KOMMUNREVISIONEN
Missivskrivelse

Datum:
2020-02-21

Diarienummer:
KRN-2020/60

Mottagare
Kommunstyrelsen

Kommunfullmäktige för kännedom

Granskning av kommunens informationssäkerhet

KPMG har av Uppsala kommuns revisorer fått i uppdrag att granska kommunens rutiner kring informations- och IT-säkerheten. Uppdraget ingår i revisionsplanen för år 2019. Granskningens syfte har varit att konstatera om kommunen har ett ändamålsenligt och systematiskt arbetssätt med sin informationssäkerhet (där IT-säkerhet ingår som en del).

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen inte fullt ut säkerställt ett ändamålsenligt och systematiskt arbete med sin informationssäkerhet. Baserat på styrdokument och intervjuades beskrivning av pågående utvecklingsarbete har Uppsala kommun en hög ambitionsnivå när det kommer till informationssäkerhetsarbetet. Vi bedömer det som positivt att flera åtgärder har och är planerade att genomföras för att förbättra kommunens organisation för informationssäkerhet. Vår bedömning är dock att organisationen inte implementerats fullt ut och ännu inte klarar att leva upp till den höga ambitionsnivån. Framförallt är verksamheten inte tillräckligt förankrad i arbetet vilket medför att IT-staben har tagit en stor roll.

Det har nyligen införts en funktion för informationssäkerhet där flera områden i Uppsala kommuns organisation är representerade. Det är chefen för IT-staben, CIO, som leder det strategiska arbetet avseende informationssäkerhet. Vi bedömer det som en risk då ansvarig för det strategiska informationssäkerhetsarbetet samtidigt ska vara kravställare gentemot IT. Det arbetet riskerar att försvåras om arbetet leds från samma organisation.

Det har även påbörjats ett arbete med att säkerhetsklassa informationen i kommunens olika system för att bättre kunna anpassa resurser utifrån informationssäkerhetsrisker. En del åtgärdsplaner utifrån klassningen har upprättats. Det är dock ett nyligen påbörjat arbete och har inte genomförts fullt ut.

Postadress: Uppsala kommun, Kommunrevisionen, 753 75 Uppsala
Kommunrevisionens kansli, telefon: 018-727 11 32
E-post: Kommunrevisionen@uppsala.se
www.uppsala.se

Vi lämnar följande rekommendationer till kommunstyrelsen:

- Säkerställ att funktionen för informationssäkerhet utvärderas och att dess syfte och funktion tydliggörs.
- Säkerställ att roller och ansvar mellan IT och verksamhet tydliggörs.
- Säkerställ att tillräcklig utbildning ges för att medvetandegöra informationssäkerhetsansvaret för alla inom Uppsala kommun.
- Säkerställ att arbetet med informationssäkerhetsklassning implementeras fullt ut i kommunen.

Revisionen begär yttrande över revisionens iakttagelser från kommunstyrelsen senast 2020-05-31 till kommunrevisionen@uppsala.se.

För kommunrevisionen

Per Davidsson

Per Davidsson, ordförande

Granskning av kommunens informationssäkerhet

Rapport

Uppsala kommun

KPMG AB

2020-02-21

Antal sidor 24

Antal bilagor 1

Uppsala kommun
Granskning av kommunens informationssäkerhet

2020-02-21

Innehållsförteckning

1 Sammanfattning

Vi har av Uppsala kommuns revisorer fått i uppdrag att granska kommunens rutiner kring informationssäkerhet. Uppdraget ingår i revisionsplanen för år 2019.

Granskningens syfte har varit att konstatera om kommunen har ett ändamålsenligt och systematiskt arbetssätt med sin informationssäkerhet.

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen inte fullt ut säkerställt ett ändamålsenligt och systematiskt arbete med sin informationssäkerhet. Baserat på styrdokument och intervjuades beskrivning av pågående utvecklingsarbete bedömer vi att Uppsala kommun har en hög ambitionsnivå när det kommer till informationssäkerhetsarbetet. Vi bedömer det som positivt att flera åtgärder har och är planerade att genomföras för att förbättra kommunens organisation för informationssäkerhet. Vår bedömning är dock att organisationen inte implementerats fullt ut och ännu inte klarar att leva upp till den höga ambitionsnivån. Framförallt är verksamheten inte tillräckligt förankrad i arbetet vilket medför att IT-staben har tagit en stor roll.

Det har nyligen införts en funktion för informationssäkerhet där flera områden i Uppsala kommuns organisation är representerade. Det är chefen för IT-staben, CIO[1], som leder det strategiska arbetet avseende informationssäkerhet. Vi bedömer det som en risk då ansvarig för det strategiska informationssäkerhetsarbetet samtidigt ska vara kravställare gentemot IT. Det arbetet riskerar att försvåras om arbetet leds från samma organisation.

Det har även påbörjats ett arbete med att säkerhetsklassa informationen i kommunens olika system för att bättre kunna anpassa resurser utifrån informationssäkerhetsrisker. En del åtgärdsplaner utifrån klassningen har upprättats. Det är dock ett nyligen påbörjat arbete och har inte genomförts fullt ut.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Säkerställa att funktionen för informationssäkerhet utvärderas och att dess syfte och funktion tydliggörs.
- Säkerställa att roller och ansvar mellan IT och verksamhet tydliggörs.
- Säkerställa att tillräcklig utbildning ges för att medvetandegöra informationssäkerhetsansvaret för alla inom Uppsala kommun.
- Säkerställa att arbetet med informationssäkerhetsklassning implementeras fullt ut i kommunen.

[1] Chief Information Officer

2 Inledning/bakgrund

Vi har av Uppsala kommuns revisorer fått i uppdrag att granska kommunens rutiner kring informations- och IT-säkerhet. Uppdraget ingår i revisionsplanen för år 2019.

Informationssäkerhet (där IT-säkerhet ingår som en del) är ett begrepp som används om informationssäkerhet för information som hanteras i kommunens IT-system. Allt mer information hanteras idag med olika tekniska lösningar och aldrig förr har kommunerna hanterat sådana mängder information som görs idag. Verksamheternas ökade beroende av informationsteknik (IT) innebär ökade risker i form av dataintrång, bedrägerier och spridning av skadlig kod.

Många verksamheter inom kommunen är idag helt beroende av väl fungerande IT. För flera verksamheter handlar ett väl fungerande IT-stöd såväl om säkerhet som möjlighet till en fungerande verksamhet utan driftstörningar. Ett kritiskt område är ofta äldreomsorg där driftstörningar i journalsystem och schemaprogram kan få stora direkta konsekvenser för brukarna. Ett annat område är kommunens elevregister där stora mängder personlig information om eleverna i kommunens skolor finns samlat.

Informationssäkerhet innebär att skydda information utifrån dess krav på konfidentialitet, riktighet och tillgänglighet i alla kommunens system. För att kunna hantera detta på ett ändamålsenligt sätt krävs att kommunen har ett systematiskt informationssäkerhetsarbete där flera funktioner i kommunen är involverade och rätt organiserade för uppdraget. Informationssäkerhet är inte en IT-fråga utan en fråga om att säkra och trygga driften av kommunens kärnverksamheter.

Revisorerna bedömer risken att det systematiska informationssäkerhetsarbetet inte är ändamålsenligt och att det finns risk för brister i kommunens organisering och arbetssätt inom området.

Med anledning av ovanstående drar kommunens revisorer slutsatsen i sin riskanalys, att kommunens rutiner avseende informationssäkerheten behöver granskas.

2.1 Syfte, revisionsfråga och avgränsning

Granskningen syftar till att konstatera om kommunen har ett ändamålsenligt och systematiskt arbetssätt med sin informationssäkerhet.

Granskningen ska besvara följande revisionsfrågor:

— Finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna i kommunen?

— Finns ett systematiskt och ändamålsenligt arbetssätt för att uppnå god informationssäkerhet dokumenterat och förankrat i kommunens verksamheter?

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

— Arbetar kommunens verksamheter systematiskt med att identifiera och analysera risker för informationssäkerheten?

— Görs systematiska uppföljningar av genomförda åtgärder för att kontinuerligt förbättra informationssäkerheten?

Granskningen avgränsas till att omfatta kommunstyrelsens ansvar för IT.

Granskningen avser kommunstyrelsen.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller

— Tillämpbara interna regelverk, policyer och beslut
— MSBs metodstöd avseende Ledningssystem för informationssäkerhet
— NIS-direktivet i tillämpliga delar avseende kartläggning och analys av risker

2.3 Metod

Granskningen har genomförts genom:

— Dokumentstudier
— Intervjuer med berörda tjänstepersoner däribland CIO, enhetschef för IT-strategi, enhetschef för IT-infrastruktur, informationssäkerhetstrateg, säkerhetschef, stadsjurist, objektledare för utvalda objekt samt ansvarig för pm3-modellen[2].

Rapporten är faktakontrollerad av samtliga intervjuade.

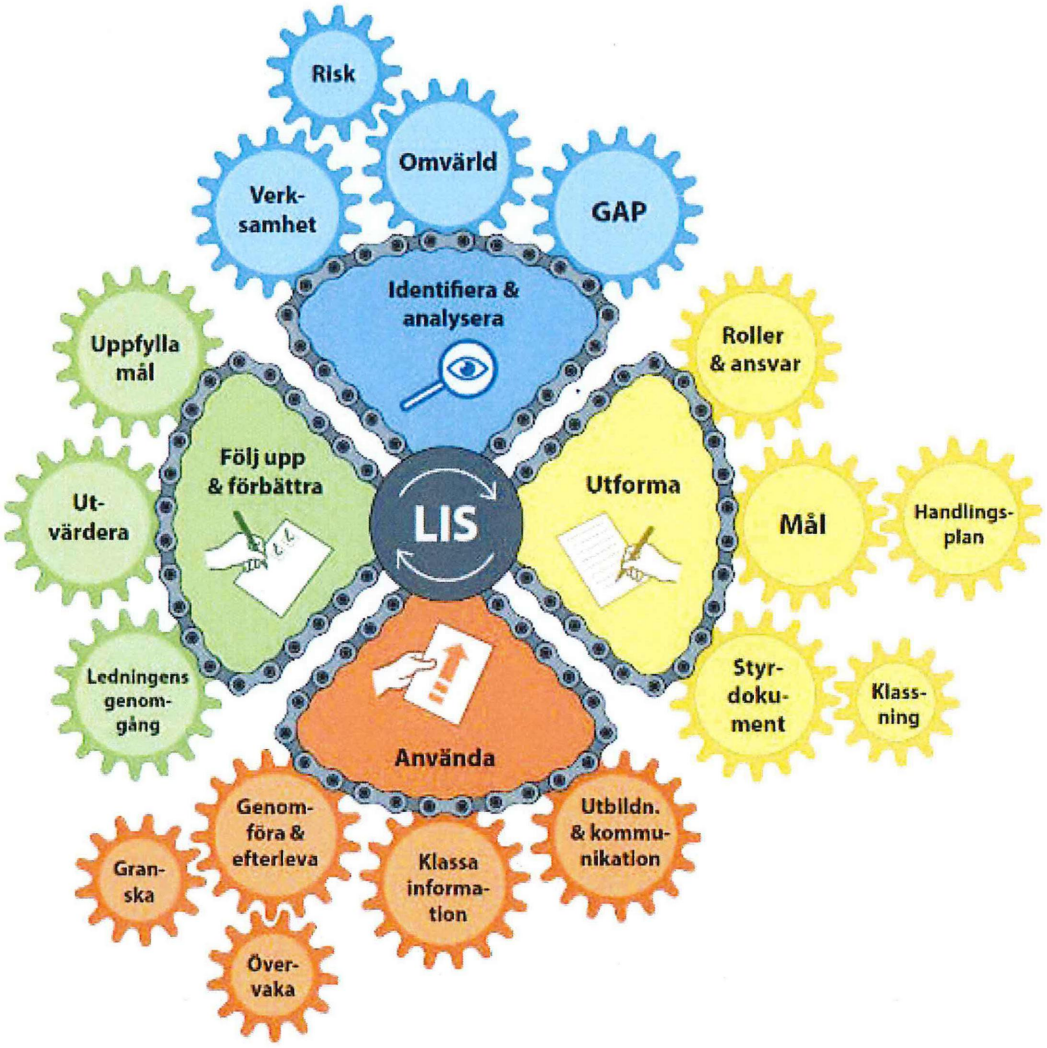
3 Resultat av granskningen

3.1 MSB:s metodstöd för systematiskt informationssäkerhetsarbete

MSB[3] har tagit fram ett metodstöd till organisationer avseende informationssäkerhetsarbetet. Metodstödet är baserat på den internationella standard-serien för informationssäkerhet, ISO/ IEC 27000 och ämnar till att förtydliga hur informationssäkerhetsarbetet kan utformas.

Metodstödet består av fyra olika metodsteg för informationssäkerhetsarbetet vilka illustreras i nedanstående figur.

[2] Organisationsmodell för systemförvaltning
[3] Myndigheten för Samhällsskydd och Beredskap



Metodstödet och de fyra metodstegen med underliggande metoddelar.

3.2 Styrdokument

I Uppsala kommun finns en omfattande mängd styrdokument som berör informationssäkerhetsområdet. Det framgår av intervjuer att flera av de intervjuade upplever mängden styrdokument vara omfattande och problematiska för verksamheten att hantera. För en redovisning av samtliga styrdokument se *Bilaga A.*

På Uppsala kommuns intranät *Insidan* framgår att det finns två policyer inom kommunen som på ett övergripande plan styr arbetet med informationssäkerhet.

- *Policy för IT-utveckling och digitalisering*
- *Policy för trygghet och säkerhet*

Utifrån ovan nämnda policyer har följande planer för kommunens arbete på området tagits fram:

- *Strategisk plan för IT-utveckling och digitalisering*
- *Handlingsplan för trygghet och säkerhet*

Nedan följer en kort beskrivning av ovan nämnda policyer och handlingsplaner:

3.2.1 Policy för IT-utveckling och digitalisering

I policyn anges den övergripande politiska inriktningen för IT-utveckling och digitalisering. Där beskrivs kommunens vision, strategiska styrprinciper, vilken nytta arbetet ska ge Uppsala kommuns invånare och företag samt hur det stärker demokrati och öppenhet, hur det skapas tydliga och transparanta strukturer för IT-utveckling samt ansvar och uppföljning.

3.2.2 Policy för trygghet och säkerhet[4]

Policyn syftar till att beskriva kommunens förhållningssätt till begreppen trygghet och säkerhet. Den tydliggör principerna för ordning och planering av Uppsala kommuns trygghets- och säkerhetsarbetet före, under och efter oönskade händelser samt hur kommunen ska bidra till trygghet och säkerhet i det offentliga rummet och i de kommunala verksamheterna.

Policyn beskriver även Uppsala kommuns långsiktiga och systematiska trygghets- och säkerhetsarbete som främjar ett fortsatt hållbart växande Uppsala.

• Uppsala kommun ska vara en trygg och säker kommun för alla som bor, besöker och verkar här samt för kommunens verksamheter, egendom och ekonomi.

• Allas rätt att röra sig fritt i det offentliga rummet och att ta del av kommunens verksamheter ska inte begränsas av otrygghet.

Policyn vänder sig till hela kommunkoncernen, nämnder och bolag.

3.2.3 Strategisk plan för IT-utveckling och digitalisering

Planen utgår från *Policy för IT- utveckling och digitalisering* och har ett flerårigt perspektiv med fokus på hållbar verksamhetsutveckling kopplat till IT- och digitalisering. Det ska säkerställas utifrån fyra övergripande mål:

1. IT- styrning- Förändringar i IT-miljön sker samordnat i kommunen och leder till samutnyttjande av IT-lösningar, minimerande dubbelfunktioner och ett effektivt underhåll. IT-styrningen är integrerad i kommunens ledarskap och stärker innovationskraft och utveckling av framtida samhällslösningar.

[4] Beslutad av kommunfullmäktige 2018-06-11

2. Digitalisering- Kommunen är föredöme på att tillvarata och utveckla digitaliseringens möjligheter. Digitaliseringen utvecklar medborgardialogen och främjar hållbara lösningar. Digitalt är norm och det är enkelt att ha kontakt med kommunen. Öppna data inom kommunen stimulerar till innovation och underlättar insyn.
3. Verksamhetssystem- En tydligt dokumenterad uppsättning verksamhetssystem som drivs och utvecklas utifrån en gemensam IT-arkitektur.
4. IT-infrastruktur- En digital arbetsplats som främjar delaktighet, samverkan, hållbar utveckling och kommunens attraktivitet som arbetsgivare. En trygg och tillförlitlig IT-infrastruktur som utgör en stabil plattform för kommunens IT. Certifiering för hållbar och ansvarsfull produktion.

3.2.4 Handlingsplan för trygghet och säkerhet[5]

Handlingsplanens syfte är att beskriva det Uppsala kommun vill uppnå inom området trygghet och säkerhet. Där framgår även för tillfället pågående aktiviteter. Vidare är syftet att tydliggöra ordning och ansvarsfördelning när det gäller genomförande och uppföljning.

3.3 Organisation

I MSB:s metodstöd för systematiskt informationssäkerhetsarbete framgår hur ansvaret för arbetet med informationssäkerhet bör fördelas[6].

Det bör finnas en person inom organisationen med ansvar för att samordna informationssäkerhetsarbetet. I Uppsala kommun kallas den personen för *informationssäkerhetsstrateg*. Grundprincipen är att ansvaret för informationssäkerhetsarbete ska följa det ordinarie verksamhetsansvaret från ledning ner till enskilda medarbetare. Informationssäkerhetsstrategen har därmed inget formellt ansvar för informationssäkerheten utan ska verka som ett stöd för att den övriga organisationen innefattande ledning, verksamhetschefer och medarbetare tar sitt ansvar för informationssäkerhet i verksamheten.

Det är viktigt att tydligt klargöra informationssäkerhetstrategens roll och vilket mandat och rapporteringsplikt som ska ingå i rollen.

Var i organisationen informationssäkerhetsstrategen eller motsvarande är placerad beror på, enligt MSB:s metodstöd, på organisationens struktur men bör generellt vara placerad nära ledningen, exempelvis i en ledningsstab. Enligt metodstödet är vanliga organisatoriska placeringar exempelvis:

- Säkerhet
- Kvalitet
- Juridik

[5] Beslutad av kommunfullmäktige 2018-06-11. Gäller för perioden 2018-2020
[6] Avser en generell organisation. Enheter och likande i exemplet är inte direkt applicerbara på Uppsala kommuns organisation.

I de fall rollen är placerad i en strategisk IT-funktion såsom CIO-stab bör funktionen vara åtskild från organisationens interna IT-produktion och drift. Anledningen till det är att informationssäkerhetsstrategen både ska granska och vara kravställande gentemot IT-driften och riskerar annars att brista i opartiskhet.

3.3.1 Olika rollers ansvar avseende trygghet och säkerhet

I Uppsala kommuns policy för trygghet och säkerhet[7] framgår ansvarsfördelningen när det kommer till trygghets- och säkerhetsarbetet:

Kommunfullmäktige

- Beslutar om Policy för trygghet och säkerhet
- Beslutar om övergripande styrdokument

Kommunstyrelsen

- Samordnar, stödjer och följer upp kommunkoncernens trygghets- och säkerhetsarbete enligt reglementet
- Ansvarar för kommunikation och implementering samt uppföljning av policyn
- Samordnar arbetet inför och vid extraordinära händelser, säkerhetsskyddet samt allmän och intern säkerhet
- Leder kommunens arbete med civilt försvar
- Tar fram förslag till handlingsprogram för förebyggande verksamhet mot andra olyckor än bränder enligt lagen om skydd mot olyckor

Nämnder och bolagsstyrelser

- Svarar för trygghets-, säkerhets- och krisberedskapsarbetet inom sitt respektive verksamhetsområde samt har god kännedom om vilka särskilda skyldigheter som åligger dem gentemot personal, kommuninvånare och kommunens egendom
- Vid behov tar nämnder och bolag fram vägledningar och rutiner för att mer konkret beskriva hur arbetet ska utföras inom respektive organisatorisk enhet

Chefer och arbetsledare

- Ansvarar för att uppmärksamma risker och säkerhetsproblem samt initiera att åtgärder vidtas inom sina verksamhetsområden.
- Bidrar till kommunens samlade säkerhetsarbete i samverkan med andra interna och externa aktörer

Alla förtroendevalda och medarbetare

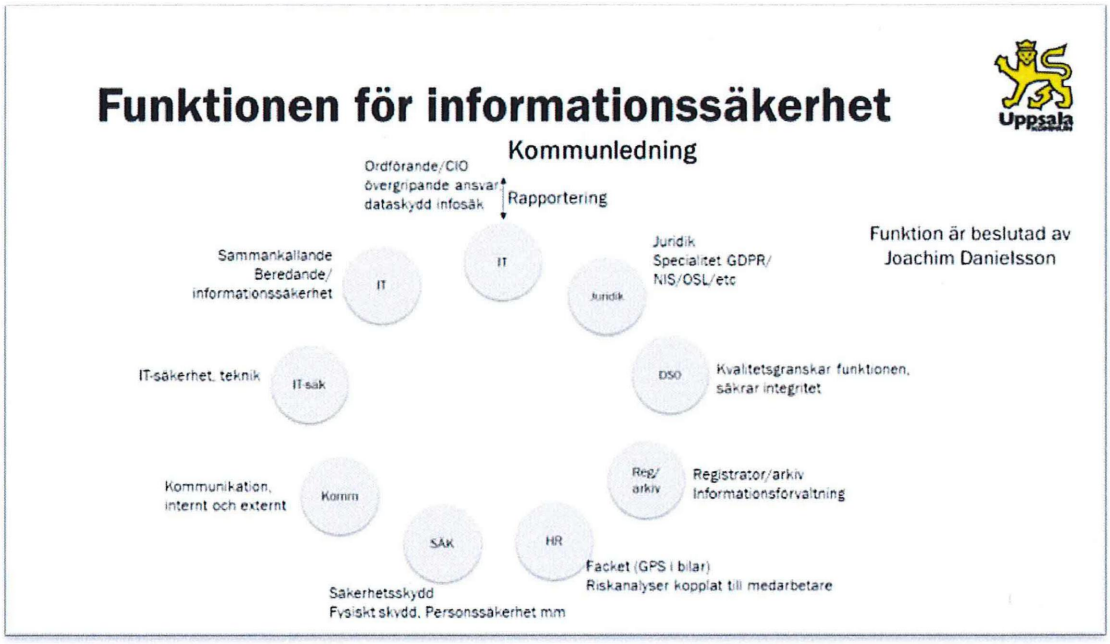
- Har ett personligt ansvar för att uppmärksamma och rapportera risker och säkerhetsproblem, samt

[7] Beslutad av KF 2018-06-11

- Att följa givna säkerhetsbestämmelser

3.3.2 Funktion för informationssäkerhet[8]

I Uppsala kommun finns en funktion för informationssäkerhet med syfte att strategiskt samordna frågor som rör informationssäkerhet och GDPR. Funktionen hade sitt första sammanträde i januari 2019 och har som mål att träffas sex gånger per år där fokus ska vara uppföljning av risker och incidenter samt aktiviteter.



Organisationskarta över Funktionen för informationssäkerhet

Funktionen är inte en del av linjeorganisationen i Uppsala kommun utan flera områden från verksamheten är representerade. Ordförande för funktionen är CIO och sammankallande för sammanträden är informationssäkerhetstrateg.

I linjeorganisationen ansvarar CIO för fem enheter, IT-strategi, IT-infrastruktur samt tre stycken systemförvaltningsenheter.

Informationssäkerhetsstrategen är organisatoriskt placerad under enheten för Strategi för IT-strategi. Enligt intervjuer anses opartiskheten i funktionen vara säkerställt i och med att flera andra verksamhetsområden är representerade. Bakgrunden till organiseringen och varför ordförandeskapet inte ligger på exempelvis säkerhetsfunktionen är enligt intervjuer att det historiskt sett funnits bättre förutsättningar och kompetens på området inom IT-organisationen.

[8] Beslutad av kommunledningen maj 2018

Säkerhetsfunktionen representeras i funktionen för informationssäkerhet av biträdande säkerhetsskyddschef.

Funktionen beskrivs i intervjuer som ett bra forum när det kommer till att identifiera och diskutera frågor som rör informationssäkerhet samt GDPR men funktionen befinner sig organisatoriskt i ett utvecklingsstadium. Det finns än så länge inget tydligt uppdrag, syfte och ansvar för gruppen. I handlingsplan för trygghet- och säkerhetsarbetet i Uppsala kommun[9] är en åtgärd att utvärdera funktionen och dess ändamålsenlighet.

3.3.3 IT-styrning

I Uppsala kommun används pm3-modellen för styrning av IT-system med fokus på förvaltning. Pm3 är en styrmodell med grund i systemförvaltning. Modellen bygger på samverkan mellan verksamhet och IT-stab och utgår i grunden från ett verksamhetsperspektiv. Modellen är tänkt att underlätta för verksamheten när det kommer till att tillgodose systembehov i dialog med IT och att säkerställa ett strukturerat arbete med bland annat informationssäkerhet. Modellen ska integreras med övriga arbetsformer för att fungera.

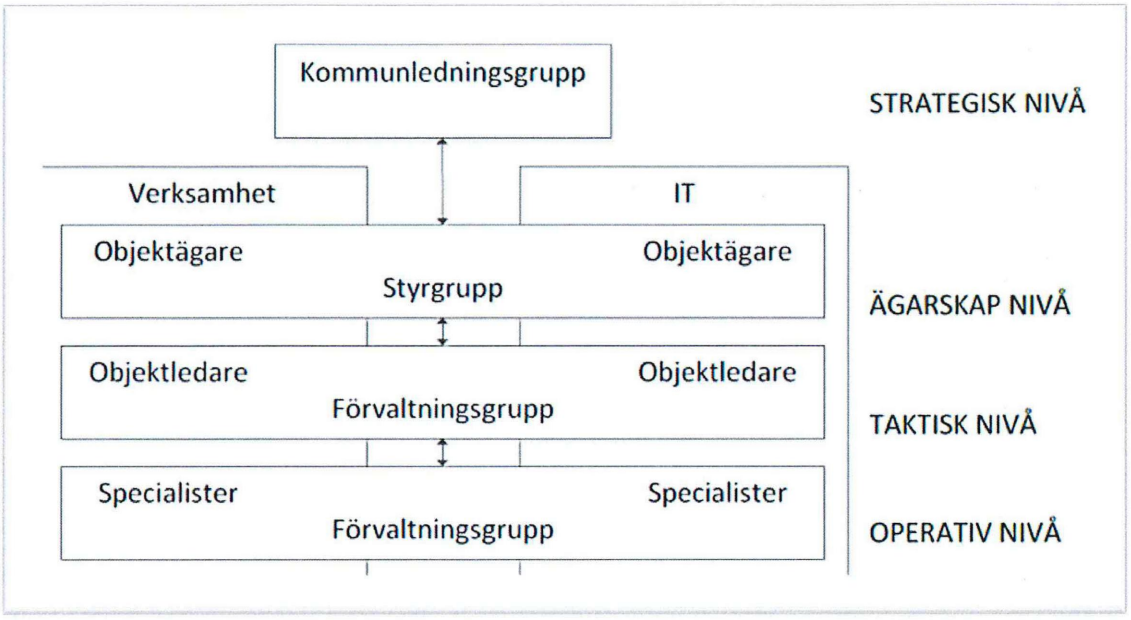
Det framgår av Uppsala kommuns riktlinje för förvaltningsstyrning av IT[10] hur modellen implementeras i kommunen. IT i Upsala kommun ska stödja verksamhet inom boende och trafik, företag och arbete, kultur och fritid, stöd och omsorg, skola och förskola samt styrning och den demokratiska processen.

Det förvaltas i form av objekt som styrs genom en objektplan med årlig förvaltningscykel. Antalet objekt bestäms utifrån hur kostnadseffektivt det är samt vad som ger bäst förutsättningar för största möjliga nytta i verksamheten genom IT. Ett objekt består av ett antal IT-system som grupperas utifrån vilken verksamhet de stödjer. Bilden nedan visar hur objekten är organiserade i Uppsala kommun.

[9] Se avsnitt 3.4.2
[10] Beslutad av Stadsdirektör och gällande för förvaltningar och kontor i Uppsala kommun.

Uppsala kommuns objekt.

Styrningen av IT sker i fyra beslutsnivåer: strategisk, ägarskap, taktisk och operativ. Varje av de fyra beslutsnivåerna utgår från två perspektiv: IT och verksamhet.



Struktur för förvaltningsorganisationen.

I nedanstående bild beskrivs vilket ansvar respektive funktion har:

	Roll	Ansvar och befogenhet
Strategisk nivå	**Kommunledning** KLG/Stadsdirektör CIO	• Besluta om indelning av kommunens förvaltningsobjekt. • Säkrar verksamhetsnytta och kostnadseffektiv hantering ur ett kommungemensamt helhetsperspektiv genom att verka för att realisera IT-policyn.
Ägarskap	**Objektägare verksamhet** Förvaltningsdirektör/er för den/de förvaltning/ar ett förvaltningsobjekt stödjer	• Att verksamheten följer gällande lagar och regler • Att förvaltningsobjektet har en förvaltningsplan • Att förvaltningsplanen följs upp periodiskt • Informationsansvar • Att riskanalys genomförs • Att besluta om större ändringar av förvaltningsplan • Säkra finansiering av förvaltningsplan
	Objektägare IT Enhetschef/er IT	• Att verksamhetens behov av IT tillgodoses • Att IT-stödet följer gällande lagar, riktlinjer, policyer och strategier
Taktiskt	**Objektledare verksamhet** Rollen tillsätts av objektägare verksamhet	• Utarbeta och verkställa förvaltningsplanen Beskrivning och sammanställning av krav • Prioritera, besluta, planera och följa upp aktiviteter inom plan • Eskalera behov till styrgrupp, till exempel resursbehov • Dokumentation • Genomföra riskanalys
	Objektledare IT Rollen tillsätts av objektägare IT	• Utarbeta och verkställa förvaltningsplanen • Prioritera, följa upp och planera IT-aktiviteter • Samordna resurser på IT-sidan enligt beslutade aktiviteter i förvaltningsplan • Samordna arbetet med problem, incident, test och release • Ställa krav på andra objekt och utvecklingsprojekt • Rapportera avvikelser till objektledare verksamhet och styrgrupp • Dokumentation • Genomföra riskanalys
Operativ	**Specialister** Varierar beroende av uppgift	Utför uppgifter enligt förvaltningsplan

Ansvarsbeskrivning för förvaltningsorganisationen.

Det ska varje år skapas en objektplan utifrån vilken förvaltningsobjekten styrs. Planen ska säkerställa att verksamhetsnyttan i mål och aktiveter överensstämmer med ett kommungemensamt helhetsperspektiv. Där ska följande ingå:

- Förvaltningsorganisation, roller, ansvar och befogenheter
- IT-system som ingår i förvaltningsobjektet samt beroenden till andra förvaltningsobjekt
- Mål, aktiviteter och budget
- Förvaltningsaktiviteter, anger hur förvaltningen genomförs, till exempel felhantering, ändringshantering, bevarande och gallring, periodisk översyn
- Bokföring av kostnader, möjliggör ekonomisk uppföljning
- Mötes- och beslutsforum

Enligt intervjuer infördes pm3 som förvaltningsmodell i början av 2010-talet men har inte lyckats fullt ut etableras. Det förklaras bland annat av personalförändringar som påverkat kontinuiteten i arbetet. Det är framförallt på förvaltningarna (verksamheten) som modellen inte fullt ut har etablerats. Enligt intervjuer är det en kulturfråga där ansvarsfördelningen mellan verksamheten respektive IT-funktionen upplevs som otydlig. Flera av objektledarna på verksamhetssidan har andra roller i linjeorganisationen utöver rollen som objektledare. Vidare har personalomsättningen för objektledare för en del objekt varit hög.

I intervjuer lyfts även en otydlighet avseende roller och ansvar mellan objektägare och objektledare. Förvaltningsmodellen pm3 är en matrisorganisation, med andra ord en organisationsmodell som går tvärs igenom den ordinarie linjeorganisationen. Objektägaren för verksamheten är ofta förvaltningsdirektör och har budgetansvar och linjemandat men är inte involverade i objektets taktiska arbete utan det arbetet leds av objektledaren. Objektledaren ansvarar för planering av förvaltningsplanen men vad som ska prioriteras bestäms av objektägaren vilket kan innebära en utmaning för objektledaren då denne ej har mandat för att genomföra förändringar som anses krävas. Enligt intervjuer är förståelsen låg för objektledarnas funktion på verksamhetssidan och det händer ofta att verksamhetens frågor går direkt via objektledaren på IT-sidan istället.

Det har genomförts utbildning i pm3 för objektledare men flera upplever trots det, enligt intervjuer, en osäkerhet i sin roll.

3.3.4 Bedömning

Finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna i kommunen?

Delvis. Vår bedömning baserat på styrdokument och intervjuades beskrivning av utvecklingsarbetet är att det finns en hög ambition avseende arbetet med informationssäkerhetsfrågor i Uppsala kommun men att organisationen än så länge inte är fullt implementerad. Pm3-modellen kräver mycket resurser. Att det är

resurskrävande märks tydligt på verksamhetssidan. Där upplevs en otydlighet och modellen behöver tydligare förankras för att fullt ut kunna implementeras i kommunen.

Vi ser positivt på att kommunen infört en funktion för informationssäkerhet som lyckas inkludera flera olika verksamhetsområden i informationssäkerhetsfrågorna vilket skapar förutsättningar för att flera olika perspektiv fångas upp. Däremot är funktionen än så länge i ett tidigt stadium och behöver utvärderas för att dess syfte ska tydliggöras. Vår bedömning är därför att funktionens syfte och funktion för närvarande är otydligt.

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

Nej. Vår bedömning är att roller och ansvar för informationssäkerheten inte är fullt ut tydliggjorda och uppfattade mellan verksamhet och IT-organisation.

Vi ser en risk i att kommunens CIO innehar ordförandeskapet för funktionen för informationssäkerhet. CIO ansvarar även för IT-drift samtidigt som CIO:n i sin roll som ordförande för funktionen för informationssäkerhet är kravställare och granskare av IT-driften. Utifrån vår bedömning att funktionen för informationssäkerhet för närvarande inte har ett tydliggjort syfte, uppdrag och ansvar går det inte att uttala sig om huruvida CIOs ordförandeskap för funktionen innebär någon risk eller ej.

Även informationssäkerhetsstrategen är placerad i IT-organisationen men avskild från enheten för IT-drift. Vi ser därmed ingen anmärkningsvärd risk avseende informationssäkerhetsstrategens placering.

Avseende styrningen av informationssäkerheten är vår bedömning att det framförallt från ett verksamhetsperspektiv är otydligt i pm3-modellen vad som förväntas av verksamheten och vilka krav som kan ställas på IT-funktionen avseende arbetet med informations- och IT-säkerhet.

3.4 Informationssäkerhetsarbete

3.4.1 Säkerhetsklassningar

För att tydliggöra att olika typer av information har olika värde för verksamheten genomför Uppsala kommun säkerhetsklassningar. Kommunen ska därefter kunna skapa förutsättningar för lämpliga skyddsnivåer. Detta görs genom två verktyg, dels kommunens systemöversikt och dels med stöd av KLASSA, framtaget av SKR[11]. Enligt KLASSA ska tre aspekter bedömas i en informationsklassning:

- Konfidentialitet
- Riktighet
- Tillgänglighet

Utifrån varje aspekt ska informationen klassas utifrån följande nivåer:

[11] Sveriges Kommuner och Regioner

- Nivå 0= ingen eller försumbar skada
- Nivå 1= måttlig skada
- Nivå 2= betydande skada
- Nivå 3= allvarlig skada
- Nivå 4= synnerligen allvarlig skada

Eftersom skadeverkningarna av bristande säkerhet uppstår hos informationsägaren, dvs verksamheten, är det informationsägaren som måste bedöma risker och ställa krav bland annat genom informationsklassning. Efter klassningen ska åtgärdsplaner upprättas.

Enligt intervjuer har klassning av system inte genomförts fullt ut och i varierande grad mellan olika förvaltningsobjekt. Fokus har legat på de system som bedöms som mest kritiska. Klassningen genomförs av objektledarna för respektive förvaltningsobjekt med stöd av informationssäkerhetsstrateg.. Det varierar, enligt intervjuer, i vilken utsträckning objektledarna på verksamhetssidan involveras i informationsklassningen, i vissa fall har objektledaren för IT-funktionen själv genomfört klassningen. När det kommer till att upprätta åtgärdsplaner baserat på säkerhetsklassningen har det arbetet nyligen startat och endast ett fåtal åtgärdsplaner är färdigställda.

Det finns dokumenterade rutiner för riskhantering i Uppsala kommun[12] Där framgår att hanteringen ska ge välgrundade beslutsunderlag. Fokus är de risker som kan hindra verksamheten från att uppfylla sitt uppdrag. Den som leder arbetet med riskhanteringen ska ha kompetens som krävs och sträva efter att förhålla sig objektiv till det område som riskhantering gäller. Riskhanteringen ska även dokumenteras på ett sätt som gör det möjligt att följa risken från identifiering till åtgärd och att personer som inte varit involverade ska kunna förstå det.

3.4.2 Handlingsplan för trygghet- och säkerhet med fokus på informations- och cybersäkerhet

Informations- och cybersäkerhet är ett utav sex målområden för ökad säkerhet[13] i Uppsala kommuns handlingsplan för trygghet- och säkerhet 2018-2022[14].

Det övergripande målet avseende informations- och cybersäkerhet formuleras som följer:

”Uppsala kommuns arbete inom informations- och cybersäkerhet håller en hög nivå för att säkerställa att kommunens information är tillgänglig, riktig och hanteras på ett konfidentiellt och spårbart sätt utifrån ett verksamhetsperspektiv.”

[12] Beslutat av kvalitetschef 2018-10-11
[13] Övriga målområden: Internt skydd- och personsäkerhet, skydd mot olyckor, riskhänsyn vid samhällsplanering och byggande, krisberedskap, civilt försvar
[14] Antagen av kommunfullmäktige 2018-06-11

I vilken omfattning informations- och cybersäkerhet omfattas styrs av verksamhetsbehovet. Informations- och cybersäkerhet syftar till att informationen utifrån ett verksamhetsperspektiv:

- Ska vara tillgänglig när den behövs
- Ska vara tillförlitlig
- Inte sprids till obehöriga
- Är spårbar i avseendet att det går att följa hur och när informationen hanterats.

I handlingsplanen presenteras ett antal åtgärder som ska vidtas för området. Vissa åtgärder avser 2018 då handlingsplanen beslutades, vissa avser medellång sikt, 2019–2020.

Åtgärder	Huvudansvarig för åtgärd	Andra berörda aktörer	Tidplan för genomförande
Åtgärder 2018			
63. Ta fram och implementera styrdokument för informationssäkerhet	KS	Nämnder och berörda styrelser	2018
64. Stödja nämnder och bolag i implementering av nya styrdokument inom området	KS		
65. Etablera en för kommunen gemensam funktion för informationssäkerhet	KS	Nämnder och berörda styrelser informeras inför beslut om dataskyddsombud	2018
66. Införa generell IT-lösning för säker lagring och kommunikation	KS		2018
67. Vidareutveckla former och arbetssätt för informationssäkerhet inom verksamhetsutveckling	KS		2018
68. Genomföra projekt gällande hantering av personuppgifter i enlighet med dataskyddsförordningen	KS		2018
Åtgärder på medellång sikt 2019-2020			
69. Etablera process för informationssäkerhets incidenter	KS	Nämnder och berörda styrelser informeras	2019
70. Genomföra en utbildning i informationssäkerhet för högre ledning, nämnder och styrelser	KS		2019-2020
71. Utvärdera styrning och effekthemtagning av funktion	KS		2019-2021

för informationssäkerhet samt vid behov besluta om åtgärder			

Åtgärder från handlingsplanen avseende Informations- och cybersäkerhet.

3.4.3 Intern kontroll

I kommunstyrelsens internkontrollplan för 2019[15] berörde två kontrollmoment informationssäkerhetsområdet:

16. **Kontrollmoment: Säkerhetsklassificerad information – utan anmärkning**

Förslag på åtgärder utifrån kontrollmomentet: *"Resultatet visar att det finns en tydlig ansvarsfördelning och väl fungerande rutiner för att säkerhetsklassificera information i kommunens IT-system. Kontrollmomentet fortsätter att följas upp under 2019."*

Uppföljning 2019- mindre anmärkning

Förslag på åtgärder utifrån uppföljningen: *Rutiner för uppdatering av systemöversikten och Klassa ska ses över, implementeras och genomföras senast hösten 2019. I samband med detta ska även objektledare utbildas både i informationssäkerhetsklassning och i verktyget Klassa. Klassa som system behöver under året placeras i ett förvaltningsobjekt för att därigenom upprätthålla användarstöd samt även kunna påverka SKL i vidareutveckling av verktyget avseende användbarhet och rapportmöjligheter. År 2020 ska modell, verktyg och arbetssätt för informationssäkerhetsklassning av information, handlingar och andra informationstillgångar vara framtaget.*

17. **Kontrollmoment: Informationssäkerhet – mindre anmärkning**

Förslag på åtgärder utifrån kontrollmomentet: "*Resultatet av granskningen återrapporteras till nämnden i samband med uppföljning av kommunstyrelsens internkontrollplan 2019."*

Uppföljning 2019- mindre anmärkning

Förslag på åtgärder utifrån uppföljningen: *Utöver redan pågående åtgärder behöver följande genomföras inom ramen för förvaltningsobjekten:*

- *Arbetssätt avseende riskhantering, upprättande av riskregister och uppföljning av åtgärder. Klart Q2 2020*
- *Riktade insatser inom åtkomststyrning utifrån riskexponering behöver genomföras liksom medvetandehöjande åtgärder. Klart Q2 2020*
- *Utbildning incidenthantering. Klart Q4 2019*

[15] Uppföljning beslutad av KS 2018-11-19

3.4.4 Utbildning

Utifrån intranätssidan *Insidan* framgår att Uppsala kommun genomför utbildning i informationssäkerhet i form av en digital utbildning framtagen av Myndigheten för samhällsskydd och beredskap (MSB), *Informationssäkerhet i praktiken*. Syftet är att medarbetarna ska få en översiktlig bild av hur det systematiska informationssäkerhetsarbetet kan stödja det dagliga arbetet.

Utbildningen sker genom ”nanolearning” där varje deltagare får avsnitt om ca 3-5 min skickade via e-post. Totalt består utbildningen av 12 pass:

1. En introduktion till informationssäkerhet.
2. Vem arbetar med informationssäkerhet?
3. Analysera mera (information om bl.a. om att kartlägga processer, informationssäkerhetsklassa, riskanalyser samt ta fram informationshanteringsplaner).
4. Verksamhetsanalys.
5. Omvärldsanalys.
6. Informationssäkerhetsklassning.
7. Riskanalys del 1.
8. Riskanalys del 2.
9. Riskanalys del 3.
10. GAP-analys.
11. Riskhantering.
12. Avslutning.

Utbildningen genomfördes för första gången år 2019 och det är kommunledningskontoret, ledamöter i nämnder och styrelser, de kommunala bolagen samt förvaltningsdirektörer som fått inbjudan. Enligt uppgift ska utbildningen utvecklas mot att 2020 nå ut till fler.

3.4.5 Bedömning

Finns ett systematiskt och ändamålsenligt arbetssätt för att uppnå god informationssäkerhet dokumenterat och förankrat i kommunens verksamheter?

Delvis. Vår bedömning är att det finns en ambitiös struktur som kommunen inte fullt ut efterlever. Information i verksamhetens olika system säkerhetsklassas i en del fall av objektledare för IT-funktionen istället för verksamheten. Vi bedömer det som en risk då det är verksamheten som tar skada om säkerheten i systemen inte är tillräcklig. Verksamheten är kravställare gentemot IT och vi bedömer det därför ej som ändamålsenligt att IT-organisationen själv innehar den rollen.

Vi bedömer det som positivt att utbildning i informationssäkerhet har börjat genomföras men att detta arbete måste utvecklas för att säkerställa att alla med ansvar för informationssäkerhet har tillräcklig kunskap och kännedom.

Arbetar kommunens verksamheter systematiskt med att identifiera och analysera risker för informationssäkerheten?

Delvis. Risker avseende informationssäkerheten har lyfts i kommunens interna kontrollplan. Det genomförs delvis informationssäkerhetsklassningar av en del system men det arbetet är inte fullt ut genomfört. Dessutom är organisationen för att arbeta med klassningen inte fullt ut implementerat i verksamheten. Vår bedömning är därför att kommunens verksamheter arbetar med att identifiera och analysera risker för informationssäkerheten men att det än så länge inte sker systematiskt.

Görs systematiska uppföljningar av genomförda åtgärder för att kontinuerligt förbättra informationssäkerheten?

Delvis. Kommunen har utifrån policy för trygghet och säkerhet utvecklat en handlingsplan med åtgärder för att förbättra informationssäkerheten men det arbetet är i ett tidigt stadium.

När det kommer till åtgärdsplaner utifrån KLASSA har det till viss del upprättats men inte fullt ut. Vidare har åtgärder föreslagits utifrån de risker avseende informationssäkerhet som identifierades i kommunstyrelsens internkontrollplan 2019 vilka har följts upp under året.

Vår bedömning är därmed att en del uppföljningar genomförs men stora delar av arbetet är nyligen påbörjat och sker inte systematiskt.

4 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen inte fullt ut säkerställt ett ändamålsenligt och systematiskt arbete med sin informationssäkerhet. Baserat på styrdokument och intervjuades beskrivning av pågående utvecklingsarbete har Uppsala kommun en hög ambitionsnivå när det kommer till informationssäkerhetsarbetet. Vi bedömer det som positivt att flera åtgärder har och är planerade att genomföras för att förbättra kommunens organisation för informationssäkerhet. Vår bedömning är dock att organisationen inte implementerats fullt ut och ännu inte klarar att leva upp till den höga ambitionsnivån. Framförallt är verksamheten inte tillräckligt förankrad i arbetet vilket medför att IT-staben har tagit en stor roll.

Det har nyligen införts en funktion för informationssäkerhet där flera områden i Uppsala kommuns organisation är representerade. Det är chefen för IT-staben, CIO, som leder det strategiska arbetet avseende informationssäkerhet. Vi bedömer det som en risk då ansvarig för det strategiska informationssäkerhetsarbetet samtidigt ska vara kravställare gentemot IT. Det arbetet riskerar att försvåras om arbetet leds från samma organisation.

Det har även påbörjats ett arbete med att säkerhetsklassa informationen i kommunens olika system för att bättre kunna anpassa resurser utifrån informationssäkerhetsrisker.

En del åtgärdsplaner utifrån klassningen har upprättats. Det är dock ett nyligen påbörjat arbete och har inte genomförts fullt ut.

4.1 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen att:

- Säkerställa att funktionen för informationssäkerhet utvärderas och att dess syfte och funktion tydliggörs.
- Säkerställa att roller och ansvar mellan IT och verksamhet tydliggörs.
- Säkerställa att tillräcklig utbildning ges för att medvetandegöra informationssäkerhetsansvaret för alla inom Uppsala kommun.
- Säkerställa att arbetet med informationssäkerhetsklassning implementeras fullt ut i kommunen.

Datum som ovan

KPMG AB

Sara Linge
Certifierad kommunal yrkesrevisor

Daniel Strandberg
Kommunal revisor

A Styrdokument, riktlinjer och policyer

Titel	Fastställt	Av vem	Typ
Policy för trygghet och säkerhet	2018-06-11	KF	Policy
Policy för IT-utveckling och digitalisering	2015-10-05	KF	Policy
Riktlinje för riskhantering	2016-09-14	KS	Riktlinje
Rutin för riskhantering	2018-10-11	Kvalitetschef	Rutin
Strategisk plan för IT-utveckling och digitalisering	2016-09-14	KF	Övriga planer
Program för digital transformation och utveckling	Utkast	KF	Program
IT-utveckling	Okänt	Okänt	Riktlinje
Styrning av kommunens IT-system	Okänt	Okänt	Riktlinje
Incidenthantering	Okänt	Okänt	Riktlinje
Öppna data (anvisning)	Okänt	Okänt	Riktlinje
Riktlinje för nätverksanslutna skrivare	2007-01-09	IT-strateg	Riktlinje
Regler för internetanvändning	Okänt	Stadsdirektör	Styrdokument
Riktlinjer för sociala medier	2012-03-07	KS	Riktlinje
Riktlinjer för tjänstetelefon	2017-08-18	Okänt	Riktlinje

Regler och riktlinjer för användning av e-post	2018-12-20 (rev)	Okänt	Styrdokument
Beslut om automatisk vidarebefordran av e-post	2019-05-14	CIO	Beslut
Handlingsplan för trygghet och säkerhet	2018-06-11	KF	Övriga planer
Riktlinjer för styrning av IT	2012-05-09	KS	Riktlinje
Åtagande för verksamhetsansvarig i samband med behörighetshantering	2011-11-11	Okänt	Styrdokument
Regler för lösenord	2018-08-09	IT-strateg	Insidan
Läs mer om rutinen för granskning av behörigheter i kommungemensamma system	2013-06-15	Informationssäkertsstrateg	Rutin
Rutinbeskrivning vid skyddad identitet för anställd	2018-05-23	Okänt	Rutin
Policy för upphandling och inköp	2018-03-26	KF	Policy
Riktlinjer för upphandling och inköp	2018-03-26	KF	Riktlinje
Vägledning för Facebook	2017-10-10	Presschef	Vägledning
Vägledning för Instagram	2017-10-10	Presschef	Vägledning
Vägledning för Linkedin	2017-10-10	Presschef	Vägledning
Vägledning för Twitter	2017-10-10	Presschef	Vägledning
Riktlinjer distansarbete	Okänt	Okänt	Riktlinje

Ansluta till nätverket utifrån	2019-04-02	EC IT	Insidan
Arbete i hemmet och utanför kontoret	2018-01-22	Förvaltningsdirektör SCF	Rutin
informationssäkerhet i projekt	2018-01-22	Okänt	Insidan
Informationssäkerhetsklassning	2019-03-15	KLK	Insidan
Säkerhetsskydd	2019-05-14	Säkerhetssamordnare	Insidan
Lär dig mer om informationssäkerhet	2017-11-09	Informationssäkertsstrateg	Insidan
Mobil telefoni	2018-02-27	FO	Insidan
E-post guider Office 365	2017-03-13	FO	Insidan
Att arbeta med IT-utveckling	2016-11-04	IT-strateg	Insidan
Förteckning riskhantering i kommunen	2018-12-03	Kvalitetschef	Insidan
Personuppgiftsbiträdesavtal	2018-07-02	IT-strateg	Insidan
Säkerhet, personuppgifter och sekretess	2018-07-16	Webbutveckling	Insidan
Nyhet för säker kommunikation via e-post	2018-02-13	Kommunikation KLK	Insidan