Uppföljning av IT-säkerhets-/ cybersäkerhetsgranskningar från år 2018 samt förstudie av GDPR-anpassningen

Region Norrbotten

Mars 2021

Projektledare:
Erik Jansen, revisionskonsult
Projektmedarbetare:
Anna Nordqvist, revisionskonsult
Jonathan Melkko, revisionskonsult
Mantautas Neniskis, expert, Risk Advisory Services
Markus Månsson, expert, Digital Trust
Kvalitetssäkrare:
Hans Forsström, certifierad kommunal revisor

pwc

Innehållsförteckning

Sammanfattning

PwC har på uppdrag av Region Norrbottens revisorer genomfört en samlad uppföljande granskning av två tidigare revisionsgranskningar samt en förstudie från åren 2018-2019.

Syftet med granskningen har varit att bedöma om regionstyrelsen vidtagit ändamålsenliga åtgärder samt utövat en tillräcklig intern kontroll över de åtgärder som vidtagits efter revisionens två IT- säkerhets-/cybersäkerhetsgranskningar, samt om GDPR-anpassningen har genomförts på ett ändamålsenligt sätt.

Uppföljningen har skett genom att följande fem revisionsfrågor har besvarats:

1. Vilka åtgärder har regionstyrelsen beslutat om utifrån sin behandling av respektive IT-säkerhets-/cybersäkerhetsgranskningar från 2018?
2. I vilken utsträckning har resultatet av regionstyrelsens beslutade åtgärder återrapporteras till styrelsen?
3. Har regionstyrelsen, utifrån den återrapportering som ev. erhållits, analyserat kvarstående åtgärdsbehov inom området?
4. Vilken sammanställning finns av GDPR-implementeringen och vilken återrapportering avs detta projekt har styrelsen erhållit?
5. I vilken utsträckning har ev. analys om kvarstående åtgärdsbehov föranlett styrelsen att fatta ytterligare aktiva beslut inom området?

Resultatet redovisas i tabellen nedan (grå markering avser att revisionsfrågan ej är hänförlig till berörd tidigare granskning/förstudie):

Granskning	Beslut om åtgärder	Återrapportering av åtgärder	Analys av kvarstående åtgärdsbehov	Sammanställning av GDPR-implementeringen samt återrapportering	Ytterligare aktiva beslut
1. IT-säkerhet avseende intrångsskydd	Uppfyllt	Uppfyllt	Delvis uppfyllt		Ej uppfyllt
2. Cybersäkerhet	Uppfyllt	Uppfyllt	Delvis uppfyllt		Ej uppfyllt
3. GDPR (förstudie)				Delvis uppfyllt	Ej uppfyllt

Revisionell bedömning

Den samlade revisionella bedömningen är att regionstyrelsen *i allt väsentligt* har vidtagit ändamålsenliga åtgärder men *inte helt* har utövat tillräcklig intern kontroll över vidtagna åtgärder efter revisionens två IT- säkerhets-/cybersäkerhetsgranskningar.

Vidare bedöms att GDPR-anpassningen *inte helt* har genomförts på ett ändamålsenligt sätt.

Rekommendationer

Utifrån genomförd granskning rekommenderar vi regionstyrelsen att:

- säkerställa att kvarstående åtgärdsbehovet inom berörda områden avhjälps.
- säkerställa en tillräcklig grad av internkontroll inom området.

1. Inledning

1.1 Bakgrund

Revisionen genomförde hösten 2018 två granskningar av såväl det övergripande som det externa och interna IT-intrångsskyddet. Granskningarna visade på omfattande utvecklings- och förbättringsbehov.

Granskning av IT-säkerhet avseende intrångsskydd (2018)

Den sammanfattande revisionella bedömningen var att regionstyrelsen *i begränsad utsträckning* säkerställt att Region Norrbottens dåvarande tekniska IT-säkerhet var tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå. Bedömningen baserades på bl.a. följande iakttagelser:

- IT-säkerheten höll inte en tillräcklig hög nivå och detta område behövde prioriteras för att minimera framtida incidenter.
- De dokument som granskades var delvis uppdaterade och delvis inaktuella/daterade.
- Den informationssäkerhetspolicy som då fanns bedömdes vara inaktuell/föråldrad. Samtidigt noterades att policyn var under revidering.

Cybersäkerhet – övergripande granskning (2018)

Den sammanfattande revisionella bedömningen var att den interna kontrollen avseende regionens cybersäkerhet *i begränsad utsträckning* var tillräcklig.

Bedömningen baserades bl.a. på följande iakttagelser:

- Det saknades ett strukturerat arbete med att identifiera hot och risker mot regionens informations- och IT-säkerhet
- Förmågan att övervaka och således upptäcka avvikelser i regionens system och IT-infrastruktur var ett utvecklingsområde.
- Rapportering till regionstyrelsen behövde utvecklas för att styrelsen framgent skulle kunna hållas informerad/uppdaterad avseende regionens informations- och IT-säkerhet.

GDPR

Vidare genomförde revisionen en förstudie årsskiftet 2018/2019 över hur regionen bedrev sitt implementeringsprojekt för GDPR-anpassning. Vid regionstyrelsens sammanträde 19-10-03 informerade revisionen om utfallet av förstudien med särskilt fokus på de risker och negativa konsekvenser en otillräcklig GDPR-anpassning kan medföra.

Utfallet av implementeringsprojektet bedöms lämpligt att granska nu i slutet av 2020 med utgångspunkt i de risker och behov som förstudien lyfte fram.

Sammantaget motiverar granskningsresultaten ovan att vidtagna åtgärder avseende IT-intrångsskydd respektive GDPR-anpassning följs upp under revisionsåret 2020.

1.2 Syfte och revisionsfrågor

Granskningen syftar till att bedöma om regionstyrelsen vidtagit ändamålsenliga åtgärder samt utövat en tillräcklig intern kontroll över de åtgärder som vidtagits efter revisionens två IT-säkerhets-/cybersäkerhetsgranskningar från år 2018 samt om GDPR-anpassningen har genomförts på ett ändamålsenligt sätt.

Revisionsobjekt i denna granskning är regionstyrelsen, RS.

Revisionsfrågor

1. Vilka åtgärder har regionstyrelsen beslutat om utifrån sin behandling av respektive IT-säkerhets-/cybersäkerhetsgranskning från 2018?

2. I vilken utsträckning har resultatet av regionstyrelsens beslutade åtgärder återrapporteras till styrelsen?

3. Har regionstyrelsen, utifrån den återrapportering som ev. erhållits, analyserat kvarstående åtgärdsbehov inom området?
Fokus på att även beskriva vilka dessa ev. åtgärdsbehov analyserats att vara.

4. Vilken sammanställning finns av GDPR-implementeringen och vilken återrapportering avs detta projekt har styrelsen erhållit?

5. I vilken utsträckning har ev. analys om kvarstående åtgärdsbehov föranlett styrelsen att fatta ytterligare aktiva beslut inom området?

1.3 Revisionskriterier

- Kommunallag kap 6 § 6
- GDPR-lagstiftningen
- Regionens strategiska plan
- Iakttagelser från tidigare IT-säkerhets-/cybersäkerhetsgranskningar (2018)
- Regionstyrelsen protokoll och beslut med anledning av tidigare IT-säkerhets-/cybersäkerhetsgranskningar (2018)
- Övriga för granskningen relevanta styrdokument, process- och rutinbeskrivningar.

1.4 Avgränsning

Granskningen avgränsas enligt syfte och revisionsfrågor, samt även metod och genomförande.

1.5 Metod

Dokumentstudier av styrelsens yttrande över revisionsrapporterna, fattade beslut och åtgärder med anledning av rapporterna, samt övriga relevanta dokument och protokoll.

Intervjuer har genomförts med IT/MT-direktör, företrädare inom regiondirektörens stab samt företrädare för Division Länsteknik.

Därefter:

- Sammanställning och rapportskrivande.
- De som intervjuats för granskningen har haft möjlighet att faktagranska innehållet i rapporten innan den fastställdes.
- Därutöver har regiondirektör och regionstyrelsens ordförande fått möjlighet att läsa och lämna kommentarer/synpunkter på rapporten innan den fastställdes.

- Revisionsfråga 3 och 4 har särskilt beskrivits, analyserats och bedömts tillsammans med medarbetare inom PwC Risk Advisory Services samt PwC Digital Trust.
- Rapporten har kvalitetssäkrats av Hans Forsström, certifierad kommunal revisor, PwC.
- Redovisning av granskningsresultat för de förtroendevalda revisorerna i regionen.

2. Iakttagelser och bedömningar

2.1 Granskning av tidigare IT-granskningar

2.1.1 Sammanfattning av tidigare rapporter

Granskning av intrångsskydd (2018)

Den tidigare revisionsgranskningen avseende intrångsskydd syftade till att bedöma huruvida regionstyrelsen säkerställt att Region Norrbottens dåvarande tekniska IT-säkerhet var tillräcklig och tillfredsställande för att reducera risker för obehörigt intrång till en acceptabel nivå. Den sammanfattande revisionella bedömningen var att regionstyrelsen *i begränsad utsträckning* säkerställt detta.

I rapporten återfinns bland annat följande iakttagelser som lett fram till bedömningen:

- IT-avdelningen uppmärksammade PwC:s angrepp/intrångsförsök och notifierade PwC att de blivit upptäckta. Upptäckten verkade dock ske via manuella metoder.
- IT-säkerheten höll inte en tillräckligt hög nivå. Detta område behöver prioriteras för att minimera framtida incidenter.
- Majoriteten av de styrande dokumenten inom området IT-säkerhet är daterade till 2016, men ett antal har inte uppdaterats sedan 2008/2009.
- Informationssäkerhetspolicyn bedömdes vara föråldrad. Policyn uppgavs dock vara under revidering.

Cybersäkerhet övergripande granskning (2018)

Den övergripande granskningen av Region Norrbottens cybersäkerhet syftade till att granska om regionstyrelsens säkerställt att den interna kontrollen avseende regionens cybersäkerhet var tillräcklig. Granskningen fokuserade på processer, personal och teknik inom granskningsområdet utifrån de fem områdena som innefattas i det amerikanska cybersäkerhetsramverket NIST[1]:

1. Identifiera - Fokus på IT-tillgångar, processer och policy, styrning, riskanalys och riskhanteringsstrategi.
2. Skydda - Fokus på behörighetskontroll, utbildning och övning, IT-/dataskydd, informationssäkerhet, förvaltning och tekniskt skydd.
3. Upptäcka - Fokus på anomalier/händelser, kontinuerlig övervakning och processer att upptäcka händelser.
4. Respondera/Agera - Fokus på incidenthantering, incidentrespondering, krishantering/kommunikation, analys, IT-incidenthantering och erfarenhetsåterföring.
5. Återställa - Fokus på kontinuitetsplanering, avbrottsplanering, erfarenhetsåterföring och varumärkesskydd.

När en utvärdering av en organisation sker med hjälp av ramverket NIST erhålls en nivå på en skala (1-4) som indikerar på en organisations grad av mognad kopplat till

[1] National Institute of Standards and Technology - Ramverket omfattar en riskbaserad sammanställning av riktlinjer som syftar till att hjälpa organisationer att identifiera, genomföra och förbättra sin säkerhetspraxis. Ramverket tillhandahåller en graderad utvärdering som gör att verksamheten kan identifiera dess nuvarande cybersäkerhetsförmåga, sätta individuella mål och upprätta planer för åtgärder (Revisionsrapport: Cybersäkerhet - övergripande granskning, 2018, s. 5.).

cybersäkerhet. Av rapporten framgår att Region Norrbottens generella mognadsgrad bedömdes var *låg* inom fyra av fem områden, och *mycket låg* inom området *identifiera*.

Den sammanlagda revisionella bedömningen var att den interna kontrollen avseende regionens cybersäkerhet *i begränsad utsträckning* var tillräcklig.

Bedömningen baserades bland annat på följande iakttagelser:

- Det saknades ett strukturerat arbete med att identifiera hot och risker mot regionens informations- och IT-säkerhet.
- Förmågan att övervaka och således upptäcka avvikelser i regionens system och IT-infrastruktur var ett utvecklingsområde.
- Rapportering till regionstyrelsen behövde utvecklas för att styrelsen framgent skulle kunna hållas informerad/uppdaterad avseende regionens information- och IT-säkerhet.

Följande rekommendationer lämnades i rapporten till regionstyrelsen:

- Implementera en övergripande informationssäkerhetspolicy.
- Implementera ett ledningssystem för informationssäkerhet (LIS) för att säkerställa ett systematiskt risk- och informationsklassningsarbete i hela organisationen.
- Uppdatera gällande styrdokument och kommunicera ut i organisationen (kan vara en del av LIS-arbetet).
- Utveckla rapporteringen till regionstyrelsen, exempelvis i form av en säkerhetsrapport.

2.1.2 Revisionsfråga 1 & 2: Beslutade åtgärder och återrapportering

Granskning av intrångsskydd (2018)

Revisionsrapporten behandlades vid regionstyrelsens sammanträde 2019-01-30 § 28. Av ärendet framgår bland annat att:

- Inom regionen har ett arbete påbörjats avseende införande av ledningssystem, kartläggning av skyddsvärda system utifrån ett riskperspektiv samt omvärldsbevakning inom säkerhetsområdet.
- De mest akuta bristerna som påvisades åtgärdades i samband med överlämnandet av rapporten.
- En genomgång och uppdatering av styrande IT-dokument samt en årlig revidering av dokumentationen införs.

Följande beslut fattades av regionstyrelsen *"Regionstyrelsen ger regiondirektören i uppdrag att vidta lämpliga åtgärder med anledning av revisionsrapporten samt att återrapportera vilka åtgärder som vidtagits till regionstyrelsen".*

Återrapportering till regionstyrelsen skedde vid sammanträdet 2019-11-13 § 241. Av ärendet framgår bland annat att:

- Regionen har, utöver de bristerna som revisorerna listade, planerat och vidtagit ett antal åtgärder. Bland annat kommer intrångstester att genomföras med jämna mellanrum.

- Division Länsteknik har införskaffat verktyg för att kunna utföra sårbarhetsanalyser på system och applikationer.
- Ett arbete pågår för att skapa en dedikerad roll inom Division Länsteknik för att hantera IT-säkerhet på en övergripande strukturell nivå.
- Regionens fortsatta arbete med IT-säkerhet ska bedrivas enligt riktlinjen för säkerhet som föreläggs styrelsen vid sammanträdet.

Regionstyrelsen beslutade vid sammanträdet att:

- lägga revisionsrapporten till handlingarna med beaktande av redovisade åtgärder.
- Internkontroll inom området ska säkerställas.

Cybersäkerhet - övergripande granskning (2018)

Revisionsrapporten behandlades vid sammanträdet 2019-01-30 § 27. I ärendet listas bland annat de rekommendationer (se avsnitt 2.2.1 ovan) som revisorerna föreslagit regionstyrelsen att vidta för att utveckla regionens informations- och IT-säkerhet.

Följande beslut fattades av regionstyrelsen vid sammanträdet:

- *"Regionstyrelsen ger regiondirektören i uppdrag att vidta lämpliga åtgärder med anledning av revisionsrapporten samt att återrapportera vilka åtgärder som vidtagits till regionstyrelsen".*

Återrapportering till regionstyrelsen skedde vid sammanträdet 2019-11-13 § 242. Av protokollet framgår bland annat att regionen vidtagit ett antal åtgärder med anledning av de sammanfattande rekommendationer som revisorerna lämnade:

- En ny säkerhetspolicy har antagits (2019-06-18). Denna, underordnad riktlinje säkerhet (2019-11-13), innehåller bl.a. informationssäkerhetspolicy och 13 andra säkerhetsfunktioner.
- Övriga nivåer av ledningssystem för informationssäkerhet fortsätter att utvecklas och innehåller de grundläggande kraven för ett ledningssystem enligt standarden ISO/IEC 27001.
- Styrdokument kommer att uppdateras och läggas upp i regionens dokumentsystem.
- Underlag för rapportering till regionstyrelsen är under utveckling och ska presenteras för återföring och dialog.

Regionstyrelsen beslutade vid sammanträdet att:

- lägga revisionsrapporten till handlingarna med beaktande av redovisade åtgärder.
- Internkontroll inom området ska säkerställas.

Vi har inom granskningen även tagit del av underlaget till återrapporteringen. Där kommenteras och utvärderas samtliga av de förbättringsområden som identifierades i revisionsrapporten *Cybersäkerhet - övergripande granskning.* De områden som rapporten utgick från var, som nämnts ovan, de fem områden som ingår i NIST-ramverket: Identifiera Skydda, Upptäcka, Respondera/Agera, Återställa.

Av underlaget till återrapporteringen framgår att Regionen bedömer statusen som *pågående* avseende genomförandet av åtgärder inom samtliga fem områden.

2.1.3 Revisionsfråga 3 & 5: Regionstyrelsens analys av kvarstående åtgärdsbehov samt ytterligare aktiva beslut inom området

Beskrivningen i avsnittet nedan innefattar både Cybersäkerhetsgranskningen (2018) och Intrångsskyddsgranskningen (2018) utifrån att de återrapporterades vid samma tillfälle till regionstyrelsen, samt har behandlats på ett samlat sätt av styrelsen sedan dess.

Som nämns ovan kan vi vid regiondirektörens återrapportering 2019-11-13 styrka att regionstyrelsen beslutade att "Internkontroll inom området ska säkerställas". Vi kan därutöver ej styrka att regionstyrelsen genomfört någon analys av kvarstående åtgärdsbehov, eller att detta särskilt efterfrågats av styrelsen. Sedan återrapporteringen framgår det inte att ytterligare aktiva beslut fattats av styrelsen inom området utifrån tidigare revisionsrapporter.

Av intervjuer framgår att åtgärder i enlighet med revisorernas rekommendationer vidtagits löpande inom området inom tjänsteorganisationen. Bland annat har styrande dokument reviderats och uppdaterats. Av Bilaga 1 framgår en förteckning av de dokument vi tagit del av inom granskningen. Vår översiktliga granskning av dessa dokument visar att uppdatering av dessa skett utifrån de rekommendationer som tidigare revisionsrapporter lämnat.

Vid intervjuer framgår även att det löpande sker ett arbete med kvalitetsförbättringar för att skapa en ökad intern kontroll inom området. Utvecklingsområden för framtiden framhålls av intervjuade vara att dels stärka formerna för systematisk kompetens-utveckling inom berörda delar av organisationen så att den interna kontrollmiljön stärks. Därutöver framhålls även formerna för analys och systematiserad/automatiserad kontroll av efterlevnad utifrån uppdaterade styrande dokument vara utvecklingsområden.

Vi noterar att intervjuade framhåller att formerna för rapportering till styrelsen inom området upplevts ha tydliggjorts över tid. För verksamhetsåret 2020 har ingen särskild rapportering/information lämnats till styrelsen inom området. För verksamhetsåret 2021 finns det dock i årshjulet en plan om att inom ramen för säkerhetsrapportering/ information till styrelsen även lämna rapport om åtgärder inom berört område.

2.1.4 Bedömning

Av nedanstående tabell framgår bedömningen av revisionsfråga 1, 2, 3 och 5 kopplat till de tidigare genomförda granskningarna Cybersäkerhet - övergripande granskning (2018) och Granskning av intrångsskydd (2018).

Revisionsfråga	**Bedömning**	**Kommentar**
1. Vilka åtgärder har regionstyrelsen beslutat om utifrån sin behandling av granskningarna?	Uppfyllt	Regionstyrelsen har 2019-01-30 behandlat de tidigare två granskningarna och beslutat om åtgärder utifrån resultatet av dessa. Se vidare beskrivning under avsnitt 2.1.2.
2. I vilken utsträckning har resultatet av regionstyrelsens beslutade åtgärder	Uppfyllt	Regionstyrelsen har erhållit återrapportering avseende genomförda åtgärder 2019-11-13.

återrapporteras till styrelsen?		
3. Har regionstyrelsen, utifrån den återrapportering som ev erhållits, analyserat kvarstående åtgärdsbehov inom området? *Fokus på att även beskriva vilka dessa ev. Åtgärdsbehov analyserats att vara.*	Delvis uppfyllt	Vi kan ej styrka att regionstyrelsen genomfört någon analys av kvarstående åtgärdsbehov efter erhållen återrapportering. Det framgår däremot av intervjuer att det inom förvaltningen löpande sker ett arbete med kvalitetsförbättringar för att skapa en ökad intern kontroll inom området. Ett visst kvarstående åtgärdsbehov finns fortsatt inom området. Se vidare beskrivning under avsnitt 2.1.3.
5. I vilken utsträckning har ev. analys om kvarstående åtgärdsbehov föranlett styrelsen att fatta ytterligare aktiva beslut inom området?	Ej uppfyllt	Det kan inte inom ramen för granskningen styrkas att regionstyrelsen efterfrågat någon analys av kvarstående åtgärdsbehov eller att ytterligare aktiva beslut inom området har fattats efter erhållen återrapportering.

2.2 GDPR-implementeringen

2.2.1 Sammanfattning av förstudie

För att Region Norrbotten skulle säkerställa att de efterlever kraven i dataskyddsförordningen och bedriver ett effektivt dataskyddsarbete togs ett projektdirektiv fram under hösten 2018. Beslut att starta projektet Förbättrad Informationssäkerhet fattades i Utvecklingsrådet 2018-11-02, och projektet planerades att genomföras under två års tid.

Revisorerna genomförde under 2019 en förstudie över regionens anpassning till GDPR-regelverket. Målet med förstudien var att övergripande bilda sig en förståelse för hur väl Region Norrbotten anpassat sig för GDPR. Rapporten omfattar samtliga områden där dataskyddsförordningen ställer krav, och en bedömning görs avseende hur väl de åtgärder som regionen redan vidtagit lever upp till de ställda kraven, samt hur projektdirektivets design förväntas leva upp till de ställda kraven i GDPR. Resultatet visade på vilka områden som anses fungerar tillfredsställande samt vilka områden där ytterligare insatser kan komma att krävas.

I förstudien föreslås att en djupare granskning bör genomföras för att följa upp de rekommendationerna som lämnades inom de olika områdena samt för att utvärdera projektet utifrån målen i projektdirektivet.

Följande områden omfattades av förstudien:

1. Styrning & utbildning
2. Roller och ansvar
3. Behandlingsregister
4. Dokumentation
5. Registrerades rättigheter
6. Säkerhetsåtgärder

2.2.2 Revisionsfråga 4: Sammanställning och återrapportering avseende GDPR-implementeringen

Vad som inledningsvis bör noteras är att förstudien avseende GDPR compliance (2019) inte överlämnats som en revisionsrapport till regionstyrelsen. Regionstyrelsen har dock blivit informerade om att förstudien har genomförts (2019-10-03). Med anledning av detta fokuserar denna granskning på att övergripande beskriva hur GDPR-implementeringen skett på förvaltningsnivå, samt hur uppföljningen/återrapporteringen av projektet har sett ut.

Beslut att starta projektet Förbättrad Informationssäkerhet fattades i Utvecklingsrådet 2018-11-02. Följande framgår av dokumentet *Projektplan Förbättrad Informationssäkerhet* (2019-11-25):

Det övergripande projektmålet är att "*...Region Norrbotten ska förbättra sin informationssäkerhet och leva upp till gällande lagkrav inom informations- och personuppgiftshantering genom att implementera ett systematiskt informationssäkerhetsarbete genom utveckling och inrättandet av ett ledningssystem för informationssäkerhet".*

- Nio delmål har identifierats och följer nedan:
    1. God struktur för informationssäkerhet
    2. Upprättad och kvalitetssäkrad registerförteckning
    3. Etablera rapportering av personuppgiftsincidenter
    4. Rättssäkrade avtal
    5. Välinformerade medborgare
    6. God kännedom om informationssäkerhet
    7. Etablerad modell för konsekvensbedömning
    8. Säkrad digital kommunikation
    9. Ledningssystem för informationssäkerhet
- Under delmålen återfinns de aktiviteter som ska genomföras för att nå målet.
- Av tidplanen för projektet framgår att samtliga aktiviteter planeras vara klara december 2020.
- Rapportering inom projektet ska ske genom veckovisa avstämningsmöten i projektet. Uppföljningsmöten i projektet inför styrgruppen ska ske en gång/månad. Styrgruppsmöten ska hållas en gång/månad.

Inom granskningen har vi tagit del av styrgruppsmötets underlag till årsavslutet 2020 för projektet. Av underlaget framgår att statusen på samtliga delmål med tillhörande delaktiviteter inom projektet har utvärderats med hjälp av en färg/bedömningsskala. Sammantaget ser sammanställningen av statusen på de totalt 41 olika delaktiviteterna ut enligt följande:

Status på aktivitet	Ej påbörjat	Blockerat	Pausat	Pågående	Klart	Accepterat
Antal aktiviteter	4	2	13	9	5	8

Vi har inom granskningen tagit del av en uppdaterad version (2021-02-12) av årsavslutningen där status på aktiviteterna förändrats med anledning av att fler aktiviteter genomförts sedan årsskiftet. Sammanfattningsvis är den största förändringen i den uppföljning som genomförts en bit in på år 2021 att 15 områden nu betraktas ha accepterats.

De fyra delaktiviteter som i den senaste versionen markerats som ej påbörjade (blå) samt den aktivitet som markerats som blockerad (röd) framgår nedan:

- Etablera ett regionalt dataskyddsråd (expertgrupp inom RD-staben). Gruppen kommer under projekttiden utgöras av projektgruppen och har som syfte att vara ett forum för hanteringen av informationssäkerhet/dataskyddsfrågor samt vara rådgivande för verksamheten. Efter projektavslut fortsätter gruppen att samverka och hantera dataskyddsfrågor.
  - *Regionens kommentar: Finns inofficiellt.*
- Etablera lokala ombud i verksamheten som får i uppdrag att vara dataskyddsrådets förlängda arm i verksamheten.
- Genomför riskanalyser och konsekvensbedömningar för de personuppgifts-behandlingar som redan idag kan bedömas utgöra en hög risk för att i ett tidigt skede minimera eventuella risker.
  - *Regionens kommentar: Saknar resurser.*
- Säkerställ att RN:s systemleverantörer lever upp till kraven på inbyggt dataskydd och dataskydd som standard genom att utveckla en rutin och inkorporera denna som ett steg i inköps- och upphandlingsprocessen.
  - *Regionens kommentar: Saknar resurser. CISO ansvarar inte för riskhantering av tredje part.*
- Utvärdera beroenden mellan kartläggningen av personuppgiftsbehandlingar och kartläggningen av regionens förvaltningsobjekt.
  - *Regionens kommentar: Saknar resurser.*

Vi noterar ett antal åtgärder som regionen vidtagit för att avhjälpa de brister som identifierades i revisorernas förstudie 2019. Nedan beskrivs några av de åtgärder som har vidtagits.

Ett flertal styrande dokument relaterat till dataskydd har etablerats. Utöver detta har regionen implementerat ett nytt verktyg för att genomföra digitala utbildningar relaterat till GDPR, med möjlighet att följa upp hur många som genomför respektive utbildning. Det uppges även att regionen på ett väl dokumenterat sätt inkluderat strukturerade personuppgiftsbehandlingar i regionens behandlingsregister. Regionen har även etablerat en organisation för informationssäkerhet.

Vi notera även utifrån vår granskning följande kopplat till området:

- Det finns en avsaknad av ostrukturerade personuppgiftsbehandlingar i regionens behandlingsregister. Till skillnad från tidigare lagstiftning (PUL) så omfattar data-skyddsförordningen även ostrukturerad behandlingar av personuppgifter (som ofta återfinns i anteckningar, dokument, e-post etc.). Detta medför att dataskyddsför-ordningen ställer samma krav på hantering av personuppgifter i ostrukturerat format som i strukturerat format (i system, databaser etc.). Regionens behandlingsregister behöver därför kompletteras med ostrukturerade personuppgiftsbehandlingar.

- Regionen har inte utsett ett centralt dataskyddsråd och inte heller lokala ombud för dataskyddsfrågor.
- Regionen har inte säkerställt att befintliga tredjelandsöverföringar (överföring av personuppgifter till länder utanför EU/EES) sker på ett lagenligt sätt. Dock beskrivs det i intervju att regionen har vidtagit åtgärder för att säkerställa att inga nya tredjelandsöverföringar etableras.
- Konsekvensbedömningar har inte genomförts för personuppgiftsbehandlingar som kan leda till höga risker för de registrerade. I dokumentation som tillgängliggjorts i granskningen beskrivs att det saknas resurser för att genomföra denna aktivitet.

Gällande återrapportering avseende GDPR-implementeringen kan vi inte inom granskningen styrka att regionstyrelsen efterfrågat eller erhållit någon särskild rapportering avseende projektet.

2.2.3 Revisionsfråga 5: Aktiva beslut med anledning av eventuell analys av kvarstående åtgärdsbehov

Av genomförd dokumentanalys samt utifrån våra intervjuer framgår att det på förvaltningsnivå bedrivs ett arbete för att säkerställa att lagkraven inom GDPR-området efterlevs. Av intervjuer konstateras även att det inom regionen bedrivs ett arbete i syfte att åtgärda de iakttagelser som identifierades i förstudien 2019.

Kombinationen av de åtgärder som regionen redan har vidtagit, de åtgärder som regionen arbetar med för tillfället samt de åtgärder som finns med i planen för förbättrad informationssäkerhet framhålls som väsentliga delar i regionens styrning för att successivt säkerställa att kraven i dataskyddsförordningen efterlevs.

Vi kan dock inte styrka att regionstyrelsen efterfrågat någon analys av kvarstående åtgärdsbehovet avseende GDPR-implementeringen eller att några ytterligare aktiva beslut fattats av styrelsen inom området sedan genomförandet av förstudien. I sammanhanget noterar vi däremot att det under år 2021 planeras att regionstyrelsen ska erhålla verksamhetsinformation med en analys inom området.

2.2.4 Bedömning

Av nedanstående tabell framgår bedömningen avseende revisionsfråga 4 och 5 kopplat till GDPR-implementeringen.

Revisionsfråga	**Bedömning**	**Kommentar**
4. Vilken sammanställning finns av GDPR-implementeringen och vilken återrapportering avs detta projekt har styrelsen erhållit?	Delvis uppfyllt	Det kan inom ramen för granskningen styrkas att det på förvaltningsnivå bedrivs ett strukturerat aktivt arbete med GDPR-implementeringen och att en sammanställning avseende detta arbete finns. Vi kan inte inom granskningen styrka att region-styrelsen efterfrågat eller erhållit särskild rapportering avseende projektet.

5: I vilken utsträckning har eventuell analys om kvarstående åtgärds-behov föranlett styrelsen att fatta ytterligare aktiva beslut inom området?	Ej uppfyllt	Det kan inte inom ramen för granskningen styrkas att regionstyrelsen efterfrågat någon analys av kvarstående åtgärdsbehov eller att aktiva beslut inom området har fattats. Av intervjuer och dokument-analys framgår att ett arbete bedrivs för att efterleva gällande lagkrav. För en övergripande beskrivning av det bedömda kvarstående åtgärdsbehovet se avsnitt 2.2.3 ovan. Vi noterar att det under år 2021 planeras att regionstyrelsen ska erhålla verksamhetsinformation med en analys inom området.

2021-03-11

Hans Forsström

Uppdragsledare

Erik Jansen

Projektledare

Bilaga 1 - Dokumentförteckning

Arbetsinstruktioner: Instruktion Informationssäkerhetsstrateg (2021-01-14)

Anvisning för anskaffning av IT-system inom Region Norrbotten (2020-12-01)

Anvisning för IT och informationssäkerhet (2021-01-21)

Information: Författningssamling för informationssäkerhet (2021-01-14)

Information: Återrapportering PWC cybersäkerhet rekommendation - Ej daterad

Information till användare (2020-10-14)

LIS - Uttalande om Tillämplighet - Ej daterad

Rutin för hantering av tillgångar (2021-01-12)

Rutin för klassificering av information (2020-10-07)

Rutin för hantering av IT- och informationssäkerhetsincidenter (2020-12-14)

Rutin för hantering av e-post (2021-01-14)

Rutin för hantering av loggkontroll och intrång i journal- och passagesystem (2020-12-14)

Rutin för att skydda flyttbara lagringsmedium (2020-10-13)

Rutin för granskning av användares åtkomsträttigheter (2020-03-20)

Rutin: Anvisning för lösenord (2020-01-08)

Rutin för genomförande av riskanalys för informationssäkerhet och dataskydd (2021-01-22)

Policydokument: Säkerhetspolicy Region Norrbotten (2019-07-23)

Rapport: Sammanställning av Region Norrbottens informationssäkerhetsarbete 2019 (2020-11-17)

Riktlinje säkerhet (2019-11-21)

Riktlinje: Kravbeskrivning för all utrustning eller system som ska kunna anslutas till NLLNET (2020-09-03)

Styrgruppsmöte årsavslut 2020 - Ej daterad