04764

www.pwc.se

Revisionsrapport

Cybersäkerhet – övergripande granskning

Region Norrbotten

Robert Bergman
Projektledare

Erik Jansen
Projektmedarbetare

Linus Owman
Projektmedarbetare

November 2018

pwc

Innehåll

Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Region Norrbotten har PwC granskat om regionstyrelsen har säkerställt att den interna kontrollen avseende regionens cybersäkerhet är tillräcklig. Granskningen har skett utifrån det s.k. NIST cybersäkerhetsramverk som belyser organisationers mognadsgrad och förmågor inom följande fem kategorier:

- *Identifiera, Skydda, Upptäcka, Respondera/Agera och Återställa.*

Vår sammanfattande revisionella bedömning är att den interna kontrollen avseende regionens cybersäkerhet i begränsad utsträckning är tillräcklig. Bedömningen baseras bl.a. på följande iakttagelser:

- Det saknas 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 är ett utvecklingsområde.
- Rapportering till regionstyrelsen behöver utvecklas för att styrelsen ska kunna hållas informerad/uppdaterad avseende regionens information- och IT-säkerhet.

Iakttagelser och grund för bedömningar gjorda i granskningen redovisas i rapporten.

Utifrån genomförd granskning och vår sammanfattande bedömning lämnar vi följande rekommendationer till regionstyrelsen i syfte att utveckla regionens informations- och IT säkerhet.

- *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.*

1. Inledning

1.1. Bakgrund

Regionens revisorer har med hänsyn till risk och väsentlighet bedömt det angeläget att göra en granskning inom ovan rubricerat område.

All verksamhet bedrivs idag, i varierad grad, med IT-stöd. Det är därför av stor vikt att IT-stödet är drifts- och informationssäkert. Regionens förtroende och verksamhet står inför stora risker och utmaningar i samband med att cyberrelaterade incidenter ökar kraftigt, medan arbetet med att stärka cybersäkerhetsförmågan ofta står stilla.

Medborgarna kommer framöver kräva alltfler digitala lösningar. Tillgänglighet är a och o i dagens samhälle samtidigt som toleransen för säkerhetsbrister, bristande tillgänglighet och avbrott minskar.

Revisionsobjekt i granskningen är regionstyrelsen.

1.2. Syfte och revisionsfråga

Revisorernas uppdrag regleras i kommunallagen kapitel 12. Granskningen ska besvara följande revisionsfråga: Har regionstyrelsen säkerställt att den interna kontrollen avseende regionens cybersäkerhet är tillräcklig.

Granskningen fokuserar på processer, personal och teknik inom granskningsområdet utifrån följande kategorier:

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

Revisionskriterier i denna granskning utgörs av kommunallagen 6 kap § 6 samt regioninterna styrdokument som rör granskningsområdet. I övrigt hänvisas till ovan fem kontrollområden.

1.3. Avgränsning och metod

I tid avgränsas granskningen i huvudsak till år 2018. I övrigt hänvisas till syfte, revisionsfråga och granskningens fem kontrollområden.

Regionens övergripande IT- och informationssäkerhetsmognad har granskats utifrån anpassade funktioner som hämtats från det amerikanska ramverket NIST Cyber Security Framework samt PwC good practice och referensdata. Granskningens resultat ger en bild över vilka förmågor som är mer respektive mindre mogna inom regionen, vilket skapar förutsättningar för planering, prioritering och utveckling av regionens informations- och IT-säkerhetsarbete. Granskningen inkluderar även en benchmark mot andra offentliga aktörer, vilket bidrar till att öka förståelsen ytterligare en dimension kring hur mogen regionen är jämfört med andra.

Bedömningen av NIST cybersäkerhetsramverkets fem kontrollområden sker i förhållande till vad som anses vara adekvat mognadsnivå för organisationen utifrån dess förutsättningar. Rimlig mognadsnivå för en organisation som Region Norrbotten är medel-hög (3-4) på en 4-gradig skala. Detta mot bakgrund av regionens samhällsviktiga uppdrag, den mängd och typ av information som regionens organisation hanterar samt regionens att omfattning/storlek ställer höga krav hög cybersäkerhet. En otillräcklig mognad/förmåga kan medföra att organisationen lider ekonomisk skada, materiella skador samt förtroendeskada mot medborgare.

Granskningen genomförs genom analys av för granskningen relevant dokumentation, två workshops samt en kompletterande intervju. Personer som har deltagit i samband med granskningen utgörs av följande nyckelpersoner:

- Regiondirektör
- IT/MT-direktör
- IT-strateg
- Divisionschefer
- Säkerhetsstrateger

Deltagare vid workshops har lämnats möjlighet att sakgranska denna rapport.

2. *NIST Cyber Security Framework*

NIST cybersäkerhetsramverket 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 repetitiv process utformad för att utvecklas i synkronisering med förändringar när det kommer till säkerhetshot, processer och lösningar. Som ett resultat av detta skapar ramverket förutsättningar för en effektiv och dynamisk säkerhetsloop som inkluderar alltifrån hot till lösningar. Ramverket introducerar inga nya standarder eller koncept, snarare integrerar det redan etablerade standarder[1] och praxis. Ramverket består vidare av fem funktioner; *Identify, Protect, Detect, Respond* och *Recover.*

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. Implementationsnivåerna bidrar till att skapa en kontext vilken möjliggör för organisationen att förstå hur dess nuvarande säkerhet och riskhanteringsförmåga ser ut i förhållande till andra aktörer i samma bransch. Nivåerna (som beskrivs nedan), varierar mellan 1 – 4, där 1 indikerar att medvetenheten om risker är låg, medan 4 indikerar att processer och program har etablerats och blivit väl implementerade i verksamheten. Organisationer rekommenderas att sträva mot att uppnå nivå 3 eller 4.

Nivåer av mognad kopplad till cybersäkerhet

Nivå 1	Låg	Ad hoc riskhantering. Låg riskmedvetenhet, inget samarbete med andra organisationer.
Nivå 2	Låg-medel	Riskhanteringsprocesser- och program är etablerade men är inte integrerade i hela organisationen. Organisationen har insett värdet av samarbete men saknar formella förmågor.
Nivå 3	Medel-hög	Formella policys för riskhantreringsprocesser- och program är integrerade genom hela organisationen. Visst samarbete med externa organisationer sker.
Nivå 4	Hög	Riskhanteringsprocesser- och program baseras på erfarenhetsåterföring och utgör en del av organisationskulturen. Ett proaktivt samarbete med andra organisationer äger rum.

[1] Exempel på standarder och ramverk; COBIT, ISO, ISA.

3. Iakttagelser och bedömningar

3.1. Regionstyrelsens ansvar och roll

Regionstyrelsens ansvarsområden regleras bl.a. i reglemente. Bland styrelsens övergripande uppgifter är att leda arbetet med och samordna utformningen av övergripande och strategiska mål, riktlinjer och ramar för styrningen av hela verksamheten samt göra framställningar i målfrågor som inte är förbehållna annan nämnd. Vidare har regionstyrelsen ett övergripande ansvar för interna säkerhetsfrågor i regionen, ansvara bl.a. för regionens personaladministrativa system, ekonomisystem, dokument- och ärendesystem, e-postsystem, IT-system, kommunikationssystem och skaderapporteringssystem.

Regionstyrelsen har även ett ansvar för att utforma och utveckla regionens system för intern kontroll i enlighet med vad fullmäktige särskilt beslutar.

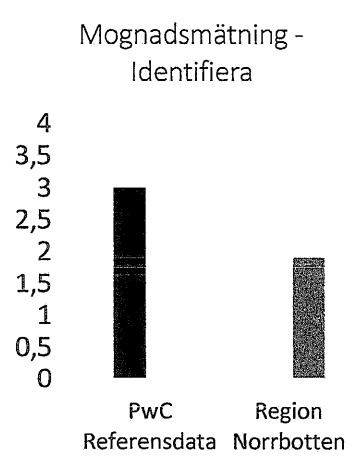
3.2. Identifiera

Identifiera, omfattar Region Norrbottens 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 granskningen bland annat sett till vilka processer som finns kopplade till riskhantering samt klassificering av befintliga tillgångar.

Nedan redovisas iakttagelser som vi har gjort i samband med workshoparna och analys av relevanta underlag. Resultatet har sammanfattats med ett värde mellan 0-4 för att beskriva regionens mognadsgrad samt vilken nivå organisationen bör ligga på för att uppnå ett adekvat skydd kopplat till informations- och IT-säkerhet.

3.2.1. Iakttagelser - Identifiera

Granskningen visar att regionens generella mognadsgrad för området *identifiera* uppgår till mognadsnivå 1,9 (mycket låg) på en 4-gradig skala. Adekvat nivå för området är 3.0. Till grund för denna bedömning är följande iakttagelser:



Granskningen visar att det saknas ett systematiskt arbete med risk- och informationsklassning, vilket innebär att det inte är tydligt hur information ska hanteras i organisationen, t ex vilken information som är mest skyddsvärd eller vilka risker/konsekvenser som har identifierats om hantering inte sker på ett korrekt sätt.

De styrkor som vi, inom ramen för denna granskning, har identifierat är bl.a. att regionen har forum i form av säkerhetsråd och datacentergrupp där identifierade hot och risker kan hanteras. Regionen har vidare bedrivit projekt kopplat till GDPR i syfte att säkerställa att persondata hanteras utifrån de nya reglerna.

De förbättringsområden som vi har konstaterat inom området identifiera är följande:

- *Systematik saknas kring riskidentifiering, riskhantering, och att fastställa organisationens riskaptit. Regionen har heller inga system för att klassificera den information som hanteras/lagras i organisationen. En möjlig lösning på detta är att införa ett ledningssystem för informationssäkerhet.*
- *Regionen saknar i dagsläget en aktuell informationssäkerhetspolicy. I sammanhanget noteras att det pågår en översyn av den nu gällande policyn.*
- *Regionens informationssäkerhetsarbete sköts i dagsläget av en person, vilket får anses vara lite i en organisation av regionens storlek. Vi ser även att samverkan på strategisk nivå mellan informationssäkerhet och IT är liten och att funktionerna är placerade långt ifrån varandra.*
- *Processer kopplade till identifiering av risker och potentiella hot samt hur dessa kan påverka verksamheten har inte dokumenterats. I dagsläget sker riskidentifieringen ad hoc, exempelvis vid förändringar i organisationen eller vid införande av nytt system.*
- *Tröskelvärden för risker har inte upprättats.*
- *Inventering av mjukvara sker utifrån ett licensperspektiv (kostnader) och inte utifrån ett säkerhetsperspektiv.*

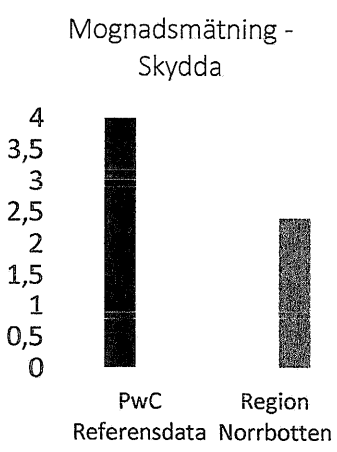
3.3. Skydda

Detta område fokuserar på Region Norrbottens nuvarande tillstånd när det kommer till att skydda regionens information samt avskräcka från hot. Denna kategori inbegriper även förmågan att bl.a. hantera behörighetskonton samt säkerhet kopplad till data.

Nedan redovisas iakttagelser som vi har gjort i samband med workshops och genomgång av relevanta underlag. I likhet med föregående område har resultatet sammanfattats med ett värde mellan 0-4 för att beskriva regionens mognadsgrad samt vilken nivå organisationen bör ligga på.

3.3.1. Iakttagelser - Skydda

Granskningen visar att regionens generella mognadsgrad för området *skydda* uppgår till 2,4 (låg). Adekvat nivå för området är 4. Till grund för bedömningen ligger följande iakttagelser:



Utifrån vår granskning kan vi konstatera att det finns grundläggande skydd genom bl.a brandväggar och att det regelbundet tas back-up på information som lagras inom regionen.

Vår granskning visar vidare att det finns en implementerad process för hantering av behörigheter och konton, däribland att standardbehörigheter har upprättats. Vidare kan vi konstatera att regionen har jobbat med eLearning-insatser för att bl.a. höja medarbetarnas digitala kompetens.

Vi konstaterar även att regionen tillämpar segregerade nätverk för att begränsa/hindra obehöriga åtkomst till regionens infrastruktur.

De förbättringsområden som vi har konstaterat inom området skydda är bl.a. följande:

- *Rutiner för att hantera behörighet brister i vissa avseenden. Om en person har varit anställd under en längre tid blir personen inte av med behörigheter till olika system etc. Detta innebär att efter en viss tid i verksamheten är personens behörigheter summan av alla behörigheter som personen har haft under sin tjänstgöring. I sammanhanget noteras att det pågår ett arbete med att segmentera behörigheter. Vidare saknas system som säkerställer att åtkomst till system inte sker på flera ställen samtidigt.*
- *Det är möjligt att, via USB, flytta ut data/information. Detta trots att det finns rutiner för flyttbar media som dock inte tillämpas.*
- *Det finns en generell avsaknad av dokumenterade processer exempelvis beträffande hantering av sårbarheter och sårbarhetsscanning.*

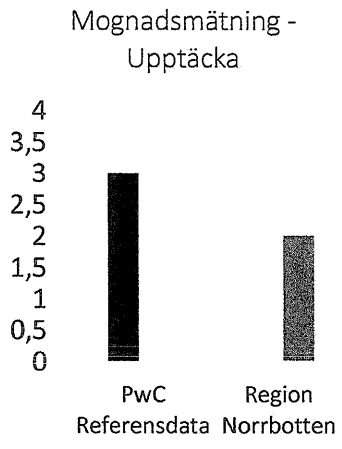
3.4. Upptäcka

Upptäcka, inkluderar bland annat Region Norrbottens förmåga att övervaka IT- och säkerhetsrelaterade händelser. Detta medför bland annat möjlighet till nätverksövervakning, sökning efter skadlig kod och sårbarheter.

Nedan redovisas iakttagelser som vi i granskningen har gjort i samband med våra workshops och genomgång av relevanta underlag.

3.4.1. Iakttagelser - Upptäcka

Granskningen visar att regionens mognadsgrad för området *upptäcka* uppgår till 2,0 (låg). Adekvat nivå för området är 3,0. Till grund för bedömningen ligger följande iakttagelser:



Granskningen visar att avvikelser som upptäcks via nätverk och system analyseras. Det finns även system för att dokumentera incidenter, vilket skapar förutsättningar för att kunna vidta åtgärder.

Det finns även möjligheter att meddela anställda inom regionen om, exempelvis, en virusattack pågår.

Inom ramen för GDPR och NIS-direktivet finns incidentrapporteringskrav. Granskningen visar att kopplat till implementeringen av GDPR finns process implementerad för detta syfte.

De förbättringsområden som vi har konstaterat inom området upptäcka är bl.a. följande:

- Det finns ingen fastställd grundnivå för dataflöden och nätverk för att underlätta upptäckten av avvikelser.
- Det finns heller inga verktyg för att möjliggöra övervakning av användarnas aktiviteter i regionens IT-infrastruktur.

- Överlag saknas i stort dokumentation kring befintliga processer som kopplar till att övervaka system, exempelvis för att hantera malware och genomföra antivirus-åtgärder.
- Kontroller av journalsystem sker manuellt då verktyg för att analysera loggar saknas. Det är dock positivt att kontroller sker på ett systematiskt sätt.

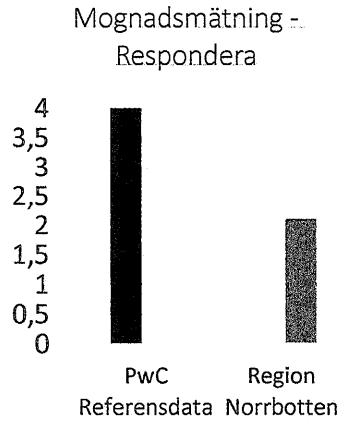
3.5. Agera

Agera, täcker Region Norrbottens rutiner för åtgärdsplanering och aktiviteter kopplade till interna och externa intressenter vid en eventuell incident. Denna förmåga inkluderar bland annat forensik och incidenthantering.

Nedan redovisas iakttagelser som vi i granskningen har gjort i samband med våra workshopar och analys av relevanta underlag.

3.5.1. Iakttagelser – Respondera/Agera

Granskningen visar att regionens generella mognadsgrad för området *respondera* uppgår till 2,1 (låg). Adekvat nivå för området är 4,0. Till grund för bedömningen ligger följande iakttagelser:



Granskningen visar att regionen har en dokumenterad incidentprocess med definitioner av vad som utgör en incident. Länsteknik har sedan behörighet att agera i enlighet med vad som bedöms vara ändamålsenliga åtgärder vid inträffad incident.

Vidare konstateras att lärdomar diskuteras på gruppnivå och rutiner ses över för att bättre kunna agera vid framtida incidenter.

De förbättringsområden som vi har konstaterat inom området agera är bl.a. följande:

- Roller och ansvar kopplat till åtgärder vid en (informationssäkerhets-)incident har inte dokumenterats.
- Sammanställningar görs av incidenter, avbrott m.m. och bedömningar hur robusta system olika system är. Däremot sker det ingen strukturerad/dokumenterad rapportering till regionstyrelsen.
- Det finns begränsad intern förmåga kopplad till forensisk analys av inträffade händelser, exempelvis att återskapa vad som skett på en PC. Vi noterar dock att samverkan med Polis sker vid behov.

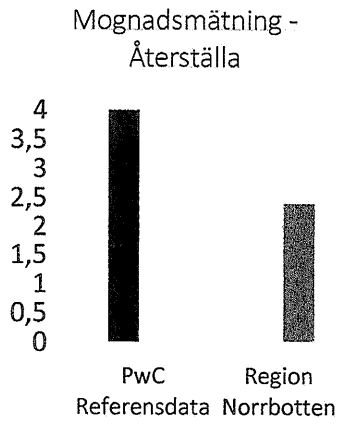
3.6. Återställa

Återställa, relaterar till Region Norrbottens processer för kontinuitetshantering och förmågor relaterade till robusthet och återhämtning efter hantering av incidenter. Kommunikation och publika relationer (PR) inkluderas även i denna kategori.

Nedan redovisas iakttagelser som vi i granskningen har gjort i samband med våra workshops och genomgång av relevanta underlag

3.6.1. Iakttagelser – Återställa

Granskningen visar att mognadsgraden för området *återställa* uppgår till 2,4 (låg). Adekvat nivå för området är 4.0. Till grund för bedömningen ligger bl.a. följande iakttagelser:



Av våra workshops kan vi konstatera att regionen har varit relativt förskonade från allvarligare incidenter. De gånger som krisberedskapen har satts på prov har den fungerat på ett tillfredställande sätt. En styrka som flera framhåller är regionens kommunikationsfunktion och att det alltid finns en tjänsteman i beredskap.

Förbättringsområden inom området återställa som vi har konstaterat är bl.a. följande:

- Regionen saknar implanterade återställningsplaner
- Det finns även en avsaknad av formaliserade processer i form av strategier och styrande dokument som beskriver åtgärder för återställning av de mest kritiska funktionerna i verksamheten efter en inträffad kris/incident.

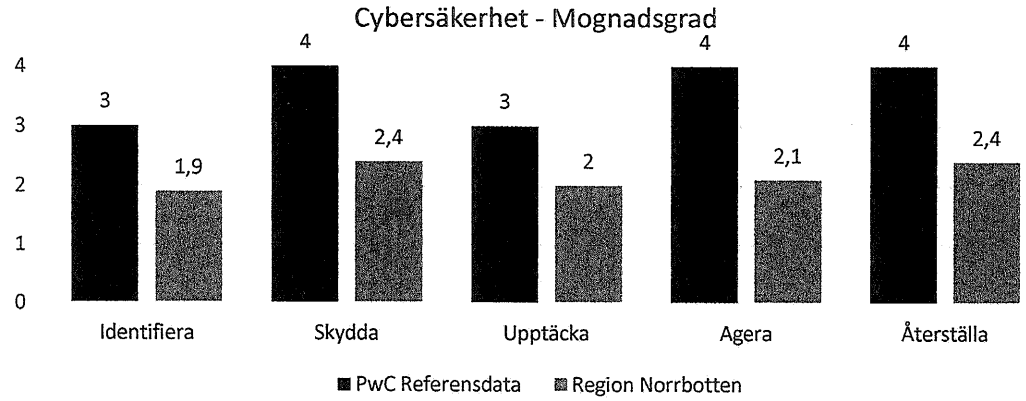
4. *Revisionell bedömning*

Granskningen ska besvara följande revisionsfråga: *Har regionstyrelsen, säkerställt att den interna kontrollen avseende regionens cybersäkerhet är tillräcklig.* Granskningen har fokuserat på processer, personal och teknik inom granskningsområdet utifrån följande kategorier; *identifiera, skydda, upptäcka, respondera/agera och återställa.*

Bedömningen av mognadsnivå kopplat till cybersäkerhet har skett utifrån följande skala:

Nivå 1	Låg
Nivå 2	Låg-medel
Nivå 3	Medel-hög
Nivå 4	Hög

I nedan figur sammanfattas granskningens resultat för respektive kontrollområde:



Vår sammanfattande revisionella bedömning är att den interna kontrollen avseende regionens cybersäkerhet i begränsad utsträckning är tillräcklig. Bedömningen baseras på följande:

Vår granskning visar att regionens mognadsgrad är låg i jämförelse med liknande organisationer och beaktat den typ av samhällsviktig verksamhet som regionen bedriver. Vår granskning har visat att det bl.a. saknas ett strukturerat arbete att identifiera hot och risker mot regionens informations- och IT-säkerhet. Vi noterar även att förmågan att övervaka och således upptäcka avvikelser i regionens system och IT-infrastruktur är ett utvecklingsområde. Rapportering till regionstyrelsen behöver utvecklas för att styrelsen ska kunna hållas informerad/uppdaterad avseende regionens information- och IT-säkerhet.

4.1. Rekommendationer

Utifrån genomförd granskning och vår sammanfattande bedömning lämnar vi följande rekommendationer till regionstyrelsen i syfte att utveckla verksamheten:

- *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.*

2018-11-13

Marie Lindblad
Uppdragsledare

Robert Bergman
Projektledare