Revisionsrapport

Cybersäkerhet – övergripande granskning

Strömsunds kommun

Peter Swedberg
Projektledare

Robert Bergman
Projektmedarbetare

April 2018

pwc

Innehåll

Sammanfattning

På uppdrag av de förtroendevalda revisorerna i Strömsunds kommun har PwC granskat om kommunstyrelsen har säkerställt att den interna kontrollen avseende kommunens 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.*

Utifrån genomförd granskning är vår sammanfattade revisionella bedömning att den interna kontrollen avseende kommunens cybersäkerhet inte är tillräcklig. Bedömningen baseras bl.a. på följande iakttagelser:

- Det saknas genomgående styrning i form av strategier, planer och riktlinjer. Denna typ av dokumentation bidrar till Strömsunds kommuns förmåga att arbeta systematiskt med cybersäkerhet. Styrningen kan med fördel vara baserad på risk- och sårbarhetsanalyser som vi i denna granskning inte kan se genomförs utifrån ett cyber-säkerhetsperspektiv.
- Roll- och ansvarsfördelningen i organisationen är inte tydlig. Bl.a. saknas det ansvarig för kommunens informationssäkerhetsarbete.
- Det säkerställs inte att befintliga riktlinjer såsom exempelvis hantering av lagringsmedia.
- Kommunens ledningsfunktion övar inte utifrån cybersäkerhetsscenarion.
- Vi har noterat att det pågår projekt kopplat till GDPR samt genomlysning/inventering av kommunens hård- och mjukvaror.
- Strömsunds kommun saknar strategier kopplade till att såväl åtgärda en incident som att återställa verksamheten efter densamma så att följdverkningarna minimeras.

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

- Kommunstyrelsen säkerställer att identifiering av hot och risker kopplat till kommunens IT-säkerhet sker på ett systematiskt sätt samt att tillräckliga kontrollmoment sker i syfte att verifiera att IT-säkerheten är tillfredställande.
- Kommunstyrelsen säkerställer att det finns strategier och planer för hantering av incidenter kopplat till kommunens IT-säkerhet.
- Kommunstyrelsen säkerställer att det finns strategier och planer för att återställa verksamhet och system efter att en incident har hanterats.
- Kommunstyrelsen säkerställer uppföljning och kontroll av informations- och IT säkerhetsarbetet i kommunen. Detta kan med fördel ske inom ramen för kommunens internkontroll.

1. Inledning

1.1. Bakgrund

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

All kommunal verksamhet bedrivs idag med IT-stöd. Det är därför av stor vikt att IT-stödet är driftssäkert. Kommunernas förtroende och verksamhet står inför stora 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 från sina kommuner, tillgänglighet är a och o i dagens samhälle, samtidigt som toleransen för otillgänglighet och avbrott minskar.

Revisionsobjekt i granskningen är kommunstyrelsen.

1.2. Syfte och revisionsfråga

Revisorernas uppdrag regleras i kommunallagen kapitel 9. Granskningen ska besvara följande revisionsfråga: Har kommunstyrelsen säkerställt att den interna kontrollen avseende kommunens 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: 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 § 7 samt kommuninterna styrdokument som rör granskningsområdet. I övrigt hänvisas till ovan fem kontrollområden.

1.3. Avgränsning och metod

I tid avgränsas granskningen i huvudsak till år 2017. I övrigt hänvisas till syfte, revisionsfråga och granskningens fem kontrollområden.

Kommunens 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 kommunen, vilket skapar förutsättningar för planering, prioritering och utveckling av kommunens 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 kommunen är jämfört med andra. Denna del av granskningen redovisas separat vid ett senare tillfälle.

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 Strömsunds kommun är låg-medel (2,5-3) på en 4-gradig skala. Detta mot bakgrund av att det, i jämförelse med exempelvis bankinstitut, inte finns samma höga krav och förutsättningar på cybersäkerhet.

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 IT-chef och tekniker, kommunchef samt chefer för bl.a. ekonomi, personal, utbildning och socialtjänst.

Företrädare som intervjuats i granskningen har haft 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. Kommunstyrelsens roll och ansvar

Kommunstyrelsens 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 den kommunala verksamheten samt göra framställningar i målfrågor som inte är förbehållna annan nämnd. Vidare har kommunstyrelsen ett övergripande ansvar för interna säkerhetsfrågor i kommunen, ansvara bl.a. för kommunens personaladministrativa system, ekonomisystem, dokument- och ärendesystem, e-postsystem, IT-system, kommunikationssystem och skaderapporteringssystem.

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

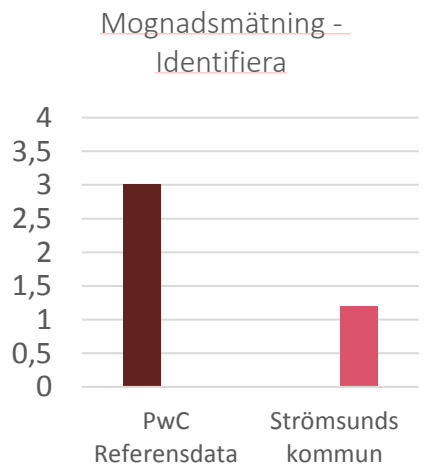
3.2. Identifiera

Identifiera, omfattar Strömsunds kommuns förmåga att identifiera kritiska informations tillgångar 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 kommunens 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 kommunens generella mognadsgrad för området *identifiera* uppgår till mognadsnivå 1,2 (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 överlag saknas processer för att identifiera hot och risker kopplat till kommunens informationssäkerhet. Inom den sociala verksamheten finns vissa arbetssätt att jobba med generell riskidentifiering. Liknande rutiner/arbetssätt har vi inte kunnat styrka finns i övriga verksamheter.

Granskningen visar att det idag inte sker någon systematiskt klassificering eller prioritering av information som lagras i kommunen. Av intervjuer framgår att kommunens informationssäkerhetspolicy är föråldrad och det behövs en samsyn kring vilka policys och riktlinjer som behövs för informationssäkerhetsarbetet.

Vidare konstateras att i gällande reglemente för intern kontroll framgår att styrelsen och nämnderna ska i rimlig nivå säkerställa kontroller så att möjliga risker inringas, bedöms och förebyggs. Vår granskning av kommunstyrelsens internkontrollplan visar att planen saknas kontrollmoment som rör IT- och informationssäkerhet. Av intervjuer framgår att rutinerna för arbetet med den interna kontrollen är ett identifierat utvecklingsområde.

De förbättringsområden som vi har konstaterat i denna granskning är följande:

- Risk- och sårbarhetsanalyser genomförs inte utifrån ett informations- och IT säkerhetsperspektiv. Det sker heller ingen klassificering av information. En förutsättning för att uppnå en god säkerhet kring hanteringen information är att ha kontrollmoment i syfte att säkerställa att informationen hanteras på ett säkert och korrekt sätt. Kontrollen av hur hanteringen sker bör ske regelbundet och vid upprepade tillfällen.
- Styrningen för området behöver uppdateras, exempelvis i form av en aktuell informationssäkerhetspolicy.

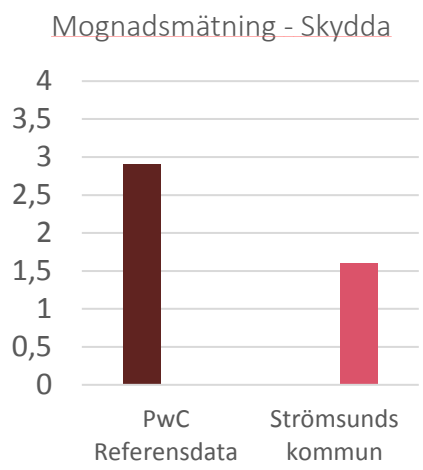
3.3. Skydda

Detta område fokuserar på Strömsunds kommuns nuvarande tillstånd när det kommer till att skydda kommunens 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 kommunens mognadsgrad samt vilken nivå organisationen bör ligga på.

3.3.1. Iakttagelser - Skydda

Granskningen visar att kommunens generella mognadsgrad för området *skydda* uppgår till 1,6 (låg). Adekvat nivå för området är 2,9. Till grund för bedömningen ligger följande iakttagelser:



Granskningen visar att de åtgärder som vidtas för att skydda från att obehöriga kommer åt information eller får åtkomst till system sker bl.a. genom grundläggande behörigheter till användare, krav på lösenord vid inloggning och sk. mailtvätt mot skadlig kod.

Vidare kan vi konstatera att uppdateringar av, exempelvis datorer, sker regelbundet och är tvingande. Det finns även visst skydd mot förlorad data genom BitLocker samt att kommunen har brandvägg och virusskydd som förhindrar obehöriga åtkomst till kommunens nät.

Granskningen visar att backuper och säkerhetskopiering sker regelbundet. Däremot sker inte tester av backuper på ett systematiskt sätt. Det finns heller ingen dokumentation kring de tester som sker, exempelvis vad som fungerade bra/dåligt eller när i tid senast återläsning/test skedde.

Granskningen kan däremot inte styrka att det finns dokumenterade rutiner för hanteringen av behörigheter, lösenord eller hur loggning och annan övervakning av kommunens IT-infrastruktur ska gå till.

Det saknas en plan/strategi för utbildning av användarna. Det finns heller ingen tydlig bild över vilka behov som användarna har när det gäller utbildning. Av intervju framgår det är viktigt att ledningen känner till vilket behov av utbildning som föreligger så att rätt typ av utbildning kan erbjudas.

Granskningen visar vidare att det inte sker några tester av IT-säkerheten, exempelvis penetrationstester.

Vi noterar även att det saknas policy för hur flyttbar lagring, exempelvis USB-stickor, ska hanteras. Det är idag inte känt i vilken utsträckning som exempelvis USB-stickor används.

De förbättringsområden som vi har konstaterat i denna granskning är bl.a. följande:

- Tester av IT-säkerhet sker inte på ett systematiskt sätt.
- Det saknas en tydlig bild över vilket utbildningsbehov användarna har för att använda IT på ett säkert sätt.
- Det saknas kunskap hur användning av flyttbar lagring används. Vidare konstateras att det saknas policys/riktlinjer för hur flyttbar lagring ska användas.
- Det saknas implementerade återställningsplaner kopplade till informations- och IT säkerhetsincidenter, övergripande men även för särskilda system.
- Det finns en generell avsaknad av dokumenterade processer som, exempelvis, beskriver hanteringen av cyberrelaterade hot och sårbarheter. Bl.a. saknas dokumentation för tester och rutiner för återställande (backuper).

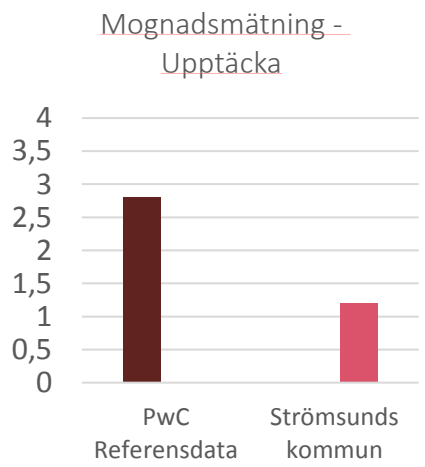
3.4. Upptäcka

Upptäcka, inkluderar bland annat Strömsunds kommuns 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 kommunens mognadsgrad för området *upptäcka* uppgår till 1,2 (mycket låg). Adekvat nivå för området är 2,8. Till grund för bedömningen ligger följande iakttagelser:



Granskningen visar att det inte sker någon systematisk utvärdering av dataflödet i kommunens nät. Utvärdering sker först när en incident har skett. Vidare kan vi konstatera att det saknas processer/strukturerade arbetssätt för att dokumentera händelser och på så vis skapa en kunskapsbank kring möjliga lösningar på incidenter och problem som har inträffat. Information inom IT-enheten överförs till stor del muntligt.

Ett sätt att kunna bedöma hur allvarlig en avvikelse är att införa sk. tröskelvärden. Granskningen visar att detta saknas. Vi kan vidare konstatera att det inte sker någon systematiskt övervakning av otillåten användning, exempelvis nedladdning av program eller om användare besöker olämpliga hemsidor. Av intervjuer framgår att en ny brandvägg kommer att implementeras och att det då kommer finnas bättre förutsättningar för att kunna följa upp aktiviteten i kommunens nät.

Vi noterar även att kommunens antivirus-skydd inte har testats i labbmiljö och att det finns liten styrning hur mobila enheter ska hanteras, exempelvis mobiltelefoner. Av intervju framgår att medvetenheten bland användarna, om vilka risker som är förenade med användande av mobila enheter, bedöms vara låg.

De förbättringsområden som vi kan konstatera är bl.a. följande:

- Det sker ingen systematisk övervakning av vilka program som laddas ner eller om användarna besöker olämpliga hemsidor.
- Analyser av avvikelser, i ett proaktivt syfte, sker inte/i mycket låg utsträckning. Exempelvis saknas s k. tröskelvärden för att bedöma hur allvarlig en avvikelse/incident är.
- Dokumentation kring befintliga processer kopplade till övervakning av system saknas.
- Formella processer för att hantera larm eller signaler om avvikelser saknas.

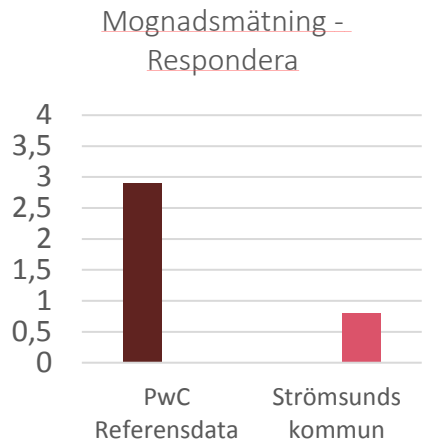
3.5. Respondera/Agera

Respondera/agera, täcker Strömsunds kommuns 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 kommunens generella mognadsgrad för området *respondera* uppgår till 0,8 (mycket låg). Adekvat nivå för området är 2,9. Till grund för bedömningen ligger följande iakttagelser:



Kommunens lägre mognadsnivå, i förhållande till adekvat nivå för området, beror främst på avsaknaden av dokumenterade åtgärdsplaner och strategier. Detta medför en risk för att anställda inte är medvetna om hur roller och ansvar är fördelade vid en eventuell incident. Följaktligen kan detta medföra större konsekvenser för verksamheten än om roller och ansvar vore tydligt kommunicerade genom exempelvis en formellt antagen strategi, plan eller riktlinje.

Granskningen visar vidare att när en avvikelse/incident inträffar hanteras detta i hög utsträckning ad hoc, dvs situationen löses av IT-enheten men inte utifrån någon given strategi. Det finns ingen/liten dokumentation kring inträffade incidenter. Vi kan vidare konstatera att förmågan/möjligheten att utreda incidenter/avvikelser inom IT-enheten är begränsad och sker främst i mån av tid.

Tillgången till forensisk kapacitet är låg och rutiner och riktlinjer för detta område saknas. Exempelvis skulle dessa riktlinjer reglera hur IT-enheten/verksamheterna ska agera om det finns misstankar om brott (vem ska anmäla, hur bevis säkras etc).

Granskningen visar att dokumenterade rutiner/strategier för att begränsa en incident saknas. Av intervjuer sker detta från fall till fall. Exempel på åtgärder som har vidtagits vid incidenter är bl.a. att begränsa nätacessen och att fysiskt koppla ur nätverkskort för att hindra eventuell spridning av skadlig kod.

De förbättringsområden som vi kan konstatera är bl.a. följande:

- Roller och ansvar kopplat till informations- och IT säkerhetsincidenter behöver dokumenteras/förtydligas.
- Åtgärdsplaner för informations- och IT säkerhetsincidenter behöver upprättas.
- Trots ett arbetssätt där lärdomar från incidenter identifieras har inga rutiner upprättats för att formalisera och säkerställa att kunskapsöverföring sker. Kunskapsåterföringen sker ad hoc och utan att dokumenteras.

- Nyckelpersonberoende är en stor risk som identifierats i granskningen. Ett bortfall kan medföra stora problem för organisationen att exempelvis kunna hejda incidenter då endast ett fåtal har kännedom om hur detta skulle kunna förhindras.

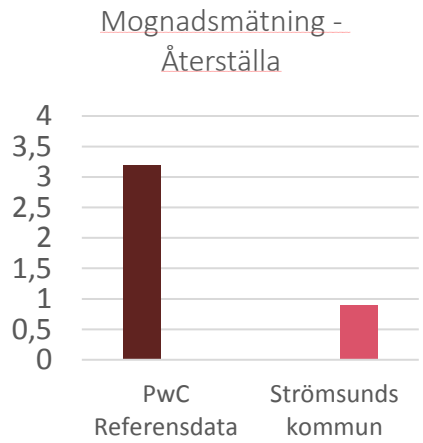
3.6. Återställa

Återställa, relaterar till Strömsunds kommuns 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 0,9 (mycket låg). Adekvat nivå för området är 3.2. Till grund för bedömningen ligger bl.a. följande iakttagelser:



Granskningen visar att det saknas planer och strategier kopplade till att återställa verksamheten från ett incidentläge till normal drift. Av intervjuer framgår att kommundirektören och ledningsgruppen diskuterar om ”nedtrappning” ska ske efter en incident. Till stöd finns kommunens säkerhetssamordnare.

Inom IT-enheten saknas strategier/planer som beskriver hur återställning ska ske, exempelvis om det finns prioriteringar mellan olika verksamheter eller system.

När det gäller informationsinhämtning och PR är det i huvudsak kommundirektör, säkerhetssamordnaren och kommunens kommunikatör som bevakar och utvärderar situationen eller incidenten. Oftast kommer det information från förvaltningscheferna om vad som har inträffat.

När det gäller ryktesspridning hanteras detta primärt av kommunikatören. Strategin är att bedöma och bemöta detta så snart som det uppstått, exempelvis om medborgare har skrivit något på sociala medier. Någon dokumenterad plan/strategi finns dock inte hur exempelvis verifiering av rykten/information ska ske.

Förbättringsområden som vi utifrån granskningen kan konstatera är följande:

- Det saknas en dokumenterad plan/strategi för att bemöta rykten etc som potentiellt kan skada kommunens anseende.
- Implementerad återställningsplan saknas, varken på övergripande nivå eller för enskilda system.
- Erfarenhetsöverföring efter återställning av verksamheten sker ad hoc och utan att dokumenteras.
- Strategier och styrande dokument för återställning av verksamheten saknas.

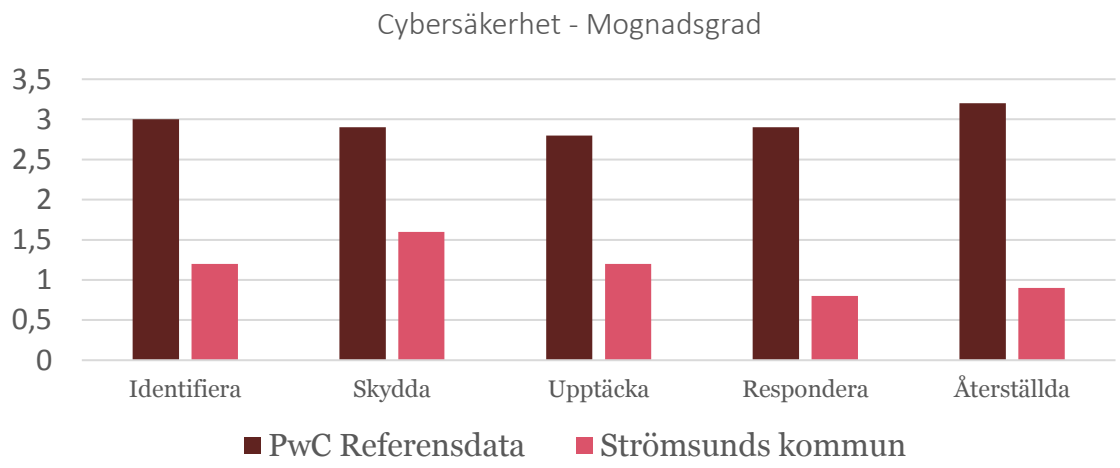
4. Revisionell bedömning

Granskningen ska besvara följande revisionsfråga: *Har kommunstyrelsen, säkerställt att den interna kontrollen avseende kommunens 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 kommunens cybersäkerhet inte är tillräcklig. Bedömningen baseras på följande:

Vår granskning visar att kommunens mognadsgrad avseende cybersäkerhet inte uppnår adekvat nivå. Granskningen har visat att det genomgående saknas styrning i form av strategier, planer och riktlinjer. Denna styrning bör med fördel vara baserad på ett systematiskt arbete med cybersäkerhet samt risk- och sårbarhetsanalyser. Det saknas även ett strukturerat arbete med att säkerställa att riktlinjer som finns för användare, exempelvis hantering av lagringsmedia, efterlevs i tillräcklig omfattning för att upprätthålla en god informations- och IT säkerhet. Vi har även identifierat brister när det gäller kommunens förmåga att skydda mot incidenter och hantera incidenter när dessa väl har inträffat.

4.1. Rekommendationer

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

- Kommunstyrelsen säkerställer att identifiering av hot och risker kopplat till kommunens IT-säkerhet sker på ett systematiskt sätt samt att tillräckliga kontrollmoment sker i syfte att verifiera att IT-säkerheten är tillfredställande.
- Kommunstyrelsen säkerställer att det finns strategier och planer för hantering av incidenter kopplat till kommunens IT-säkerhet.
- Kommunstyrelsen säkerställer att det finns strategier och planer för att återställa verksamhet och system efter att en incident har hanterats.
- Kommunstyrelsen säkerställer uppföljning och kontroll av informations- och IT säkerhetsarbetet i kommunen. Detta kan med fördel ske inom ramen för kommunens internkontroll.

2018-04-13

Anneth Nyqvist	***Peter Swedberg***
Uppdragsledare	*Projektledare*