Uppföljning internkontrollplan

Kommunstyrelsen

Tertial 3 2023

NACKA KOMMUN

Innehållsförteckning

1 Sammanfattning

Under 2023 har internkontrollarbetet inom Kommunstyrelsens fortgått utifrån den internkontrollplan för 2023 som kommunstyrelsen beslutat i december 2022. Sammanfattningsvis har inga väsentliga avvikelser identifierats, och för de avvikelser av ej väsentlig omfattning som identifierats har respektive verksamhet genomfört uppföljande arbete och vidtagit erforderliga åtgärder.

Generellt kan dock nämnas att det allmänna omvärldsläget med intensifierade IT-attacker och tydliga konsekvenser för drabbade aktörer ökar fokuset i kommunen på IT-säkerhetsfrågan och kontinuitetsplanering, det vill säga förmågan att hantera en allvarlig samhällsstörning, allvarliga incidenter och kriser för verksamheterna. Det har under året varit ett ökat antal försök att penetrera och skapa störande påverkan i Nacka kommuns IT-miljö och det finns därför ett behov av ett ökat IT-säkerhetsfokus och krisberedskap.

Detta har inneburit att några kontrollmoments risknivå har höjts från ”Hög” till ”Kritisk” med syfte att skapa förutsättningar för kommunen att säkerställa och riskminimera sin IT-infrastruktur och att upprätthålla ett stort fokus i organisationen med att höja medvetandet samt genomföra kontinuitetsplanering.

2 Periodens riskanalys

Risk	Ursprunglig risk för året	Periodens riskanalys	Riskvärdering per tertial
Bristande efterlevnad av dataskyddsförordningen	Hög (12)	Ett kontinuerligt arbete med att efterleva kraven i GDPR pågår, främst i form av kartläggning av personuppgiftsbehandlingar, analys av risker och utbildning av medarbetare. I december 2023 har en ny ordinarie DSO för kommunens nämnder samt NEAB och NVOA tillträtt. Arbete för att kvalitetssäkra den övergripande processen för personuppgiftsincidenthantering är påbörjad. Arbete för att kvalitetssäkra en säker behandling av skyddade personuppgifter (d.v.s. personuppgifter för personer med skyddad identitet), och relevant incidenthantering rörande dessa, pågår i samarbete med informationssäkerhetssamordnaren. Även revidering/förtydligande av styrdokument och stöddokument pågår.	Hög
Bristande styrning i stadsbyggnadsprojekt	Medium (8)	Modellen för projektstyrning har varit grundläggande för arbetsprocessen under året, dock återstår viss finjustering av processen. Ett aktivt och strukturerat arbete kring riskeliminering har bedrivits och nya rutiner för att kvalitetssäkra arbetet med projektering och utbyggnad har tagits fram. Kvalitetssäkringen har gjorts i syfte att minimera osäkerhetsfaktorer i utbyggnadsfasen, att säkerställa projektens tidplan, budget och upphandlingsdokumentation genom projektens olika faser (t.ex. systematiskt riskarbete, ny kalkylprocess och granskning av förfrågningsunderlag). Gällande ekonomiska risker har dessa setts över löpande. Trots genomfört arbete under året bedöms risken till hög då det tar tid att implementera ovan förbättringsåtgärder och arbetssätt i organisationen samt att marknaden är mer osäker än tidigare och många risker kan påverka varandra. Fokus på ökad styrning i våra projekt och i vår rapportering är stort. Det sker täta avstämningar mellan projektledare och projektchefer med syfte att säkra bland annat framdrift, kalkyler och underlag. För hela stadsutvecklingsprocessen finns Forum för projektrapportering där varje projekt granskas och gås igenom med syfte att hålla god kvalité i prognoser och planer. Det har också utvecklats ett processgemensamt analysverktyg	Hög

Risk	Ursprunglig risk för året	Periodens riskanalys	Riskvärdering per tertial
		för att minska risken för felaktigheter i prognosarbetet och för projekt i aktiv genomförandefas finns ett nyinrättat forum hos Anläggningsenheten med särskilt fokus kvalité i prognoser. Det kommer dock ta tid att implementera ovan förbättringsåtgärder och arbetssätt. Inga väsentliga avvikelser i projektstyrningen har identifierats under året.	
Allvarliga brister i anläggningar och fastigheter.	Hög (15)	Åtgärder / kontrollmoment: Regelbundna besiktningar och kontroller. Uppdaterade underhållsplaner avseende både kortare och längre sikt. Metod: Uppföljning av att besiktningar/kontroller görs och att underhållsplaner finns. Besiktningar och kontroller har genomförts regelbundet och underhållsplaner finns.	Hög
Allvarliga brister i leverans av välfärdstjänster	Medium (10)	Välfärd skola och Välfärd samhällsservice har fungerande ledningssystem och rutiner för kvalitet, arbetsmiljö, riskhantering samt ekonomistyrning. Systemen och innehållet utvecklas löpande. Produktionsområdena följer upp verksamheterna regelbundet.	Medium
Förtroendeskadligt agerande	Hög (12)	För att minimera risken för förtroendeskadligt agerande kommer stadsdirektören under våren 2024 att besluta om *Så här gör vi i Nacka rekrytering.* I styrdokumentet tydliggörs hur kommunen agerar för att minska risken för förtroendeskadligt agerande genom en än mer gedigen rekryteringsprocess med bakgrundskontroller vid rekrytering. Styrdokumentet tar arbetsgivaren fram efter samråd med fackliga företrädare och Nacka kommuns expertkonsult för att genomföra bakgrundskontroll. Utbildning/"Lärlabb" för chefer genomförs kontinuerligt kring lojalitet, otillåten påverkan och hantering av bisysslor som ett led i att tydliggöra förväntan på ett professionellt – och inte förtroendeskadligt agerande. Rutinen för anmälan om bisysslor har införts som en e-tjänst för att säkerställa en kvalitetssäkrad rutin för hantering av bisysslor. Riskvärdering oförändrad jmf med internkontrollplanen.	Hög
Brister i inköps- och avtalshantering	Hög (12)	Omvärldsanalys inom samtliga 10 kategorier är genomförd under 2023 vilka dessa presenterades vid internt kategoriseminarium. Marknadsanalys genomförs principiellt vid alla upphandlingar då det är en del av inköpsprocessen. Nacka kommun har en leverantörstrohet på ca 77% och 20% av kommunens leverantörer står för över 96% av "spenden". I enlighet med inköpspolicyn och delegationsordningen är verksamheterna är ansvariga för att gällande avtal följs. Spendanalyser genomförs regelbundet genom vilka direktupphandlingar kan identifieras. Riskvärdering oförändrad jmf med internkontrollplanen.	Hög
Svårigheter att rekrytera och behålla kompetent personal	Hög (12)	Det pågår ett målinriktat arbete för att kunna rekrytera och behålla personal såsom utveckling av rekryterings- och introduktionsprocesserna och arbetsmiljö- och hälsoarbetet. En FOKUS-uppföljning genomförts som en uppföljning av medarbetarundersökningen och sambandsanalyser har genomförts för att skapa insikt i det som driver på utvecklingen av ambassadörskap för arbetsplatsen och kommunen.	Hög

Risk	Ursprunglig risk för året	Periodens riskanalys	Riskvärdering per tertial
		Genom att ha fokus på utmärkt ledarskap, jämställdhet, mångfald, bra arbetsförutsättningar såsom förväntas utifrån medarbetarpolicyn, kvalitetsutveckling som leder till stolthet över Nackas framgångar och employerbranding positionerar sig Nacka kommun som en attraktiv arbetsgivare i framkant. I systemstödet för att följa upp arbetssökandes upplevelser av rekryteringsprocessen finns även en modul för att kunna göra riktade enkäter till medarbetare som slutar sin anställning i kommunen för att på ett än mer systematiskt sätt kunna ta tillvara synpunkter och råd från medarbetare som slutar. Riskvärdering oförändrad jmf med internkontrollplanen.	
Avbrott i digitala system	Hög (12)	Det allmänna omvärldsläget med intensifierade IT-attacker och tydliga konsekvenser för drabbade aktörer ökar fokuset i kommunen på IT-säkerhetsfrågan och kontinuitetsplanering för verksamheter. Vi har under året sett ett ökat antal försök att penetrera och skapa störande påverkan i Nacka kommuns IT-miljö och ser därför ett behov av ett ökat IT-säkerhetsfokus och stöd för detta i våra styrdokument. **Riskvärdering** Med tanke på omvärldsläget och de rörelser som vi ser i Nacka så bedömer vi att riskvärderingen bör höjas från ”Hög” till ”Kritisk” med syfte att skapa rätt förutsättningar för kommunen att säkerställa och riskminimera sin IT-infrastruktur och att upprätthålla ett stort fokus i organisationen på medvetandehöjande åtgärder samt kontinuitetsplanering.	Kritisk
Brister i informationssäkerhet	Medium (9)	Med anledning av den ökade hotbilden i vår omvärld, ökade antalet negativa oplanerade händelser som drabbat leverantörer till offentliga myndigheter samt externa krav på kommunens nätverk och informationssystem, är bedömningen att risker för brister i informationssäkerhetsarbetet ökat. Den tidplan som beslutats och de åtgärder som prioriterats tidigare är inte tillräckliga för att möta de utmaningar som den reviderade riskanalysen identifierat. Målbilden för informationssäkerhetsarbetet t.o.m. 2025, som beslutades under T2 2023, står sig väl men delar av denna måste på plats mycket tidigare än den ursprungliga tidplanen. Arbetet som genomförts fram till och med T3 2023 har följt den ursprungliga tidplanen vilken nu är i behov av revidering och resurssättning.	Hög
Bristande attestrutiner	Medium (9)	De manuella utbetalningsordrarna som kontrollerats har tillräckliga underlag och rätt attester. Kan tilläggas att urvalet inte bara rört KS-ansvar. I underlagen till fakturor i systemet förekommer brister och kunskapen om regler och delegationer som rör förtäring, representation, konferenser och liknande är inte alltid tillräcklig. Redovisningsenhetens erfarenhet är att det är svårare att kommunicera om bristerna i systemet och där är det även tekniska utmaningar att attestera rätt. Resultatet av testerna tar vi med oss och kommer att arbeta mer med upplysning och lathundar till strategiska grupper som har mer av den här typen av kostnader.	Medium

Risk	Ursprunglig risk för året	Periodens riskanalys	Riskvärdering per tertial
Brister i bemötande och samspel	Medium (9)	Aktiviteter kopplat till vidareutveckling och kvalitetssäkring inom bemötande och samspel fortlöper enligt plan. Riskvärdering oförändrad jmf med internkontrollplanen. Hösten 2023 har den obligatoriska webbutbildningen Glänsa lanserats till medarbetare inom stadshusets enheter plus de kommunala bolagen. I nästa moment lanseras Glänsa till kollegorna inom produktionen.	Medium
Oegentligt nyttjande av kommunens bidragssystem, kundvalssystem och upphandlade tjänster	Hög (15)	En kartläggning av hur verksamheterna arbetar kring välfärdsbrottslighet och otillåten påverkan har utförts under 2023. Kartläggningen omfattar alla nämnder och dess verksamheter och ser över om det finns relevanta rutiner och handlingsplaner, hur lagen och rutinerna efterlevs och om det finns information om tidigare upptäckta fall av välfärdsbrottslighet eller misstänkt sådana. Utifrån kartläggningen har det genomförts en analys som utgör grunden för framtagandet av åtgärdsplan, gemensamma riktlinjer och rutiner för att motverka välfärdsbrottslighet. Arbete pågår med att skapa en kommunövergripande struktur för att hantera välfärdsbrott och otillåten påverkan. Det pågår projekt med syftet är att stärka förmågan att upptäcka och förhindra välfärdsbrottslighet. På daglig basis arbetar verksamheterna med att upptäcka brister hos anordnare likväl hos medborgare som otillbörligen utnyttjar kommunala medel för egen vinning.	Hög
Allvarlig händelse eller kris	Hög (15)	Kommunens övergripande risk- och sårbarhetsanalys (RSA) syftar till att ge en tydlig grund för verksamheternas kontinuitetsplanering, det vill säga förmågan att hantera en allvarlig samhällsstörning, allvarliga incidenter och kriser. Genom det försämrade säkerhetspolitiska läget i Europa ökar behovet av att öva verksamheterna inför kommande kriser. Utbildnings- och övningsplanen ger grunden för vilka som ska övas, vad som ska övas och vad som är viktigt att beakta. Under slutet av året lämnades en ansökan in till framtidsfonderna med syftet att skapa en gemensam struktur och plattform för kommunens övningsverksamhet inom krisberedskap och civilt försvar. Under 2023 påbörjades även en digital utbildning i krisberedskap för nackaborna i samarbete med Myndigheten för samhällsskydd och beredskap (MSB), Länsstyrelsen i Stockholms län och Civilförsvarsförbundet. Utbildningen ska vara klar i början av hösten 2024. Under 2023 har inga allvarliga incidenter föranlett initiering av en kommunövergripande krisledning. Riskvärdering är oförändrad jämfört med internkontrollplanen.	Hög
Cyberattack eller IT-haveri	Hög (15)	Det sker löpande försök till attacker mot Nackas infrastruktur, i huvudsak mot Nacka.se och till inloggningsserver. Attackerna är inte direkt riktade mot Nacka kommun utan är en del av ett större angrepp mot företag, kommuner och myndigheter i Sverige. Vid ett fåtal tillfällen har attackerna inneburit kortare perioder med nedtid för vår webbplats (Räknat i minuter) men i sin helhet så har vårt skydd motstått försöken. Under året har en ny policy, ”Så här gör vi i Nacka – IT-säkerhet” fastslagits i KS och kommunicerats till alla medarbetare i olika kanaler. Ett antal	Hög

Risk	Ursprunglig risk för året	Periodens riskanalys	Riskvärdering per tertial
		aktiviteter med stöd i dokumentet är initierade och kommer att utföras under året. Nacka har även tagit initiativ till samverkan i Stockholmsregionen där Länsstyrelsen nu har tagit på sig att samordna formerna för att kunna dela information i händelse av incidenter. Detta i syfte att så snabbt som möjlig få kunskap om vad som har hänt och vilka åtgärder som har vidtagits så att alla berörda kommuner har möjlighet att genomföra tidiga insatser för att undvika sårbarheter. Riskvärdering oförändrad jmf med internkontrollplanen.	
Bristande kommunikation	Hög (12)	Kommunikationsplaner tas fram löpande kopplat till kommunikationsstabens uppdrag. Kontinuerlig samverkan med SSR sker i den omfattning som krävs. Likaså sker tät samverkan med ledningsstaben och kommunledning. Den övergripande kriskommunikationsplanering är i al väsentligt uppdaterad. Det finns dock behov av att träna organisationen och kommunikatörerna i krishantering. För att stärka kriskommunikationen ytterligare kan KIB (Kommunikatör i beredskap) införas. Detta är dock en budgetfråga. För att stärka kommunikationsarbetet ytterligare ska Kommunikationsstrategis uppdateras under 2024. Det ska också tas fram en varumärkesplattform och en kommunövergripande kommunikationsplan.	Hög
Kommunstyrelsebeslut genomförs ej	Medium (10)	Uppföljning av politiska beslut görs enligt plan och inga avvikelser har inträffat under året. Riskvärdering oförändrad jmf med internkontrollplanen.	Medium