Granskning av kommunens IT- och informationssäkerhet

Rapport

Eskilstuna kommun

KPMG AB

2020-10-07

Antal sidor 20

Antal bilagor 1

Granskning av Eskilstuna kommuns IT- och informationssäkerhet

Eskilstuna kommun
Granskning av kommunens IT- och informationssäkerhet

2020-10-07

Innehållsförteckning

1 Sammanfattning

KPMG har av de förtroendevalda revisorerna i Eskilstuna kommun fått i uppdrag att genomföra en granskning av kommunens styrning och ledning av informations-säkerhetsarbete och tillhörande IT-säkerhetsåtgärder. Uppdraget ingår i revisionsplanen för 2020.

Granskningen har syftat till att konstatera om kommunstyrelsen säkerställt en tillräcklig mognad och medvetenhet i organisationen för sitt informationssäkerhetsarbete. Därtill skulle granskningen bedöma om kommunen har processer, rutiner och ändamålsenlig kontroll över IT-säkerheten och att de åtgärder som vidtas baseras på risker och behov som ansvariga för kommunens informationstillgångar har fastställt.

Vår sammanfattade bedömning utifrån granskningens syfte är att kommunstyrelsen inte har säkerställt ett ändamålsenligt och systematiskt arbete med IT- och informationssäkerhet. Flertalet av de styrande dokumenten är ofullständiga, föråldrade och inte fullt ut tillämpbara i nuvarande organisation. Vi har även identifierat ett starkt personberoende kopplat till centralt utsedda roller vilket kan resultera i en otydlighet vem som är formellt ansvarig, vara sårbart vid organisations- eller personalförändringar samt försvåra uppföljningsarbetet. Vi anser inte att verksamheterna har tagit sitt ansvar för att skydda sina informationstillgångar och informationssäkerhetsarbetet är inte integrerat i övriga styrprocesser.

Kommunen har under våren infört en informationsklassningsmodell och tagit fram hanteringsregler. Vår bedömning är dock att arbetet är i uppstart och inte fullt ut implementerat och sker inte systematiskt.

Vi ser det som en allvarlig säkerhetsrisk att det är tillåtet i verksamheterna att använda datorer och utrustning som inte tillhandahålls av IT-avdelningen. Det innebär att de inställningar och tjänster som IT-avdelningen anser behövs för en tillräcklig säkerhet inte finns implementerade. Lokala administratörer kan genom denna hantering komma åt information via kommunens IT-miljö som inte IT-avdelningen kan övervaka och kan därmed inte fullgöra sitt ansvar för IT-säkerheten i kommunen.

I granskningen har en sårbarhetsscanning genomförts av två interna nätverk i kommunen. Detta test identifierade ett antal sårbarheter avseende upprättad IT-säkerhet. Majoriteten av dessa sårbarheter grundar sig i ett behov av att uppdatera programvara för att minimera risken att drabbas av incidenter med betydande påverkan på Eskilstuna kommuns nätverk.

Det har till viss del erbjudits utbildningar i informations- och IT-säkerhet som e-utbildning eller i föreläsningsform för att ge grundläggande kunskaper och kännedom om var och ens ansvar. Det har dock inte skett någon uppföljning över hur många som deltagit. En tillräcklig medvetenhet är väsentligt för att medarbetare ska kunna ta sitt ansvar för informations- och IT-säkerheten och upptäcka eventuella informationssäkerhetsincidenter när de inträffar. Idag saknas rutiner och process för hantering av incidenter och det finns inte någon översikt över hur stort antal incidenter som sker.

Vi ser det som positivt att flera åtgärder är planerade att genomföras för att förbättra organisationens IT- och informationssäkerhetsarbete. Vår bedömning utifrån vår

analysmodell CMA är att Eskilstuna kommun på kommunövergripande nivå i nuläget har en låg mognadsnivå och medvetenhet för IT- och informationssäkerhet där endast vissa nyckelpersoner har en hög medvetenhet och utför sitt arbete utifrån rådande förutsättningar.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Säkerställa att styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter revideras och uppdateras.
- Säkerställa att roller och ansvar mellan verksamheten, kommunstrateg informationssäkerhet och IT tydliggörs.
- Säkerställa att IT-avdelningen har kontroll på och ansvar för samtliga datorer som används i kommunens IT-miljö genom att dessa tillhandahålls med den paketering som är nödvändig utifrån ansvaret för IT-säkerhet
- Säkerställa att tillräcklig utbildning ges för att medvetandegöra informationssäkerhetsansvaret inom Eskilstuna kommun.
- Som ett krav för kommunens samtliga förvaltningsobjekt säkerställa att arbete med informationssäkerhetsklassning och riskhantering implementeras fullt ut.
- Säkerställa att kunskap finns och rutiner är kända över hantering och rapportering av informationssäkerhetsincidenter.
- Säkerställa att tekniska kontroller implementeras samt att identifierade sårbarheter från sårbarhetsscanningen bedöms och åtgärdas för att skydda Eskilstuna kommuns nätverk och motverka intrång.

2 Bakgrund

KPMG har av de förtroendevalda revisorerna i Eskilstuna kommun fått i uppdrag att genomföra en granskning av kommunens styrning och ledning av informationssäkerhetsarbete och tillhörande IT-säkerhetsåtgärder. Uppdraget ingår i revisionsplanen för år 2020.

Organisationer i offentlig sektor hanterar ovärderliga informationstillgångar och blir alltmer beroende av sina informationssystem. Ny teknik innebär nya möjligheter men introducerar även nya risker som ställer krav på ett balanserat risktagande och ett väl fungerande säkerhetsarbete. Brister i hanteringen kan bland annat leda till förtroendeskada för organisationen.

Informationssäkerhet innebär att skydda information utifrån krav på dess konfidentialitet, riktighet och tillgänglighet och att informationen ska skyddas mot obehörig åtkomst, såväl externt som internt. En avgörande parameter i arbetet för att säkerställa kommunens informationssäkerhetsarbete är att granska hur medveten och mogen organisationen är för att styra och leda sitt informationssäkerhetsarbete. Ansvaret finns hos var och en och berör hela organisationen varpå medvetenhet är väsentlig för en tillräcklig efterlevnad.

Hotbilden med risker för intrång förändras kontinuerligt och säkerhetsarbetet behöver därför vara en ständigt pågående process för att säkerställa att kommunens informationstillgångar har ett tillräckligt skydd. IT-säkerhet avser en avgränsad del av informations-säkerheten och består av delarna systemsäkerhet och kommunikationssäkerhet. Vidtagna IT-säkerhetsåtgärder ska stå i relation till informationstillgångarnas värde och de risker och behov som ansvariga för informationen har fastställt. Detta då IT-säkerheten avser att säkra och trygga driften och hanteringen av kommunens kärnverksamheter.

För att kunna hantera det på ett ändamålsenligt sätt krävs att kommunen har ett systematiskt informationssäkerhetsarbete där flera funktioner i kommunen är involverade och rätt organiserade för uppdraget.

Med anledning av ovanstående drar kommunens revisorer slutsatsen i sin riskanalys, att kommunens styrning och ledning av informationssäkerhetsarbetet behöver granskas.

2.1 Syfte, revisionsfråga och avgränsning

Granskningen har syftat till att konstatera om kommunstyrelsen säkerställt en tillräcklig mognad och medvetenhet i organisationen för sitt informationssäkerhetsarbete. Den syftar även till att bedöma om kommunen har processer, rutiner och ändamålsenlig kontroll över IT-säkerheten och att de åtgärder som vidtas baseras på risker och behov som ansvariga för kommunens informationstillgångar har fastställt.

Granskningen ska besvara följande revisionsfrågor:

- Har kommunstyrelsen tillsett att det finns aktuella styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter, som tydliggör vilka krav som ställs och hur arbetet ska bedrivas?
- Är roller och ansvar för informationssäkerheten tydliggjord och uppfattad mellan verksamhet och IT-organisation?
- Finns ett systematiskt arbete för att identifiera och analysera risker och behov för informationssäkerheten?
- Finns ett strukturerat arbete för att säkerställa en tillräckligt IT-säkerhet?
- Finns det former för att säkerställa efterlevnaden av beslutad IT-säkerhet?
- Görs systematiska uppföljningar av vidtagna IT-säkerhetsåtgärder för att upptäcka eventuella brister?
- Har kommunstyrelsen säkerställt en tillräcklig mognad och medvetenhet i organisationen för ett tillräckligt informationssäkerhetsarbete?

Granskningen avser kommunstyrelsen och samtliga nämnder avseende informationssäkerhetsarbetet och kommunstyrelsens ansvar för IT gällande IT-säkerhet.

Granskningen avser revisionsåret 2020.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller:

- Tillämpbara interna regelverk, policys och beslut
- MSB[1]s rekommendationer avseende Ledningssystem för informationssäkerhet
- NIS-direktivet i tillämpliga delar avseende kartläggning och analys av risker.

2.3 Metod

Granskningen har genomförts genom dokumentstudier och intervjuer med relevanta nyckelpersoner (se bilaga 1) inom Eskilstuna kommun. Som avslutning på granskningen genomfördes en hearing i syfte att återge de iakttagelser som gjorts under granskningen. Detta för att sätta kommunens nuläge i arbetet i relation till ett systematiskt informationssäkerhetsarbete i enlighet med gällande standards.

Vid hearingen deltog kommunstyrelsens presidium, kommundirektör, förvaltningschefer, kommunstrateg informationssäkerhet, IT-chef, IT-säkerhetsansvarig samt representanter från de förtroendevalda revisorerna och sakkunniga biträde från KPMG.

[1] Myndigheten för samhällsskydd och beredskap

Bedömning av mognadsgrad bygger på KPMG:s beprövade informationssäkerhetsramverk, *Cyber Maturity Assessment* (CMA) och omfattar sex områden:

- Ledarskap och styrning
- Mänskliga faktorer
- Information och riskhantering
- Kontinuitetshantering
- Drift och teknik
- Regelefterlevnad.

Vidare har en sårbarhetsscanning gjorts. Sårbarhetsscanningen har utförts genom planering inför genomförande med nyckelpersoner (se bilaga 1) från kommunen. Därefter har scanning av två interna nätverk genomförts via verktyget Nessus Professional. Identifierade sårbarheter har analyserats med stöd av KPMG:s egna script, för att säkerställa relevans, risk och prioritering.

Granskningen har genomförts av Jenny Thörn, kommunal revisor, Olivia Johansson, informationssäkerhetsexpert, Sofia Nacke, IT-säkerhetsexpert under ledning av kundansvarig certifierad kommunal revisor Mikael Lind.

3 Resultat av granskningen

3.1 Ledarskap och styrning

3.1.1 Policy och styrande dokument

Eskilstuna kommun har ett utkast till en IT-policy där det framgår att information- och IT-säkerhet ska ingå som en central del i IT-styrningen och IT-verksamheten för att säkerställa att information är ändamålsenligt skyddad i enlighet med tilldelad skyddsnivå. I utkast till IT-policy framgår det att koncernens verksamheter ska ha etablerade och kommunicerade kontinuitetsplaner som tar utgångspunkt i verksamhetens prioriterade behov. Kommunövergripande effekter ska uppnås genom effektiv och säker hantering av information.

Arbetet med informationssäkerhet i Eskilstuna kommun baseras på en Informationssäkerhetsplan som beslutades av kommunfullmäktige 2013-05-30, senast reviderad 2014-03-27. Dokumentet beskriver på övergripande nivå kommunens plan för informationssäkerhetsarbetet och de mål som ligger till grund för arbetet. Det framgår i intervjuer att planen inte aktivt har kommunicerats de senaste åren till medarbetare, däremot finns dokumentet tillgängligt på intranätet. Flera av de intervjuade belyser svagheten i att nuvarande styrdokument är gamla och inte längre relevanta för kommunens informationssäkerhetsarbete.

I dokumentet Riktlinjer för Eskilstuna kommuns IT-verksamhet som beslutades av kommunfullmäktige 2018-03-28, finns ansvarsfördelning tydliggjord och riktlinjerna syftar till att styra kommunens IT-verksamhet så att den uppnår uppsatta verksamhetsmål och blir så effektiv som möjligt.

Under intervjuer har det framkommit att det har initierats ett arbete i början av 2020 med att revidera, uppdatera och ta fram ny policy och styrdokument. I planeringen ingår även att tillhandahålla instruktioner om handhavande och utbildningar inom ramen för informationssäkerhet. I granskningen har vi tagit del av utkast till nya styrdokument. Dessa består av en Informationssäkerhetspolicy och fyra tillhörande anvisningar. Vid hearingen beskrivs att nya styrdokument ska följa ISO27000 och MSB:s rekommendationer. Det finns i nuläget ingen fastlagd plan för hur de nya styrdokumenten ska implementeras och göras kända i verksamheterna.

3.1.2 Roller och ansvar

Enligt MSB:s metodstöd för hur ett systematiskt informationssäkerhetsarbete ska bedrivas framgår det hur ansvaret för arbetet med informationssäkerhet bör fördelas. MSB betonar att varje organisation bör ha en utpekad person med ansvar för att samordna informationssäkerhetsarbetet. Eskilstuna kommuns organisationsstruktur för informationssäkerhet finns angivet i de två styrdokumenten Informationssäkerhetsplan och Riktlinjer för Eskilstuna kommuns IT-verksamhet.

Kommunledningsgruppen (KLG): har det övergripande ansvaret för informationssäkerheten inom Eskilstuna kommun och beslutar om informationssäkerhetsplanen och instruktioner för informationssäkerhet.

Kommunledningskontoret (KLK): ansvarar för informationssäkerhetsplanen med tillhörande instruktioner och att driften av Eskilstuna kommuns informationssystem sköts i enlighet med framtagen plan och instruktioner. Eskilstuna kommun har även en utpekad kommunstrateg informationssäkerhet som ansvarar för övergripande krav och rutiner gällande IT- och informationssäkerhet.

Konsult och uppdrag IT (KoU): ansvarar för att säkerställa att IT- och informationssäkerheten följer de grundkrav som finns i gällande lagstiftning och att basöverenskommelser och SLA[2]:er finns beskrivna. Vidare ansvar KoU för hanteringen av brandväggar, spamfilter, lösenord och övriga säkerhetsrutiner.

Verksamheten/förvaltningsorganisationen: ansvarar för förvaltningens informationssystem. Inom denna grupp finns en informationssäkerhetssamordnare som ansvarar för att respektive verksamhet/förvaltning följer anvisningar/riktlinjer informerar om säkerhetsfrågor och koordinerar nödvändiga utbildningsinsatser. Här ingår exempelvis systemägare, systemförvaltare, användare och brukare.

Styrgruppen IT (*Samrådsorgan):* består av kommunledningskontorets IT-chef, kommunstrateg informationssäkerhet, KoU IT:s områdeschef samt representanter från barn- och utbildningsnämndens och vård- och omsorgsnämndens förvaltningar. Styrgruppen verkar som ett stöd till IT-chefens beslutsfattande, utifrån framlagda beslutsunderlag avseende nya behov eller avsteg från gällande BAS-överenskommelse.

Under intervjuer framgår det att organisationen har förändrats sedan styrdokumenten beslutades vilket medför att roller och ansvar inte är tillämpligt i alla delar. Den enhet som uppges till stor del ansvara för IT-säkerheten, KoU IT, finns inte kvar som enhet i organisationen. Hänvisningar kring deras ansvar i dessa frågor kan vara otydligt då styrdokument och den praktiska hanteringen av IT-frågor inte överensstämmer i nuläget.

Intervjupersoner har även beskrivit att roller och ansvarsfördelning behöver förtydligas. Det saknas en tydlig inriktning och länk för vem som ansvarar för vad inom IT- och informationssäkerhet. I kommunens operativa arbete förekommer det etablerade nätverk med syfte att diskutera styrning, process och genomförande av IT- och informationssäkerhet. Det upplevs av intervjupersoner saknas en tydlig koppling och interaktion mellan kommunledningsgruppen och kommunledningskontoret samt styrgrupper och nätverk.

Det finns utsedda informationssäkerhetssamordnare på varje förvaltning men deras roll måste tydliggöras. Detta kommer att ske dels i nya styrdokument där roller ska beskrivas.

Vidare framkommer det genom intervjuer att det finns ett starkt personberoende till centralt utsedda roller där ett flertal personer hänvisar till att kommunstrateg informationssäkerhet är enskilt ansvarig för att införa ett systematiskt informationssäkerhetsarbete inom hela kommunen. Våra iakttagelser kring personberoendet bekräftades under den hearing som genomfördes där deltagarna inte kunde redogöra för hur ansvaret mellan verksamheterna, kommunstrateg informationssäkerhet och IT-avdelningen såg ut i kommunen. Där lyfter en av

[2] Service Level Agreement, detta är överenskommelser om teknisk support för att säkerställa en säker drift av verksamhetskänsliga informationssystem.

deltagarna att ansvaret mellan kommunstrateg informationssäkerhet och förvaltningarna behöver tydliggöras.

3.1.3 Strategi och vision

På Eskilstuna kommuns hemsida framgår det att kommunen ska ha en tydlig definierad inriktning för informationssäkerhet, där system har hög säkerhetsklass, medarbetarkunskap om ämnet och kontinuerligt uppdaterade kring nya krav och riktlinjer.

Utifrån insamlat material och intervjusvar framgår inte att en informationssäkerhetsstrategi och vision systematisk finns etablerad i kommunen. I enlighet med intervjusvar finns det en vision att strategiskt skapa ett ledningssystem för informationssäkerhet (LIS) för att kunna organisera och styra kommunen under respektive mandatperiod, detta arbete är påbörjat genom revidering av styrdokument och fortsätter sedan utifrån en planering som tagits fram av kommunstrateg informationssäkerhet och förankrats hos administrativ chef.

3.2 Mänskliga faktorer

En viktig del i ett systematiskt informations- och IT-säkerhetsarbete är att det finns en tillräcklig medvetenhet hos de som har tillgång till kommunens information. I kommunen är detta bland annat förtroendevalda, medarbetare, elever, externa konsulter och brukare.

3.2.1 Medvetenhet och förståelse

Vid intervjuerna har förståelsen för IT- och informationssäkerhet framställts som låg på kommunövergripande nivå. Förståelsen är hög hos enskilda med uppdrag att utveckla arbetet med kommunens Informations- och IT-säkerhet. Behovet av en ökad medvetenhet och gemensam förståelse kring informationssäkerhet har under ett flertal intervjuer lyfts och ett flertal intervjupersoner hänvisar saknaden av en förståelse för information som ett led av ett bristande ledarskap.

Vidare har det framkommit att det finns en stor utmaning kring att förmedla och kommunicera budskap till kommunens alla användare. Eskilstuna kommun har ett strukturerat intranät med definierade kommunikationskanaler, däremot saknas metodiskt stöd i att proaktivt arbeta med att förmedla säkerhetsaspekter generellt och således uppnå en kultur som bygger på ett systematiskt säkerhetsarbete.

På intranätet finns publicerad information om informationssäkerhet och exempel på informationsklasser och skyddsvärde för informationen. Det finns länkar till styrdokument, utbildning som erbjuds via Myndigheten för samhällsskydd och beredskap samt annan väsentlig information.

Kommunen har sedan två år tillbaka haft ett stort fokus på GDPR[3] vilket resulterat i att ett förtydligande av informationssäkerhet krävs för att skapa en förståelse för hur ett systematiskt säkerhetsarbete skall bedrivas.

[3] The General Data Protection Regulation, på svenska översatt till Den allmänna dataskyddsförordningen som 2018 ersatte tidigare Personuppgiftslag, PuL.

3.2.2 Utbildning

Det finns ett fåtal utbildningar inom ramen för IT- och informationssäkerhet. Dessa har dock varit begränsade till utbildningar för utförande av informationsklassningar och hantering av personuppgifter, och har endast genomförts för de användare inom kommunen vars arbete direkt påverkas av informationsklassningsrutinerna respektive innefattar personuppgiftshantering. Övergripande utbildning för kommunens anställda inom informationssäkerhet har till viss del genomförts och föreläsningar har erbjudits förvaltningarna av tidigare kommunstrateg för informationssäkerhet. Det har dock inte skett någon uppföljning av vilka som genomfört utbildning eller hur medvetenheten och kunskaper ser ut hos kommunens medarbetare.

Från intervjuer framgår en vision kring att kunna erbjuda en grundläggande e-utbildning, dock har ingen plan för genomförandet framställs.

3.2.3 Förmågor och kompetens

De resurser som på kommunövergripande nivå i huvudsak arbetar med Eskilstuna kommuns informationssäkerhet är kommunstrateg informationssäkerhet och säkerhetschefen, IT-chef och IT-säkerhetsansvarig. I genomförda intervjuer har det framförts att det finns ett behov av att utöka resurser avseende tid och kompetens inom informationssäkerhet på central nivå för att förbättra förutsättningarna att stödja förvaltningarna i deras utvecklingsarbete inom informationssäkerhet.

Liknande kompetens som efterfrågats på central nivå har i intervjuer efterlysts i verksamheternas organisationer. Vidare saknas en integration av informationssäkerhet i kommunens ordinarie processer. Med hänsyn till kommunens alla verksamhetssystem och korrelerande roller fattas emellertid systematik för att göra en korrekt helhetsbedömning av resurstillgången. Det pågår ett arbete med att tydliggöra kommunens arbete med systemförvaltning genom etablering av förvaltningsmodellen pm3. Anvisningar för detta finns i utkastform och ska fastställas. I intervjuer beskrivs att tanken med nya anvisningar för informationssäkerhet ska möta anvisningar för systemförvaltning i enlighet med pm3 och genom det förtydliga integrationen där emellan.

3.2.4 Anställningsprocess

Eskilstuna kommun har en central anställningsprocess och hanteras av rekryteringsenheten. Introduktionsprogram är dock ett ansvar hos anställande förvaltning och enhet att säkerställa för sina nya medarbetare. Kommunen ställer inga krav på att bakgrundskontroller utförs i samband med anställning. Kommunen har en ambition av att införa övergripande kontroller för efterlevnad av policy på anställda men saknar en konkret plan för verkställande. Följaktligen tillämpar kommunen inga disciplinära åtgärder utifrån gemensamma regler i de fall en anställd inte följer policys eller styrande dokument utan detta sker utifrån ansvarig chefs bedömning.

Genom granskningen har det även framkommit att kommunen saknar en process för säkerhetsklassning, vilket resulterat i att det finns ett pågående initiativ för att skapa policy och riktlinjer för säkerhetsskydd.

3.3 Information och riskhantering

3.3.1 Informationsklassificering

Kommunen tillämpar SKR:s KLASSA-verktyg i arbetet att identifiera och klassificera vilka av kommunens informationssystem som innehåller skyddsvärd information. Kommunen har under år 2020 tagit fram utkast på metodstöd för hur informationsklassningen skall genomföras och hanteras. Vidare belyser även metoden regler för undantagshantering.

Informationsklassning har genomförts med egen metod innan beslut om användning av KLASSA tagits. Det innebär att ett flertal system är klassade sedan tidigare men behov finns att revidera dessa utifrån nuvarande förutsättningar. Vid de klassningar som genomförts har medarbetare från IT, handläggare från verksamheten och systemförvaltare deltagit. Det pågår ett arbete med att utveckla en styrmodell i kommunen där systemförvaltning, IT-komponenter och verksamhetskomponenter ingår för att säkerställa att förvaltningsstödet möter användarnas behov. Informationsklassning är tänkt att ingå som aktivitet i denna styrmodell.

För befintliga externa leverantörer och redan upphandlade informationssystem har inga centrala riktlinjer för uppföljning av informationssäkerhet definierats. Regelbundna möten bedrivs med de externa leverantörerna med fokus på driftskaraktär. Informationssäkerhetsrelaterade ämnen är sällan en del av agendan.

Det finns en övergripande registerförteckning för kommunens IT-komponenter med information om förvaltningsobjektet. I förteckningen finns dokumenterat objektägare, förvaltare, registerförteckningen i enlighet med dataskyddsförordningen, klassning mm. Det framgår dock i intervjuer att förteckningen är i behov av uppdatering och att den ska göras mer känd i verksamheterna.

3.3.2 Riskhantering

Enligt Eskilstuna kommuns riktlinjer för IT-verksamheten är ambitionen att hitta en optimal balans mellan driftsäkra lösningar och anpassning till ny utveckling och snabba förändringar. Allt inom den ekonomiska ram som finns tillgänglig. Det ska ske en effektiv hantering av risker och angrepp på kommunens system. Från intervjuer framkommer det att risk- och sårbarhetsanalyser görs en gång per mandatperiod. Arbetet med risk- och sårbarhetsanalysen ska enligt kommunens plan för krisberedskap genomföras utifrån FORSA modellen (totalförsvarets forskningsinstitut FOI:s risk och sårbarhetsmodell). Vidare framgår det enligt krisberedskapsplanen att underlaget från analysen skall användas i samband med planering och genomförande av åtgärder för att öka förmågan att kontinuerligt bedriva samhällsviktig verksamhet samt stärka förmågan att hantera extraordinära händelser. I intervjuer framkommer att det finns behov av att revidera dessa planer gällande IT-området då alla verksamheter har ett stort behov av IT.

Utöver detta har det genomförts risk- och sårbarhetsanalyser av "särskilt känsliga system" samt hårdvara som server, lagring och nät. Det utförs även konsekvensbedömningar utifrån dataskyddsförordningen där utsett dataskyddsombud deltar.

3.3.3 Tredjepartsrisker

Tredjepartsrisker är de risker som en kommun exponeras mot eller kan exponeras mot som ett resultat av ett avtal med en annan part. Ofta benämns tredjepartsrisker i samband med utkontraktering eller outsourcing, det vill säga när en kommun sluter avtal med en leverantör om att utföra (helt eller delvis) en process, tjänst eller annan aktivitet som kommunen i annat fall själv skulle utföra.

I riktlinjer för IT-verksamheten finns beskrivning av anskaffning av IT-system eller ny funktionalitet. Det framgår i dessa att en dokumenterad förstudie med ett skriftligt beslutsunderlag ligger till grund för upphandlingen. Beslutsunderlaget skall bland annat innehålla en analys av risker och konsekvenser. Vidare skall KoU IT komplettera verksamhetsförstudien med en teknisk förstudie i samarbete med verksamheten. Den tekniska studien kan bland annat innehålla beskrivning av behörighets- och säkerhetssystem, förteckning enligt dataskyddsförordningen, genomförd risk- och konsekvensanalys och informationssäkerhetsklassning.

För de leverantörer som hanterar personuppgifter ställer dataskyddsförordningen krav på att personuppgiftsbiträdesavtal (PUB-avtal) med anvisningar för säker personuppgiftshantering och sekretess tecknas. I kommunens anvisningar för behandling av personuppgifter förmedlas personuppgiftsbiträdandes ansvar.

3.3.4 Behandling av personuppgifter

Eskilstuna kommun har efter dataskyddsförordningens (GDPR) införande i maj 2018 bedrivit ett kontinuerligt arbete för att nå efterlevnad av det nya lagkravet. Arbetet har bland annat resulterat i att rollen som dataskyddsombud (DSO) har tillsatts.

Kommunfullmäktige har beslutat om Riktlinje för behandling av personuppgifter i vilken den framgår att personuppgiftsansvariga ska upprätta en registerförteckning som visar vilka personuppgiftsbehandlingar som hanteras. Därigenom ska varje nämnd ha en samlad registerförteckning för sina personuppgiftsbehandlingar.

Vidare har kommunen i enlighet med krav i dataskyddsförordningen, valt att klassificera personuppgifter enligt ”känsliga” och ”extra skyddsvärda personuppgifter”. Klassificeringen görs enligt en konsekvensbedömning där risker identifieras samt handlingsplan tas fram.

För dokumentation, gallring och arkivering har krav definierats där respektive personuppgiftsansvarig skall ansvara för registrering av dokument i kommunens dokument- och ärendehanteringssystem. Det förekommer inga riktlinjer kring efterlevnad och uppföljning av uppgifterna.

Personuppgiftsincidenter skall rapporteras till respektive förvaltnings dataskyddssamordnare via Internportalen. För rapportering av incidenter har kommunen definierade instruktioner och formulär för hur personuppgiftsincidenter skall registreras och hanteras.

3.4 Kontinuitetshantering

Eskilstuna kommun har i informationssäkerhetsplanen en dokumenterad strategi för att uppnå övergripande mål. En del av denna strategi är att krishanteringsförmågan upprätthålls. Eskilstuna kommun hanterar stora mängder information och data vilka

levereras av kommunens tekniska resurser. Att information och data är tillgängligt vid behov inom kommunens verksamhetsområden är således av hög relevans.

3.4.1 Kontinuitetsplan

Riktlinjer för Eskilstuna kommuns IT-verksamhet fastställdes 28 mars 2018 och klargör att KoU IT enhet ansvarar för att upprätta och vidmakthålla kontinuitetsplanering avseende IT infrastruktur. Den beslutade informationssäkerhetsplanen beskriver att kontinuitetansvaret innebär att säkra organisationens förmåga att upprätthålla och återstarta erforderlig teknik och tjänster inom överenskommen tid och med bibehållen kvalitet. Driftansvariga inom kommunen ansvarar för den tekniska driften av ett informationssystem. Systemsäkerhetsanalys ska genomföras för samtliga verksamhetskritiska system, där fördjupande drift/kontinuitetsinstruktioner skall tas fram. Vidare beskrivs att alla som nyttjar kommunens IT-resurser ska genomgå den utbildning som krävs, vilken ska följas upp och kompletteras vid behov, för att informationssäkerheten ska upprätthållas. Även i utkast till IT-policy finns beskrivning att etablerade och kommunicerade kontinuitetsplaner utefter verksamhetens behov ska finnas för koncernens verksamheter.

Intervjusvar visar att kommunens förvaltningar självständigt ansvarar för framtagande av en eller flera kontinuitetsplaner som godkänns av respektive förvaltningschef alternativt ledningsgrupp. Vidare framkommer det under intervjuer att enskilda förvaltningars kontinuitetsplanering är beroende av bibehållen drift av IT och digitala system, vilket står under IT-förvaltningens ansvar.

Granskningen har genom intervjusvar samt erhållen dokumentation kunnat fastställa att en övergripande och gemensam kontinuitetsplan för kommunen saknas. Intervjusvar samt dokumentation visar att strukturerad testning och/eller övning av kontinuitetsplaner inte är ställt som krav och därmed ej utförs. Utbildning inom området kontinuitet med syfte att upprätthålla informationssäkerheten har heller inte genomförts.

3.4.2 Incidenthantering

I informationssäkerhetsplanen beskrivs att händelser i informationssystem som kan leda till negativa konsekvenser skall förebyggas och incidenter av betydelse för informationssäkerheten ska loggas. I kommunens utkast för IT-policy beskrivs att IT-verksamheten ska ha tillämpliga och dokumenterade rutiner för systemåterställning efter allvarliga incidenter. Granskningen har mottagit tre dokument, skrivna i rapportformat utan information om ansvarig, innehållande logg över händelser i Eskilstuna kommuns nätverk och datatrafik.

I intervjuer framkommer att det i nuläget inte finns en tydliggjord process och rutin för informationssäkerhetsincidenter. Vid hearingen som genomfördes som en del i granskningen bekräftades att kunskap om incidenter samt kännedom om rutiner för hantering av sådana när de uppkommer är angeläget att förankra i kommunen. Deltagare under hearing anger att det antagligen finns ett stort mörkertal över inträffade incidenter som helt enkelt inte upptäcks i verksamheterna. Det finns ingen dokumentation över inträffade informationssäkerhetsincidenter och det är inte känt hur många incidenter som faktiskt sker då kunskap och medvetenhet om detta inte är etablerat i verksamheten för att identifiera incidenter.

Ett arbete pågår för att förtydliga processen av informations- och it-säkerhetsincidenter.

3.4.3 Rapportering och eskalering

Vid misstänkt, pågående eller bekräftad incident ska denne eskaleras och rapporteras till funktionen IT-kundservice för vidare åtgärd. Vid incidenter som bedöms som allvarliga ska dessa rapporteras löpande till IT-chef och kommunstrateg informationssäkerhet. Under intervjuer framkommer en osäkerhet över hur eskaleringsrutiner ska fungera vilket påvisar att kommunen saknar en systematik och regelbunden efterlevnad gällande dokumenterade rutiner och processer för incidentrapportering och eskaleringsvägar.

3.5 Drift och teknik

IT-avdelningen hanterar och levererar tjänster inom IT som står till stöd för det strategiska arbetet samt den operativa verksamheten. Med stöd av IT-komponenter skall kommunen uppnå de kommunövergripande verksamhetsmålen, vilket medför att drift och teknik ses som en av kommunens viktigaste resurser.

I informationssäkerhetsplanen framgår att kommunens strategi är att investeringar i form av informationshantering och teknisk utrustning ska skyddas i tillräcklig grad, att infrastruktur för extern och intern data-kommunikation ska vara väl definierad, gemensam och säker, samt att dokumentation ska finnas för alla IT-system.

3.5.1 Fysisk säkerhet

Informationssäkerhetsinstruktion Systemägare, vilken är upprättad 20 juni 2014, fastslår att fysiskt tillgängliga tekniska resurser vilka innehåller informationssystem och nyttjas av Eskilstuna kommun ska driftas i låsta utrymmen samt med korrekt stöd för att hantera dess funktionalitet. In- och utpassering ska kontrolleras med system och ansvarig enhetschef hos KoU - IT står som ansvarig för att besluta om tillgång till serverhallar. Vidare beskriver dokumentet att underleverantörers tillgång till serverhallar ska redovisas i överenskommelse och lagringsmedia ska hanteras på ett lämpligt sätt för att säkerställa att data inte går att återskapa.

I användarinstruktion kund, brukare, externa konsulter, upprättad 30 juni 2014, har Eskilstuna kommun fastställt att tillgång till kommunens nätverk och/eller informationssystem ska kräva identifiering. Ansvaret för behörigheter till dessa är delat mellan systemförvaltare och IT-avdelningen. Det ser olika ut mellan förvaltningarna hur hanteringen fungerar och även om det sker några kontroller eller inte av tilldelade behörigheter. Det är oftast delegerat till systemförvaltare att genomföra kontroll att rätt behörigheter finns. För vissa system sker en loggkontroll över tillgång till information för enskilda. Det framkommer vid hearingen att denna rutin behöver utvecklas för de informationssystem som har skyddsvärd information med känsliga uppgifter.

Intervjusvar bekräftar att tillgång till kommunens lokaler, för anställda, kräver identifiering med individuella passerkort samt lösenordskrav. Tillgång till kommunens lokaler för besökare är begränsat genom separerad fysisk miljö.

3.5.2 IT-säkerhetsåtgärder

Intervjusvar visar att Eskilstuna kommun nyttjar brandväggar för att skilja servernät från klientnät. Kommunen nyttjar även Windows Defender för skydd mot virus. Detta skydd

är dock enbart applicerbart för de datorer som IT-avdelningen tillhandahåller och har getts möjlighet att paketera med de tjänster och system som anses nödvändiga för en tillräcklig IT-säkerhet. För dessa datorer har IT-avdelningen administratörsrättigheter vilket minskar möjligheten till enskilda att ladda ner information som skulle kunna orsaka skada. Mottagen dokumentation samt intervjusvar kan däremot inte bekräfta hur många datorer det finns med tillgång till kommunens information som inte har detta skydd.

Samtliga användardatorer i kommunens nätverk ska övervakas och regelbundet kontrolleras för att säkerställa att dessa är uppdaterade och att säkerheten fullgod. Vidare ska lagringsmedia från uttjänta servrar destrueras på lämpligt sätt så att data ej går att återskapa. Intervjusvar visar att kryptering ej nyttjas som standard.

3.5.3 Testning och utveckling

Intervjusvar visar att kommunen bedriver egen utveckling i liten utsträckning, merparten av all utveckling sker genom nyttjandet av externa konsulter. Utveckling ska ske genom tre separata miljöer: produktionsmiljö, verifieringsmiljö och icke produktionsmiljö. Utveckling samt uppdatering tillåts på så vis att ske utan påverkan på den operativa driften. Intervjusvaren visar dock att kommunens förvaltningar själva avgör vilka miljöer som dess utveckling ska ske i, således har granskningen inte tagit del av en kommunövergripande rutin för utveckling.

Vidare visar intervjusvaren att en strukturerad testning av tekniska miljön, genom sårbarhetsscanning alternativt penetrationstestning, inte genomförs. Det sker dock en viss testning av tekniska miljön ur ett riskbaserat perspektiv utifrån behov som uppstår.

3.6 Regelefterlevnad

3.6.1 Regelverk och legala krav

Kommunens informationshantering är till stor del reglerad av lagar och förordningar, till exempel Tryckfrihetsförordningen, Offentlighet- och sekretesslagen, Dataskyddsförordningen, Arkivlagen, Säkerhetsskyddslagen och Patientdatalagen. Kommunen arbetar systematiskt med dokumentation för att säkerställa regelefterlevnad. Vidare har granskning för huruvida Eskilstuna Kommun lever upp till diverse regelverk har inte gjorts.

3.6.2 Standarder och certifiering

Eskilstuna kommuns informationssäkerhetsplan tar hänsyn till ISO/IEC 27000-serien där målsättningen är att alla informationssystem minst skall uppfylla den basnivå för informationssäkerhet som rekommenderas i standarden. I intervjuer framgår det dock att kommunen i enlighet med gällande principbeslut att inte certifiera verksamheten mot standarder inte heller har för avsikt att certifiera sig enligt ISO/IEC 27000-serien. Granskning för huruvida kommunen efterlever basnivån för informationssäkerhet enligt ISO/IEC 27000-serien har inte gjorts.

3.6.3 Efterlevnad av krav

Granskningen har inte fått ta del av dokumentation rörande stickprov, tillsyn eller kontroll för att kommunen efterlever regelverk och legala krav inom ramen för informationssäkerhet.

3.6.4 NIS-direktivet

Under genomförda intervjuer har det framförts att en avsaknad av samstämmighet råder kring om kommunen lyder under NIS-direktivet. Kommunen ska ha påbörjat ett arbete för att identifiera om verksamheten bedriver samhällsviktiga tjänster som är av rapporteringspliktig karaktär till MSB.

I samband med genomförandet av hearing framkommer att kommunen har identifierat verksamheten inom hälso- och sjukvård som samhällsviktig och därmed lyder under NIS-direktivet. Kommunen har även verksamhet som drivs i bolagsform inom VA och energi som är identifierad som samhällsviktig.

Kommunen har inte vidtagit några särskilda säkerhetsåtgärder sedan denna bedömning gjordes.

4 Sårbarhetsscanning

Den 1 juni 2020 genomförde vi som en del i granskningen en sårbarhetsscanning där två interna nät scannades. Resultatet genererade en rapport där sårbarheter, beroende på nivå av relaterad risk, klassificerades. Sårbarhetsklassificeringen är indelad i fyra kategorier: kritisk, hög, medium och låg. Genomförd scanning listar sårbarheter där eventuellt ytterligare teknisk analys krävs för att verifiera nivå av sårbarhet och risk för konsekvens. I granskningsresultatet har vi valt att inkludera sårbarheter oavsett dess potentiella behov av verifiering. Vidare har granskningen valt att enbart lista sårbarheter kategoriserade som kritiska och höga.

Antalet identifierade unika sårbarheter med klassificering kritisk uppgår till 10. Majoriteten av dessa sårbarheter grundar sig i ett behov av att uppdatera programvara för att minimera risken att drabbas av incidenter med betydande påverkan på Eskilstuna kommuns nätverk (se bilaga 3 för detaljer kring sårbarheter).

Antalet identifierade unika sårbarheter med klassificering hög uppgår till 36. Del av dessa sårbarheter grundar sig i ett behov av uppdaterad programvara, patchning, kryptering och åtkomstpunkter.

Genom resultatet av sårbarhetsscanningen framgår det att Eskilstuna kommun bör se över sårbarheter i de två scannade interna nätverken. Vidare har sårbarhetsscanningen identifierat risker som kan leda till allvarliga incidenter, således bör Eskilstuna kommun se över kommunens förmåga att identifiera, motverka och hantera incidenter.

Granskningsresultatet redovisas inte vidare i denna rapport utan i en enskild bilaga då informationen är säkerhetsklassad och hanteras enligt gällande rutiner för detta.

5 Bedömning, slutsats och rekommendationer

5.1 Bedömning

Har kommunstyrelsen tillsett att det finns aktuella styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter, som tydliggör vilka krav som ställs och hur arbetet ska bedrivas?

Nej. Vår bedömning baserat på styrdokument och intervjuades beskrivning är att flertalet av de styrande dokument och policys som finns tillgängliga är ofullständiga, föråldrade och inte fullt ut tillämpbara. Däremot pågår ett arbete av kommunstrateg informationssäkerhet att se över alla styrande dokument, policys, handhavande och utbildningar inom ramen för informationssäkerhet under år 2020.

Är roller och ansvar för informationssäkerheten tydliggjord och uppfattad mellan verksamhet och IT-organisation?

Delvis. Eskilstuna kommun har definierat roller och ansvar för IT-verksamheten där vissa delar inom IT- och informationssäkerhet omfattas. Däremot saknas ett tydliggörande av roller och ansvar i riktlinjerna för informationssäkerhet. Vi bedömer det som en risk att det saknas en tydlig koppling mellan verksamhet och IT-organisation.

I Eskilstuna kommun finns även ett starkt personberoende till centralt utsedda roller, både inom IT- och informationssäkerhet vilket vi ser som en risk i kommunens arbete att införa ett systematiskt säkerhetsarbete.

Finns ett systematiskt arbete för att identifiera och analysera risker och behov för informationssäkerheten?

Delvis. Risker avseende IT- och informationssäkerheten har lyfts i kommunens riskanalys. Inom kommunen finns det även en definierad process för risk- och sårbarhetsanalyser som genomförs i enlighet med FORSA-modellen varje mandatperiod. Kommunen genomför även informationssäkerhetsklassningar av en del system, dock är inte processen, metoden och arbetet fullt implementerat i verksamheten. Vår bedömning är således att kommunens verksamheter arbetar med att identifiera och analysera risker för informationssäkerheten men att detta än så länge inte sker systematiskt.

Finns ett strukturerat arbete för att säkerställa en tillräckligt IT-säkerhet?

Delvis. Genom intervjuer samt genomförd sårbarhetsscanning kan granskningen bekräfta att Eskilstuna kommun har implementerat tekniska kontroller för att begränsa möjligheten för aktörer att påverka IT-miljön. Vid intervjuer har det framkommit att det förekommer datorer som inte IT-avdelningen styr över. Därigenom har de inte implementerat de tjänster och system som de anser nödvändiga ur ett säkerhetsperspektiv för att ta sitt ansvar för IT-säkerheten. Därtill finns även möjlighet att upprätta lokala administratörer på datorer som förekommer i Eskilstunas kommuns IT-miljö som inte IT-avdelningen kan övervaka aktiviteten för. Vi bedömer detta som en betydande risk för IT-säkerheten. Därtill har granskningen inte tagit del styrande

dokumentation rörande gällande rutiner, processer, testning, kontroller och IT-system som gjorts för att säkerställa ett strukturerat arbete inom området IT-säkerhet.

Vår bedömning är således att kommunen arbetar med att öka den tekniska IT-säkerheten men att tillräckliga förutsättningar att säkert kontrollera klienter inom kommunens nätverk saknas. Vidare är vår bedömning att konkreta former saknas för att säkerställa strukturerat arbete för tillräcklig IT-säkerhet.

Finns det former för att säkerställa efterlevnaden av beslutad IT-säkerhet?

Delvis. Kommunen har utifrån vissa styrdokument utvecklat handlingsplaner för att säkerställa efterlevnaden av beslutad IT-säkerhet, exempelvis behandling av personuppgifter. Däremot har granskningen inte fått ta del av dokumentation rörande stickprov, tillsyn eller kontroller som gjorts för att säkerställa att kommunen efterlever regelverk och legala krav inom ramen för informationssäkerhet. Vår bedömning är således att kommunen saknar konkreta former för att säkerställa efterlevnaden av beslutad IT-säkerhet.

Görs systematiska uppföljningar av vidtagna IT-säkerhetsåtgärder för att upptäcka eventuella brister?

Nej. Eskilstuna kommun kontrollerar att system och programvara som nyttjas fungerar i enlighet med kommunens behov, där kontroller utförs med huvudsakligt syfte att säkerställa kommunens funktionalitet. Granskningen har inte tagit del av dokumentation eller information som styrker att systematiska uppföljningar genomförs av vidtagna IT-säkerhetsåtgärder i syfte att upptäcka eventuella brister.

Vår bedömning är att kunskap om IT-säkerhetsrisker samt prioritering av kontroller för att minimera dessa inte sker i tillräcklig utsträckning. Vidare bedömer vi att Eskilstuna kommun saknar konkreta former för att möjliggöra ett systematiskt arbete för uppföljning av vidtagna IT-säkerhetsåtgärder.

Har kommunstyrelsen säkerställt en tillräcklig mognad och medvetenhet i organisationen för ett tillräckligt informationssäkerhetsarbete?

Nej. Eskilstuna kommun saknar en gemensam förståelse för IT- och informationssäkerhet. Behovet av en ökad medvetenhet och gemensam förståelse kring informationssäkerhet har under ett flertal intervjuer med nyckelpersoner lyfts som avgörande för hur kommunen ska få ett systematiskt arbete inom detta. Bristen på mognad och medvetenhet visar sig dels i att det saknas kunskap om vad som är informationssäkerhetsincidenter och därför inte upptäcks och rapporteras.

Vidare har utbildningar inom ramen för IT- och informationssäkerhet endast till viss del erbjudits genom e-utbildning och föreläsningar. Det har inte skett någon uppföljning över antal som deltagit eller att tillräckliga kunskaper och medvetenhet erhållits genom de insatser som genomförts.

Vår bedömning är därmed att det saknas en tillräcklig mognad och medvetenhet i organisationen. Vår bedömning stärks av KPMGs beprövade Cyber Maturity

Assessment (CMA) ramverk som visar att Eskilstuna kommun saknar tillräckliga skyddsmekanismer för att identifiera, upptäcka, skydda, hantera och återhämta vid ett angrepp.

Eskilstuna kommuns mognadsnivå i förhållande till gällande standard för informationssäkerhet ISO/IEC 27001 visar att kommunens IT- och informationssäkerhetsarbete är i ett inledande stadie. Inom vissa områden finns definierade processer och rutiner med repetitiva uppgifter medan andra områden sker ad-hoc och saknar kontroll.

5.2 Slutsats

Vår sammanfattade bedömning utifrån granskningens syfte är att kommunstyrelsen inte har säkerställt ett ändamålsenligt och systematiskt arbete med IT-och informationssäkerhet. Flertalet av de styrande dokumenten är ofullständiga, föråldrade och inte fullt ut tillämpbara. Vidare bedömer vi att det saknas ett tydliggörande av roller och ansvar i gällande styrdokument. Kommunen har ett starkt personberoende till respektive roll vilket vi bedömer som en risk för att införa ett systematiskt säkerhetsarbete. Inom området drift och teknik bedömer vi att det saknas dokumenterade processer, riktlinjer och systemspecifikationer för att möta Eskilstuna kommuns målsättning gällande IT- och informationssäkerhet. Övriga verksamhetsområden är beroende kommunens IT-verksamhet, varav vi bedömer bristen på styrdokumentation inom drift och teknik som en risk vad avser kontinuitets- och avbrottshantering.

Vi bedömer det som positivt att flera åtgärder har och är planerade att genomföras för att förbättra organisationens IT- och informationssäkerhetsarbete. Beslut har tagits om införande av en informationsklassningsmodell med tillhörande hanteringsanvisningar. Däremot är arbetet med klassningen inte fullt implementerad i kommunen. Vidare arbetar kommunen med risk-och sårbarhetsanalyser som genomförs varje mandatperiod samt till viss del riskbedömningar av IT-komponenter utifrån behov. Vår bedömning är således att kommunens verksamheter arbetar med att identifiera och analysera risker för IT- och informationssäkerheten men att detta än så länge inte sker systematiskt.

Det råder även en brist för en gemensam förståelse, plan och vision för IT- och informationssäkerhet. Vidare behöver kommunen genomföra ytterligare utbildningar och informationsinsatser inom området informationssäkerhet som personal och användare av kommunens tekniska resurser kan ta del av. Vår bedömning är således att kommunstyrelsen för Eskilstuna kommun inte säkerställt en tillräcklig mognad och medvetenhet i organisationen för sitt IT- och informationssäkerhetsarbete.

5.3 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Säkerställa att styrande dokument, såsom policy med tillhörande tillämpningsföreskrifter revideras och uppdateras.
- Säkerställa att roller och ansvar mellan verksamheten, kommunstrateg informationssäkerhet och IT tydliggörs.
- Säkerställa att IT-avdelningen har kontroll på och ansvar för samtliga datorer som används i kommunens IT-miljö genom att dessa tillhandahålls med den paketering som är nödvändig utifrån ansvaret för IT-säkerhet
- Säkerställa att tillräcklig utbildning ges för att medvetandegöra informationssäkerhetsansvaret inom Eskilstuna kommun.
- Säkerställa att arbete med informationssäkerhetsklassning och riskhantering implementeras fullt ut.
- Säkerställa att kunskap finns och rutiner är kända över hantering och rapportering av informationssäkerhetsincidenter.
- Säkerställa att tekniska kontroller implementeras samt att identifierade sårbarheter från sårbarhetsscanningen bedöms och åtgärdas för att skydda Eskilstuna kommuns nätverk och motverka intrång.

2020-08-31

KPMG AB

Jenny Thörn	Mikael Lind
Kommunal revisor	Kundansvarig certifierad kommunal revisor

Bilaga 1: Intervjupersoner och dokumentgranskning

Intervjuade roller:

- CIO/IT-chef
- Kommunstrateg informationssäkerhet
- IT-säkerhetsansvarig
- Kommunstrateg HR
- Säkerhetschef
- Administrativ direktör IT
- IT-strateg
- Objektledare verksamhet
- Objektledare IT
- Enhetschef IT
- Områdeschef IT

Dokumentation:

Titel	Datum för fastställande	Ansvarig	Dokumenttyp
2020 Januari	2020-01-30	Saknas	Rapport
2020 Februari	2020-02-30	Saknas	Rapport
2020 Mars	2020-03-30	Saknas	Rapport
Användarinstruktion Förskola, Skola, Vuxenutbildning	2014-10-21	KLK	Instruktion
Användarinstruktion Informationssäkerhet användare, medarbetare och förtroendevalda	2014-06-02	KLK, HG	Instruktion
Användarinstruktion Kund, Brukare, Externa konsulter	2014-06-30	KLK	Instruktion
Basöverenskommelse infrastruktur 2020, SEF IT	2019-11-18	KLK	Riktlinje
Informationsklassning hanteringsregler	Saknas	Saknas	Riktlinjer

Informationssäkerhetsinstruktion Förvaltning, systemägare	2014-06-30	KLK	Instruktion
Informationssäkerhetsplan för Eskilstuna kommun	2014-03-27	KLK	Plan
IT-policy Eskilstuna kommun, utkast	Saknas	KLK	Policy
Plan för Eskilstuna kommunkoncerns IT-utveckling, utkast	Saknas	KLK	Plan
Riktlinjer för behandling av personuppgifter	2019-05-16	KF	Riktlinjer
Riktlinjer för Eskilstuna kommuns IT-verksamhet	2018-03-28	KF	Riktlinjer
Riktlinjer för anskaffning av IT KSKF, utkast	2020	KLK	Riktlinjer
Riktlinjer för utkontraktering av IT KSKF, utkast	2020	KF	Riktlinjer
Rutin kapad e-post	2020-03-03	KLK	Instruktion
Plan för Krisberedskap	2020	KF	Plan