Nacka kommun

Rapport: IT- och informationssäkerhet

7 september 2017

Building a better working world

Sammanfattning

Bakgrund

På uppdrag av de förtroendevalda revisorerna i Nacka har EY genomfört en granskning av IT- och informationssäkerhet vad gäller hantering av informations- och IT-säkerhetsfrågor på övergripande nivå i kommunen. Syftet med revisionsprojektet har varit att granska på vilket sätt kommunen jobbar för att upprätta en god säkerhet. Granskningen har gjorts mot utvalda delar av EYs Cyber Program Assessment-ramverk.

Övergripande slutsatser

Av samtliga 63 granskningspunkter är fördelningen av bedömningarna följande:

Kontrollen finns och fungerar tillfredsställande:	21 %
Kontrollen finns och fungerar delvis:	35 %
Kontrollen finns ej eller fungerar ej tillfredsställande:	44 %
Ej tillämplig, kontrollen behövs ej av särskilda skäl:	0 %

Det ramverk som använts för granskningen har inga preferenser i sig om outsourcing av IT-verksamhet är bättre eller sämre ur intern kontrollsynpunkt. Huruvida IT-verksamheten är outsourcad eller inte kräver dock olika överväganden vad gäller utformning av den interna kontrollen.

Nacka kommun har en decentraliserad organisation som till stor del är beroende av externa leverantörer inom IT-området. Det leder till ett behov av tydlig styrning och frekvent uppföljning av leverantörer för att säkerställa att avtal uppfylls bland annat vad gäller att IT-säkerheten är tillräcklig. Utan en tillräcklig styrning kan det leda till stora risker för verksamheterna. Nacka kommuns beroende av externa leverantörer kan också leda till stora risker för verksamheten om avtal inte följs upp och leverantörer inte tillhandahåller de servicenivåer som överenskommits.

Kommunen har interna resurser som är ansvariga och engagerade i frågorna och arbetar med att ta fram processor och ramverk som kan stödja den nya dataskyddslagstiftningen. Granskningen visar att Nacka kommun i stort har goda förutsättningar för ett ändamålsenligt arbete med informationssäkerhet. Dock saknas processer och rutiner i nuläget för att effektivt kunna arbeta med dessa frågor och för att säkerställa en tillräcklig intern kontroll inom området. Kommunens starka sidor finns inom områdena tredjepartsleverantör, personalresurser och förberedelse för implementation av GDPR. Förbättringsområden har identifierats främst inom information och utbildning, efterlevnad av styrdokument, rutiner för behörighetsadministration och hantering av telefonmeddelanden och sms.

Iakttagelser

Nedan listas våra mest väsentliga iakttagelser och rekommendationer. Fullständiga iakttagelser och rekommendationer återfinns i kapitel 4.

	Iakttagelse och rekommendation	Prioritet
1.	Kommunen saknar standardiserade och definierade rutiner och processer kring informationssäkerhet samt styrning av dessa. Detta innebär risk att organisationens olika ansatser inom informationssäkerhet inte genomförs på ett enhetligt och målinriktat sätt och utan en övergripande struktur. Det rekommenderas att centrala riktlinjer skapas och sprids för att säkerställa en enhetlig informationssäkerhetsbild. Efter granskningen påbörjades och intervjuer genomfördes har ett styrdokument tagits fram, benämnt "Samverkansmodell Nacka."	Hög
2.	Kommunen har inte uppdaterat sin informationssäkerhetspolicy på tre år, vilket innebär en risk att den inte är anpassad efter förändrade omständigheter i organisationen och omvärlden. Vi rekommenderar att policyn ses över löpande, åtminstone en gång per år.	Hög
3.	Kommunen genomför inga utbildningsinsatser inom informationssäkerhet. I och med detta riskerar bristande kunskap och medvetenhet exponera och utsätta organisationen för informationssäkerhetsrisker. Det rekommenderas att ett strukturerat utbildningsinitiativ startas. Enligt uppgift planeras för en utbildningsinsats av samtliga medarbetare under hösten 2017.	Hög
4.	Kommunen saknar tillräckliga incidenthanteringsrutiner och processer kring informationssäkerhet, samt en gedigen incidentshanteringsplan. Detta medför risk för att eventuella brister eller incidenter ej åtgärdas. Vi rekommenderar att riktlinjer, rutiner och processer etableras och sprids genom organisationen. Efter att granskningen påbörjades och intervjuer genomfördes har ett styrdokument tagits fram, benämnt "Samverkansmodell Nacka."	Hög
5.	Kommunen har i nuläget roller med ansvar inom informationssäkerhet, dock är dessa spridda i organisationen. Det saknas en dedikerad avdelning eller grupp som äger dessa frågar och driver de fullt ut – med t.ex. kompletta rutinbeskrivningar samt etablering av behörighetsadministrationsprocesser.	Medel
6.	Kommunen genomför inte några penetrationstester utan förlitar sig helt på tredjepartsleverantörer och verksamhetsenheter inom den decentraliserade organisationen. Penetrationstester syftar till att identifiera tekniska sårbarheter som kan vara blottade för en eventuell angripare. Kommunen genomför i dagsläget inga externa penetrationstester, dvs. tester utifrån ett externt angreppsutfall, och inga interna penetrationstester, dvs. tester utifrån ett insiderperspektiv.	Medel

Innehåll

1. Bakgrund

Idag bedrivs så gott som all verksamhet i en kommun med någon form av datoriserat stöd. Stödet har med tiden utvecklat sig till att bli en förutsättning för att kunna bedriva verksamhet och antalet olika programvaror är stort. För att uppnå målen för en kommuns verksamhet krävs att informationen i verksamhetsstödet är tillgänglig, riktig, har tillräckligt starkt skydd och är spårbar.

Inom Nacka kommun hanteras de gemensamma IT-frågorna av digitaliseringsenheten. Kommunstyrelsen ansvarar för den verksamhet som bedrivs inom digitaliseringsenheten. Digitaliseringsfunktionens uppdrag är att med hög kompetens, delaktighet och god serviceanda erbjuda ett brett utbud av IT-tjänster som stödjer arbetet för välfärd och ett gott liv i Nacka. Detta görs i form av:

- Strategiskt stöd: Digitaliseringsfunktionen levererar modeller, principer, tekniska plattformar och informationssäkerhet.
- IT-tjänster: Tjänsterna är utredningar, processkartläggningar, projektledning, kravspecifikationer/förberedelser inför upphandling, förvaltning och systemutveckling, installation, drift och support av verksamhetssystem, infrastruktur och arbetsplats-utrustning.

1.1 Syfte

Syftet med granskningen har varit att bedöma hur effektivt Nacka kommun arbetar med IT-säkerhet i dag. För att besvara granskningens syfte och bedöma nämndernas rutiner har granskningen utgått från följande revisionsfrågor:

- Finns en tydlig styrning av informationssäkerhet och IT-säkerhet i kommunen genom tydliga och ändamålsenliga policys och styrdokument? Är dokumenten på övergripande nivå beslutade av kommunstyrelsen?
- Finns en process för strukturerad kontroll och uppföljning avseende att policys och styrdokument efterlevs? Sker dokumenterad återrapportering av styrdokumentens efterlevnad till berörd beslutsfattare för styrdokumenten?
- Nacka kommuns styrning och uppföljning och kontroll vad gäller olika IT-leverantörer?
- Finns risker gällande kommunens informationssäkerhet dokumenterade och uppdateras denna dokumentation löpande?
- Finns det en tydlig ansvarsfördelning gällande ansvar för kommunens informationssäkerhet och säkerhetsarbete? Finns risker kopplat till den decentraliserade organisationen?
- Finns säkra rutiner för ändring och avslut av behörigheter?
- Finns det en tillräcklig intern kontroll och följer ansvariga nämnder upp arbetet med informationssäkerhet?
- Får kommunens anställda tillräcklig och ändamålsenlig information och utbildning gällande IT-säkerhet? Hur sker detta?
- Finns det någon policy för hur inkomna telefonmeddelanden och sms ska hanteras?
- En översiktlig bedömning av hur Nacka kommun förbereder sig för införandet av den nya dataskyddsförordningen maj 2018?

1.2 Metod

Revisionsfrågorna har besvarats genom en granskning mot så kallad god praxis inom informationssäkerhetsområdet. Granskningen har gjorts mot utvalda delar av EY:s ramverk *Cyber Program Assessment*. Ramverket bygger på de svenska och internationella standarderna ISO/IEC 27000, COBiT och ITIL. EY har genomfört en övergripande kartläggning av rutiner, kontroller samt IT-säkerheten.

Granskningen genomfördes genom insamling av bakgrundsinformation inför intervjuer. Relevant information utgjordes av befintliga styrande dokument, instruktioner m.m. Därefter genomfördes intervjuer och enkäter med relevant personal för djupare förståelse för övergripande rutiner och kontroller. Under granskningen har dock inga stickprovstester utförts, vilket innebär att vi inte granskat efterlevnad av dessa rutiner och kontroller.

Under granskningen intervjuade vi:

- IT-chef
- IT-säkerhetsansvarig
- Juridik-och kanslienhetschef
- Serviceenhetschef

Därefter har denna rapport utformats som underlag för revisorernas bedömning av hur ändamålsenlig IT- och informationssäkerheten är i kommunen. Rapporten beskriver vår bedömning av kommunens mognadsgrad per huvudområde, och även våra iakttagelser och rekommendationer.

Följande huvudområden har granskats och utvärderats:

- Policyer och styrdokument
- Kontroll och uppföljning av policyer och styrdokument
- IT-leverantörer
- Risker kopplade till informationssäkerhet
- Ansvarsfördelning
- Behörighetshantering
- Intern kontroll
- Information och utbildning
- Policyer/riktlinjer för SMS
- General Data Protection Regulation (GDPR)

2. Granskning

2.1 Granskningsprotokoll

Granskningspunkt		Kommentar	Utvärdering
1 Policyer och Styrdokument			
1.1	Beskriv organisationens policyer för informationssäkerhet.	Det finns en informationssäkerhetspolicy som fastställdes av kommunstyrelsen för tre år sedan och har inte uppdaterats sedan dess. Policyn är på två sidor och definierar Nacka kommuns syn på informationssäkerhet, övergripande mål och organisationens intention med informationssäkerhet. Dokumenten *Så här arbetar vi med informationssäkerhet i Nacka kommun* beskriver vad som måste etableras för att uppfylla informationssäkerhets-policyn.	2
1.2	Vem äger policyer relaterade till informationssäkerhet, standarder och riktlinjer inom organisationen?	Kommunstyrelsen äger Informationssäkerhetspolicyn men den har inte uppdaterats sedan den skapades för tre år sedan.	3
2 Kontroll och uppföljning av policyer och styrdokument			
2.1	Finns en process för strukturerad kontroll och uppföljning avseende att policyer och styrdokument efterlevs?	Det finns en process för strukturerad kontroll och uppföljning avseende policyers och styrdokuments efterlevnad, men kommunen har beslutat att inte uppdatera informationssäkerhetspolicyn vilket gör kontrollprocessen mindre relevant.	3
2.2	Har ni en (acceptabel) användarpolicy för epost och Internet?	Nacka kommun använder sig av dokumenten *Så här gör vi i Nacka* som en användarpolicy för epost och internet. I dessa finns det inte tillräcklig information om hur användare ska använda epost och internet för att klassificeras som acceptabel.	2
2.3	Har ni en process för versionskontroll av integritetspolicyer och notiser/meddelanden?	Alla policyer diarieförs när de är beslutade.	5
2.4	Har kommunstyrelsen godkänt integritetspolicyn?	Kommunstyrelsen har godkänt integritetspolicyn.	5
3 IT-leverantörer			
3.1	Hur använder ni er av tredjepartsleverantörer?	Kommunen använder sig av tredjepartsleverantör för alla sina system och IT-tjänster. Systemen och tjänsterna upphandlas av digitaliseringsenheten samt juridik- och kanslienheten enligt definierade riktlinjer.	5
3.2	Hur hanteras avtal med tredjepartsleverantörer?	Avtal hanteras både centralt och av varje enskild verksamhet. De som hanteras centralt resulterar i en mycket högre kvalitet och uppföljning än de som upphandlas ute i verksamheten enligt kommunen.	3
4 Risker kopplade till informationssäkerhet			
4.1	Finns en formell grupp för incidenthantering?	Servicecenter är ansvarig för incidenthantering och det finns en formell process dokumenterat i *"Samverkansmodell Nacka v.0.4"* som togs fram efter granskningen hade påbörjats. De som jobbar med incidenthantering inom organisationen är inte experter men de förstärkas och stödjas av externa parter som är experter inom dessa område. Den information vi fått om processen är till vissa delar motstridig. Den process som finns har inte formellt spridits genom organisationen.	3
4.2	Har organisationen ett dokumenterat och implementerat program för integritetsincidenter och hantering av brott som innefattar identifiering av misstänkta brott samt hantering av dem?	Det finns en process för hantering av incidenter men ingen specifik process för hantering av informationssäkerhetsincidenter. Kommunen använder sig av leverantörer för att säkerställa hantering av incidenter. Det finns ingen utbildning kring hantering av informationssäkerhetshantering och processerna kring detta är inte väl spridda genom kommunen.	3

Granskningspunkt		Kommentar	Utvärdering
4.3	Vad är omfattningen och strategin för övervakning av säkerhet inom organisationen?	Alla incidenter hanteras av Servicecenter, även informationssäkerhetsincidenter. Det finns inte en specifik funktion som har ett samlat ansvar för övervakning av säkerhet i organisationen istället har kommunen anställt en tredjepartsleverantör för att stödja strategin för övervakning av säkerhet inom organisationen.	3
4.4	Beskriv organisationens modell för översyn och strategisk ledning av (programmet för) övervakning av säkerhet?	Managementteamet är ansvariga och engagerade i översyn och strategisk ledning kring säkerhet. Dock ligger större delen av driftverksamheten hos leverantörer utanför Nacka kommun och det saknas tillräcklig uppföljning av dessa.	3
5 Ansvarsfördelning			
5.1	Finns definierade roller och ansvar för informationssäkerhetsarbetet?	Nacka kommun är en decentraliserad organisation. Det finns definierade roller och ansvar kring informations-säkerhet men ingen sammanhängde kartläggning eller överblick. Detta kan leda till problem med exempelvis dataskyddsförordningen (GDPR) då det kan finnas överlapp mellan områden som ska täckas av både digitaliseringsenheten och juridikenheten.	3
5.2	Hur drivs arbetet med informationssäkerhet i organisationen?	Informationssäkerhet drivs från olika håll men det är digitaliseringsenheten som är ansvarig för detta. Ansvar ligger på varje enskild avdelning att implementera arbetet.	3
5.3	Finns en grupp dedikerad till övervakning av säkerhet?	På grund av den decentraliserade organisationen finns det ingen grupp dedikerad till övervakning av säkerhet. Istället använder kommunen sig av tredjepartsleverantörer för övervakning av säkerhet och det finns det roller som jobbar med övervakning av säkerhet för särskilda system.	4
6 Behörighetshantering			
6.1	Beskriv de standardiserade processer som finns för behörighetshantering.	Det finns inga standardiserade processer för behörighetshantering. Det beror på system och systemägare men Servicecenter är ofta inblandat.	2
6.2	Hur skapas behörigheter?	Det beror på system och systemägare och Service Centre är ofta inblandat.	2
7 Intern kontroll			
7.1	Vad är omfattningen och strategin för övervakning av säkerhet inom organisationen?	Nacka kommun IT-drift är helt outsourcad. Outsourcing i sig innebär inte att den interna kontrollen behöver vara bättre eller sämre men kräver att kommunen har en relevant och gedigen uppföljning av leverantörerna. Enligt "*Samverkansmodell Nacka v.0.4*" som togs fram efter granskningen hade påbörjats finns det bra uppföljning av de centrala systemen och tredjepartsleverantörer men inte lika mycket dokumentation eller struktur kring systemen som upphandlas av verksamheten. Kommunen har inte kunnat förevisa någon uppföljning av tredjepartsleverantörer undre granskningen.	3
7.2	Beskriv organisationens modell för översyn och strategisk ledning för övervakning av säkerhet?	Nacka kommun använder sig av tredjepartsleverantör för översyn och strategisk ledning för övervakning av säkerhet. Centralt styrda avtal är väl hanterade enligt kommunen när det kommer till det här området men resultatet är inte samma för de avtal som inte är centralt upphandlade.	3
7.3	Beskriv organisationens strategi för informationssäkerhet. Hur ofta granskas strategin för informationssäkerhet och av vem?	Informationssäkerhetsstrategin har skapats av informationssäkerhetsprojektgruppen och uppdateras regelbundet.	4
7.4	Har ni ett program för identifiering av attacker/intrång (t.ex. APT)?	Inget program för identifiering av attacker/intrång finns i nuläget, men det finns planer att implementera ett sådant system i framtiden. För de centrala systemen är det tredjepartsleverantörer som är ansvarig för identifiering av attacker/intrång.	1

Granskningspunkt		Kommentar	Utvärdering
7.5	Beskriv organisationens hantering av hot och sårbarhet, innefattandes tilldelning av ansvar samt rapportering till kommunstyrelsen.	Det finns inga formella rutiner för hantering av hot och sårbarhet. Kommunen använder sig av tredjepartsleverantörer för hantering av hot och sårbarhet.	3
7.6	Beskriv hur ni definierar lämplig omfattning då ni genomför bedömningar av attacker och penetrationstestning mot era tillgångar.	Nacka kommun använder sig av tredjepartsleverantörer för bedömningar av attacker och penetrationstestning mot deras tillgångar. Det finns tydliga kontroller för centrala systemen men mindre kontroll kring de system som sitter i verksamheten.	3
7.7	Hur utvärderas hot mot nya och framväxande teknologier (t.ex. molnlagring och BYOD)?	Nacka kommun använder sig av tredjepartsleverantörer för att genomföra sådana utvärderingar vilket ligger på olika nivåer inom organisationen.	2
8 Information och utbildning			
8.1	Är informationssäkerhetsutbildning obligatorisk för samtliga användare då de börjar arbeta i organisationen?	I nuläget finns det ingen informationssäkerhetsutbildning för samtliga användare i kommunen. Mognaden kring utbildning inom informationssäkerhet är låg, men det finns planer att genomföra utbildningar i framtiden. Kommunen har en planerad insats för informationssäkerhetsutbildning under höst 2017.	1
8.2	Finns program för medvetenhet om säkerhetsfrågor som täcker hela organisationen?	I nuläget finns det inget program för medvetenhet om säkerhetsfrågor som täcker hela organisationen.	1
8.3	Hur sprids säkerhetspolicyer, standarder och riktlinjer inom organisationen?	Säkerhetspolicyer, standarder och riktlinjer sprids via enskilda personer i organisationen. I avsaknad av formaliserade rutiner är organisationen beroende av enskilda individers initiativ för att dessa ska spridas.	2
8.4	Hur kommuniceras strategin för informationsstrategi inom organisationen?	Informationssäkerhetsstrategin är tillgänglig på intranätet men den läses av medarbetare endast i mycket begränsad omfattning. Strategin sprids mestadels via samtal med de som arbetar inom området.	2
9 Policyer/riktlinjer för SMS			
9.1	Finns formella policyer och riktlinjer för säkerhet kring hantering av SMS, chatt m.m. etablerade och kommunicerade till hela organisationen?	Det finns inga formella styrdokument för säkerhet kring hantering av SMS, chat m.m. etablerade och inga är planerade.	1
9.2	Finns formella processer etablerade för hantering av SMS, chatt m.m.?	Det finns inga formella processer etablerade för hantering av SMS, chat m.m. och inga är planerade.	1
10 GDPR			
10.1	Finns ett uppgiftsskyddsombud (Data Protection Officer)?	Det finns inte någon anställd med denna roll i nuläget men det finns en PuL-ombud anställd fram till maj 2018 för att hantera uppgiftsskyddsombuds ansvar fram till dess. Kommunen har skapat en rollbeskrivning för den nya rollen och kommer att rekrytera framöver.	3
10.2	Finns det specifika regler, processer och verktyg för att möjliggöra effektiv hantering av sekretess och informationsintegritet?	Kommunen har processer och regler, men inte standardiserad utbildning för nyanställda. Materialet sprids inte på ett effektivt sätt och därmed finns inte möjlighet att säkerställa att lagar och regelverk efterlevs.	3
10.3	Har ni en sekretess/integritetspolicy?	Kommunen har inte någon sekretess-/integritetspolicy.	1
10.4	Finns det krav på att anställda känner till, följer samt godkänner sekretesspolicyn? (svara detaljerat)	Nej, anställda förväntas att följa rådande lagar och regelverk.	1
10.5	Har ni en användarpolicy för email och internet?	"Så här gör vi i Nacka" sätter mål för informationssäkerhet, men detaljerar inte tydliga användarbeteende för email och internet.	2
10.6	Finns det en definierad process för identifiering av affärsprocesser som använder, samlar in, arkiverar, kasserar och inkluderar avslöjande av personlig information?	I nuläget saknas det en process, men arbete pågår med initiativ för att få detta på plats	1
10.7	Är dataskydd en del av riskbedömning och rapportering?	Pågående arbete kring affärsrisker samt rapportering, detta är inte slutfört men det finns en resurs med som bär ansvar och arbetar regelbundet med denna fråga.	4

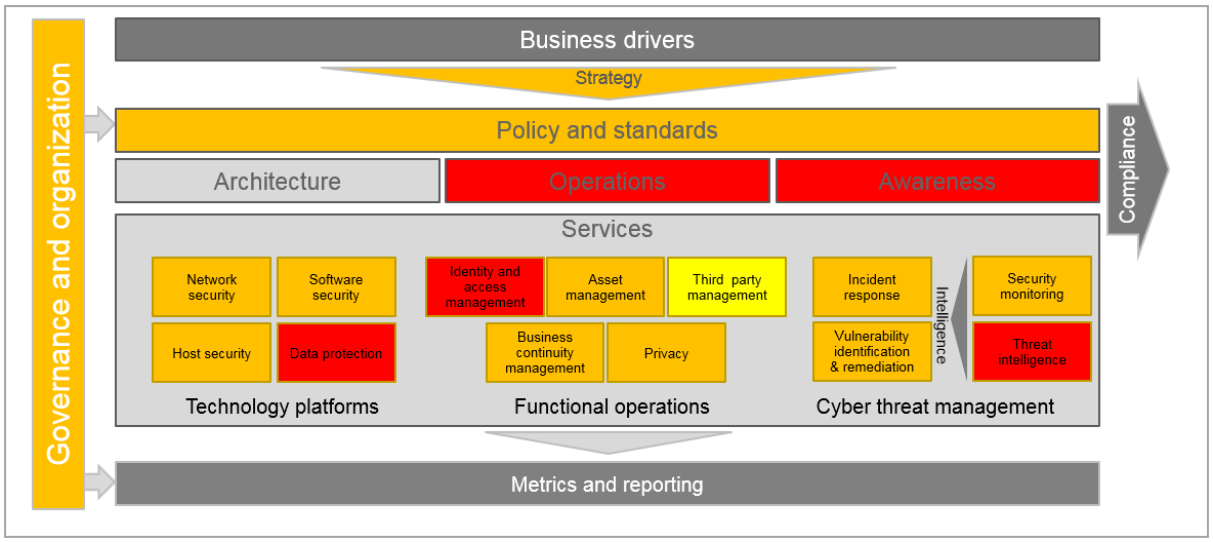
Granskningspunkt		Kommentar	Utvärdering
10.8	Utför er organisation Data Protection Impact Assessments (DPIA) för att bedöma risker för nya projekt eller system?	Avdelningarna genomför själva riskanalyser kring sina projekt och system.	4
10.9	Genomförs insatser för att kommunicera med dataobjekt (t.ex. anställda eller kommunmedborgare) kring hur personinformation används då den samlas in (t.ex. via utskick)?	Samtycke tas i samband med insamling av personuppgifter. Det har inte gjorts några dokumenterade analyser av om nuvarande rutiner är tillräckliga i förhållande till GDPR.	3
10.10	Har ni fastställda perioder för kvarhållandet av persondata? (om ja, vänligen svara detaljerat)	Ja, detta ingår allmänt när nämnderna antar dokumenthanteringsplaner där det framgår hur handlingar ska förvaras och när/om de ska gallras. Dock saknas det specifika regler för persondata.	3
10.11	Finns det riktlinjer eller förfaranden för radering av persondata? (Om ja, vänligen beskriv de processer som finns på plats för detta)	Det saknas ett centralt stöd för detta. Uppfyllnad av säkerhetskrav är upp till varje enskild systemägare.	2
10.12	Finns det processer för säkerställandet av dataobjekts rättigheter, t.ex. ämnesförfrågningar, rätten att modifiera data samt rätten att motsätta sig processandet av data?	Det saknas ett centralt stöd för detta, uppfyllnad av säkerhetskrav är upp till varje enskild systemägare.	2
10.13	Har era informationssystem tillräckliga revisions- och spårbarhetsfunktioner för att kunna producera detaljerad information, som även bör finnas tillgänglig på användares begäran, kring vilka källor som används samt användandet av deras personuppgifter?	Det saknas ett centralt stöd för detta, uppfyllnad av säkerhetskrav är upp till varje enskild systemägare. För system som bedöms som ha behov kan särskilda säkerhetsgranskningar göras.	2
10.14	Vilka kontroller finns för att autentisera användare som har åtkomst till system som används för att processa persondata (t.ex. tvåfaktorsautentisering)?	Varierar från system till system. De vanligaste lösningarna är SITHs kort samt Mobilt BankID.	4
10.15	Vilka lösenordskrav finns till de system som används för att processa persondata, inklusive: - minimumkrav på längd - komplexitet - tvingad återställning - låsning vid misslyckade inloggningsförsök - låsningsgräns - ålder på lösenord - inaktivitet - lösenordshistorik	Detta varierar beroende på system.	2
10.16	Hur skyddas den fysiska åtkomsten till persondata? (t.ex. punktskydd eller skalskydd för lokaler)	Detta varierar beroende på system.	2
10.17	Har ni en krypteringspolicy eller process?	Nej.	1
10.18	Har ni ett informationssäkerhetsteam?	Finns roller med informationssäkerhetsansvar men inte ett dedikerat team.	3
10.19	Tillhandahåller ni en lista med de legala krav kring dataskydd ni är skyldiga att följa?	Nej.	1
10.20	Är Datainspektionen informerade om persondata som processas?	Kommunen bibehåller ett register över vilka personuppgiftsbehandlingar de har. Uppgifter är klassificerat enligt typ av persondata, om data är känslig eller inte och enligt system.	5

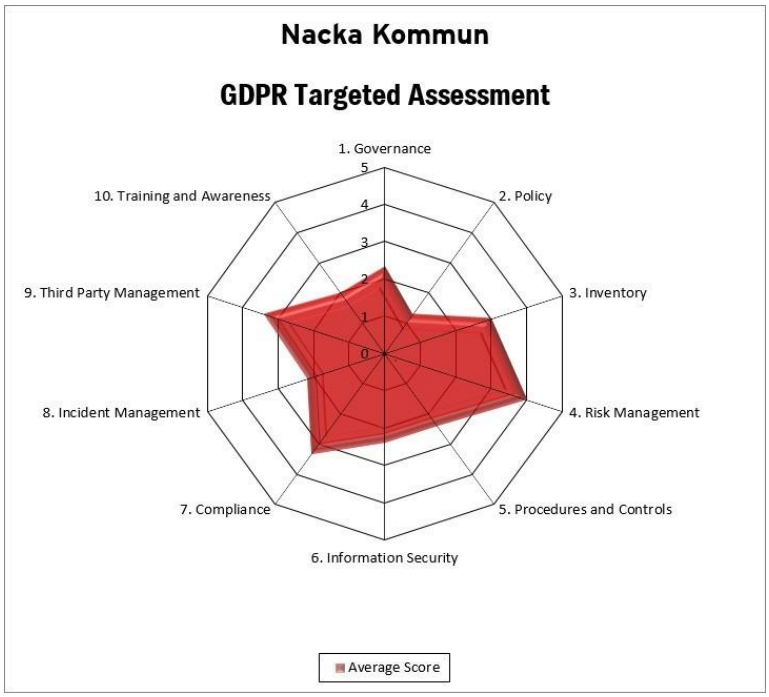
Granskningspunkt		Kommentar	Utvärdering
10.21	Har ni ett program för att säkerställa att ni följer policyer, regleringar och andra skyldigheter rörande användandet samt skyddandet av persondata?	Nej, men ett program är på ingång.	1
10.22	Har ni rapporterat några fall då ni inte efterlevt dataskyddslagstiftning till Datainspektionen under de senaste 12 månaderna?	Nej.	5
10.23	Har ni dokumenterat det juridiska underlaget för hantering av persondata?	Ja, detta dokumenteras för varje personuppgiftsbehandling.	5
10.24	Har ni en dokumenterad process för rapportering och respons till potentiella incidenter angående persondata? (detaljerat svar)	Nej, en sådan är planerad att tas fram under hösten 2017.	1
10.25	Har ni en responspolicy kring informationsbrister med utsedda ansvariga?	Nej.	1
10.26	Har några persondataincidenter inträffat under de senaste åren? (om ja, detaljerat svar)	Nej.	5
10.27	Vilka steg tas för säkerställandet av tredjeparters efterlevnad av lagar och regelverk för dataskydd?	Ingår personuppgiftsbiträdesavtal	3
10.28	Inkluderas dataskyddsklausuler i kontrakt med tredjeparter? (detaljerat svar)	I vissa fall vävs dataskydd in i tjänsteavtal, i andra fall förlitar man sig på bilagor till personuppgiftsbiträdes-avtalet	3
10.29	Hur genomförs den kontinuerliga bedömningen av tredjeparters efterlevnad av dataskyddslagsstiftning?	Genom personuppgiftsbiträdesavtal	3
10.30	Har ni granskat kontrakt med tredjeparter för att avgöra huruvida förändringar eller ytterligare avtal krävs för att efterleva de nya kraven för datahanteringsavtal?	Inventering pågår av olika personuppgiftsbehandlingar – inom denna inkluderas personuppgiftsbiträdesavtalen från ett GDPR perspektiv.	5
10.31	Finns det en specialiserad utbildning om personinformation?	Nej.	1
10.32	Hur säkerställs anställdas förståelse kring dataskyddsåtaganden?	Efter sommaren kommer informationsträffar att anordnas, personuppgiftsansvariga kommer att informeras och riktlinjer kommer att publiceras på hemsidan.	3
10.33	Hur kommuniceras åtaganden rörande dataskydd till nyanställda?	Det finns information tillgängligt passivt på deras hemsida samt eventuellt via utbildningar vid behov	2

3. Spindel diagram/nuvarande status ramverk dashboard

Följande diagram visar en sammanställning av de kontroller som genomförts under granskningen. Dessa kommer ifrån EY Cyber Program Assessment som är baserat på den svenska och internationella standarderna ISO/IEC 27000, COBiT and ITIL. Diagrammen är färgkodade enligt följande:

- Grön representerar kontroller som fungerar tillfredsställande
- Gul representerar kontroller som fungerar delvis
- Röd representerar kontroller som inte finns eller fungerar inte tillfredställande
- Grå representerar kontroller som inte är använda i denna granskning





4. Slutsatser och rekommendationer

4.1 Slutsatser

Av samtliga 63 granskningspunkter är fördelningen av bedömningarna följande:

Kontrollen finns och fungerar tillfredsställande:	21 %
Kontrollen finns och fungerar delvis:	35 %
Kontrollen finns ej eller fungerar ej tillfredsställande:	44 %
Ej tillämplig, kontrollen behövs ej av särskilda skäl:	0 %

Hur ändamålsenlig är IT-säkerheten för de behov kommunens verksamhet har?

Granskningen visar att Nacka kommun har goda förutsättningar för ett ändamålsenligt arbete med informationssäkerhet. Kommunen har interna resurser som är ansvariga och engagerade i frågorna och arbetar med att ta fram processor och ramverk som kan stödja den nya dataskyddslagstiftningen.

Dock saknas processer och rutiner i nuläget för att effektivt kunna arbeta med dessa frågor och för att säkerställa en tillräcklig intern kontroll inom området. Kommunens starka sidor finns inom områdena tredjepartsleverantör, personalresurser och förberedelse för implementation av GDPR. Förbättringsområden har identifierats främst inom information och utbildning, efterlevnad av styrdokument, rutiner för behörighetsadministration och hantering av telefonmeddelanden och sms.

Nedan har samtliga identifierade förbättringsområden och rekommendationer beskrivits.

4.2 Rekommendationer

Nedan följer våra rekommendationer samt vårt förslag på prioritering utifrån bedömd risk och väsentlighet. Rekommendationerna är prioriterade enligt följande:

Hög	Observation av kritisk karaktär som kan riskera kommunens möjlighet att driva verksamhet eller leda till materiella förluster för kommunen. Observation som graderas som "hög" bör omedelbart åtgärdas.
Medel	Observation som anses kunna ha påverkan på verksamhetens mål, rykte, finansiell information, materiella tillgångar och/eller möjlighet att efterleva lagar och regelverk samt interna policys och riktlinjer. Observationen skulle kunna leda till ineffektivt nyttjande av kommunens resurser. Bristen bör åtgärdas för att säkerställa god intern kontroll på lång sikt.
Låg	Observation som ej direkt påverkar verksamhetens mål, men kan medföra ineffektiv verksamhet, mindre fel i information, mindre brister i efterlevnad av interna policys och riktlinjer eller avvikande från god praxis.

	Iakttagelse och rekommendationer	Prioritet
1.	**Kommunen saknar standardiserade och definierade rutiner och processer kring informationssäkerhet samt styrning kring dessa** Organisationen har endast en övergripande målbild definierad. Det saknas användaravtal och styrdokument för e-mail, sms, telefon, behörigheter samt incidenthantering. **Risk** Finns ingen enhetlig process kring informationssäkerhet vilket gör att ansatserna inom verksamheten ser väldigt olika ut och ger inte en övergripande strukturerad säkerhetsbild. **Rekommendation** Trots organisationens decentralisering behövs centrala riktlinjer kring IT- och informationssäkerhet för att säkerställa en enhetlig säkerhetsbild.	Hög
2.	**Kommunen har inte uppdaterat sin IT- och informationssäkerhetspolicy** Policyn förförfattades för ca 3 år sedan och har inte uppdaterats sedan dess. **Risk** Policyn täcker inte viktiga områden eller är anpassad till organisations och omvärldens förändra omständigheter. **Rekommendation** Uppdatera policyn kontinuerligt så den reflekterarar organisations nuvarande behov.	Hög
3.	**Kommunen genomför inga utbildningsinsatser inom IT- och informationssäkerhet** Det saknas ett strukturerat och gediget utbildningsprogram inom organisationen för att säkerställ adekvat kunskapsnivå. **Risk** Utan utbildning saknas en medvetenhet kring säkerhetsfrågor vilka kan utsätta organisation för flertalet risker. **Rekommendation** Det rekommenderas att kommunen startat ett utbildningsinitiativ för att öka medvetenheten samt kunskapsnivåerna för att på så sätt minska risken för informationssäkerhetsbrister	Hög
4.	**Kommunen saknar tillräckliga rutiner och processer kring informationssäkerhet, samt en gedigen incidentshanteringsplan.** Kommunens processer och rutiner för säkerhetsriskhantering, incidenter och eskalering av dessa är relativt okänd inom den vidare organisationen. De saknas en lämplig disseminering av dessa inom den vidare organisationen. Incidentshanteringsplanen är inte anpassad för informationssäkerhet utan är av en generell karaktär. **Risk** Vid eventuella bister eller incidenter rörande informationssäkerhet kan inte personal rapportera och påbörja åtgärder som processen föreskriver. **Rekommendation** Kommunen rekommenderas att skapa rutiner och processer för hantering av informationssäkerhet och incidenter samt säkerställa dess spridning inom organisationen, speciellt då de relevanta verksamhetsrollerna. Efter granskningen påbörjades och intervjuer genomfördes har ett styrdokument tagits fram, nämligen "Samverkansmodell Nacka v0.04" som inte verkar ha beslutas av kommunstyrelsen men som är ett första steg mot tillräckliga rutiner och processer kring informationssäkerhet.	Hög
5.	**Kommunen saknar centrala befattningar som innehar en överblick kring informationssäkerhetsarbete** Kommunen har i nuläget roller med ansvar inom informationssäkerhet, dock är dessa spridda i organisationen. Det saknas en dedikerad avdelning eller grupp som äger dessa frågar och driver de fullt ut – med t.ex. kompletta rutinbeskrivningar samt etablering av behörighetsadministrationsprocesser. **Risk** Utan en dedikerad grupp saknas medarbetare som innehar en komplett bild av kommunens informationssäkerhet. Risken finns att rutiner och processer är inkompletta och orsaker brister i säkerheten. **Rekommendation** Skapa en grupp eller avdelning som fullt ut äger informationssäkerheten och ansvarar för att organisationen följer de riktlinjer och policyer som etableras.	Medel

	Iakttagelse och rekommendationer	Prioritet
6.	**Kommunen genomför inte några penetrationstester utan förlitar sig helt på tredjepartsleverantörer och verksamhetsenheter inom den decentraliserade organisationen** Penetrationstester syftar till att identifiera tekniska sårbarheter som kan vara blottade för en eventuell angripare. Kommunen genomför i dagsläget inga externa penetrationstester, dvs. tester utifrån ett externt angreppsutfall, och inga interna penetrationstester, dvs. tester utifrån ett insiderperspektiv **Risk** Avsaknaden av penetrationstester medför risker för brister inom informationssäkerheten. Att förlita sig på tredjepartsleverantörer utan att granska deras avtalsuppfyllnad öppnar även det för risker inom informationssäkerheten. **Rekommendation** Kommunen har till stor del sin IT-verksamhet outsourcad. De Kommunen förlitar sig helt på att leverantörerna håller sin del av avtalet och genomför inte själva några säkerhetstester för att identifiera sårbarheter. Samtidigt kunde inte kommunen ta fram något bevis om granskning eller uppföljning av leverantörerna. Det rekommenderas att granskning efterlevnad av avtal görs.	Medel
7.	**Kommunens förberedelse inför GDPR 2018 har påbörjats och bedöms som adekvat. Det finns goda förutsättningar för att kunna implementera ändamålsenliga förändring.** Överlag bedöms förberedelsearbetet för GDPR har startats på ett ändamålsenligt sätt. Dock kvarstår en hel del arbete för att säkerställa att regelverket efterlevs när lagen träder i kraft. Bland annat behöver kommunen identifiera vilka system som omfattas, utarbeta en GAP-analys samt vidta åtgärder för att överbrygga de gap som identifieras. **Risk** Utan ökade resurser och central styrning av övergångsarbetet finns det en risk att organisationen inte fullt ut kommer efterleva nya regelverket när lagen träder i kraft. **Rekommendation** Kommunen rekommenderas att investera mer i arbetet med GDPR för att säkerställa full efterlevnad av det nya regelverket. Specifikt ses initiativ inom utbildning, riktlinjer och processer som områden med behov av mer resurser och medvetenhet.	Medel
8.	**Det saknas en standardiserad avtalsmodell vilket gör att kraven på tredjepartsleverantörer varierar mellan olika enheter och system inom verksamheten** Kommunen upphandlar IT-tjänster inom olika delar av organisationen med varierande resultat. Avtal styrda centralt är generellt av högre kvalitet och möte organisationens behov bättre. Centrala avtal är också i större grad uppföljda jämfört med avtal upphandlade ute i verksamheten. **Risk** Den varierande kvaliteten i upphandadlade avtal medför en risk för verksamheten då dessa förlitar sig på tjänster som inte möter organisationens behov fullt ut. **Rekommendation** Det rekommenderas att verksamheten inom kommunen arbetar med den centrala enheten för att säkerställa avtal av hög kvalitet och anpassning till organisationens behov.	Låg

5. Källförteckning

5.1 Kommungemensamma dokument

- Informationssäkerhetspolicy för Nacka kommun
- Så här gör vi i Nacka
- EY GDPR Targeted Assessment
- Efter att granskningen påbörjades och intervjuer genomfördes har följande dokument tagits fram: Samverkansmodell Nacka v.04 där det inte framgår vilken beslutsnivå som har beslutat om dokumenten