliga informationstillgångar används. Under 2023 klassificerades 27 av regionens ca 650 system, medan ytterligare några system uppges ha analyserats tidigare. Gemensamt register för dokumentation av genomförda analyser saknas. Dessutom utförs ingen systematisk uppföljning av att beslutade skyddsåtgärder har implementerats och tillämpas. Digital utgångspunkt (system) exkluderar dessutom manuella, **analoga**, behandlingar (exempelvis notering, kopiering, kommunikation, fax) där känsliga informationsslag hanteras.

Regionen **saknar** ett gemensamt register för känsliga informationstillgångar samt dess koppling till behandlingar där dessa används inom regionens olika verksamheter.

Vid ett flertal intervjuer, bland annat med representanter från Digitalisering IT/MT, framkom att ett flertal av analyserna utförts enbart med deltagande från Digitalisering IT/MT och **utan medverkan** av personal från respektive förvaltning där systemen används som stöd vid olika behandlingar. Detta skapar en risk för felaktigheter utifrån otillräcklig kunskap om förekommande behandlingar samt dess utformning, ändamål och betydelse. Ingående verksamhetskunskap är en viktig tillgång vid bedömningen av vilka åtgärder som är mest ändamålsenliga och samtidigt genomförbara.

Mot bakgrund av ovan beskriven status rekommenderar vi regionstyrelsen att vidta åtgärder för att genomföra klassificeringsarbetet med utgångspunkt från **behandlingar** (processer) där känsliga informationstillgångar hanteras, samt att detta utförs med **lokalt/decentralt** ansvar. Behovet av kompetens från olika expertområden (exempelvis IT) bör tillföras beroende på de aktuella behandlingarnas natur. I de fall likartade behandlingar förekommer vid ett flertal förvaltningar/operativa avdelningar (exempelvis finansiella-, eller personalprocesser) och som stöds av samma system bör klassificering/riskanalys utföras med representation från förekommande användargrupper.

Sådana åtgärder bör inkludera

- **Utbildning** – för att skapa förmåga att genomföra arbetet decentralt
- **Identifiera, dokumentera** samtliga regionens behandlingar med känsliga/värdefulla informationstillgångar i ett regiongemensamt **register**
- Fastställ en regiongemensam **kravdatabas** med koppling mellan klassificeringsnivå och krav – för ökad enhetlighet och oberoende vid beslut om skyddsåtgärd.
- Säkerställ lokalt/decentralt **ansvar** för såväl genomförande samt beslut om samt tillämpning av skydd. Av naturliga skäl bör ansvarsfördelningen för arbetet där likartade behandlingar sker vid flertalet förvaltningar/operativa enheter, och som stöds av samma system, bör bestämmas separat.
- Fastställ en regiongemensam **dokumentationsform** för alla delar av analysarbetet för att säkerställa enhetlighet samt uppföljningsmöjligheter av aktuell status per verksamhet
- Besluta om regelbundna **oberoende uppföljningar** med rapportering till beslutande instans

Nedan följer övriga väsentliga noteringar/rekommendationer. Hänvisning till respektive punkt i rapporten anges inom parentes. Vi rekommenderar att

— autentiseringskraven för Raindance förstärks (*9.1.1*)

— besluta om förkortad periodicitet av inaktivitet i Raindance för inaktivering av användarkonto (*9.1.1*)

— monitoreringsrutin införs för att säkerställa att användarnas systemrättigheter i Raindance är aktuella (*9.1.3*)

— kontroller införs för att säkerställa att användarkonton med starka rättigheter i Raindance är aktuella, minimeras till antalet, samt ej används till oönskade aktiviteter (9.1.3)

— gruppkonton (med undantag för systemkonton) undviks för att säkerställa spårbarhet (9.1.4).

2 Bakgrund

KPMG har på uppdrag av Region Skånes revisorer följt upp noteringar från *”KPMG Granskningsrapport IT säkerhet 2022*”. Granskningen från 2022 var samtidigt en uppföljning av rapporten *”IT-säkerhet med inriktning på system som har betydelse för intern kontroll inom redovisningen”* från 2019. Dessa båda ursprungliga granskningar inkluderade även översiktligt regionens arbete med informationssäkerhet (inklusive dataskydd och IT säkerhet).

Eftersom granskningarna utgör en del av respektive års redovisningsrevision har de centrala ekonomi- och personalsystemen Raindance och Personec P varit centrala.

3 Syfte/revisionsfrågor

Granskningen syftar till att bedöma om Region Skåne bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete som utgångspunkt för en bedömning av den kontrollmiljö som tillämpas för regionens redovisningsprocesser. Detta eftersom syftet med informationssäkerhet är att säkerställa att behandlingar (processer) inom regionen utförs med beaktande av beslutade kontroller/skyddsåtgärder.

Granskningen, som utgör en del av årets redovisningsrevision, är en uppföljning av motsvarande granskning tidigare år. Detta inkluderar även en uppföljning av att användares rättigheter i Raindance på ett lämpligt sätt begränsats till respektive användares eget ansvarsområde.

4 Avgränsning

Då uppdraget är en uppföljning av tidigare granskning är den med avseende på IT-miljön avgränsad till de versioner av systemen Raindance och Personec P som användes under 2023.

5 Revisionskriterier

De revisionskriterier som legat till grund för tidigare granskningar har varit enligt följande:

- Gällande lagstiftning inom området (förordning 2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster (NIS) samt Dataskyddsförordningen (2018:218)
- Relevanta styrdokument
- Relevanta delar från användandet av ISO 27001:2013

Dessa kriterier är oförändrade sedan tidigare års motsvarande granskning.

6 Ansvarig nämnd

Granskningen omfattar Regionstyrelsen. Eftersom granskningen inkluderar noteringar om regionens arbete med informationssäkerhet omfattas de flesta av regionens nämnder av dessa noteringar, inte minst "*Nämnden för operativ regiongemensam verksamhet*".

7 Metod

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

- Informationssäkerhetschef
- Verksamhetschef Informationsstyrning, informationsförvaltning Koncernkontoret

- Chef IT-säkerhetsenheten Digitalisering IT/MT
- Controller, Verksamhetsansvarig Affärssystem, Koncernstab Inköp & Ekonomistyrning
- Systemansvarig Raindance, Digitalisering IT och MT
- IT-säkerhetsansvarig, Digitalisering IT och MT
- Tf. Enhetschef IT stöd HR
- Riskanalysledare IT-säkerhetsenheten
- Projektledare U537 IT-säkerhetsenheten
- Informationssäkerhetsspecialist
- Dataskyddsombud
- Strategisk dataskydds- och informationssäkerhetssamordnare
- Verksamhetsspecialist Raindance, Gemensam Service, Regionservice
- Tf. Enhetschef Enheten för Informationssäkerhet, dataskydd och informationsoffentlighet Informationsstyrning och informationsförvaltning

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 fördelats.

Vi har därutöver erhållit ett antal styrdokument vilka granskats som utgångspunkt för respektive granskningsområde.

Rapporten har faktagranskats av ansvariga tjänstemän inom regionen.

8 Projektorganisation

Granskningen har genomförts av Jan-Inge Hedin från KPMG under januari – februari 2024.

9 Granskning

9.1 Inledning

Nedan följer en kortfattad version av noteringar och rekommendationer inom områdena ”Raindance”, ”Personec P”, ”Analys av användarrättigheter i Raindance”, ”IT säkerhet” samt ”Informationssäkerhet”.

9.1.1 Raindance

- Den version av Raindance (regionens centrala ekonomisystem) som använts under 2023 har **inte** klassificerats/riskanalyserats. Syftet med klassificering är att besluta om ändamålsenliga skyddsåtgärder (krav) att tillämpa vid behandlingar/processer som stöds av systemet. Svaga autentiseringskrav, förekomst av anonyma konton, aktiva konton som inte använts under lång tid mm (se punkt 9.1.3) samt ett stort antal konton med starka rättigheter också utanför ”eget område” är noteringar som visar behov av att förstärka nuvarande krav.
- Arbete med att implementera ny version av Raindance pågår och planeras vara i drift under januari 2025. Enligt intervju kommer detta arbete att inkludera klassificering/riskanalys av den nya versionen.

- *Rekommendation:* Vi rekommenderar regionen att genomföra klassificering/riskanalys för att säkerställa att ändamålsenliga krav tillämpas vid hanteringen av de behandlingar/processer som stöds av systemet.

— Raindance levereras av extern leverantör (CGI). Regionen följer exempelvis regelbundet upp tillgänglighet, kostnader och leveranser i form av uppgraderingar som avtalet ger rätt till. Däremot sker ingen granskning av att leverantörers interna rutiner för hanteringen av Region Skånes system följer avtal (exempelvis rutiner för åtkomst, ändringshantering, drift, kontinuitet).

- *Rekommendation:* Vi rekommenderar regionen att tillämpa rutiner för att verifiera att externa parter följer tecknade avtal. Detta för att säkerställa att inga oönskade risker föreligger i regionens verksamhet.

9.1.2 Personec P

— Den version av Personec P (regionens centrala personalsystem) som använts under 2023 har **inte** klassificerats/riskanalyserats. Syftet med klassificering är att besluta om ändamålsenliga skyddsåtgärder (krav) att tillämpa vid behandlingar/processer som stöds av systemet. Tidigare planer att införa multifaktorautentisering har ännu inte genomförts. Enligt intervju finns dessutom behov att effektivisera monitoreringsrutinen. Monitorering innebär att respektive chef regelbundet får förteckning över användares rättigheter med ansvar att återkomma med rättelsebehov. Härigenom minskar risken för fel samtidigt som ansvarsfördelningen förtydligas.

- *Rekommendation:* Vi rekommenderar regionen att genomföra klassificering/riskanalys för att säkerställa ändamålsenliga skyddsåtgärder vid behandlingar/processer som stöds av systemet.

9.1.3 Analys av användarrättigheter av Raindance

Vi har analyserat användarkonton samt dess rättigheter i Raindance utifrån ett extrakt vid slutet av november 2023.

Vid analysen har vi exkluderat spärrade och inaktiverade användarkonton. De konton som beskrivs nedan är aktiva (10 008 konton).

Vi har noterat att det förekommer ett flertal aktiva konton som endera saknar datum (ca 25 % av samtliga aktiva konton) för ”*Senast inlog*” eller som inte använts under lång tid. Avsaknad av datum beror sannolikt på att de aldrig använts. Dessa är ändå inte inaktiverade.

Det förekommer också ett flertal konton som undantagits från generellt krav på regelbundet byte av lösenord, också detta i strid mot beslutad policy. Rutin för monitorering saknas. Monitorering innebär att respektive chef regelbundet tillställs förteckning över användare samt dess rättigheter. Aktuella chefer har ansvar för att återkoppla angående inaktuella eller felaktiga uppgifter. Förutom att säkerställa att uppgifterna är aktuella, förtydligar rutinen ansvarsfördelningen för systemets användarrättigheter.

Det förekommer också konton som inte är individuella vilket kan vara acceptabelt för systemkonton. Eftersom ett antal av dessa konton inte använts under lång tid finns det anledning att utvärdera dess aktualitet. Anonyma, individuella, konton bör helt undvikas eftersom spårbarheten äventyras.

Ett stort antal konton har tilldelats starka rättigheter vilket, i olika utsträckning, erfordras för systemförvaltare eller administratörer. De flesta av dessa tillhör extern leverantör. Konton med starka rättigheter bör alltid begränsas så långt det är möjligt och alltid vara aktuella. Eftersom ett antal av dessa konton dessutom inte använts under lång tid finns det anledning att utvärdera dess behov.

Vår kontroll av att användares rättigheter begränsats till ”eget område” visar att det förekommer ett flertal användare med rättigheter till samtliga företag (”-1”) i Raindance. Detta beror enligt intervju på att nuvarande version av Raindance har ett komplext behörighetssystem kombinerat med frekventa organisatoriska förändringar.

Dessutom har vi följt upp regionens beslut om separation mellan rättigheterna att ”Hantera faktura” och att ”Registrera attesträtt” samt ”Registrera ny leverantör”. Vi noterar att för de användare som tilldelats rättigheter i de avsedda behörighetsgrupperna (G24 och G16), följs separationsbeslutet helt. Däremot förekommer ett flertal användare med starka rättigheter där dessa rättigheter inte separerats. Detta skapar ett behov att tillämpa kontroller (skyddsåtgärder) med syfte att dels minimera antalet konton med dessa rättigheter, men också att förhindra/upptäcka ett oönskat användande.

- *Rekommendation:* Vi rekommenderar regionen att genomföra klassificering/riskanalys för att säkerställa ändamålsenliga skyddsåtgärder vid behandlingar/processer som stöds av Raindance.

9.1.4 Informationssäkerhet

9.1.4.1 Inledning

Syftet med informationssäkerhet är att besluta om ändamålsenliga krav (kontroller, skyddsåtgärder) för att skydda organisationens hantering (behandlingar) av känsliga informationstillgångar (informationsslag eller för verksamheten viktiga systemfunktioner). Exempel på sådana krav är kryptering, autentisering, loggning, spegling av lagringsmiljöer. Skyddsåtgärder bestäms utifrån bedömd ”känslighetgrad” (genom klassificering, riskbedömning) av behandlingar där värdefulla eller kritiska informationstillgångar används. Klassificering sker utifrån behovet av ”*Tillgänglighet”, ”Konfidentialitet” och ”Riktighet”*.

Det yttersta **syftet** med informationssäkerhet är således att uppnå en situation där **alla** behandlingar som inkluderar känsliga informationsslag, eller för verksamheten kritiska systemfunktioner, utförs med **tillämpning** av beslutat skydd. **Uppföljning** bör ske utifrån detta syfte.

Arbetsstrukturen för informationssäkerhet kan beskrivas med följande bild.

Bild 1.

Vår granskning visar att hittills genomförda klassificeringar/riskanalyser har genomförts med utgångspunkt från de system som används inom regionen och inte de behandlingar där värdefulla informationstillgångar används. Under 2023 klassificerades 27 av regionens ca 650 system, medan ytterligare några system uppges ha analyserats tidigare. För regionen gemensamt register över genomförda klassificeringar saknas. Uppföljning av att beslutade skyddsåtgärder faktiskt tillämpas förekommer inte. Regionen saknar en gemensam kravdatabas med koppling mellan klassificeringsgrad och skyddsåtgärd/krav. Dessutom saknas beslut om gemensam dokumentationsform för arbetet med informationssäkerhet, vilket medfört att uppföljning av aktuell status utifrån syftet med informationssäkerhet inte har kunnat genomföras.

Rekommendation: Mot bakgrund av ovan beskriven status rekommenderar vi regionstyrelsen att vidta åtgärder för att genomföra klassificeringsarbetet med utgångspunkt från **behandlingar** (processer) där känsliga informationstillgångar hanteras, samt att detta

utförs **lokalt/decentralt** vid respektive förvaltning/operativ enhet där kunskapen om förekommande behandlingar, dess utformning och betydelse, finns. Behovet av kompetens från olika expertområden (exempelvis IT) bör tillföras beroende på de aktuella behandlingarnas natur. I de fall likartade behandlingar förekommer vid ett flertal förvaltningar/operativa avdelningar (exempelvis finansiella-, eller personalprocesser) och som stöds av samma system bör klassificering/riskanalys utföras med representation från förekommande användargrupper. Sådana åtgärder bör inkludera

- **Utbildning** – för att skapa förmåga att genomföra arbetet decentralt
- **Identifiera** samt **dokumentera** värdefulla informationstillgångar med koppling till behandlingar där dessa används i ett gemensamt **register**
- Fastställ en regiongemensam **kravdatabas** med koppling mellan klassificeringsnivå och krav – för ökad enhetlighet och oberoende.
- Säkerställ lokalt/decentralt **ansvar** för såväl genomförande samt beslut om samt tillämpning av skydd. Av effektivitetsskäl bör ansvarsfördelningen för arbetet där likartade behandlingar sker vid flertalet förvaltningar/operativa enheter, och som stöds av samma system, bör bestämmas separat.
- Fastställ en regiongemensam **dokumentationsform** för att säkerställa enhetlighet samt uppföljningsmöjligheter för de olika delarna av arbetet med informationssäkerhet
- Besluta om **KPI:er** (Key Performance Indicators) för uppföljning av respektive operativ enhets arbetsstatus
- Besluta om regelbundna **oberoende uppföljningar**

9.1.5 IT säkerhet

De områden som tas upp under denna rubrik är i huvudsak av teknisk karaktär där genomförandet hanteras av Digitalisering IT/MT. Beslut om införande fattas dock oftast av verksamhetsansvariga inom andra delar av organisationen vilket bortses från i denna beskrivning.

Uppföljning av tidigare granskning visar att **gruppkonton** fortfarande förekommer samt att Single-Sign-On (SSO) ännu inte införts. Syftet med SSO är regionens strävan att tillämpa säkrare autentisering. Förutom SSO undersöks möjligheten att kombinera användningen av olika systems lösenord med personliga kort samt ett användande av Microsofts Identity Management (MIM).

- *Rekommendation:* Med undantag för systemkonton bör inte anonyma, eller gruppanvända, konton förekomma eftersom detta äventyrar spårbarhet. Vi rekommenderar dessutom att genomföra klassificeringar/riskanalyser för att säkerställa att behandlingar som stöds av värdefulla systemfunktioner utförs med ändamålsenliga skyddsåtgärder.

2024-03-27

KPMG AB

Jan-Inge Hedin

Senior Manager