Revisorerna

2020-03-31

Nyköping

Kommunstyrelsen

För kännedom:
Kommunfullmäktige

Granskning av informationssäkerhet och GDPR

PwC har på uppdrag av de förtroendevalda revisorerna i Nyköpings kommun granskat kommunens arbete med informationssäkerhet och GDPR. Granskningens syfte har varit att bedöma om kommunstyrelsen säkerställer ett ändamålsenligt informationssäkerhetsarbete och om detta sker med tillräcklig intern kontroll.

Efter genomförd granskning bedömer vi det mycket allvarligt att kommunstyrelsen **inte** säkerhetsställer en ändamålsenlig informationssäkerhet och att det saknas tillräcklig intern kontroll. Bedömningen baseras på kontrollmålen för granskningen som redovisas i revisionsrapporten.

Efter genomförd granskning lämnas följande rekommendationer:

- Dokumentera huvudsakliga informationssäkerhetsprocesser. Säkerställ och tydliggör roller, ansvar och mandat.
- Säkerställ att samtlig dokumentation är uppdaterad och aktuell.
- Implementera ett ledningssystem för informationssäkerhet.
- Säkerställ att utbildningar och övningar för att utveckla och säkerställa kompetens om informationssäkerhet genomförs regelbundet.
- Minska personberoendet för att säkerställa att verksamheter kan fortlöpa vid ett eventuellt personalbortfall.
- Genomför informationsklassning från ett informationsperspektiv istället för systemperspektiv.
- Identifiera och definiera mätbara mål samt tilldela ansvar för samtliga mål i *Planering för informationssäkerhetsarbetet Nyköpings kommun 2019* i syfte att följa upp dessa kontinuerligt.
- Kommunstyrelsen bör säkerställa att det finns en baslinje för säkerhetsinställningar samt att det kommer att implementeras på relevanta servrar inom domänen.

- Kommunstyrelsen bör genomföra en granskning av de konton vars lösenord aldrig går ut, för att utvärdera om andra konton än systemkonton har "lösenord aldrig går ut" aktiverat.

- En utvärdering av de användarkonton i AD:t som aldrig använts bör genomföras för att undersöka nödvändigheten av dessa.

- Kommunstyrelsen bör undersöka om processen för att granska inaktiverade nätverksanvändare i tid måste förbättras. Vid granskningen gjorda iakttagelser redovisas i bilagd rapport, som härmed översänds för yttrande och åtgärder.

Skriftligt svar önskas senast 2020-08-15

REVISORERNA

Anne-Marie Wigertz
Ordförande

Gunnar Johansson
Vice ordförande

1.1

Granskning av informationssäkerhet och GDPR

Nyköpings kommun

Mars 2020

Fredrika Jönander
Tua Lennartsson
Malin Lindvall

pwc

Revisionsrapport

Innehållsförteckning

Sammanfattning

PwC har på uppdrag av de förtroendevalda revisorerna i Nyköpings kommun granskat kommunens arbete med informationssäkerhet och GDPR. Granskningens syfte har varit att bedöma om kommunstyrelsen säkerställer ett ändamålsenligt informationssäkerhetsarbete och om detta sker med tillräcklig intern kontroll.

Efter genomförd granskning bedömer vi att kommunstyrelsen **inte** säkerhetsställer ett ändamålsenligt informationssäkerhet och att det saknas tillräcklig intern kontroll.

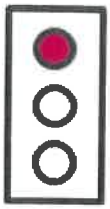
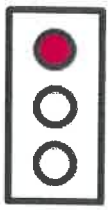
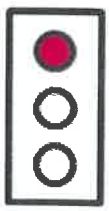
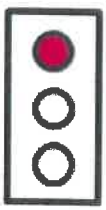
Efter genomförd granskning kan vi konstatera att det finns en begränsad organisation kopplat till GDPR, men att denna behöver tydliggöras och att roller och ansvar behöver dokumenteras och säkerställas. Organisationen för GDPR innehar även inslag av personberoende. Det saknas i dagsläget en utarbetad organisation när det gäller informationssäkerhetsområdet. Det finns till viss del styrande dokument inom granskningsområdet, dock är dokumenten i behov av översyn och revidering. Det finns även ett större personberoende kopplat till informationsäkerhetsorganisationen och inslag av begränsningar i form av resurser och direktiv. Kommunen saknar väsentlig formell dokumentation för att styra sitt arbete inom informationssäkerhet och GDPR på en strategisk nivå. Det saknas även ett ledningssystem för informationssäkerhet inom kommunen, vilket resulterar i ett bristande systematiskt informationssäkerhetsarbete.

Det kan konstateras att det genomförs arbetsinsatser inom både IT- och informationssäkerhet samt GDPR. Granskningen har däremot påvisat en bristande överblick och att ett helhetsperspektiv gällande informationssäkerhet uteblir. Givet att kommunstyrelsen hittills inte regelbundet och med systematik efterfrågat någon form av återrapportering inom granskningsområdet innebär detta att inte heller kommunstyrelsen kan sägas besitta den helhetsbild som krävs för att styra, leda eller ge direktiv gällande informationssäkerhetsarbetet. Vi kan konstatera att det genomförs punktinsatser kopplat till säkerhetskulturen inom kommunen, men att det saknas ett strukturellt och systematiserat kommunövergripande arbete. Vi bedömer att det är av central vikt att det genomförs kontinuerliga utbildnings- och informationsinsatser för att medarbetarna ska påminnas om vikten av en god säkerhetskultur och informationssäkerhet.

Gällande Nyköpings kommuns Active Directory (AD) kan det noteras att vissa säkerhetsinställningar, främst relaterade till lösenordsinställningar, bör utvärderas. Sammantaget är säkerhetsinställningarna på analyserade servrar bra. Vissa områden är dock i behov av förbättringar, främst vad gäller inställningar för lösenordsparametrar. Efter genomförd analys av konton i AD indikeras att ett antal konton bör utvärderas. Vidare tyder resultaten på att rutiner för användaradministration kan behöva revideras.

Vår bedömning baseras på granskningens åtta revisionsfrågor som presenteras nedan:

Revisionsfråga	Kommentar	
Det finns en tydlig organisation, roll- och ansvarsfördelning kopplat till informationssäkerhet respektive GDPR?	**Delvis uppfyllt** Det finns organisationer för både informationssäkerhet och GDPR, dessa är dock begränsade och präglas av brist på resurser och ett tydligt personberoende. Det saknas en tydlig roll- och ansvarsfördelning kopplat till kravställan.	
Finns styrande informationssäkerhets-dokument och riktlinjer som är implementerade i verksamheten (inkl. GDPR)?	**Delvis uppfyllt** Det finns styrande dokument, dock är dessa i behov av översyn och revidering. Det saknas tilldelat ansvar för revidering och det saknas en tydlig dokumentationshierarki.	
Finns ett ledningssystem för informationssäkerhet?	**Ej uppfyllt** Nyköpings kommun saknar ett ledningssystem för informationssäkerhet. Det har inte fattats beslut om implementering och det ingår inte i den närtida planeringen.	
Arbetar informationssäkerhets-organisationen respektive GDPR-organisationen aktivt med efterlevnad av informationssäkerheten?	**Delvis uppfyllt** Det genomförs arbetsinsatser inom både IT- och informationssäkerhet samt GDPR. Det saknas dock både systematik och aktiv efterlevnad i full utsträckning.	

Finns ett aktivt arbete för att främja en god säkerhetskultur inom informationssäkerhets-området?	**Ej uppfyllt** Det genomförs punktinsatser kopplat till säkerhetskultur gällande informationssäkerhet och GDPR, men det saknas ett strukturellt och systematiserat kommunövergripande arbete. Utbildningar sker sällan och endast till delar av de anställda.	
Utförs kontinuerligt stickprov på behörigheterna i behörighetssystemet?	**Ej uppfyllt** Nyköpings kommun genomför inte stickprov på behörigheterna i behörighetssystemet.	
Finns en god kontohantering implementerad?	**Ej uppfyllt** Det saknas inställningar för lösenordsparametrar, en mängd användarkonton har aldrig använts, det finns en stor mängd konton med administrativa konton varav flertalet med inställningen att lösenorden aldrig går ut.	
Finns det en rutin för att kontinuerligt revidera användarkonton och efterlevs rutinen?	**Ej uppfyllt** Det saknas kontinuerlig revidering av användarkonton i behörighetssystemet. Behörigheter revideras endast vid slumpmässiga upptäckanden av felaktigheter.	

Rekommendationer

Efter genomförd granskning lämnas följande rekommendationer:

- Dokumentera huvudsakliga informationssäkerhetsprocesser. Säkerställ och tydliggör roller, ansvar och mandat.
- Säkerställ att samtlig dokumentation är uppdaterad och aktuell.
- Implementera ett ledningssystem för informationssäkerhet.
- Säkerställ att utbildningar och övningar för att utveckla och säkerställa kompetens om informationssäkerhet genomförs regelbundet.
- Minska personberoendet för att säkerställa att verksamheter kan fortlöpa vid ett eventuellt personalbortfall.
- Genomför informationsklassning från ett informationsperspektiv istället för systemperspektiv.
- Identifiera och definiera mätbara mål samt tilldela ansvar för samtliga mål i *Planering för informationssäkerhetsarbetet Nyköpings kommun 2019* i syfte att följa upp dessa kontinuerligt.
- Kommunstyrelsen bör säkerställa att det finns en baslinje för säkerhetsinställningar samt att det kommer att implementeras på relevanta servrar inom domänen.
- Kommunstyrelsen bör genomföra en granskning av de konton vars lösenord aldrig går ut, för att utvärdera om andra konton än systemkonton har "lösenord aldrig går ut" aktiverat.
- En utvärdering av de användarkonton i AD:t som aldrig använts bör genomföras för att undersöka nödvändigheten av dessa.
- Kommunstyrelsen bör undersöka om processen för att granska inaktiverade nätverksanvändare i tid måste förbättras.

Inledning

1.1 Bakgrund

Kommuner och regioner har ett av de svenska samhällets mest komplexa uppdrag. Detta då en stor del av den samhällsviktiga verksamheten räknas till deras ansvarsområde. Förtroende för en organisation tar lång tid att bygga upp, men kan snabbt raseras av en enskild säkerhetsincident. Med dagens snabba digitalisering blir informationssäkerhet allt viktigare. Klassning av informationstillgångar är viktigt för att säkerställa att den mest skyddsvärda informationen verkligen får det skydd som krävs.

Det övergripande syftet med informationssäkerhet är att säkerställa att information för medarbetare, medborgare och andra intressenter hanteras med utgångspunkt i tillgänglighet, riktighet och konfidentialitet.

Information är värdefull och behöver många gånger skyddas. Ett proaktivt informationssäkerhetsarbete är en förutsättning för en effektiv och korrekt informationshantering. Vilket i sin tur skapar förtroende både inom och utanför organisationen.

Revisorerna har i sin riskanalys för 2019 bedömt att det finns en risk att kommunstyrelsen inte har säkerställt att det finns en god informationssäkerhet inom kommunen och har därför gett PwC ett uppdrag att granska området.

1.2 Syfte och revisionsfrågor

Granskningens syfte är att bedöma om kommunstyrelsen säkerställer ett ändamålsenligt informationssäkerhetsarbete och om detta sker med tillräcklig intern kontroll.

För att kunna bedöma detta består granskningen av följande revisionsfrågor:

- Det finns en tydlig organisation, roll- och ansvarsfördelning kopplat till informationssäkerhet respektive GDPR?
- Finns styrande informationssäkerhetsdokument och riktlinjer som är implementerade i verksamheten (inkl. GDPR)?
- Finns ett ledningssystem för informationssäkerhet?
- Arbetar informationssäkerhetsorganisationen respektive GDPR-organisationen aktivt med efterlevnad av informationssäkerheten?
- Finns ett aktivt arbete för att främja en god säkerhetskultur inom informationssäkerhetsområdet?
- Utförs kontinuerligt stickprov på behörigheterna i behörighetssystemet?
- Finns en god kontohantering implementerad?
- Finns det en rutin för att kontinuerligt revidera användarkonton och efterlevs rutinen?

1.3 Revisionskriterier

- Kommunallagen
- IT-styrdokument
- Informationssäkerhetsdokumentation
- Kontoinformation från Active Directory

1.5 Avgränsning

I tid avgränsas granskningen till år 2019 och 2020 samt till granskningens revisionsfrågor. Den tekniska delen av granskningen avgränsas till en domänkontrollant samt valfri annan server. Granskad nämnd är kommunstyrelsen.

1.6 Metod

Granskningen har genomförts med hjälp av intervjuer med nyckelpersoner inom kommunen samt inläsning och genomgång av tillgänglig dokumentation.

Den tekniska delen genomförs med hjälp av "Baseline Security Assessment", vilket innebär en genomgång av systemuppsättning genom utläsning och analys av kontoinformation i Active Directory.

Intervjuer har genomförts med följande:

- Enhetschef IFO
- Handläggare IFO
- IT-chef
- Chef informationsförvaltningen
- Systemförvaltningssamordnare
- Dataskyddsombud och informationssäkerhetssamordnare

Samtliga intervjuade har erbjudits möjlighet att sakgranska ett utkast av rapporten.

2. Iakttagelser och bedömningar

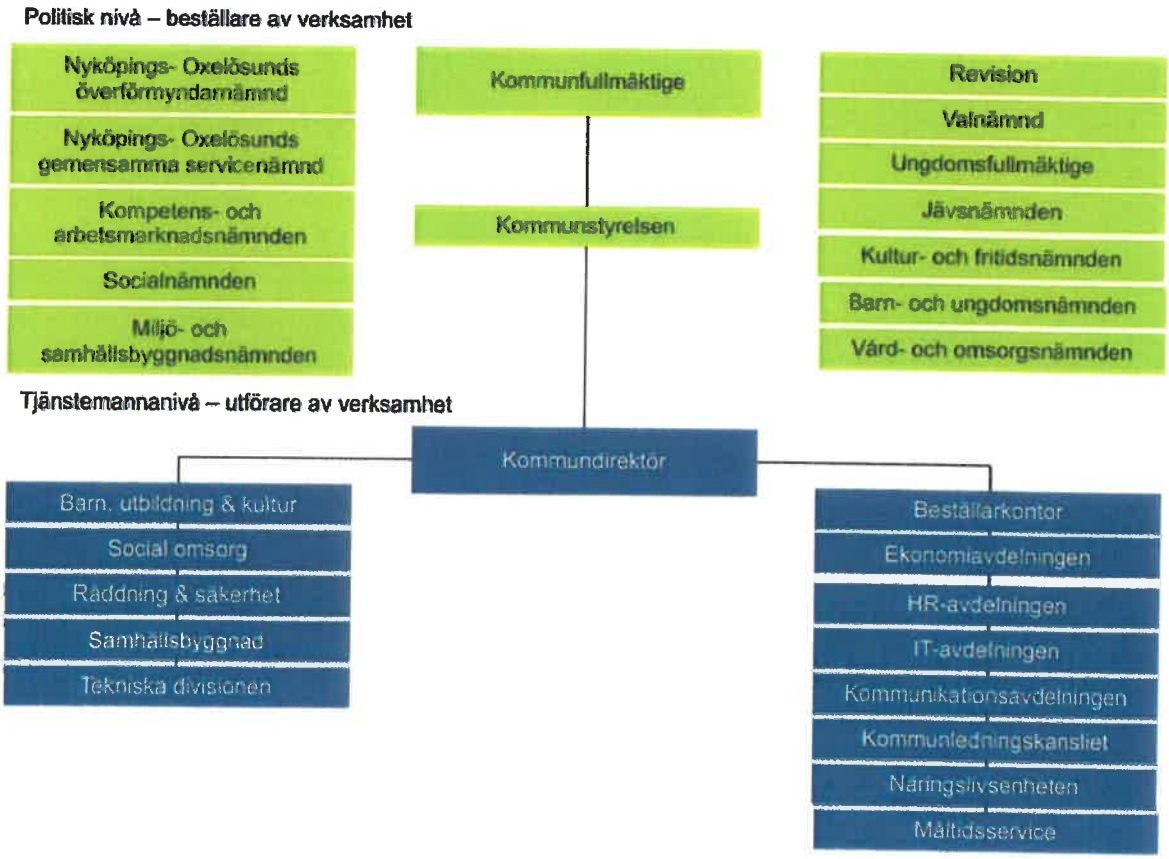
2.1 Tydlig organisation och roll och ansvarsfördelning (T)

Revisionsfråga 1: Det finns en tydlig organisation, roll- och ansvarsfördelning kopplat till informationssäkerhet respektive GDPR?

2.1.1 Iakttagelser

Nyköpings kommun har valt att organisera de säkerhetsaspekterna IT-säkerhet och informationssäkerhet hos olika enheter. Det är Informationsförvaltningen som samordnar arbetet med informationssäkerhet och avdelningen befinner sig organisatoriskt under kommunledningskansliet. Informationsförvaltningen tillkom under år 2019, och är således en relativt ny förvaltning inom kommunen. IT-säkerhetsfrågor hanteras av IT-avdelningen. Se nedan för ett organisationsschema över kommunen.

Bild 1. Organisationsschema över Nyköpings kommun



Inom Informationsförvaltningen återfinns kommunens informationssäkerhetssamordnare och dataskyddsombud (DSO). Det är samma tjänsteperson som innehar de två rollerna, vilket vid intervjuer framkommer som något problematiskt då det krävs både mer tid och resurser för att bedriva ett ändamålsenligt arbete inom de två områdena. Under de

senaste åren har även ett stort fokus varit på arbetet inför ikraftträdandet av GDPR, vilket har påverkat informationssäkerhetsarbetet. Det framgår att det inom informationsförvaltningen finns backup om dataskyddsombudet skulle vara frånvarande och det inkommer frågor eller rapportering om avvikelser/incidenter.

Nyköpings kommuns *Policy för IT-säkerhet i Nyköpings kommun,* vilken även innehåller kommunens *Policy för informationssäkerhet,* beslutades av fullmäktige år 2009 och har inte reviderats sedan dess. Av denna framgår att det är kommundirektören som har det övergripande ansvaret när det gäller verksamheternas tillämpning av policyn. Det anges även att kommundirektören ansvarar för samordning av arbetet med informationssäkerhet. Av intervjuer framkommer att denna roll- och ansvarsfördelning inte längre är aktuell, detta eftersom det i dagsläget finns en informationssäkerhetssamordnare inom kommunen som bland annat ansvarar för samordningen inom området. Informationssäkerhetssamordnaren ansvarar dock inte för kommunens informationssäkerhet och det finns en osäkerhet kring vem som har det yttersta ansvaret i dagsläget.

Kopplat till IT-policyn finns även *Riktlinjer för IT-resurser inom Nyköpings kommun.* Det framgår inte av riktlinjen huruvida den är politiskt fastställd. Dokumentet beskriver de riktlinjer som gäller för hantering av digital information och informationsbärare. Av dokumentet framgår även vilken ansvarsfördelning som råder när det gäller de olika områdena.

Vid intervjuer framkommer att det finns en tydlighet kring vem som ska kontaktas vid frågor gällande informationssäkerhet och GDPR. Det finns däremot inte någon tydlig roll- och ansvarsbeskrivning i kommunens dokumentation, vilket är något som betonas som bristfälligt. När det gäller GDPR-frågor så finns det i samtliga verksamheter en eller flera personuppgiftskoordinatorer som ska fungera som stöd till dataskyddsombudet och verksamheterna i det dagliga arbetet. Personuppgiftskoordinatorerna syftar till att fungera som stöd och extrakompetens när det gäller frågor kopplat till GDPR och hantering av personuppgifter. Vid intervjuer uppges dock att det finns en otydlighet kopplat till rollen som personuppgiftskoordinator, då det varken finns en tydlig rollbeskrivning eller kontinuerliga utbildningsinsatser. Denna typ av organisation, med representanter inom samtliga verksamhetsområden, finns inte inom informationssäkerhet, något som uppges vara en brist.

För att ytterligare tydliggöra och förenkla processerna vid händelse av incidenter så finns ett påbörjat arbete med att skapa en gemensam incident-funktionsbrevlåda för säkerhetsincidenter. Syftet med detta arbete är att få en bättre bild av hotbilden mot Nyköpings kommun samt en överblick över säkerhetsläget i kommunen. Det framkommer att det i dagsläget ofta finns svårigheter för medarbetare att veta vem som ska kontaktas vid olika typer av incidenter och att en gemensam funktionsbrevlåda skulle kunna förenkla processen samt säkerställa att inte något ärende faller mellan stolarna. Det påtalas att informationssäkerhetsarbetet i kommunen till viss del är fragmenterat och att det därmed finns svårigheter att skapa en helhetsbild. Detta är således ett område med förbättringspotential. Det sker samverkan mellan

informationsförvaltningen och IT-avdelningen samt mellan informationsförvaltningen och säkerhetsavdelningen men det uppges däremot saknas formella nätverk.

Vid intervju med representanter från IT-avdelningen framkommer att det anses finnas en problematik kopplat till kravställan och att IT-avdelningen, som hanterar IT-säkerhet, både behöver kravställa och utföra arbetet. Det uppges finnas en önskan om att informationsförvaltningen framgent kommer vara kravställare, men att organisationen i dagsläget inte fungerar så. Det upplevs även saknas en kravställan på IT-säkerhetsfrågor från kommunstyrelsen samt att styrelsen skulle behöva vara tydligare när det gäller vilka ambitioner som finns kopplat till informationssäkerhet och GDPR.

2.1.2 Bedömning

Vi bedömer att revisionsfrågan utifrån iakttagelser från dokumentationsgranskning och intervjuer **delvis är uppfylld**.

Det finns en organisation kopplat till GDPR, med dataskyddsombud och personuppgifts-koordinatorer, dock behöver detta tydliggöras och roller och ansvar behöver dokumenteras och säkerställas. Inom informationssäkerhetsområdet finns det inte någon liknande utarbetad organisation. Med anledning av att det saknas en tydlig och dokumenterad organisation så leder detta till ett stort personberoende inom arbetet, vilket i sin tur genererar en sårbarhet.

Det kan konstateras att det krävs en översyn av kommunens styrdokument, särskilt finns ett behov en aktualisering av *IT-policy* och *Riktlinjer för IT-resurser*. Vid intervjuer, och dokumentationsgenomgång, framkommer att kommunens dokumentation avseende informationssäkerhet är i behov av aktualisering och revidering. Vid en översyn finns även behov av att tydliggöra roller och ansvar kopplat till både informationssäkerhet och GDPR.

Vidare finns det en otydlig roll- och ansvarsfördelning kopplat till kravställan och att det finns behov av att tydliggöra detta. Att IT-avdelningen både kravställer och utför bedöms problematiskt.

2.2. Implementerade styrdokument (T)

Revisionsfråga 2: Finns styrande informationssäkerhetsdokument och riktlinjer som är implementerade i verksamheten (inkl. GDPR)?

2.2 1 Iakttagelser

Vid intervjuer framgår att det, till viss del, finns styrdokument kopplat till informationssäkerhet och GDPR. Det framkommer även att dessa finns på kommunens intranät, vilket således innebär att de är tillgängliga för samtliga medarbetare. Dokumenten uppges vara en del av introduktionen av nyanställda men huruvida medarbetarna faktiskt har läst dokumenten, och har tagit till sig kunskapen, är ingenting

som kontrolleras. Detta är något som betonas som problematiskt i de fall en incident, inom informationssäkerhet eller GDPR, skulle ske.

De styrdokument som vi, inom ramen för denna granskning, har tagit del av är följande:

- Policy för IT-säkerhet i Nyköpings kommun (Kommunstyrelsen, 2009-06-23)
- Riktlinjer för IT-resurser inom Nyköpings kommun (dokumentet är inte daterat och det framgår inte vilken instans som antagit dokumentet)
- Rutin för hantering av personuppgifter i Nyköpings kommun (fastställd av projektbeställare 2018-05-11, giltig fr.o.m. 2018-05-11)
- E-strategi för Nyköpings kommun (KF 2016-11-08)
- Handlingsplan för digitalisering i Nyköpings kommun 2019-2020 (KS 2019-04-29)
- Planering för informationssäkerhetsarbetet Nyköpings kommun 2019 (ej beslutad)

Enligt kommunens dokumenthierarki krävs en policy för att kunna ta fram underliggande dokumentation, såsom riktlinjer och rutiner. Det framkommer att det saknas en implementerad struktur för hur och när kommunens styrdokument ska revideras, men att det oftast är den person som arbetat fram dokumentet som också bär ansvaret för revideringen. Det framkommer dock att det däremot finns riktlinjer rörande styrdokument och när dessa ska revideras.

Under 2020 kommer Sörmlandskustens räddningstjänst arbeta med att ta fram ett nytt handlingsprogram för Nyköpings kommun. Det nya handlingsprogrammet kommer gälla från januari 2021. I dagsläget inkluderas inte informationssäkerhet i kommunens handlingsprogram och det framkommer i intervjuer att det finns en önskan om att få med informationssäkerhet i det nya handlingsprogrammet.

Vid intervju med representanter från informationsförvaltningen framkommer att den informationsklassning som sker i KLASSA, görs utifrån systemnivå. Den utgår således inte från verksamhetsprocesser. Mer om detta anges i avsnitt 2.4.1.

Kommunens dokumenthanteringsplaner har ett större fokus på verksamhetsprocesser och det framgår att alla dokumenthanteringsplaner framgent ska innehålla information om känsliga personuppgifter och sekretess. Det finns även funderingar på huruvida planerna ska döpas om till informationshanteringsplaner för att få en tydligare informationskoppling.

2.2.2 Bedömning

Vi bedömer att revisionsfrågan utifrån iakttagelser från dokumentationsgranskning och intervjuer **delvis är uppfylld**.

Det finns styrande dokument, dock är dessa i behov av översyn och revidering. Att IT-policyn är från 2009 och inte uppdaterats sedan dess anser vi vara otillfredsställande. Det kan konstateras att det saknas ett tilldelat ansvar för revidering samt att det saknas ett tydligt ägarskap för de styrdokument som finns. Nyköpings kommun har ändamålsenlig dokumentation inom vissa områden, men det saknas processer för regelbunden revision och uppdatering av dessa. Den nuvarande dokumentationen

konstateras inte fungera ändamålsenligt till följd av brist på dokument. Kommunen saknar således väsentlig formell dokumentation för att styra sitt arbete kopplat till informationssäkerhet och GDPR på en strategisk nivå som förankrar arbetet med kommunens centrala roll som leverantör av samhällsviktiga tjänster.

Nedan bild visar en vanligt förekommande struktur på dokumentationshierarki inom ett ledningssystem för informationssäkerhet, motsvarande hierarki saknas i Nyköpings kommun.

Bild 1: Exempel på dokumentationshierarki inom ett ledningssystem för informationssäkerhet

Det kan vidare konstateras att Nyköpings kommun inte arbetar aktivt med rutiner och processer med syfte att fortsätta utveckla och stärka processen med arbetet kring efterlevnad av informationssäkerhet. Ett sådant arbete skulle inkludera regelbunden revision och uppdatering av styrande dokument.

Bedömningen är sammanfattningsvis således grundad i avsaknaden av regelbunden revision, granskning och uppdatering av samtlig dokumentation, iakttagelsen att vissa processer saknar dokumentation, samt i iakttagelsen att det saknas ett strukturerat ledningsarbete som samordnar samtlig väsentlig dokumentation.

2.3 Ledningssystem för informationssäkerhet (F)

Revisionsfråga 3: Finns ett ledningssystem för informationssäkerhet?

2.3.1 Iakttagelser

Nyköpings kommun har inte implementerat ett ledningssystem för informationssäkerhet. Det framkommer under intervjuer att det efterfrågats av flertalet funktioner under en längre tidsperiod. Det har inte heller fattats något beslut hos kommunstyrelsen gällande implementerandet av ett ledningssystem för informationssäkerhet och det är inte heller planerat i framtagen budget.

I dokumentet *Planering för informationssäkerhetsarbetet i Nyköpings kommun 2019* konstateras det övergripande målet och den övergripande visionen vara "information

som hanteras av Nyköpings kommun ska skyddas på rätt sätt och efter behov". Det ska enligt dokumentet uppnås genom att systematiskt arbeta med informationssäkerhet. Det framkommer även att Nyköpings kommun ska använda MSB:s metodstöd för systematiskt informationssäkerhetsarbete som ett medel för att nå det övergripande målet. Metodstödet bygger på standarden SS-EN ISO/IEC 27001 Ledningssystem för informationssäkerhet. Det framkommer under intervjuer att delar av MSB:s metodstöd samt rekommendationer har vidtagits och implementerats, dock inte i den utsträckning att det är heltäckande. Det saknas även medvetenhet hos flertalet intervjuade kring nämnda metod för att nå det övergripande målet. Utöver ovan nämnda förekommer inte implementeringen av ett ledningssystem i någon planering för Nyköpings kommun i närtid.

2.3.2 Bedömning

Vi bedömer att revisionsfrågan utifrån iakttagelser från dokumentationsgranskning och intervjuer **ej är uppfylld**.

Nyköpings kommun saknar ett ledningssystem för informationssäkerhet med tillhörande organisatorisk struktur och dokumentation. Det kan för Nyköpings kommun konstateras att det inte finns ett etablerat mottagande för ett ledningssystem för informationssäkerhet. Givet den nuvarande organisationen, roller och resurser är mottagandet av ett till fullo implementerat ledningssystem för informationssäkerhet eventuellt inte möjligt då det saknas mottagande struktur på plats som kan möjliggöra en ändamålsenlig implementering av ett ledningssystem.

Inom ett ledningssystem för informationssäkerhet bör den strategiska inriktningen för ett informationssäkerhetsarbete fastställas av en strategi och policy. En sådan strategi eller policy för informationssäkerhet bör ge en tydlig förklaring till syftet med ett gediget informationssäkerhetsarbete och bör även förstärkas av en underordnad standard som beskriver samtliga processer som informationssäkerhet omfattar. En sådan standard bör ge en inriktning för, och en beteckning av, samtliga processer som ska utföras och bör vidare hänvisa till underordnade dokument (processbeskrivningar och rutiner) som beskriver vem som ansvarar för utförandet av underordnade aktiviteter och hur det ska utföras.

2.4 Efterlevnad av informationssäkerhet (F)

Revisionsfråga 4: Arbetar informationssäkerhetsorganisationen respektive GDPR-organisationen aktivt med efterlevnad av informationssäkerheten?

2.4.1 Iakttagelser

Nyköpings kommun har inte tagit fram någon struktur eller någon dokumentationshierarki för informationssäkerhet- eller GDPR-arbetet. Det kombinerade dokumentet *Policy för IT-säkerhet i Nyköpings kommun* och *Policy för informationssäkerhet,* beslutat av kommunstyrelsen, har inte reviderats sedan 2009-06-23.

Det finns inte heller en stor mängd dokumentation kopplat till GDPR. Kommunen har dokumentet *Rutiner för hantering av personuppgifter i Nyköpings kommun.* Rutinbeskrivningen är fastställd av projektbeställaren 2018-05-11 och det framkommer av dokumentet att det är dataskyddsombudet som ansvarar för rutinen.

Utifrån genomförda intervjuer kan vi konstatera att det har genomförts ett mer omfattande och mer strukturerat arbete kopplat till GDPR, det med anledning av att de nya dataskyddsreglerna trädde i kraft i maj 2018. Det betonas vid intervju att detta har genererat ett mindre aktivt arbete med informationssäkerheten under samma period. Som nämnts tidigare så finns det en organisation kopplat till GDPR som består av dataskyddsombud och personuppgiftskoordinatorer. Det finns ett samverkansforum för GDPR-organisationen där planen är att de ska träffas ett antal gånger per år för att diskutera och samordna personuppgiftsfrågor inom kommunen. Det framkommer däremot i intervjuer att detta inte sker enligt planen.

När det gäller klassning av system så är det IT-avdelningen som bär huvudansvaret och det är Sveriges Kommuner och Regioners (SKR) verktyg KLASSA som används. Det framkommer att det finns ett behov av att verksamheterna ska bli mer självgående när det gäller klassning och att det därför har arbetats fram förenklade arbetssätt för att underlätta detta. Det finns även en viljeriktning att klassningen ska gå från ett systemperspektiv till ett informationsperspektiv.

Verktyg KLASSA utgör ett IT-stöd för informationssäkerhet och har även ett systemförvaltarperspektiv. Det framkommer i intervjuer att det finns en stor systemflora i Nyköpings kommun samt att det finns svårigheter att systematiskt kontrollera och få ett helhetsperspektiv över de system som finns. Detta beror enligt intervjuer på att mycket ansvar läggs på respektive systemägare och systemförvaltare.

I dokumentet *Planering för informationssäkerhetsarbetet Nyköpings kommun 2019* listas bland annat vilka aktiviteter som ska prioriteras att genomföras inom informationssäkerhetsarbetet under år 2019. Vid intervju framkommer att många av dessa aktiviteter har påbörjats under året, men att få har slutförts och att det som främst kvarstår är att ta fram förslag till informationssäkerhetspolicy samt aktiviteter kopplat till klassning. Det framgår att det finns en önskan om ett formellt beslut kring hur verksamheterna ska klassa sina system, detta för att skapa en tydligare struktur och enhetlighet. Ansvaret för samtliga aktiviteter i planeringsdokumentet ligger hos informationssäkerhetssamordnaren/dataskyddssamordnaren men framgent kommer även andra tjänstepersoner/roller inom kommunen att tilldelas ansvar för uppgifter.

Vid intervjuer framgår att det inte görs någon backup på enskilda datorer eftersom all data lagras centralt. Centrala system säkerhetskopieras genom att det görs lokala backuper på lagringssystemet där det även speglas över en kopia till lagringsmiljön. Utöver detta göra en full backup till en backup-hall varje natt. Lagringen i form av backuper sker i tre skeenden; 30 dagar, 4 veckor samt 12 månader för att säkerställa att datan säkras.

När det gäller den mer fysiska informationssäkerheten, som exempelvis hantering av datorer, nycklar till enskilda kontor och arkiv samt tillträde till lokaler så framkommer att

det fortsatt finns arbete kvar för att säkerställa en mer omfattande säkerhet i vissa verksamheter. Detta kan exemplifieras genom avsaknad av kontroll på nycklar till områden där känsliga uppgifter förvaras fysiskt.

Vid upphandling av IT-system så uppges det finnas en kravställan i enlighet med KLASSA, däremot uppmärksammas det i genomförda intervjuer att informationssäkerhetsaspekten ofta saknas i upphandlingar. Under hösten 2019 påbörjade dock informationssäkerhetssamordnaren ett arbete tillsammans med inköps- och upphandlingsenheten med syftet att inkludera informationssäkerhet vid inköp och upphandlingar. I detta arbete utgår vi från MSB:s vägledning Upphandla informationssäkert Av intervjuer framgår att kommunen följer MSB:s *Upphandla informationssäkert.* Det framkommer dock att det svårigheter kopplat till direktupphandlingar då det inte finns samma typ av kontroll.

2.4.2 Bedömning

Vi bedömer att revisionsfrågan utifrån iakttagelser från dokumentationsgranskning och intervjuer **delvis är uppfylld**.

Sammanfattningsvis kan noteras att det genomförs arbetsinsatser inom både IT- och informationssäkerhet samt GDPR, men att den formella och systematiska sidan av detta arbete hittills tyngs av brister i form av tydliga rapporteringsvägar (framför allt på strategisk nivå), avsaknad av dokumentation, och delvis av avsaknad av informationsklassning ur ett informationsperspektiv istället för ett systemperspektiv. Detta resulterar i en bristande överblick och därigenom att helhetsperspektivet gällande informationssäkerhet uteblir. Vidare brister den fysiska säkerheten kopplat till informationssäkerhet till följd av bristande kontroll ur ett tillgänglighets- samt konfidentialitetsperspektiv. Här finns behov av ytterligare rutiner och ökad kunskap om vem som ska tillgång till vad samt vid vilket tillfälle.

Givet att kommunstyrelsen hittills inte regelbundet och med systematik efterfrågat någon form av återrapportering inom informationssäkerhets- eller GDPR-området innebär detta att inte heller kommunstyrelsen kan sägas besitta den helhetsbild som krävs för att styra, leda eller ge direktiv gällande informationssäkerhetsarbetet. Det otydliga slutgiltiga ägandeskapet av informationssäkerhetsfrågor kan vidare betraktas som en bidragande orsak till bristande rapportering. Att kommunstyrelsen sällan efterfrågar en rapportering resulterar i att medvetenheten om informationssäkerhet inte kan säkerställas.

2.5 God säkerhetskultur (F)

Revisionsfråga 5: Finns ett aktivt arbete för att främja en god säkerhetskultur inom informationssäkerhetsområdet?

2.5.1 Iakttagelser

Nyköpings kommun har en Utbildnings- och kommunikationsplan för 2018-2020 där det framgår vilka utbildningar som ska genomföras av vilken målgrupp/rollgrupp samt när i tiden de ska genomföras. Det finns en obligatorisk grundläggande utbildning om säkerhet i kommunen som lanserades sommaren 2019 där informationssäkerhet samt information om dataskyddsförordningen ingår. I introduktionsprogrammet för nya chefer finns en del där informationssäkerhetssamordnaren pratar om informationssäkerhet och dataskyddsfrågor.

För nyanställda finns det, bland annat i olika checklistor och på kommunens intranät, uppmaningar där anställda uppmuntras ta del av bland annat MSB:s DISA (datorstödd informationssäkerhetsutbildning) och en e-utbildning kallad "Dataskydd i offentlig verksamhet", vilka dock inte är obligatoriska. I övrigt är det endast nya chefer som genomfört den informationssäkerhetsutbildning som inkluderade allmän information om informationssäkerhet och personuppgifter. Det framgår i intervjuer att många utbildningar inte genomförs då de inte är, eller har varit, obligatoriska eller kommunicerats ut till medarbetare.

För 2020 är det planerat för att nya chefer ska genomföra en informationssäkerhetsutbildning, alla medarbetare ska gå en utbildning i GDPR och politiker ska få en genomgång av/presentation om efterlevnad av GDPR. Samtliga nya medarbetare ska även få kort information om dataskyddsförordningen.

Det konstateras under samtliga intervjuer att utbildningar inte bedrivits, skapats eller genomförts i önskad utsträckning samt att utbildningarna inte varit obligatoriska. Antalet genomförda utbildningar har inte heller utvärderats, men det kan konstateras att det har varit ca 3000 individuella visningar på säkerhetsutbildningen sedan sommaren 2019. Det innebär att ca 3000 av kommunens totalt 4251[1] anställda har öppnat/påbörjat utbildningen. Det framgår att det är upp till respektive chef att säkerställa och kontrollera att samtliga medarbetare har genomfört de utbildningar som de ska.

Vid intervjuer framkommer att det, utifrån de incident- och avvikelseanmälningar som inkommer, upplevs finnas en relativt god kunskap om främst GDPR. Detta baseras på det faktum att anmälningar inkommer från verksamheter långt ute i linjeorganisationen. Det framkommer dock, vid merparten av intervjuerna, att det finns ett behov av mer kontinuerliga utbildnings- och informationsinsatser för att ytterligare säkerställa en ändamålsenlig hantering.

Det har inte, i så stor utsträckning, genomförts praktiska övningar inom området informationssäkerhet och GDPR. Vid intervjuer framkommer att tekniska divisionen har genomfört övningar kopplat till informationssäkerhet inom NIS-direktivet. NIS-direktivet genomfördes i Sverige 2018 och ställer krav på säkerhet i både nätverk och informationssystem. I korthet så innebär den svenska NIS-regleringen krav på

[1] Nyköpings kommun, *Nyköping i siffror,* 2020-01-15, https://nykoping.se/kommun–politik/kommunfakta/nykoping-i-siffror, hämtad 2020-02-26

informationssäkerhet och incidentrapportering för leverantörer av samhällsviktiga och vissa digitala tjänster. Samhällsviktiga tjänster är tjänster som är viktiga för att upprätthålla kritisk samhällelig eller ekonomisk verksamhet, såsom exempelvis energi, transporter och digital infrastruktur. Digitala tjänster kan istället innebära internetbaserade marknadsplatser, internetbaserade sökmotorer och molntjänster.[2] Huruvida det har genomförts liknande övningar inom kommunens krisledningsgrupp är oklart. Det framgår att det inom Social omsorg inte har genomförts några praktiska övningar kopplat till varken informationssäkerhet eller hantering av personuppgifter. Det framkommer att medarbetarna inom verksamhetsområdet har en vana av att arbeta med känsliga uppgifter och att exempelvis sekretess är ett vanligt samtalsämne. Det arbetas dock inte proaktivt med frågorna utan diskussioner tas upp vid APT (arbetsplatsträffar) när en incident eller avvikelse har inträffat.

För att ytterligare kommunicera vikten av en god säkerhetskultur så medverkar Nyköpings kommun i MSB:s *Informationssäkerhetsmånad*. Temat för år 2019 var "Tänk säkert - gör smarta saker säkra"[3]. Informationsförvaltningen och kommunikationsavdelningen arbetar tillsammans med säkerhetsmånaden och kommunicerar ut information till medborgare och kommunens medarbetare. Bland annat genomförs informationsinsatser på kommunens sociala medier och Facebook, intranätet och kommunens hemsida.

2.5.2 Bedömning

Vi bedömer att revisionsfrågan utifrån iakttagelser från dokumentationsgranskning och intervjuer **ej är uppfylld**.

Det genomförs punktinsatser kopplat till säkerhetskultur gällande informationssäkerhet och GDPR, men det saknas ett strukturellt och systematiserat kommunövergripande arbete. Vi bedömer det vara av central vikt att det genomförs kontinuerliga utbildnings- och informationsinsatser för att medarbetarna ska påminnas om vikten av en god säkerhetskultur och informationssäkerhet. De tjänstepersoner som tilldelats extra ansvar inom området, såsom personuppgiftskoordinatorer, bör erbjudas mer omfattande utbildningsinsatser för att i sin roll kunna sprida information och kunskap vidare i sina organisationer.

Det kan konstateras finnas ett stort behov av att systematiskt genomföra medvetandehöjande aktiviteter för att höja mognadsnivån kopplat till kommunens säkerhetskultur i form av gemensamma kunskaper, beteenden, värderingar och föreställningar hos både individer och grupper. Detta för att skapa samt bedriva en säker

[2] Myndigheten för samhällsskydd och beredskap (MSB) https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/nis-direktivet/

[3] Myndigheten för samhällsskydd och beredskap (MSB) https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/informationssakerhetsmanaden/, hämtad 2020-02-28

verksamhet. Faktumet att det under 2020 planeras utbildningar för bland annat samtliga nyanställda och chefer bedöms dock som positivt.

2.6 Stickprov på behörigheterna i behörighetssystemet

Revisionsfråga 6: Utförs kontinuerligt stickprov på behörigheterna i behörighetssystemet?

2.6.1 Iakttagelser

Det framkommer i intervjuer att Nyköpings kommuns IT-avdelning genomför regelbundna stickprov i Active Directory (AD) där IT-avdelningen går igenom samtliga användare i AD för att undersöka huruvida det finns konton som inte varit aktiva på länge. Det framkommer dock att detta inte finns dokumenterat, men att det genomförs ungefär en gång i månaden. Om ett konto inte varit aktivt under en längre tid inaktiveras det enligt intervjusvar, likaså gällande externa konsulter. Enligt information från intervjuer saknas skriftliga rutiner för hur samt när detta ska genomföras.

Dokumentet *Rutin för Behörighet till underliggande/centrala system samt verksamhetssystem inom IT-enhetet* framhåller att rutiner för administration och uppföljning av behörigheter ska upprättas av systemägaren/systemägarombud. Det framgår även av dokumentet att behörigheter och rättigheter omgående ska revideras när förutsättningar förändras, exempelvis vid avslutning av anställning eller när väsentliga funktioner läggs till i systemet. Detta gäller dock inte Active Directory specifikt. I samma dokument framgår att behörigheter på roll- och funktionsnivå ska finnas dokumenterat, det framhålls dock inte i vilket dokument. Vidare konstateras att hänvisat dokument ska överses halvårsvis, samt att behörigheter vid samma tillfälle ska stämmas av med respektive koordinator.

Enligt den *Baseline Security Assessment* som genomförts har 17% av existerande konton aldrig använts. En bidragande faktor till det är att det finns många sällananvändare anställda i kommunen, deltidsanställda inklusive timvikarier. En anställd med aktiv anställning alternativt en elev som är inskriven som aktiv elev i kommunal skola har alltid ett aktiv AD-konto oavsett om det används eller ej. Vid intervjuer framkommer att det finns automatiska processer för rensning, vilket skiljer sig från den information och de resultat som inkommit från genomförd BSA-analys.

2.6 2 Bedömning

Vi bedömer att revisionsfrågan utifrån iakttagelser från dokumentationsgranskning, Baseline Security Assessment (BSA) och intervjuer **ej är uppfylld**.

En viktig del i behörighetsstyrningen gäller uppföljning och kontroll av befintliga behörigheter samt eventuella avvikelser. Då Nyköpings kommun saknar formaliserade processer för uppföljning i form av stickprov, finns det en stor risk inom kommunen att behörigheter hanteras felaktigt utan att det åtgärdas. Vidare leder frånvaron av styrning till ad hoc-mässiga förfaranden som präglas av osäkerhet då tillämpning av rutiner

riskerar att skilja sig från situation och person. Kommunstyrelsen bör beakta hur nyttjande och uppföljning av behörigheter ska kontrolleras för att kunna säkerställa spårbarhet.

Risken som är förknippad med avsaknaden av systemstöd innebär att kontroll är avhängig manuella processer. Manuella processer är i hög grad präglade av personberoende och underminerar systematik och uppföljning. Med särskild hänsyn till att kommunstyrelsen i nuläget saknar planer för intern kontroll, stickprov och processer blir behörighetshantering en osäker process från början till slut.

2.7 Implementerad kontohantering

Revisionsfråga 7: Finns en god kontohantering implementerad?

2.7.1 Iakttagelser

Den granskade komponenten Active Directory (AD) hanterar både anställda och elever för både Nyköpings kommun och Oxelösunds kommun.

När det gäller rutiner för behörigheter så finns det inom IT-avdelningen en systemansvarig som ansvarar för kommunens AD. AD:t har en automatisk koppling till lönesystemet vilket innebär att användarkonton tas bort vid medarbetares sista anställningsdag. Om en medarbetare endast byter tjänst inom kommunen så krävs istället en manuell hantering av behörigheter vilken innebär att ansvarig chef ska informera systemförvaltare. Något som upplevs vara problematisk är det faktum att specialbehörigheter fortfarande kan ligga kvar hos den medarbetare som bytt tjänst inom kommunen. Det framgår att det inte sker någon kontroll kopplat till detta och att det därför finns en risk att medarbetare kan ha bytt avdelning men fortsatt har kvar specialbehörigheter till ett flertal system.

Vid intervju framkommer att det finns variation inom kommunens system när det gäller lösenordshantering och hur ofta lösenord ska bytas. Kommunen har en policy för lösenord när det gäller AD, dock inte för enskilda system, vilket anges i *Riktlinjer för IT-resurser inom Nyköpings kommun*. När det gäller behörighetstilldelning i verksamhetssystem så är det inte IT-avdelningen som ansvar för detta utan det hanteras av systemansvariga i respektive verksamhet. Det framkommer att det inom kommunen saknas en samlad förteckning över samtliga behörigheter.

Det finns ett flertal framtagna rutiner rörande kontohantering i AD, bland annat:

- *Rutin för att beställa och skapa nytt användarkonto vid nyanställning,*
- *Rutin för att hantera användarkonton vid förändrade anställningsförhållanden,*
- *Rutin för att hantera användarkonton vid anställnings upphörande,* samt
- *Rutin för Användarkonton till Konsulter*

Det framgår inte när rutinerna är framtagna.

Enligt den Baseline Security Assessment (BSA) som genomförts kan det konstateras att 9% av befintliga användarkonton har lösenord som aldrig går ut. Vidare gällande

kontohantering har 17% av de konton som skapats aldrig använts. Detta tyder på att det saknas rutiner och processer för rensning, alternativt att de som finns inte följs, framförallt av konton som inte brukas. Slutligen kan det även konstateras att 43% av befintliga konton är inaktiverade, en stor del av dessa är så kallade "dummy"-konton som skapas i samband med att anställning upphör i lönesystemet, detta för att användarnamnet inte ska kunna återanvändas. Det finns 42 953 konton i AD:t och 6459 anställda i Nyköpings kommun, där heltidsanställda, deltidsanställda och andra former av anställning ingår.

Det finns även 5940 så kallade "övriga konton", vilka bland annat inkluderar systemkonton, servicekonton, funktionsbrevlådor och konsulter. Majoriteten av dessa har dels lösenord som aldrig går ut och dels är inaktiverade.

Det finns 26 AD-konton som enligt BSA konstateras ha domänadministrativa rättigheter, det vill säga de konton som har högst behörigheter. Av dessa konton finns 8 användarkonton där det saknas krav på uppdatering av lösenord, varav 6 stycken är systemkonton. Enligt intervjuer pågår det ett arbete med att minska antalet konton med domänadministrativa rättigheter.

Kopplat till Nyköpings kommuns lösenordshantering finns det enligt dokumentet *Riktlinjer för IT-resurser inom Nyköpings kommun* ett antal krav på lösenord till nätverk (Active Directory) som innehåller ett antal krav. Det kan dock konstateras, utifrån genomförd BSA, att komplexitetsfunktionen inte är påslagen, vilket innebär att det inte kan kontrolleras huruvida de krav på lösenord som ställs efterlevs eller ej.

2 7.2 Bedömning

Vi bedömer att revisionsfrågan utifrån iakttagelser från dokumentationsgranskning, Baseline Security Assessment (BSA) och intervjuer **ej är uppfylld**.

Identitets- och behörighetsstyrning har som syfte att möjliggöra att rätt person får tillgång till rätt information. Dessutom ska det finnas en skälig grund till varför en person ska ha en viss behörighet. Därför bör kommunen definiera ett tydligt ägarskap för processen för att processägaren i sin tur ska kunna ställa krav och kontrollera efterlevnad på ett adekvat sätt. Det finns en diskrepans mellan det som framkommit i intervjuer och det som framkommit från den genomförda Baseline Security Assessment (BSA).

Då Nyköpings kommun och Oxelösunds kommun delar AD är det av särskild vikt att användarkonton hålls åtskilda från varandra med separata namn och användare. Nyköping och Oxelösunds kommuner har många "dummy" konton som skapas efter att en medarbetare slutar, syftet är att reservera användarnamnet, viktigt att säkerställa att dessa konton ej innehåller någon GDPR information.

Enligt intervjuer pågår det ett arbete med att minska antalet konton med domän administrativa rättigheter, vilket innebär att det är av vikt att detta arbete fortgår på ett skyndsamt sätt.

I enlighet med den genomförda BSA som genomförts i kommunen kan det konstateras att säkerhetsinställningarna på de analyserade servrarna i kommunen sammantaget anses ändamålsenliga. Däremot kan det konstateras kommunen har ett stort behov av att regelbundet se över och granska säkerhetsinställningar i kommunens Active Directory (AD). Det kan även konstateras att det finns förbättringsområden kopplat till kommunens kontohantering, främst gällande inställningar för lösenordsparametrar.

Att 17% av befintligt existerande konton aldrig loggat in skulle kunna utgöra en säkerhetsrisk då oanvända konton är ett vanligt mål vid antagonistiska attacker utförda av hackare. Det är av yttersta vikt att skapa strukturerade processer och kontroll av behörighetshantering genom samtliga faser som hör identitets- och behörighetsstyrning till. Dessa faser innefattar hur behörigheter *tilldelas*, *ändras* och hur de *tas bort*. Att det finns 26 AD-konton med domänadministrativa rättigheter tyder på att det är fler än vad som enligt praxis anses vara nödvändigt. Att flertalet av dessa har lösenord som aldrig går ut är en stor risk ur ett säkerhetsperspektiv.

2.8 Rutin för att kontinuerligt revidera användarkonton

Revisionsfråga 8: Finns det en rutin för att kontinuerligt revidera användarkonton och efterlevs rutinen?

2.8.1 Iakttagelser

Nyköpings kommun har enligt intervjusvar en automatiserad process för att regelbundet revidera och granska användarkonton i kommunens Active Directory (AD). Det framkommer däremot även under intervjuer att det saknas en manuell process för att kontrollera att de satta rutinerna och processerna följs.

Det framkommer i den Baseline Security Assessment (BSA) som genomförts att det saknas formaliserade processer för revidering av användarkonton. Detta visar sig genom flertalet inkommen analyserad data. Som tidigare nämnt har 17% av existerande användarkonton aldrig loggat in och 43% av existerande konton är inaktiverade.

I de framtagna rutinerna gällande användarkonton i Active Directory (AD) konstateras det att manuella processer kring användarkonton i AD vid hantering av användarkonton vid förändrade anställningsförhållande eller vid anställnings upphörande endast sker vid upptäckt av felaktigheter som inte fångats upp av de automatiska rutinerna eller processerna.

2.8.2 Bedömning

Vi bedömer att revisionsfrågan utifrån iakttagelser från dokumentationsgranskning, Baseline Security Assessment (BSA) och intervjuer **ej är uppfylld**.

Kontinuerlig revidering av användarkonton i Active Directory sker inte utifrån den information som inhämtats från den BSA som genomförts. Detta kan konstateras utifrån faktumet att det fortfarande finns en större mängd användarkonton som aldrig använts eller som har en inställning som gör att lösenordet till användarkontot aldrig går ut. Detta

bedöms även utgöra en risk ur ett GDPR-perspektiv, bland annat gällande de registrerades rättigheter. Kommunstyrelsen bör säkerställa att ett tydligt ägarskap upprättas av modellen för användarkonton samt behörigheter.

3. Revisionell bedömning

PwC har på uppdrag av de förtroendevalda revisorerna i Nyköpings kommun granskat kommunens arbete med informationssäkerhet och GDPR. Granskningens syfte har varit att bedöma om kommunstyrelsen säkerställer ett ändamålsenligt informationssäkerhetsarbete och om detta sker med tillräcklig intern kontroll.

Efter genomförd granskning bedömer vi att kommunstyrelsen **inte** säkerhetsställer ett ändamålsenligt informationssäkerhet och att det saknas tillräcklig intern kontroll.

Efter genomförd granskning kan vi konstatera att det finns en begränsad organisation kopplat till GDPR, men att denna behöver tydliggöras och att roller och ansvar behöver dokumenteras och säkerställas. Organisationen för GDPR innehar även inslag av personberoende. Det saknas i dagsläget en utarbetad organisation när det gäller informationssäkerhetsområdet. Det finns till viss del styrande dokument inom granskningsområdet, dock är dokumenten i behov av översyn och revidering. Det finns även ett större personberoende kopplat till informationsäkerhetsorganisationen och inslag av begränsningar i form av resurser och direktiv. Kommunen saknar väsentlig formell dokumentation för att styra sitt arbete inom informationssäkerhet och GDPR på en strategisk nivå. Det saknas även ett ledningssystem för informationssäkerhet inom kommunen, vilket resulterar i ett bristande systematiskt informationssäkerhetsområde.

Det kan konstateras att det genomförs arbetsinsatser inom både IT- och informationssäkerhet samt GDPR. Granskningen har däremot påvisat en bristande överblick och att ett helhetsperspektiv gällande informationssäkerhet uteblir. Givet att kommunstyrelsen hittills inte regelbundet och med systematik efterfrågat någon form av återrapportering inom granskningsområdet innebär detta att inte heller kommunstyrelsen kan sägas besitta den helhetsbild som krävs för att styra, leda eller ge direktiv gällande informationssäkerhetsarbetet. Vi kan konstatera att det genomförs punktinsatser kopplat till säkerhetskulturen inom kommunen, men att det saknas ett strukturellt och systematiserat kommunövergripande arbete. Vi bedömer att det är av central vikt att det genomförs kontinuerliga utbildnings- och informationsinsatser för att medarbetarna ska påminnas om vikten av en god säkerhetskultur och informationssäkerhet.

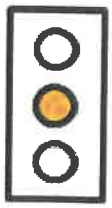
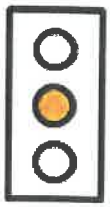
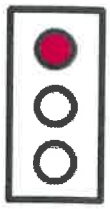
Gällande Nyköpings kommuns Active Directory (AD) kan det noteras att vissa säkerhetsinställningar, främst relaterade till lösenordsinställningar, bör utvärderas. Sammantaget är säkerhetsinställningarna på analyserade servrar bra. Vissa områden är dock i behov av förbättringar, främst vad gäller inställningar för lösenordsparametrar. Efter genomförd analys av konton i AD indikeras att ett antal konton bör utvärderas. Vidare tyder resultaten på att rutiner för användaradministration kan behöva revideras.

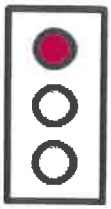
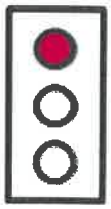
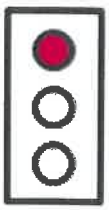
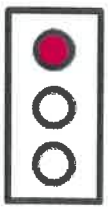
Rekommendationer

Efter genomförd granskning lämnas följande rekommendationer:

- Dokumentera huvudsakliga informationssäkerhetsprocesser. Säkerställ och tydliggör roller, ansvar och mandat.
- Säkerställ att samtlig dokumentation är uppdaterad och aktuell.
- Implementera ett ledningssystem för informationssäkerhet.
- Säkerställ att utbildningar och övningar för att utveckla och säkerställa kompetens om informationssäkerhet genomförs regelbundet.
- Minska personberoendet för att säkerställa att verksamheter kan fortlöpa vid ett eventuellt personalbortfall.
- Genomför informationsklassning från ett informationsperspektiv istället för systemperspektiv.
- Identifiera och definiera mätbara mål samt tilldela ansvar för samtliga mål i *Planering för informationssäkerhetsarbetet Nyköpings kommun 2019* i syfte att följa upp dessa kontinuerligt.
- Kommunstyrelsen bör säkerställa att det finns en baslinje för säkerhetsinställningar samt att det kommer att implementeras på relevanta servrar inom domänen.
- Kommunstyrelsen bör genomföra en granskning av de konton vars lösenord aldrig går ut, för att utvärdera om andra konton än systemkonton har "lösenord aldrig går ut" aktiverat.
- En utvärdering av de användarkonton i AD:t som aldrig använts bör genomföras för att undersöka nödvändigheten av dessa.
- Kommunstyrelsen bör undersöka om processen för att granska inaktiverade nätverksanvändare i tid måste förbättras.

4. Bedömningar utifrån kontrollmål

Revisionsfråga	Kommentar	
Det finns en tydlig organisation, roll- och ansvarsfördelning kopplat till informationssäkerhet respektive GDPR?	**Delvis uppfyllt** Det finns organisationer för både informationssäkerhet och GDPR, dessa är dock begränsade och präglas av brist på resurser och ett tydligt personberoende. Det saknas en tydlig roll- och ansvarsfördelning kopplat till kravställan.	
Finns styrande informationssäkerhets-dokument och riktlinjer som är implementerade i verksamheten (inkl. GDPR)?	**Delvis uppfyllt** Det finns styrande dokument, dock är dessa i behov av översyn och revidering. Det saknas tilldelat ansvar för revidering och det saknas en tydlig dokumentationshierarki.	
Finns ett ledningssystem för informationssäkerhet?	**Ej uppfyllt** Nyköpings kommun saknar ett ledningssystem för informationssäkerhet. Det har inte fattats beslut om implementering och det ingår inte i den närtida planeringen.	
Arbetar informationssäkerhets-organisationen respektive GDPR-organisationen aktivt med efterlevnad av informationssäkerheten?	**Delvis uppfyllt** Det genomförs arbetsinsatser inom både IT- och informationssäkerhet samt GDPR. Det saknas dock både systematik och aktiv efterlevnad i full	

	utsträckning.	
Finns ett aktivt arbete för att främja en god säkerhetskultur inom informationssäkerhets-området?	**Ej uppfyllt** Det genomförs punktinsatser kopplat till säkerhetskultur gällande informationssäkerhet och GDPR, men det saknas ett strukturellt och systematiserat kommunövergripande arbete. Utbildningar sker sällan och endast till delar av de anställda.	
Utförs kontinuerligt stickprov på behörigheterna i behörighetssystemet?	**Ej uppfyllt** Nyköpings kommun genomför inte stickprov på behörigheterna i behörighetssystemet.	
Finns en god kontohantering implementerad?	**Ej uppfyllt** Det saknas inställningar för lösenordsparametrar, en mängd användarkonton har aldrig använts, det finns en stor mängd konton med administrativa konton varav flertalet med inställningen att lösenorden aldrig går ut.	
Finns det en rutin för att kontinuerligt revidera användarkonton och efterlevs rutinen?	**Ej uppfyllt** Det saknas kontinuerlig revidering av användarkonton i behörighetssystemet. Behörigheter revideras endast vid slumpmässiga upptäckanden av felaktigheter.	

Bilagor

De dokument som vi, inom ramen för denna granskning, har tagit del av är följande:

- Policy för IT-säkerhet i Nyköpings kommun (Kommunstyrelsen, 2009-06-23)
- Riktlinjer för IT-resurser inom Nyköpings kommun (dokumentet är inte daterat och det framgår inte vilken instans som antagit dokumentet)
- Rutin för hantering av personuppgifter i Nyköpings kommun (fastställd av projektbeställare 2018-05-11, giltig fr.o.m. 2018-05-11)
- E-strategi för Nyköpings kommun (KF 2016-11-08)
- Handlingsplan för digitalisering i Nyköpings kommun 2019-2020 (KS 2019-04-29)
- Planering för informationssäkerhetsarbetet Nyköpings kommun 2019 (ej beslutad)
- Utbildnings- och kommunikationsplan 2018 - Nyköpings kommun (ej beslutad)
- Rutin för att beställa och skapa nytt användarkonto vid nyanställning (datum för upprättande framgår inte)
- Rutin för att hantera användarkonton vid anställnings upphörande (datum för upprättande framgår inte)
- Rutin för att hantera användarkonton vid förändrade anställningsförhållanden (datum för upprättande framgår inte)
- Rutin för Användarkonton till Konsulter (datum för upprättande framgår inte)
- Rutin för Behörighet till underliggande/centrala system samt verksamhetssystem inom IT-enheten (Upprättad 2015-01-16)
- Rutin för Behörighet till verksamhetssystem (Upprättad 2015-01-16)
- Rutin för Behörighetstilldelning till servrar för systemansvariga (datum för upprättande framgår inte)
- Rutin för extern åtkomst, leverantör (Upprättad 2012-11-20, ej beslutad)
- Rutin för extern åtkomst, Mobil arbetsplats (Upprättad 2012-11-20, reviderad 2017-06-09)
- Rutin för hantering av administrationslösenord (Upprättad 2016-09-01)
- Rutin för Tillträde till säkra utrymmen, Röd Zon (Upprättad 2012-01-04)

2020-03-23

Tobias Bjöörn	Fredrika Jönander
Uppdragsledare	*Projektledare*

Denna rapport har upprättats av Öhrlings PricewaterhouseCoopers AB (org nr 556029-6740) (PwC) på uppdrag av Nyköpings kommun enligt de villkor och under de förutsättningar som framgår av projektplan från den 19 december 2019. PwC ansvarar inte utan särskilt åtagande, gentemot annan som tar del av och förlitar sig på hela eller delar av denna rapport.