NORRTÄLJE KOMMUN

Internkontrollområden

Internkontrollområde Informationssäkerhet

Internkontrollområdet syftar till att säkerställa att kommunen på ett tillfredställande sätt hanterar informationssäkerheten utifrån de lagkrav GDPR (General Data Protection) ställer.

Titel	Färdiggrad

Avaktivering av användare

Beskrivning:
Kontroll att inaktuella användare är avregistrerade från åtkomst av kommunens system eller har fått reviderade behörigheter samt att media (dator, Ipad, mobiltelefon etc.) är återlämnade. Kommunen är skyldig att säkerställa att personuppgifter och information inte kommer i felaktiga händer. En viktig del i detta arbete är att media (dator, Ipad, mobiltelefon etc.) återlämnas då de kan ligga kvar innanför kommunens nätverk och kan utgöra en säkerhetsrisk.
Enligt GDPR ska användarbehörigheter utgå från minsta möjliga behörighet till personuppgifter och skyddsvärda system för att löpande säkerställa att behörigheter revideras. Kontrolleras 3 ggr/år, genom enkätundersökning

Kommentar:
En förteckning över de system som arbetas i och där det framgår vilka system som är kopplat till AD:t (digital katalog som bygger på system, användare och hårdvara) och således avslutas automatiskt vid en avslutad anställning respektive inte och måste följas upp vid ett avslutningssamtal.
Ett flöde för att säkerställa och avsluta användare i aktuella system bör upprättas och uppdateras på kommunnivå och avdelningsnivå där även ansvarig/systemförvaltare bör utses. Arbetet med detta är delvis påbörjat i kommunens PM3 modell men behöver utvecklas och färdigställas i sin helhet under 2019/2020.

För hög behörighet i system

Beskrivning:
Kontroll att inaktuella användare är avregistrerade från åtkomst av kommunens system eller har fått reviderade behörigheter samt att media (dator, Ipad, mobiltelefon etc.) är återlämnade. Kommunen är skyldig att säkerställa att personuppgifter och information inte kommer i felaktiga händer.
Enligt GDPR ska användarbehörigheter utgå från minsta möjliga behörighet till personuppgifter och skyddsvärda system. Löpande säkerställa att behörigheter revideras, dock minst 3 ggr/år, genom enkätundersökning.

Kommentar:
Stickprovskontroll är utförd i ekonomisystemet Rodret och visar på avvikelser i administratörsrättigheter, åtgärd genomförda genom att avsluta samtliga konsulter och ge aktuella konsulter en tidsbegränsad användarbehörighet.

Titel	Färdiggrad

Intrång i skyddat nätverk

Beskrivning:
Intrång i oskyddat nätverk utifrån i form av ”hacker-attacker”. Identifiera eventuella brister och stärka upp skyddet i kommunens IT-säkerhet. Kontroll 1gång /år, genomförs av en externt anlitad konsult specialiserad inom området.

Kommentar:
Intrång i oskyddat nätverk utifrån i form av ”hacker-attacker” från anlitad konsult är utförda och inget intrång har skett. Testet visade dock på förbättringsförslag inom IT och renhållning där inloggningssäkerheten behövdes förbättras, vilket är utfört.

Regelbunden gallring/uppdatering av dokumenthanteringsplan

Beskrivning:
Säkerställa att gallring och bevaranderutiner efterlevs. I samband med GDPR bedöms risk att gallring och som inte följer dokumenthanteringsplanen sker. Kontroller genomförs löpande genom stickprov.

Kommentar:
Regler för gallring finns angivna i nämndens hanteringsanvisningar samt bestämmelser om gallring finns även i arkivreglementet. Hanteringsanvisningarna är antagna 2019 och revideras vid behov.. Registraturen korrigerar och uppdaterar när eventuell avvikelse påträffas. I övriga IT-system ska kontinuerlig gallring ske.
Verksamheterna behöver även göra bevarande-/gallringsutredningar av sina IT-system samt ta fram bevarandestrategier för elektronisk information. Arkivmyndigheten har ej genomfört några inspektioner under senare år men dock är en inspektion planerad till hösten 2019.

Internkontrollområde Ekonomiska processer och uppföljning av leverans i förhållande till beslut

Internkontrollområdet syftar till att säkra kommunens tillgångar och en god ekonomisk hushållning.

Titel	Färdiggrad

Att representationspolicy ej efterlevs

Beskrivning:
Uppföljning av representationspolicyn, genomförs genom kontroller inom internrepresentation. Det innebär att förtäring vid regelbundet återkommande möten som gäller information om eller planering av det löpande arbetet t.ex. arbetsplatsträffar inte får ske. Eventuell förtäring tillsammans med kollegor i anslutning till sådana möten ska bekostas av medarbetaren. Önskad effekt är att representation sker i enlighet med policy. Kontrolleras 3 ggr/år genom stickprov från utdrag ur fakturasystemet.

Kommentar:
I kontrollmomentet har stickprovskontroller utförts i enlighet med policydokument för internrepresentation och inga avvikelser har hittats.

Titel	Förbättringsgrad

Bristande leverantörstrohet

Beskrivning:
Uppföljning av avtalstrohet/leverantörstrohet utförs via stickprov mellan beställningssystem och fakturasystem samt spendanalys mellan fakturasystem och avtalssystem. Stickprovskontroller utförs löpande och spendanalys fyra ggr/år. Internkontrollen har berört området 2018 och nya rutiner och systemstöd är under framtagande vilket medför att behovet av kontroller fortsätter under 2019.

Kommentar:
Analys av inköps och leverantörsbeteende, en s.k. spendanalys genomförs fyra gånger/år och på sikt till 2020 utökas intervallen till tolv gånger/år. Vidare lyfts resultatet av analysen in i managementrapporteringen och kommuniceras även till verksamheterna via kundansvariga inom upphandlingen. Samt genom kartläggning utforma ett dokumenterat flöde för det löpande förbättringsarbetet tillsammans med verksamheterna innan årsskiftet.
Avvikelser under delår 1 där analysen visar avvikelse på att köp sker delvis hos icke avtalade leverantörer samt att tecknade avtal i form av entreprenader och SKL ej i helhet är säkerställda i avtalsdatabasen. Inför delår 2 utfördes en insats att säkerställa referensmaterial och källor för att nå rättvisande resultat för analys.

Sena utbetalningar

Beskrivning:
Uppföljningar av att leverantörsutbetalningar sker i tid. Detta internkontrollområde fanns även med under 2018, då identifierades behovet om att förtydliga riktlinjer till verksamheterna genom exempelvis riktlinjer för bestridande av fakturor. Kontrolleras löpande med redovisning 4 ggr/år och stickprovskontroller 12 ggr/år. Internkontrollen har berört området att nya riktlinjer är under framtagande vilket medför att behovet av kontroller fortsätter under 2019.

Kommentar:
Vid genomgång av kontrollmomentet sena leverantörsutbetalningar per 31 augusti 2019 visar resultatet på att avvikelser finns. Resultatet medför att översynen kommer att fortsättas med samma bevakning och även utökas med bevakning över eventuella merkostnader. Förbättringsåtgärd i form av en dokumenterad rutin och mallar som införts under delår 2 kommer att utvärderas inför årsbokslut

Bristande rutiner vid momsåtersökning

Beskrivning:
Uppföljning av att momsåtersökning till skatteverket sker korrekt. Stickprovskontroll 3 ggr/år genom redovisningssystemet stämmer av att underlag och redovisningssystem är transparanta.

Kommentar:
Vid kontrollmomentet visas inga avvikelser dock ses ett förbättringsbehov av att ha en dokumenterad rutinbeskrivning av den systematiska uppföljningen innan årsskiftet.

Internkontrollområde Professionellt och förtroendeskapande förhållningssätt

Internkontrollområdet syftar till att skapa en internkontrollplan som säkerställer att policys, riktlinjer och handläggningsrutiner efterlevs.

Titel	Färdiggrad

Nyttjande av Internet som inte följer kommunens rutiner för IT-användande

Beskrivning:
Undersökning kring nyttjandet av internet som går emot kommunens rutiner för IT-användande. Kontrollen genomförs löpande, "loggar" kring antalet användare per verksamhet som försökt komma in på spärrade sidor . Önskad effekt är att medvetandegöra användare om kommunens jämställdhet, IT-användande, professionalitet och värdegrund. Kontrolleras 12 gånger/år, genom systemloggar.

Kommentar:
Dokumenterad rutin finns och fungerar men med utvecklingsområden inom kommunikation till verksamheterna samt ett dokumenterat flöde för en eventuell åtgärdstrappa innehållande ansvarsfördelning.

Uppföljning och vidareanmälningar av incidenter i enlighet med KIA inte sker

Beskrivning:
KIA uppföljning, arbetsmiljöansvarig chef ska efter inkommen anmälan i KIA om olycksfall, tillbud, riskobservationer och säkerhetsincidenter gör riskbedömning, utredning och åtgärder för att undvika att händelsen inträffar igen. Efter ytterligare en tidsfrist skall chef följa upp att åtgärd fått önskad effekt. Kommunstyrelsen finner det viktigt att förebygga arbetet med en god och säker arbetsmiljö sker. Önskad effekt för internkontrollområdet är att antalet anmälda och korrekt handlagda ärenden ökar med korrekt flödesprocess. Kontrolleras 12 ggr/år, genom systemloggar i KIA.

Kommentar:
Vid genomförd internkontroll framkom att uppföljningar i KIA idag sker på APT och Losam för uppföljning samt ett säkerställande att den kommuniceras och efterföljs i verksamheterna.

Efterlevnad av återkoppling till invånare

Beskrivning:
Norrtälje kommuns medarbetare ska vara tillgängliga för invånarna och ha en hög servicenivå. Detta innebär att när medarbetaren inte är anträffbar har man registrerat en korrekt hänvisning i Trio. Medarbetare förväntas svara om hänvisning inte är registrerad. Önskad effekt för interkontrollområdet är att antal omkopplingar skall minska samt att antalet obesvarade samtal från invånare minskar. Kontrolleras 6 ggr/år via systemloggar i Trio.

Kommentar:
I samband med internkontrollen för antalet returärenden som mäts per månad i Trio framkom ett utfall på 7,5% i mars 2019 (6,4%, mars 2018) och 5,2% i april 2019 (4,4%, april 2018) samt 5,1% maj 2019 (4,6% maj 2018). Rutiner för automatisk hänvisning via Outlook fungerar tillfredställande. Som förbättring föreslås se över instruktionerna för den manuella hanteringen gällande bortkoppling av telefon och identifiera kommunikationsvägar och analysera mätningsresultatet tillsammans med verksamheterna.

Titel	Förbättringsgrad
Att bisyssla strider mot tjänsteutövning	

Beskrivning:
Anställda på kommunstyrelsekontoret skall ha arbetet i Norrtälje kommun som primär sysselsättning och arbete utöver detta ska godkännas av närmaste chef. Detta internkontrollområde fanns även med under 2018 då identifierades behovet om att förtydliga riktlinjer samt att återinföra kontrollmomentet i mallen för medarbetarsamtalet. Internkontrollen under 2019 syftar till att kontrollera utfallet av framtagna riktlinjer och malländringar. Kontrolleras 4 ggr/år, genom enkät till chefer.

Kommentar:
Ej påbörjad på grund av att detta kontrollmoment genomförs i samband med medarbetardialog varje höst, vilket medför en återrapportering först till årsslut.

Att medarbetare har för högt timsaldo

Beskrivning:
Anställda på kommunstyrelsekontoret arbetar ett angivet antal timmar per år, vilket ska redovisas regelbundet till chef. Antal tillåtna över- eller understigande timmar är kopplat mot gällande riktlinjer och får inte över- eller understigas. Detta internkontrollområde fanns även med under 2018 då identifierades behovet om att förtydliga riktlinjer. Internkontrollen under 2019 syftar till att kontrollera utfallet av framtagna riktlinjer. Kontrolleras 4 ggr/år, genom enkät till chefer.

Kommentar:
Vid genomförd kontroll efter överföring till lönesystem från excelfil framkom ett par mindre avvikelser som är hanterade.

Tillsyn att beslutade åtgärder från föregående år har genomförts

Internkontrollområden från tidigare år som behöver följas upp på grund av otillfredsställande resultat

Titel	Färdiggrad
Kontroll av föregående års åtgärder	

Beskrivning:
Att följa upp och säkerställa att angivna åtgärder i föregående års internkontroll är genomförda.

Kommentar:
Områden som kvarstår från tidigare år har lyfts in i internkontrollplanen.

Bilaga

Riskmatris enligt COSO-modellen

Sammanfattning

Sammanfattningsvis är planering för fortsatt utbildning och utveckling inom samtliga kontrollerade områden samt att säkerställa och upprätthålla goda rutiner som redan finns. Inför årets slut ska samarbetsformer och förbättringsrutiner arbetas fram för att komma till rätta med konstaterade avvikelser.