Granskning av kommunens IT-säkerhet

Rapport

Orsa kommun

KPMG AB

2020-03-20

Antal sidor 11

Antal bilagor 1

Orsa kommun
Granskning av kommunens IT-säkerhet

2020-03-20

Innehållsförteckning

1 Sammanfattning

Vi har av Orsa 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 kontroll över att införda IT-säkerhetsåtgärder är baserade på de risker och behov som ansvariga för informationen har bedömt som nödvändiga utifrån informationstillgångarnas värde.

Vår sammanfattande bedömning är att arbetet bedrivs på ett strukturerat sätt utifrån fastställda styrdokument. Det finns en uppbyggd samverkan mellan förvaltningarna och IT avseende arbetet med systemförvaltning och utveckling inom IT. Utifrån granskningens syfte så är det vår bedömning att arbetet med informationsklassning behöver utvecklas så att vidtagna IT-säkerhetsåtgärder baseras på den bedömning som verksamhetsansvariga har gjort över värdet för informationen. Utan detta baseras åtgärderna på den kunskap och förutsättningar som IT-enheten har.

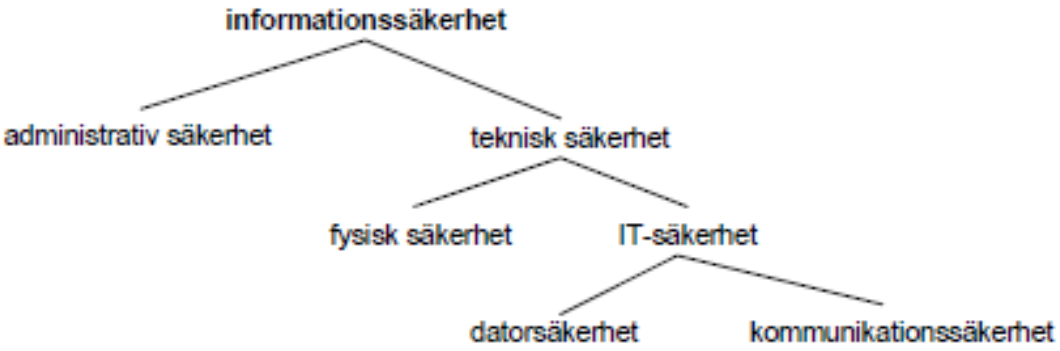
Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Säkerställa att informationsklassning av de datoriserade verksamhetssystemen genomförs.
- Säkerställa att grundläggande utbildningar inom informationssäkerhet och IT-säkerhet sker regelbundet och följs upp för att säkerställa en tillräcklig medvetenhet inom organisationen.

2 Inledning/bakgrund

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

Med IT-säkerhet avses en väl avgränsad del av det större begreppet informationssäkerhet 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 informationssäkerhet. Placeringen innebär att beslut om IT-säkerhet styrs av de beslut som tas av system- eller objektägare för att efterleva beslutad informationssäkerhetspolicy med tillhörande anvisningar. 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 har syftat till att konstatera om kommunen har kontroll över att införda IT-säkerhetsåtgärder är baserade på de risker och behov som ansvariga för informationen har bedömt som nödvändiga utifrån informationstillgångarnas värde.

[1] Ledningssystem för informationssäkerhet

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 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 representanter från kommunstyrelsen, IS/IT-nämnden och tjänstemän på ledningsnivå.

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

Rapporten är faktakontrollerad av kommunens informationssäkerhetssamordnare. IT-chef har erbjudits att faktagranska rapporten.

3 Resultat av granskningen

3.1 Organisation

Orsa kommun har tillsammans med Älvdalens kommun och Mora kommun en gemensam servicenämnd IS/IT (Informationssystem/Informationsteknologi). Mora kommun är värdkommun för nämnden som tillhör kommunens nämndstruktur.

Det finns ett reglemente för nämnden som kommunfullmäktige i Orsa antog 2016-02-15. Ett samverkansavtal finns upprättat 2016-01-01. Följande framgår avseende ändamål och omfattning ”Den gemensamma partsavsikten avser samverkan kring gemensamma IS/IT-resurser inom strategisk utveckling, projekt, systemförvaltning, drift och IT-säkerhet. Nämnden ska genom samordning av verksamheter optimera den ekonomiska effektiviteten, säkerställa kompetensförsörjningen, och verka för kvalitetsförbättringar”.

Det finns en styrgrupp för informationssäkerhet där kommundirektörerna i de tre samverkande kommunerna ingår. Informationssäkerhetssamordnaren deltar för genomgång av punkten 9.3 ledningens genomgång enligt ISO27001[2]-standarden. Anteckningar som vi tagit del av från styrgruppsmöte 2019-11-07 anger ”Föreslagna prioriterade områdena inom etablerandet av ett systematiskt

[2] ISO27001 är ledningssystem för informationssäkerhet som organisationer kan certifiera sig enligt.

informationssäkerhetsarbete i Mora, Orsa och Älvdalens kommun”. I dessa anteckningar framgår ett flertal prioriteringar som ska ske inom 1–2 år respektive 3–5 år för en utveckling av informationssäkerhetsarbetet.

Det finns ett verksamhetsplaneringsråd för IS/IT, kallat VP-råd. I gruppen ingår kommundirektörerna för de tre samverkande kommunerna och i rådet sker dialog och hantering av frågor som behöver beredas för att sedan beslutas i den gemensamma nämnden.

Rapportering av arbete med informations- och IT-säkerhet sker till den gemensamma nämnden och VP-råd för IS/IT. Vi har inte fått ta del av dokumentation från rapporteringen då denna är sekretessbelagd.

I samverkansavtalet framgår att värdkommunen ansvarar för att tillhandahålla en IS/IT-organisation och samordna de personalresurser som ingår i denna. IS/IT-enhetens organisation redovisas i enhetens verksamhetsplan. Mora kommun har fullt arbetsgivaransvar för den personal som ingår i IS/IT organisationen.

IT-enheten är indelad i drift och utveckling med olika kompetenser för dessa delar. På driftssidan finns ett uttalat ansvar för IT-säkerhet.

Förvaltningsledare IT arbetar verksamhetsspecifikt och inte som kontaktpersoner till respektive kommun. Det innebär att en förvaltningsledare IT arbetar mot alla de tre samverkanskommunernas förvaltningar gemensamt, t.ex. socialförvaltningarna. Detta för att få en samsyn och kunna effektivisera verksamhetssystem och stöd till förvaltningar inom samma ansvar.

Roller och ansvar

Vad gäller roller och ansvar så finns det beskrivet i policy för informationssäkerhet och dataskydd. Nedan beskrivning är hämtad direkt från policyn:

- Den politiska ledningen i form av kommunfullmäktige, kommunstyrelse, nämnder och bolagsstyrelser har det yttersta ansvaret för informationssäkerheten i den verksamhet som bedrivs inom deras ansvarsområden och ska ha en uppdaterad lägesbild över identifierade risker avseende informationshantering och besluta om åtgärder.
- Verksamhetsansvariga ansvarar för information inom sin verksamhet och dess säkerhet. Säkerställer att det finns rätt kompetens i organisationen. Ansvarar för att medarbetarna har ett säkerhetsmedvetande och tillräcklig kunskap för att informationssäkerhet kan uppnås.
- Medarbetare ansvarar för att följa policy för informationssäkerhet, riktlinjer, rutiner och regler. Man ansvarar även för att vara uppmärksam på brister och incidenter rörande informationssäkerhet.
- Informationssäkerhetssamordnaren har det övergripande ansvaret att leda och samordna informationssäkerhetsarbetet och arbetar i samråd med utsedda inom administrativ säkerhet, fysisk säkerhet och IT-säkerhet, dataskyddsombud samt verksamhetsrepresentanter.

3.1.1 Bedömning

Vår bedömning är att det finns en fastställd organisation med funktioner och kompetens för ett systematiskt arbete med informations- och IT-säkerhet. Roller och ansvarsförhållandet mellan förvaltning och IT-enhet inom dessa frågor är dokumenterat i styrdokument.

3.2 Styrande dokument

3.2.1 Policy för informationssäkerhet och dataskydd

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.

Orsa kommun har en policy för informationssäkerhet och dataskydd. Det framgår inte av policyn vem som är dokumentansvarig, i vilken instans den är beslutat och när i tid men genom protokollsgenomläsning har vi noterat att den är fastställd 2019-05-27 av kommunfullmäktige i Orsa kommun. I beslutet kan utläsas att policyn har utformats enligt gällande internationella standarder inom informationssäkerhet (ISO27000-serien) och att Myndigheten för samhällsskydd och beredskaps (MSB), metodstöd ska användas i kommunens utvecklingsarbete.

Riktlinje för informationssäkerhet är utifrån svar i granskningen under framtagande.

3.2.2 Policy för IT-säkerhet

Policy för IT-säkerhet redovisar övergripande mål och inriktning med IT-säkerhet samt hur ansvaret är fördelat. Dokumentet ”Riktlinjer för IT-säkerhet” är mer detaljerat och konkretiserar denna policy för IT-säkerhet.

3.2.3 Riktlinjer för IT-säkerhet

I Riktlinjer för IT-säkerhet framgår att ”Det är viktigt att IT-säkerheten är tillräckligt hög för att bemöta aktuell hotbild, att användarna har hög kunskap om IT-säkerhet och att det finns rutiner för att hantera IT-säkerhetsincidenter och förändringar i IT-miljön så att inga säkerhetsluckor uppstår”.

Det beskrivs att IT-säkerhet koncentrerar sig på hot och skydd förenade med användning av IT-komponenter. Risker och hotbilden samt sannolikheter för skada behöver balanseras mot kostnaden för säkerhetsåtgärder i förhållande till värdet av det som skyddas. Detta sker genom informationsklassning som är grunden till att kunna ställa krav på IT-säkerhet.

3.2.4 Bedömning

Vår bedömning är att det finns styrdokument som utgör en sammanhållen helhet för styrning av kommunens informations- och IT-säkerhetsarbetet. Policy för Informationssäkerhet och dataskydd finns och innehållet är i enlighet med rekommendationer från MSB vilket är den instans som anger en standard för myndigheters informationssäkerhetsarbete.

Det finns inga underliggande riktlinjer för informationssäkerhet trots att det i andra styrdokument hänvisas till detta dokument. Kommunen anger i svar att riktlinjer är under framtagande.

Det finns en Policy för IT-säkerhet och tillhörande instruktioner i form av Riktlinje för IT-säkerhet. Den omfattar avsnitt för användare, förvaltning och kontinuitet. Tre delar som är av vikt för att säkerställa säkerhetsarbetet. Innehållet beskriver på ett tydligt sätt hur arbetet med IT-säkerhet ska bedrivas och ansvarsfördelningen i det arbetet.

3.3 Redovisning av förberedande frågor

I bilaga 1 finns de frågor som vi använt i denna granskning. IT-chefen och informationssäkerhetssamordnare har svarat skriftligt på samtliga frågor. Vi (KPMG) har också diskuterat utvalda frågor vid den hearing som genomfördes 2020-02-20 i Orsa då representanter från kommunstyrelsen, gemensamma nämnden, revisionen, kommundirektör och förvaltningschefer närvarade.

3.3.1 Dokumentation och rutiner för IT-säkerhet

Ledningssystem för informationssäkerhet (LIS) saknas idag men verksamhetsplaneringsråd som består av kommundirektörer i de samverkande kommunerna har beslutat om ett införande av LIS. I Policy för informationssäkerhet och dataskydd framgår att arbetet ska ske i enlighet med etablerad standardserie SS-ISO/IEC 27000 för att upprätta, införa, underhålla och ständigt förbättra ledningssystemet för informationssäkerhet (LIS).

Uppdragsbeskrivning finns för IT-enhetens arbete genom samverkansavtal och reglemente för gemensamma nämnden.

Vid hearing beskrivs att en systemförteckning finns som redovisar driftsatta system där det framgår vem som ansvarar för systemen. Systemförvaltning finns beskrivet i en framtagen handbok och ska ske i enlighet med den av nämnden beslutade förvaltningsmodellen. I Orsa kommun används systemförvaltningsmodellen pm3 som är en styrmodell i den gemensamma nämnden för att nå gemensamma mål. Man försöker t.ex. att konsolidera IT-systemen så att man inte har flera system som gör samma saker. Modellen beskrivs under hearingen och används också för verksamhetsutveckling. Det finns ett kalendarium där olika aktiveter planeras, exempelvis registervård. IT-enheten vill även införa ett dokumentationssystem för vilken information de olika rollerna ska ha i IT-arbetet.

Under hearing framkommer att det inte är så stor andel av kommunens system som har informationsklassats ännu. Arbetet är under uppstart och drivs av informationssäkerhetssamordnaren. För de system som har informationsklassats behövdes inga ytterligare åtgärder för att förbättra säkerheten. Tillräckliga åtgärder bedömdes vara på plats. I plan för utveckling av kommunens informations-säkerhetsarbete framgår att målet är att samtliga verksamhetssystem ska vara informationsklassade inom 3–5 år. För alla nya system som ska implementeras sker en informationsklassning genom att detta finns med i enhetens projektmodell. SKR:s modell KLASSA används för klassificeringen.

Kommunernas verksamheter ska enligt samverkansavtalet teckna serviceavtal för tjänsteleveranser som IS/IT-enheten ansvarar för. Det finns inga upprättade överenskommelser för servicenivåer, så kallade SLA i nuläget men dessa är under uppbyggnad.

Kunskap och rutiner finns för att hantera incidenter, både till överordnade och till myndigheter. I policy och riktlinjer framgår att alla användare i kommunen har ett ansvar att vara uppmärksam på brister och incidenter rörande informationssäkerhet och en skyldighet att rapportera IT-säkerhetsincidenter och brister.

I riktlinje för IT-säkerhet framgår att all incidenthantering följer en fastställd rutin och ska säkerställa ett konsekvent och effektivt tillvägagångssätt för hantering av IT-säkerhetsincidenter. IT-säkerhetsincidentledare leder hanteringen av IT-säkerhetsincidenter i samverkan med relevanta roller i objektförvaltnings-organisationen. Erfarenheter från inträffade IT-säkerhetsincidenter ska ligga till grund för framtida beslut för att förbättra skyddet, t.ex. att investera i nya säkerhetslösningar.

Det finns dokumenterade kontinuitetsplaner som säkerställer återställningsrutiner vid ev. händelser som har testats under de senaste åren.

3.3.2 IT-säkerhetsåtgärder

I Riktlinjer för IT-säkerhet anges att upprätthållandet av en tillräcklig säkerhetsnivå ska ske genom regelbundna granskningar för att kontrollera att inga uppenbara sårbarheter exponeras. Sårbarheter och brister som upptäcks dokumenteras i objektförvaltningsplaner för åtgärd. Akuta sårbarheter och brister åtgärdas omedelbart. Rutiner ska finnas så att information om tekniska sårbarheter kan erhållas i tid, att sårbarheter kan analyseras och att lämpliga åtgärder kan vidtas.

Det har inte identifierats något intrångsförsök till kommunens infrastruktur under 2018 och 2019. Intrångsförsök via e-post, så kallade phisingmail, förekommer men dessa har identifierats och åtgärder vidtagits innan de skadat kommunens informationstillgångar. Penetrationstest har genomförts för kontroll av kommunens skydd mot intrång. Dessa visade att inga ytterligare åtgärder behövdes och kommunen anger att nivån för de säkerhetsåtgärder som finns bedöms vara tillräckliga utifrån kända hot. Dock är detta ett område som alltid behöver utvecklas då hot och risker förändras.

Webbutbildning för medarbetarna har genomförts inom både informationssäkerhet och IT-säkerhet för att medvetandegöra alla i verksamheten om detta. Informationssäkerhetssamordnaren har sedan 2019 som en del i implementeringen av ett ledningssystem för informationssäkerhet, LIS, infört att kommunerna årligen ska ha kunskapshöjande utbildnings- och informationsinsatser. Insatsen omfattar kommunanställda, förtroendevalda och de kommunala bolagens anställda och styrelser eftersom de också arbetar i samma IT-miljö. Under 2018 handlade webbutbildningen uteslutande om GDPR, som också är en viktig del i informationssäkerheten då det gäller att skydda information i form av personuppgifter. Det har även skett informationsinsatser på intranätet i artikelform där man upplyst om IT-säkerhet.

3.3.3 Bedömning

Det finns en medvetenhet i organisationen om att arbetet behöver vara en ständigt pågående process då risk och hot är föränderliga över tid. Av denna anledning har kommunen ett antal säkerhetsanordningar för att försvåra intrång och om det ändå sker, att upptäcka och åtgärda. Vår bedömning är att kommunen har tillsett att det finns tillräckliga former för att säkerställa efterlevnad av beslutad IT-säkerhet och de tester som genomförts visar på en tillräcklig säkerhet för att skydda kommunens informationstillgångar.

Utbildningstillfällen har genomförts genom webbutbildning till samtliga anställda i kommunen. För att upprätthålla en hög medvetenhet hos medarbetare och förtroendevalda krävs dock regelbundna utbildnings- och informationsinsatser. I Orsa kommun och övriga samverkanskommuner inom IS/IT har det införts en kampanjmånad i oktober för att uppmärksamma om informationssäkerhet. Informationssäkerhetssamordnaren arrangerar då aktiviteter för att informera och öka kunskaperna inom exempelvis lösenordshantering, intrång som kan ske via mail och hur man kan upprätthålla skydd av sin elektroniska legitimation.

3.4 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?

Kommunen har utarbetat en uppsättning dokument för både informationssäkerhet på övergripande nivå som tillsammans med styrdokument för IT-säkerhet utgör en helhet som tydliggör ansvar och hur arbetet ska bedrivas.

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

Vår bedömning är att det finns ett strukturerat arbete för att säkerställa en tillräcklig IT-säkerhet. Samverkan mellan verksamheter och IT-enheten är organiserad och styrs av en vedertagen styr- och samverkansmodell för systemförvaltning och

verksamhetsutveckling. Roller och ansvarsfördelning mellan IT-enheten och verksamheterna är tydliggjorda i styrdokument och vi upplever efter dialog vid hearingen att det även är så i praktiken.

Det är viktigt att en informationsklassning utförs för kommunens verksamhetssystem. Utan det underlaget anordnas IT-säkerhetsåtgärderna på ett sätt som IT-enheten upplever som nödvändigt utifrån sin kunskap och sina förutsättningar. Verksamhets-ansvariga har följaktligen ingen kontroll över om den information de ansvarar för hanteras korrekt. Vid utfrågningen uppfattar vi att arbetet är påbörjat men att en stor del av kommunens system inte har informationsklassats. Det går därför inte att bedöma om tillräckliga och relevanta säkerhetsåtgärder är vidtagna.

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. Vår bedömning är att kommunen har tillsett att det finns tillräckliga former för att säkerställa efterlevnad av beslutad IT-säkerhet och de tester som genomförts visar på en tillräcklig säkerhetsnivå.

De sårbarheter som finns är kända och åtgärder påbörjade eller planerade. Vid akuta sårbarheter vidtas åtgärder omedelbart och rapporters till högre instans. Det finns dokumenterade rutiner för att hantera incidenter.

Det finns dokumenterade kontinuitetsplaner som beskriver de reserv-, återställning- och återgångsrutiner som används för att säkerställa kontinuiteten i en prioriterad verksamhet eller process.

Trots alla maskinella skydd och varningssystem är det människor som ska efterleva den beslutade IT-säkerheten. För detta krävs en viss kunskapsnivå och viss insikt i vikten av informations- och IT-säkerhet. Detta har man tagit fasta på i Orsa kommun och alla anställda i kommunen genomför en webbutbildning i både informationssäkerhet och IT-säkerhet. För att upprätthålla medvetenheten hos medarbetare och förtroendevalda har man infört en kampanjmånad i oktober årligen för att uppmärksamma om informationssäkerhet. Aktiviteter har genomförts med information och kunskapshöjande insatser inom exempelvis lösenordshantering, intrång som kan ske via mail och hur man kan upprätthålla skydd av sin elektroniska legitimation.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning är att arbetet bedrivs på ett strukturerat sätt utifrån fastställda styrdokument. Det finns en uppbyggd samverkan mellan förvaltningarna och IT för arbetet med förvaltning och utveckling av kommunens IT.

Utifrån granskningens syfte så är vår bedömning att arbetet med informationsklassning behöver utvecklas så att vidtagna IT-säkerhetsåtgärder baseras på den bedömning som verksamhetsansvariga har gjort över värdet för informationen. Utan detta baseras åtgärderna på den kunskap och förutsättningar som IT-enheten har.

4.1 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Säkerställa att arbetet med informationsklassning genomförs.
- Säkerställa att grundläggande utbildningar inom informationssäkerhet och IT-säkerhet sker regelbundet och följs upp för att säkerställa en tillräcklig medvetenhet inom organisationen.

Datum som ovan

KPMG AB

Jenny Thörn
Kommunal revisor

Johan Malm
Kundansvarig 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?