Granskning av kommunens IT-säkerhet

Rapport

Sollefteå kommun

KPMG AB

2020-02-06

Antal sidor 10

Antal bilagor 1

Sollefteå kommun
Granskning av kommunens IT-säkerhet

2020-02-06

Innehållsförteckning

1 Sammanfattning

Vi har av Sollefteå kommuns revisorer fått i uppdrag att granska kommunens arbete med IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2019.

Granskningen har syftat till att konstatera om kommunen har erforderlig kontroll över att de bedömningar och beställningar som införd IT-säkerhet grundar sig på är baserade på de risker och behov som ansvariga för informationen har identifierat och kommunicerat.

Vår sammanfattande bedömning utifrån granskningens syfte är att det finns brister i kommunstyrelsens arbete för att säkerställa en tillräcklig kontroll över kommunens Informations- och IT-säkerhet. En aktuell policy finns men anvisningar är inte fastställda. Utan dessa är instruktioner på en alltför övergripande nivå för att styra arbetet med informations- och IT-säkerhet. Dialog och samverkan mellan förvaltningarna och IT behöver utvecklas gällande systemförvaltning och informationsklassning för att säkerställa informationssäkerheten och underliggande IT-säkerhetsåtgärder.

I nuläget baseras inte säkerhetsåtgärderna på risker och behov som ansvariga för informationen har fastställt. Utan det underlaget anordnas åtgärderna på ett sätt som IT-enheten upplever som nödvändigt utifrån sina förutsättningar. Det finns olika former att säkerställa att efterlevnad av beslutad IT-säkerhet sker. I de fall det inte går att säkerställa är det näst bästa att se till att incidenter upptäcks och kan åtgärdas. Vi bedömer att detta arbete inte är tillräckligt och att kommunen behöver utveckla sitt arbete med riskanalys i syfte att tydliggöra vilka hot och brister som finns i kommunens IT-miljö och avseende informationssäkerheten.

Det saknas politiska beslut och uppdrag till verksamheten för att säkerställa arbetet och ingen rapportering sker kring incidenter eller åtgärder för att upprätthålla en tillräcklig säkerhetsnivå.

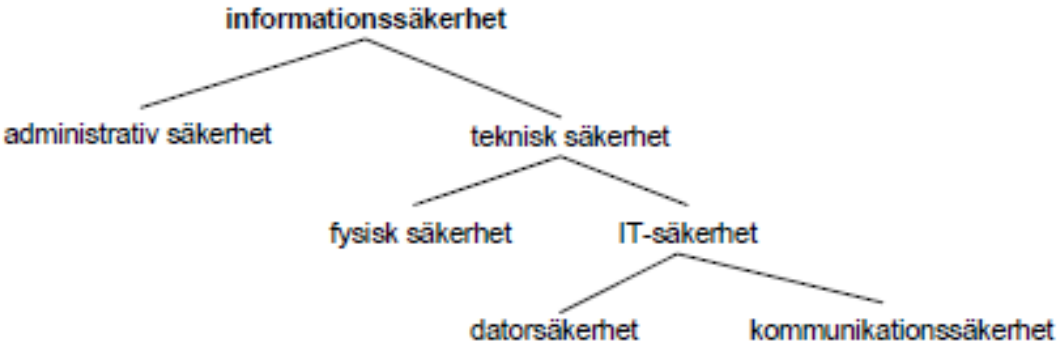
Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- säkerställa att det finns aktuella, kända och tillämpade styrdokument med tillhörande instruktioner som lägger en grund för en god informationssäkerhet och tillhörande IT-säkerhet. Dessa bör även tydliggöra ansvar och roller för arbetet.
- säkerställa att informationsklassning av de datoriserade verksamhetssystemen genomförs för att verksamhetsansvariga ska kunna bedöma vilka säkerhetsåtgärder som behöver vidtas för att skydda de informationstillgångar som de ansvarar för
- Utveckla arbetet med systemförvaltning så att en dialog förs mellan verksamhetens systemägare/systemförvaltare och IT-enheten
- ge IT-enheten i uppdrag att ta fram kontinuitetsplaner som beskriver de reserv-, återställnings- och återgångsrutiner som används för att säkerställa kontinuiteten i en prioriterad verksamhet eller process

2 Inledning/bakgrund

Vi har av Sollefteå kommuns revisorer fått i uppdrag att granska hur kommunen med underlag av sina styrande dokument avseende informationssäkerhetsrutiner anordnat sin IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2019.

Med IT-säkerhet avses en väl avgränsad del av det större begreppet informations-säkerhet och består av delarna datorsäkerhet och kommunikationssäkerhet. Bilden nedan illustrerar förhållandet mellan informationssäkerhet och IT-säkerhet.



Av standarderna i ISO 27000-serien kan utläsas att IT-säkerhet är underordnad informationssäkerheten. Placeringen innebär att beslut om IT-säkerhet styrs av de beslut som tas av system och/eller objektägare som har att efterleva beslutad informationssäkerhetspolicy med tillhörande tillämpningsföreskrifter. Alternativt tillämpar kommunen ett LIS[1]

Revisorerna utesluter inte att det finns risk för att införda IT-säkerhetsåtgärder inte står i relation till hur verksamhetsansvariga klassificerat den information de har ansvar för. Det kan i sin tur innebära att ansvarsförhållandena avseende kommunens informationstillgångar inte är tillräckligt kända och respektive ansvariga inte beställer/styr den IT-säkerhet som tillhandahålls.

Uppdraget ingår i revisionsplanen för år 2019.

2.1 Syfte, revisionsfråga och avgränsning

Granskningen syftar till att konstatera om kommunen har erforderlig kontroll över att de bedömningar och beställningar som införd IT-säkerhet grundar sig på är baserade på de risker och behov som ansvariga för informationen har identifierat och kommunicerat.

Granskningen ska besvara följande revisionsfrågor:

[1] Ledningssystem för informationssäkerhet

— 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 etablerad IT-säkerhet uppfyller interna regelverk samt policys med tillhörande tillämpningsföreskrifter.

2.3 Metod

Granskningen har genomförts genom inledande dokumentstudier och därefter en utfrågning (hearing) med deltagande av förtroendevalda, förtroendevalda revisorer och tjänstemän på förvaltningsledningsnivå.

I bilaga 1 redovisas det frågekomplex som har använts vid utfrågningen.

Rapporten är faktakontrollerad av IT-chef och informationssäkerhetssamordnare.

3 Resultat av granskningen

3.1 Organisation

Ansvarig för Informationssäkerhetsarbetet är kommunens informationssäkerhets-samordnare som är organiserad inom kommunstyrelseförvaltningen. I dokumentet Anvisning informationssäkerhet och dataskydd, som är framtaget, men ännu inte beslutat, beskrivs ansvar för samordnaren enligt följande:

”Informationssäkerhetssamordnaren planerar, leder och samordnar kommunens informationssäkerhetsarbete. Informationssäkerhetssamordnaren ger råd och stöd samt följer upp informationshanteringen genom uppföljning och kontroller”.

Sollefteå kommuns IT-enhet är också organiserad inom kommunstyrelseförvaltningen och består av IT-chef, systemtekniker, IT-tekniker och en utsedd tjänst för IT inom skolan. Övergripande ansvarig för IT-säkerhetsarbetet är IT-chef. Avdelningen är indelad i olika arbetsgrupper.

Bedömning

Vår bedömning är att det i nuläget saknas fastställda styrdokument som beskriver hur ansvarsfördelningen ser ut för Informations- och IT-säkerhetsarbetet. Ansvaret upplevs dock som tydligt för de funktioner som arbetar med frågorna idag. Utkast till ”Anvisning informationssäkerhet och dataskydd” som vi har tagit del av tydliggör rollerna. Detta är viktigt för att minska sårbarheten vid exempelvis organisations- och personalförändringar. Dokumentet ska fastställas av kommunchef och är framlagt för beslut.

3.2 Styrande dokument

3.2.1 Informationssäkerhet- och dataskyddspolicy

IT-säkerhet är underordnat informationssäkerhet. Av detta följer att beslut om IT-säkerhet styrs av det som framgår i styrdokument för informationssäkerheten och de beslut som tas angående kommunens informationstillgångar och system. Av denna anledning har vi utvidgat granskningen till att även omfatta informationssäkerheten på övergripande nivå.

Sollefteå kommun har en beslutad Informationssäkerhets- och dataskyddspolicy som antogs av kommunfullmäktige 2018-09-24.

Policyn är ett huvuddokument som ska ligga till grund för anvisningar för hur arbetet ska tillämpas och hur ansvarsfördelningen ser ut för arbetet. Det finns i nuläget inga fastställda anvisningar men det har framkommit i granskningen att dokumentet är färdigställt av informationssäkerhetssamordnaren, men inte beslutad av kommunchef ännu. Vi har tagit del av utkast till anvisningen för informationssäkerhet och dataskydd och dokumentet innehåller de väsentliga delar som behövs för att beskriva hantering av informationstillgångar och säkerställa kommunens informationssäkerhetsarbete.

3.2.2 Risk- och sårbarhetsanalys

Det finns en Risk- och sårbarhetsanalys fastställd av kommunfullmäktige 2015-12-21. I den framgår att det systematiska informationssäkerhetsarbetet behöver systematiseras i enlighet med gällande standard inom området.

3.2.3 Säkerhetsskyddsplan

En säkerhetsskyddsplan är fastställd i kommunfullmäktige 2017-12-18. I den berörs informationssäkerheten och det framgår bland annat att det är mycket betydelsefullt att informationshanteringen skyddas från såväl avsiktliga och oavsiktliga störningar.

Det framgår också vikten av att kontinuitetsplanering. I dokumentet står att ”En kontinuitetsplan ska finnas för driften av verksamhetssystem och övergripande IT-system baserad på de enskilda systemens krav på avbrotts- och katastrofplanering. En sådan ska tas fram inom kommunens informationssäkerhetsarbete.”

Bedömning

Vår bedömning är att kommunstyrelsen delvis har tillsett att det finns aktuella styrande dokument som tydliggör vilka krav som ställs och hur arbetet för att säkerställa kommunens informations- och IT-säkerhet ska organiseras.

En aktuell policy finns men anvisningar är inte fastställda. Utan dessa är instruktioner på en alltför övergripande nivå för att styra arbetet med informations- och IT-säkerhet. Utkast för Anvisning för informationssäkerhet och dataskydd, som vi tagit del av har ett relevant innehåll och beskriver roller på ett bra sätt där det även blir tydligt att ett stort ansvar för arbetet finns i verksamheterna och inte bara ett ansvar hos IT-verksamheten. Det är därför av största vikt att anvisningar beslutas av kommunstyrelsen så snart som möjligt så att denna kan förankras i verksamheten för en ökad förståelse för var och ens ansvar samt hur arbetet ska bedrivas.

3.3 Redovisning av förberedande frågor

I bilaga 1 finns de frågor som vi använt i denna granskning. IT-chef samt kommunens säkerhetssamordnare har svarat skriftligt på samtliga frågor och vi (KPMG) har också diskuterat utvalda frågor vid den hearing som genomfördes 2019-12-11 i Sollefteå.

3.3.1 Roller och ansvar för IT-säkerheten

IT-enheten anser sig ansvariga för IT-säkerheten men inte för Informationssäkerheten i sin helhet. I många fall får IT-enheten bevaka att vissa IT-relaterade säkerhets-lösningar görs. Fördelningen av ansvar är inte nedtecknad och definierad i beslut, interna avtal eller instruktioner. Rollbeskrivning finns i utkastform i dokumentet ”Anvisning för informationssäkerhet och dataskydd.”

Uppdraget definieras i nuläget till stor del av chef och medarbetare vid IT-enheten utifrån verksamheternas behov för stunden, samt de stora åtgärder som behöver genomföras både i närtid och inom överskådlig tid. Det framkommer dock att resurser i form av ekonomiska medel är en faktor som spelar in över vad som är möjligt att genomföra.

Ingen informationsklassning är genomförd. Underlag för bedömning finns i utkastform i ”Anvisning för informationssäkerhet och dataskydd”. Att genomföra informationsklass-ning hos alla verksamheter kommer ta lång tid. Informationssäkerhetssamordnaren är i nuläget även krisberedskapssamordnare och dataskyddsombud vilket begränsar möjligheterna att driva informationssäkerhetsfrågorna i tillräckligt hög grad. Fokus i verksamheten har hittills varit att säkerställa kommunens efterlevnad av GDPR.

Det finns inga överenskommelser om servicenivå, så kallade SLA, mellan IT och förvaltningarna. Interna rutiner för arbetet vid IT-enheten finns känt hos medarbetarna i de olika arbetsgrupperna. (System, Kommunikation, IT-Närservice).

IT-enheten upplever inte att de har tillräckliga resurser vilket leder till att befintlig driftpersonal har en ökad arbetsbelastning även med de strategiska rollerna för

kommunens IT, exempelvis IT-strateg och IT-arkitekt. Det leder till att vissa strategiska frågor inte kan prioriteras utan får läggas på framtiden.

Rapportering sker till kommunens ledningsgrupp där IT-chef ingår.

3.3.2 Styrande dokument och annan dokumentation

En aktuell Informations- och dataskyddspolicy finns, se även 3.2.1. I dokumentet anges att anvisningar ska tas fram och att det är kommunchef som ska tillse att så sker. Som vi beskrivit ovan så finns ett utkast till anvisning för informationssäkerhet och dataskydd. Orsak att den inte lagts fram till fastställande är att bedömning av säkerheten i kommunens molnlösningar ej gjorts pga. tidsbrist. Det finns information om regler och rutiner för användare på KomIn (kommunens intranät). Uppdatering av dokumentation inom IT-verksamheten är påbörjad men arbetet påverkas av arbetsbörda/tidsbrist.

IT-chefen uppger att Ledningssystem för informationssäkerhet (LIS) saknas. Det finns för närvarande planer på att skapa ett LIS i minsta format med tydligare rollbeskrivningar och en återkommande arbetsgång per år/mandatperiod. Det finns däremot inga förutsättningar med nuvarande resurser att implementera ett LIS som kan certifieras.

En IT-systemöversikt finns sedan tidigare och i nuläget sker en omarbetning och uppdatering där denna registreras i systemet E-sumit. Anpassningar för krav enligt GDPR sker samtidigt.

Kommunen saknar idag systemförvaltningsplaner (baserat på pm3, ITIL eller egenutvecklad organisation) för de verksamhetssystem som kommunen använder.

Vad gäller NIS-direktivet och GDPR har inte IT-enheten fått något uppdrag eller ansvar för att vidta åtgärder för att hantera dessa frågor för kommunen i stort. Rutin för att rapportera personuppgiftsincidenter enligt dataskyddsförordningen (GDPR) finns. Ett samarbete sker mellan IT-enheten och kommunens dataskyddsombud men tidsbrist inom båda funktionerna försvårar arbetet och samarbetet är inte formaliserat i arbetsgrupp eller liknande.

3.3.3 Kompetensutveckling

Det har genomförts utbildning i form av Nano lektioner utskickade via mail till alla medarbetare med en kommunal e-post. Utbildningen är en grundläggande informationssäkerhetsutbildning, till viss del anpassad utifrån Sollefteå kommun. Utskick till denna gjordes våren 2018 och våren 2019. Våren 2018 var svarsfrekvensen hög och mer än 1200 mottagare genomförde samtliga lektioner. Våren 2019 var svarsfrekvensen något lägre, runt 1000 mottagare som genomförde lektionerna. Utbildningen är en planerad årligt återkommande utbildning.

E-utbildning har genomförts för hur man som användare kan identifiera olika hot som exempelvis sker via e-post. Det kan vara att någon utger sig för att vara en trovärdig avsändare och försöker få inloggningsuppgifter eller placera virus eller liknande hos användarna i syfte att ta del av eller skada kommunens informationstillgångar.

3.3.4 IT-säkerhetsåtgärder

Rutiner och processer

Kommunens skydd av sin IT-miljö består idag av bland annat backup, redundans i internetleverans, brandvägg med redundans, e-postfilter, tvåfaktorsinloggning etc. I sina svar anger kommunen att intrångsförsök pågår kontinuerligt men att de skydd som finns hittills har förhindrat intrång och inga konsekvenser har skett för kommunens informationstillgångar. De åtgärder som vidtagits är bland annat svartlistning/blockning som utvecklas succesivt.

Kommunen har genomfört kontroller av sina säkerhetsåtgärder för att på så sätt identifiera eventuella brister för att ha möjlighet att åtgärda dessa innan det skadar kommunens informationstillgångar. De kontroller som genomförts har skett med hjälp av en extern leverantör.

Det finns ingen kontinuitetsplan eller katastrofplan framtagen men medarbetare som har ansvaret för olika delar av IT-verksamheten anser att de har kännedom om behov samt kan vidta åtgärder under ordinarie arbetstid.

Det finns ett samarbete mellan IT-enheten, dataskyddsombud och informations-säkerhetssamordnare för incidenthantering som innefattar rapportering till berörda myndigheter så som Datainspektionen (Integritetsskyddsmyndigheten) och Myndigheten för samhällsskydd och beredskap (MSB). I övriga verksamheter är inte den typen av incidentrapportering känd. Internt rapporteras incidenter till överordnad chef samt till berörd verksamhet. Det finns ingen kontinuerlig rapportering till politiken.

Sollefteå kommun planerar en implementering av Windows 10. Genom det finns en del säkerhetsåtgärder inbyggda. Ett flertal säkerhetsåtgärder är identifierade och planerade att införas om resurser tillsätts. Bland annat system för automatiserad ID- och behörighetskontroll, kontroll av nätverksåtkomst och system för central övervakning, kontroll, risk och sårbarhetsscanning.

Bedömning

Vår bedömning är att det finns brister i arbetet för att säkerställa en tillräcklig kontroll över kommunens Informations- och IT-säkerhet. I nuläget baseras inte säkerhets-åtgärderna på risker och behov som ansvariga för informationen har fastställt. Utan det underlaget anordnas åtgärderna på ett sätt som IT-enheten upplever som nödvändigt utifrån sina förutsättningar. Dialog och samverkan mellan förvaltningarna och IT-enheten för arbetet med systemförvaltning, informationsklassning och servicenivåer för att säkerställa en god IT-säkerhet behöver därför utvecklas.

Det finns ingen kontinuitetsplan i nuläget trots att det framgår av styrdokument att det är av största vikt.

Kommunen har till viss del genomfört kontroller av sina vidtagna säkerhetsåtgärder och vissa åtgärder har vidtagits utifrån resultatet av dessa. Vi anser dock att detta kan utvecklas och ske med en regelbundenhet då externa hot och risker förändras kontinuerligt.

I nuläget finns inga dokumenterade anvisningar för användare för att säkerställa att medarbetarna har fått information om deras ansvar i arbetet med informationssäkerhet men utbildningsinsatser har genomförts under 2018 och 2019 som är planerad att återkomma på årlig basis.

4 Svar på revisionsfrågorna

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?

Vår bedömning är att kommunstyrelsen delvis har tillsett att det finns aktuella styrande dokument som hur arbetet för att säkerställa kommunens informations- och IT-säkerhet ska organiseras.

En aktuell policy finns men anvisningar är inte fastställda, utan dessa är instruktioner på en alltför övergripande nivå för att styra arbetet med informations- och IT-säkerhet. Det utkast för anvisning för informationssäkerhet och dataskydd som vi tagit del av har ett relevant innehåll och beskriver roller på ett bra sätt där det även blir tydligt att ett stort ansvar för arbetet finns i verksamheterna och inte bara ett ansvar för IT-enheten. Det är därför av största vikt att anvisningar fastställs av kommunchef för att sedan implementeras i verksamheten.

Har kommunstyrelsen tillsett att det finns ett strukturerat arbete för att säkerställa en tillräcklig IT-säkerhet?

Arbetet med IT-säkerheten är ett kontinuerligt arbete som till sin struktur beskrivs i styrdokument som utgår från kommunens informationssäkerhetspolicy eller liknande policydokument för säkerhet och beredskap.

Oavsett om styrande dokument finns i någon utsträckning eller inte är det nödvändigt att en informationsklassning utförs för de datoriserade verksamhetsstöden. Utan det underlaget anordnas IT-säkerhetsåtgärderna på ett sätt som IT-enheten upplever som nödvändigt utifrån sina förutsättningar. Verksamhetsansvariga har följaktligen ingen kontroll över om den information de ansvarar för hanteras korrekt enligt externa och interna regler. Vid utfrågningen uppfattar vi att inget av de verksamhetssystem som är i drift har informationsklassats och det går därför inte att bedöma om tillräckliga och relevanta säkerhetsåtgärder är vidtagna.

Det saknas politiska beslut och uppdrag för att säkerställa arbetet med kommunens informationssäkerhet och IT-säkerhet. IT-enheten upplever att ekonomiska resurser, kompetens och förutsättningar att lägga tid saknas. Informationssäkerhetssamordnare har ett flertal roller vid sidan om sitt ansvar för informationssäkerhetsarbetet och en prioritering av arbetsuppgifter behöver göras mellan dessa som kan påverka kommunens förutsättningar att säkerställa en tillräcklig IT-säkerhet.

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

Det finns olika former för att säkerställa att efterlevnad av beslutad IT-säkerhet sker. I de fall det inte går att säkerställa är det näst bästa att se till att incidenter upptäcks och kan åtgärdas. Av denna anledning har kommunen ett antal säkerhetsanordningar för att försvåra intrång och om det ändå sker, att upptäcka och åtgärda. backup, redundans i internetleverans, brandvägg med redundans, e-postfilter, tvåfaktors-inloggning etc. Inga regelbundna penetrationstester eller intrångsförsök genomförs utan sker utifrån möjlighet och resurser. De senaste testerna har skett med hjälp av en extern leverantör och säkerhetsscanningen visade inga försök till intrång.

Det saknas kontinuitetsplan som beskriver de reserv-, återställning- och återgångs-rutiner som krävs för att säkerställa kontinuiteten i en prioriterad verksamhet eller process, utifrån vad som har inträffat.

5 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att det finns brister i kommunstyrelsens arbete för att säkerställa en tillräcklig kontroll över kommunens Informations- och IT-säkerhet.

En aktuell policy finns men anvisningar är inte fastställda. Utan dessa är instruktioner på en alltför övergripande nivå för att styra arbetet med informations- och IT-säkerhet. Dialog och samverkan mellan förvaltningarna och IT behöver utvecklas gällande systemförvaltning och informationsklassning för att säkerställa informationssäkerheten och underliggande IT-säkerhetsåtgärder.

5.1 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- säkerställa att det finns aktuella, kända och tillämpade styrdokument med tillhörande instruktioner som lägger en grund för en god informationssäkerhet och tillhörande IT-säkerhet. Dessa bör även tydliggöra ansvar och roller för arbetet.
- säkerställa att informationsklassning av de datoriserade verksamhetssystemen genomförs för att verksamhetsansvariga ska kunna bedöma vilka säkerhetsåtgärder som behöver vidtas för att skydda informationstillgångar som de ansvarar för
- Utveckla arbetet med systemförvaltning så att en dialog förs mellan verksamhetens systemägare/systemförvaltare och IT-enheten
- ge IT-enheten i uppdrag att ta fram kontinuitetsplaner som beskriver de reserv-, återställnings- och återgångsrutiner som används för att säkerställa kontinuiteten i en prioriterad verksamhet eller process

Sollefteå kommun
Granskning av kommunens IT-säkerhet

2020-02-06

Datum som ovan

KPMG AB

Jenny Thörn
Kommunal revisor

Bilaga 1

Förberedande frågor inför hearing om IT-säkerhet

Styrande dokument och annan dokumentation

1. Finns det en aktuell informationssäkerhetspolicy för kommunen med tillhörande tillämpningsföreskrifter?
2. Finns det särskilda tillämpningsföreskrifter avseende IT-säkerheten?
3. Finns det ett ledningssystem för informationssäkerhet (LIS) infört eller planeras det för ett sådant?
4. Är LIS certifierat eller finns det planer på att certifiera sig efter standarder i ISO 27000-serien?
5. Finns det en uppdragsbeskrivning för IT-avdelningen som anger eget och kommungemensamt ansvar för IT-säkerheten?
6. Om ovan nämnda dokument inte finns framtagna, vilka styrdokument anser IT-enheten att man verkar utifrån vad gäller IT-säkerheten?
7. Finns det systemförvaltningsplaner (baserad på pm3, ITIL eller egenutvecklad organisation) för de datoriserade verksamhetsstöd kommunen använder?
8. Finns det en systemförteckning som redovisar driftsatta system där det framgår vem som innehar de olika ansvar som identifierats?
9. Vilket ansvar anser/upplever IT-enheten sig ha för informationssäkerheten och IT-säkerheten? Finns detta ansvar dokumenterat och kommunicerat?
10. Har kommunen utfört någon informationsklassning och på vilket sätt har den påverkat de IT-säkerhetsåtgärder som införts?
11. Finns det servicenivåöverenskommelser (SLA) mellan IT-avdelningen och verksamhetsansvariga? På vems/vilkas initiativ är de framtagna? Vi önskar få ett eller flera exempel på ett SLA om detta finns.
12. Både NIS-direktivet och GDPR gäller från och med första halvåret 2018. Vilka instruktioner/uppdrag/ansvar har IT-avdelningen erhållit för att anpassa verksamheten för att säkerställa att kommunen efterlever dessa?
13. Har IT-enheten tagit stöd/involverats av kommunens dataskyddsombud (ett eller flera) under anpassningen till GDPR?
14. Finns det kunskap om och etablerade rutiner för:
    a. Incidenthantering som innefattar rapportering till överordnade, politiken, berörd verksamhet, anställda och kommunmedborgare?

   b. Incidenthantering som innefattar rapportering till berörda myndigheter så som Datainspektionen (Integritetsskyddsmyndigheten), Myndigheten för samhällsskydd och beredskap (MSB).

15. Finns det dokumenterade manuella rutiner/kontinuitetsplaner/katastrofplaner innefattande IT-säkerhetsåtgärder som testats någon gång(er) under de senaste två åren?

IT-säkerhetsåtgärder

16. Vi behöver en beskrivning av samt motivet (analysen) för de IT-säkerhetsåtgärder som vid utfrågningstillfället:
    a. Är i drift.
    b. Planeras sättas i drift innan årsskiftet 2019.
    c. Planeras sättas i drift efter årsskiftet 2019.
    d. Planeras förändras och/eller avvecklas.
17. Finns det vid utfrågningstillfället IT-säkerhetsrisker där åtgärder inte är i drift eller där befintliga åtgärder är bristfälliga?
18. Har det identifierats något intrångsförsök till kommunens infrastruktur och/eller system under 2018-2019? Vilken form av intrång och vad blev effekten?
19. Vilka åtgärder har vidtagits efter detta?
20. Har det utförts eller planeras det för penetrationstest av kommuns skydd mot intrång?
21. Anser IT-avdelningen att de har de resurser (ekonomi och kompetens internt och/eller extern personal) som behövs för att uppnå den IT-säkerhet som erfordras den kommunala verksamheten?
22. Vem/Vilka rapporterar IT-enheten till avseende IT-säkerheten? Med vilken periodicitet? Finns rapportering för 2018-2019 dokumenterad tar vi gärna del av den.
23. I vilka grupperingar (arbets- samordning-, samverkans- etc.) medverkar personer från IT-avdelningen när informationssäkerhet diskuteras/planeras/införs?
24. Finns det en dokumenterad och fastställd utbildningsplan för IT-avdelningen där IT-säkerhet ingår och är den fullföljd?
25. Finns det en fastställd utbildningsplan för kommunens övriga medarbetare avseende deras ansvar för kommunens IT-säkerhet på en grundläggande nivå?