Uppföljande granskning av IT-säkerhet

Rapport

Piteå kommun

KPMG AB

2022-02-02

Antal sidor 9

Piteå kommun
Uppföljande granskning av

2022-02-02

Innehållsförteckning

Piteå kommun
Uppföljande granskning av

2022-02-02

1 Sammanfattning

Vi har av Piteå kommuns revisorer fått i uppdrag att genomföra en uppföljande granskning gällande IT-säkerhet som genomfördes år 2019. Uppdraget ingår i revisionsplanen för år 2021.

Syftet med granskningen är att med utgångspunkt i den tidigare genomförda granskningen kring IT-säkerhet (2019) bedöma om kommunen i nuläget har en IT-säkerhet som är baserad på de risker som finns inom kommunens olika verksamheter.

Vår sammanfattande bedömning utifrån granskningens syfte är att det till viss del finns en tillfredsställande IT-säkerhet däremot kan den stärkas ytterligare genom en tydligare systematik.

Vi kan konstatera att det skett ett arbete för att rusta upp och organisera sig kring IT-säkerhetsarbetet. Detta har bidragit till stegförflyttningar framåt i IT-säkerhetsarbetet och vi bedömer att det finns en bra organisation och struktur kring säkerhetsarbetet vilket möjliggör ett systematiskt arbetssätt kring IT-säkerheten. Vi bedömer även att det finns en tydlig roll och ansvarsfördelning kring arbetet med IT-säkerhet.

Vi kan dock konstatera att det fortfarande bedrivs ett arbete med att upprätta och förvalta relevanta styrande dokument som tydliggör kommunens IT-säkerhetsarbete. Vi noterar att arbetet inte färdigställts ännu och att detta främst beror på att informationssäkerheten ska bygga på den nya ISO-standarden. Vi ser dock allvarligt på att påtalade brister gällande de styrande dokumenten kring IT-säkerheten ännu inte är åtgärdade.

Vi bedömer att det finns upprättade samverkansforum för att kunna arbeta strategiskt men även för att kunna hantera uppkomna problem i det dagliga arbetet samt bolla tankar och idéer. Vi konstaterar dock att det inte skett några riktade utbildningar kring IT-säkerhet, vi noterar däremot att det finns en tanke kring att under hösten 2022 genomföra en obligatorisk utbildning. Vi bedömer att det är av vikt att det upprättas en systematik kring IT-säkerheten där utbildningar bör utgöra en naturlig del i det systematiska arbetet kring IT-säkerheten. Vi rekommenderar därför att kommunstyrelsen ser över och säkerställer en systematik kring IT-säkerheten.

Det pågår arbete med att färdigställa kontinuitetsplaneringen vilket vi bedömer är av vikt för att säkerställa en tydlig struktur och minska sårbarheten kring de olika IT-systemen.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- se över och säkerställa ett systematiskt arbete kring IT-säkerheten, se avsnitt 3.1 och 3.2

2 Inledning/bakgrund

Vi har av Piteå kommuns revisorer fått i uppdrag att genomföra en uppföljande granskning gällande IT-säkerhet som genomfördes år 2019. Uppdraget ingår i revisionsplanen för år 2021.

Piteå kommuns revisorer har med utgångspunkt i sin risk- och väsentlighetsanalys gjort bedömningen att det är angeläget att genomföra en uppföljande granskning på området.

2.1 Syfte, revisionsfråga och avgränsning

Syftet med granskningen är att med utgångspunkt i den tidigare genomförda granskningen kring IT-säkerhet (2019) bedöma om kommunen i nuläget har en IT-säkerhet som är baserad på de risker som finns inom kommunens olika verksamheter.

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?
- Har kommunstyrelsen tillsett att det finns ett strukturerat arbete för att säkerställa en tillräcklig IT-säkerhet?
- Finns det former för att säkerställa efterlevnaden av beslutad IT-säkerhet?

Granskningen avser kommunstyrelsen.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller

- Kommunallagen 6 kap § 6
- Tillämpbara interna regelverk och policys

2.3 Metod

Granskningen har genomförts genom:

- Dokumentstudier av relevanta dokument såsom LIS – uttalande om tillämplighet, Digitaliseringsplan, policy för intern kontroll och styrning samt rutin för incidenthantering
- Intervjuer med berörda tjänstemän däribland IT-chef, teamledare IT-drift, teamledare IT-service samt informationssäkerhetsstrateg/dataskyddsombud.

Rapporten är faktakontrollerad av IT-chef, teamledare IT-drift, teamledare IT-service samt informationssäkerhetsstrateg/dataskyddsombud.

3 Resultat av granskningen

Granskningen bygger på de rekommendationer som lämnades vid granskningen av IT-säkerhet under 2019. Vid denna granskning konstaterades att kommunstyrelsen inte tillsett att det finns aktuella styrande dokument som tydliggör vilka krav som ställs och hur arbetet med IT-säkerhet ska bedrivas. Vidare framgick att IT-enheten saknar en modern och verksamhetsanpassad uppdragsbeskrivning som anger eget och kommungemensamt ansvar för IT-säkerheten.

Vid granskningen fastställdes det även att det fanns risk för att tidplanen för att lämna in risk- och sårbarhetsanalysen (RSA) till länsstyrelsen inte kan hållas.

3.1 Styrning och ansvar

Det har sedan 2019/2020 skett ett stegvis arbete för att organisera sig och rusta kommunen för att organisera IT-säkerhetsarbetet. Det har bl.a. upprättats Teamledare inom IT-service och IT-drift samtidigt som två nya informationssäkerhetsstrateger (säkerhetsskyddschef samt dataskyddsombud) tillträtt under våren 2021.

Det framgår att IT-chefen har det yttersta ansvaret för utveckling, implementation samt underhåll av IT-avdelningens arbete med IT-säkerhet. Ledningen inom IT-avdelningen ansvarar för att utveckla säkerhetsarbetet samt upprätta mötesformer som stimulerar analys och reflektion över händelser och resultat. Teamledarna ansvarar för kunskaps- och informationsspridning i teamen i syfte att stimulera utvecklande och förbättrande arbetssätt. Teamledarna har även ansvar över att se till att arbetsområdesfördelningen och övriga nödvändiga åtgärder regelbundet ses över och revideras vid behov.

Enligt intervjuade bedrivs ett aktivt arbete med att upprätta och förvalta relevanta styrande dokument som förtydligar kommunens informationssäkerhetsarbete. Det har under 2021 skett revideringar och analyser som identifierat vilka utvecklingsbehov som finns. Framförallt har det identifierats att det finns behov av att upprätta ytterligare styrande dokument. En stor anledning till varför detta arbete dröjer är enligt intervjuade för att det finns en tanke om de styrande dokumenten ska bygga på avsnittsstrukturen i den kommande versionen av standarden ISO 27002[1]. I nuläget arbetar kommunen med stöd av styrningen från ISO 27001[2]. Det har varit ett tydligt fokus på att revidera de användarnära dokumenten för att säkerställa att användarinformationen är relevant. Det sker ett arbete med att se över styrningen inom IT-avdelningen ur ett drift och kommunikationssäkerhetsperspektiv. Det har även skett ett arbete kring systemförvaltningsmodellen att säkerställa ett förtydligande av anskaffningsprocessen och kravställningen kring upphandlingar. Detta arbete är dock inte formaliserat och godkänt vid intervjutillfället. Det har enligt intervjuade sedan organisationen skapades varit ett tydligt fokus att identifiera och applicera ett systematiskt arbetssätt. Detta för att kunna ta fram relevanta policys, rutiner, riktlinjer etc. Det finns även framtaget en intern rutin kring hur styrande dokument tas fram.

[1] Uppdaterad version av ISO 27001, Förväntas utges i januari 2022
[2] ISO/IEC-standard från Information Security Management System (ISMS) gällande informationssäkerhet publicerat av internationella standardorganisationen (ISO) och den internationella elektrotekniska kommissionen (IEC).

Vi har tagit del av ett utkast för säkerhetsåtgärder inom IT-avdelningen som syftar till att beskriva de tekniska och organisatoriska säkerhetsåtgärder och kontroller som IT-avdelningen utför för att skydda personlig data, personuppgifter, säkerställa konfidentialiteten, integriteten och tillgängligheten av kommunens produkter och tjänster samt det fysiska skyddet som omger avdelningens IT-utrymmen.

Enligt intervjuade kommer den nuvarande informationssäkerhetspolicyn att revideras för att ge tydliga och konkreta instruktioner om vilken nivå informationssäkerheten ska ligga på samt att denna kommer att kompletteras med tillämpningsföreskrifter. Tanken är att ta stöd av internationella standarder för att på ett bättre sätt kunna implementera ett IT-ramverk. Det framgår även av intervjuade att roll och ansvarsbeskrivningen inte är aktuell och det finns en tanke om att kunna säkerställa att kommunen i policyn tar höjd för dataskyddsansvaret.

Systemförvaltningsmodellen baserad på PM3[3] är under uppbyggnad där utvecklingsenheten ansvarar för upprättande och förvaltning av modellen. Enligt uppgifter finns styrgrupper etablerade inom kommunledningsförvaltningen för tre olika nivåer: enkelt och öppet, smart och optimerat samt uppkopplat och tillgängligt. Det har även skett utbildningar i modellen med förvaltningsledningar och IT-strateger. Det pågår även en systemkartläggning med nulägesbeskrivningar med perspektiven teknik, förvaltningsorganisation, förvaltningsarbete och ekonomi. Det finns framtagna principer när systemförvaltningsmodellen ska utnyttjas, exempelvis till samhällsviktiga, kritiska tjänster eller system som handhar mycket personuppgifter. Det framkommer däremot att dataskyddsombudet inte varit involverad i framtagandet av systemförvaltningsmodellen. Vidare framkommer det även att implementeringen av modellen inte är tillfredsställande.

IT-avdelningen har i samverkan med informationssäkerhetsstrateger påbörjat ett arbete med att upprätta ett ”LIS - uttalande om tillämplighet” (förteckning över informationssäkerhetsåtgärder). Förteckningen innehåller tillämpbara åtgärder utifrån ISO 27002[4] samt CIS 18 ramverket[5]. Vi har här tagit del av ett utkast för detta. Enligt intervjuade kommer samtliga ISO 27002 att vara tillämpbara för att efterleva författningskrav såsom NIS och GDPR. Åtgärderna enligt CIS 18 ska säkerställa mappningen till författningskrav och möjliggöra riskminimering.

3.1.1 Bedömning

Vi kan konstatera att det skett ett arbete för att rusta upp och organisera sig kring IT-säkerhetsarbetet. Detta har bidragit till stegförflyttningar framåt i IT-säkerhetsarbetet och vi bedömer att det finns en bra organisation och struktur kring säkerhetsarbetet vilket möjliggör ett systematiskt arbetssätt kring IT-säkerheten. Vi bedömer även att det finns en tydlig roll och ansvarsfördelning kring arbetet med IT-säkerhet.

Vi kan dock konstatera att det fortfarande bedrivs ett arbete med att upprätta och förvalta relevanta styrande dokument som tydliggör kommunens IT-säkerhetsarbete. Vi noterar att arbetet inte färdigställts ännu och att detta uppges beror på att

[3] En modell för hur systemförvaltning ska organiseras för att förvalta IT-baserade system.
[4] Informationssäkerhetsstandard framtaget av ISO och IEC
[5] Critical Security Contrls

informationssäkerheten ska bygga på den nya ISO-standarden. Vi ser dock allvarligt på att påtalade brister gällande de styrande dokumenten kring IT-säkerheten ännu inte är åtgärdade. Vi bedömer att det är av vikt att det finns styrande dokument kring IT-säkerheten som också revideras vid behov, som ett led i det systematiska arbetet kring IT-säkerhet.

Vi noterar däremot att det pågår ett arbete med att revidera informationssäkerhetspolicyn samt att det pågår ett arbete med att upprätta en förteckning över informationssäkerhetsåtgärder, vilket vi ser positivt på.

3.2 Löpande arbete och uppföljning

Under 2021 har det anställts två informationssäkerhetstrateger som är organiserade under avdelningen för styrning och ledning. Detta för att vidareutveckla det systematiska och riskbaserade säkerhetsarbetet. Som ett led i att säkerställa adressering och hanteringen av säkerhetsrelaterade IT-frågor och åtgärder har kommunen utsett en IT-säkerhetssamordnare.

Enligt uppgifter finns en gemensam dokumenthanteringsplattform (DokIT) för IT-avdelningens tekniska dokumentation. I samband med en uppdatering av DokIT kommer även dokument och rutinhantering för IT-service att infalla under samma plattform. Enligt de intervjuade blir uppdateringen av DokIT en rejäl höjning från den tidigare versionen. För den löpande uppföljningen av frågor och oförutsedda händelser finns ett DSU-forum (Daily Stand Up) det sker även drifts- och servicemöten veckovis för att löpande följa upp och förbättra IT-avdelningens interna processer samt identifiera, dokumentera händelser och avvikelser, förebygga, fastställa och åtgärda orsaker samt förändringsarbeten internt.

Det finns upprättade IT-strategsträffar där samtliga förvaltningar och bolag finns representerade detta i syfte att arbeta proaktivt på en strategisk nivå där IT-säkerhet är del av innehållet. Detta används bl.a. som ett sätt att upprätthålla en medvetenhet kring IT-säkerhet men även för att kunna identifiera behov och signalera om saker behöver lyftas/förändras. Det upplevs dock av intervjuade finnas svårigheter att hitta rätt struktur och nivå på mötena för att de ska vara givande.

Utöver detta finns en dataskyddsgrupp där bl.a. IT-strateger från kommunen samt de kommunala bolagen ingår. Enligt intervjuade är denna dock pausad då syftet för gruppen behöver tydliggöras. I dagsläget upplever de intervjuade att detta täcks upp i andra forum.

Det har tidigare under året även genomförts en informationssäkerhetskampanj tillsammans med kommunikationsavdelningen. I denna kampanj kördes det bl.a. ut generell användarinformation samt information kring incident rapportering. Detta som ett led i att säkerställa att användarinformationen var uppdaterad och känd ute i förvaltningarna. Enligt intervjuade var denna kampanj väl mottagen däremot var det inte obligatorisk utbildning till följd av kampanjen. Tanken är dock att det under hösten 2022 kommer ske en obligatorisk utbildning som ett led i att förankra kunskapen ute i förvaltningarna.

Under november 2021 har en implementering av informationssäkerhetsmodul skett i verksamhetssystemet Stratsys. Enligt intervjuade har det förts diskussioner kring hur de ska nå en ökad medvetenhet, kunskap och kompetens kring IT-säkerhet och faktiska risker. Det har därför tagits fram ett utkast till internkontrollen med specifika kontrollmoment kring just IT-säkerhetsrisker. Intervjuade anser dock att det är bekymmersamt att internkontrollarbetet utifrån ett IT-säkerhetsperspektiv inte ligger på en högre nivå.

Det pågår ett arbete med att färdigställa arbetsområdesfördelningen som bl.a. definierar ansvarig personals tillgång till uppgifter. Det har påbörjats ett samarbete mellan IT-skydds och säkerhetsgruppen samt Dataskyddsombudet där det löpande arbetet i form av granskningar och riskbedömningar ska rapporteras av de ansvariga enligt arbetsområdesfördelningen. Detta för att regelbundet kunna se över och bedöma risker för IT-avdelningens organisation samt bevaka och säkerställa policy och rutiner samt för att kunna rapportera tillståndet kring informationssäkerheten.

För att säkerställa beredskap samt planera för störningar i systemen utifrån exempelvis krissituationer och katastrofer pågår ett arbete med att färdigställa en kontinuitetsplanering. Kontinuitetsplaneringen[6] kommer att implementeras i verksamhetsplaneringen samt som en del i årshjulet för att säkerställa kontinuitet. Som en del i detta arbete sker det årligen en översyn i respektive team av kontinuitetsplaneringen. Enligt intervjuade är tanken att det inför varje sommarsemester ska ske en uppdatering av den tekniska dokumentationen i DokIT. Enligt intervjuade har det tidigare funnits ett personberoende kring de olika systemen vilket bl.a. uppmärksammats vid pensionsavgångar etc. Intervjuade upplever dock att det nu finns rutiner kring roll- och ansvarsfördelning för att minska personbundenhet och sårbarhet.

3.2.1 Bedömning

Vi konstaterar att det finns en gemensam dokumenthanteringsplattform där den tekniska dokumentationen läggs upp. Det finns samtidigt en löpande uppföljning av frågor och oförutsedda händelser i det dagliga forumet.

Vi bedömer att det finns upprättade samverkansforum för att kunna arbeta strategiskt men även för att kunna hantera uppkomna problem i det dagliga arbetet samt bolla tankar och idéer. Vi konstaterar dock att det inte skett några riktade utbildningar kring IT-säkerhet, vi noterar däremot att det finns en tanke kring att under hösten 2022 genomföra en obligatorisk utbildning. Vi bedömer att det är av vikt att det upprättas en systematik kring IT-säkerheten där utbildningar bör utgöra en naturlig del i det systematiska arbetet kring IT-säkerheten. Vi rekommenderar därför att kommunstyrelsen ser över och säkerställer en systematik kring arbetet med IT-säkerheten.

[6] Metod för att säkerställa leveransförmågan genom att planera för att fortsatt kunna upprätthålla de samhällsviktiga verksamheterna trots eventuella avbrott.

Vi kan konstatera att det pågår ett arbete med att ta fram specifika kontrollmoment till internkontrollen kring IT-säkerhetsrisker något vi ser positivt på då det möjliggör uppföljning samtidigt som det medvetandegör IT-säkerhetsrisker i det dagliga arbetet.

Det pågår arbete med att färdigställa kontinuitetsplaneringen vilket vi bedömer är av vikt för att säkerställa en tydlig struktur och minska sårbarheten kring de olika IT-systemen.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att det till viss del finns en tillfredsställande IT-säkerhet däremot kan den stärkas ytterligare genom en tydligare systematik.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- se över och säkerställa ett systematiskt arbete kring IT-säkerheten, se avsnitt 3.1 och 3.2

Datum som ovan

KPMG AB

DocuSigned by:
29FEC0EAB81B46E...

Oskar Nordmark
Certifierad kommunal revisor

DocuSigned by:
4F6BFCF9B4F744C...

Camilla Strömbäck
Certifierad Kommunal revisor