Granskning av Informationssäkerhet

Rapport

Falu kommun och kommunala bolag

KPMG AB

2020-06-10

Antal sidor 32

Antal bilagor 0

Falu kommun och kommunala bolag
Granskning av Informationssäkerhet

2020-06-10

Innehållsförteckning

1 Sammanfattning

Vi har av Falu kommuns revisorer och lekmannarevisorer fått i uppdrag att översiktligt granska kommunen och kommunala bolags rutiner kring arbetet med informationssäkerhet. Granskningen har omfattat kommunstyrelsen, kommunens samtliga nämnder, Falu Stadshus AB, Kopparstaden AB, Falu Energi & Vatten AB, Lugnet i Falun AB och Falu Elnät AB. Granskningen omfattar år 2020.

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen och bolagen inte har säkerställt ett ändamålsenligt och systematiskt arbete med sin informationssäkerhet. Det saknas tillräckliga styrdokument då de som finns inte är implementerade i verksamheten, delvis föråldrade och i behov av revidering. Det finns en otydlighet över hur de kommunala bolagen ska förhålla sig till kommunens styrdokument och ett bolag saknar idag styrande dokument.

Det saknas i nuläget en organisation för arbetet och verksamheternas ansvar är otydligt i förhållande till IT. Fram tills nu har IT-funktionen i kommunen och bolagen tagit en stor roll i arbetet utifrån sin tekniska kompetens och de lösningar som är tillgängliga utifrån resurser och inte utifrån en riskbedömning som ansvariga för informationen har gjort.

Vi bedömer det som positivt att ett utvecklingsarbete har påbörjats för ökad informationssäkerhet både i kommunen och i bolagen. För både kommunen och bolagen framgår att det strategiska utvecklingsarbetet planeras med utgångspunkt i ett ledningssystem för informationssäkerhet i enlighet med rekommendationer från MSB[1] vilka bygger på ISO27001-standarden. Vi uppfattar att dessa intentioner för kommunen och bolagens informationssäkerhetsarbete har goda förutsättningar att ge den systematik och struktur som i nuläget saknas. Slutligen är vår bedömning att samordning i arbetet för informationssäkerhet mellan kommunen och de kommunala bolagen kan utvecklas. Vår uppfattning är att kommunkoncernen både säkerhetsmässigt och ekonomiskt skulle vinna på en tydligare samordning av dessa frågor där samtliga bolag inkluderas i arbetet och det kan ske genom en utvecklad koncernsamverkan.

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen, kommunens samtliga nämnder samt bolag att:

- Säkerställa att det finns aktuella och implementerade styrdokument avseende informationssäkerhet
- Säkerställa att det finns en hållbar organisation för att driva ett systematiskt informationssäkerhetsarbete och beakta på vilka sätt en samordning mellan kommun och kommunala bolag kan ske
- Säkerställa att roller och ansvar mellan Informationssäkerhetssamordnare, IT och verksamhet tydliggörs

[1] Myndigheten för Samhällsskydd och Beredskap

- Säkerställa att tillräcklig utbildning ges för att medvetandegöra informationssäkerhetsansvaret för alla inom Falu kommun och dess kommunala bolag
- Säkerställa att arbetet med informationssäkerhetsklassning implementeras fullt ut i kommunen och de kommunala bolagen
- Tydliggöra rapporteringsvägar för informationssäkerhet och säkerställa att ledningens genomgång blir en årlig rapportering till berörda

Vidare rekommenderar vi kommunstyrelsen att:

- Tydliggöra i vilken utsträckning de kommunala bolagen omfattas av kommunens styrdokument avseende informationssäkerhet
- Tydliggöra roll och uppdrag för informationssäkerhetssamordnaren så att det framgår hur detta ansvar ser ut internt i kommunen och i förhållande till de kommunala bolagen

2 Bakgrund

KPMG har av Falu kommuns förtroendevalda revisorer och lekmannarevisorer fått i uppdrag att genomföra en granskning av kommunstyrelsens, nämndernas och de kommunala bolagens informationssäkerhetsarbete. Uppdraget ingår i revisionsplanen för år 2020.

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

Informationssäkerhet innebär att skydda information utifrån krav på dess konfidentialitet, riktighet och tillgänglighet och måste skyddas mot obehörig åtkomst, såväl externt som internt. Vidtagna IT-säkerhetsåtgärder ska stå i relation till informationstillgångarnas värde och de risker och behov som ansvariga för informationen har fastställt. Detta då IT-säkerheten avser att säkra och trygga driften och hanteringen av kommunens kärnverksamheter.

Hotbilden med risker för intrång förändras kontinuerligt och säkerhetsarbetet behöver därför vara en ständigt pågående process för att säkerställa att kommunens informationstillgångar har ett tillräckligt skydd. För att kunna hantera det på ett ändamålsenligt sätt krävs att kommunen har ett systematiskt informations-säkerhetsarbete där flera funktioner i kommunen är involverade och rätt organiserade för uppdraget.

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

2.1 Syfte, revisionsfråga och avgränsning

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

Granskningen ska besvara följande revisionsfrågor:

- Finns aktuella styrande dokument som tydliggör vilka krav som ställs och hur arbetet ska bedrivas?
- Sker en tillräcklig uppföljning att styrande dokument är kända och efterlevs?
- Finns en ändamålsenlig organisation för att arbeta med informationssäkerhetsfrågorna?
- Är roller och ansvar för informationssäkerheten tydliggjord och uppfattad mellan verksamhet och IT-organisation?
- Finns ett systematiskt arbete med att identifiera och analysera behov och risker för att säkerställa informationssäkerheten?
- Görs systematiska uppföljningar av genomförda åtgärder för att kontinuerligt förbättra informationssäkerheten?

— Finns det en ändamålsenlig samordning mellan kommunen och kommunens bolag när det gäller informationssäkerhet?

Granskningen har omfattat kommunstyrelsen, kommunens samtliga nämnder, Falu Stadshus AB, Kopparstaden AB, Falu Energi & Vatten AB, Lugnet i Falun AB och Falu Elnät AB. Granskningen omfattar år 2020.

2.2 Revisionskriterier

Vi har bedömt om rutinerna uppfyller

— Tillämpbara interna regelverk, policyer och beslut
— MSB:s metodstöd avseende Ledningssystem för informationssäkerhet
— NIS[2]-direktivet i tillämpliga delar avseende kartläggning och analys av risker

2.3 Metod

Granskningen har genomförts genom:

Dokumentstudier av:

— Informationssäkerhetspolicy och tillhörande riktlinjer
— Rutiner för incidenthantering
— Riktlinjer för hantering av personuppgifter
— Klassningsdokumentation och exempel

Intervjuer med berörda tjänstepersoner:

För Falu kommun
Kommundirektör, informationssäkerhetssamordnare, verksamhetsutvecklare socialförvaltningen, administrativ chef miljö- och samhällsbyggnadsförvaltningen, sektorchef och administrativ chef för arbetsmarknad och integrationskontoret, administrativ chef kultur- och fritidsförvaltningen, administrativ chef sektor service, kommunikatör kommunikationskontoret, systemförvaltare personalkontoret, IT-säkerhetskoordinator.

För kommunala bolag
VD Falu Stadshus AB, VD, Kopparstaden, IT-chef, Kopparstaden, VD Falu Energi och vatten, IT- och utvecklingsansvarig Falu energi och vatten, Funktionsansvarig IT Falu Energi och vatten, tf. VD Lugnet i Falun AB, chef ekonomi och administration Lugnet i Falun AB.

[2] NIS= Network and Information System. Lag om informationssäkerhet för samhällsviktiga och digitala tjänster

Granskningen har genomförts av Jenny Thörn, kommunal revisor, och Linnéa Grönvold, kommunal revisor. Magnus Larsson har medverkat som kundansvarig för revisionen i Falu kommun.

Faktagranskning för Falu kommun har genomförts av informationssäkerhetssamordnaren. För de kommunala bolagen har faktagranskning skett av VD för respektive bolag.

3 Inledning

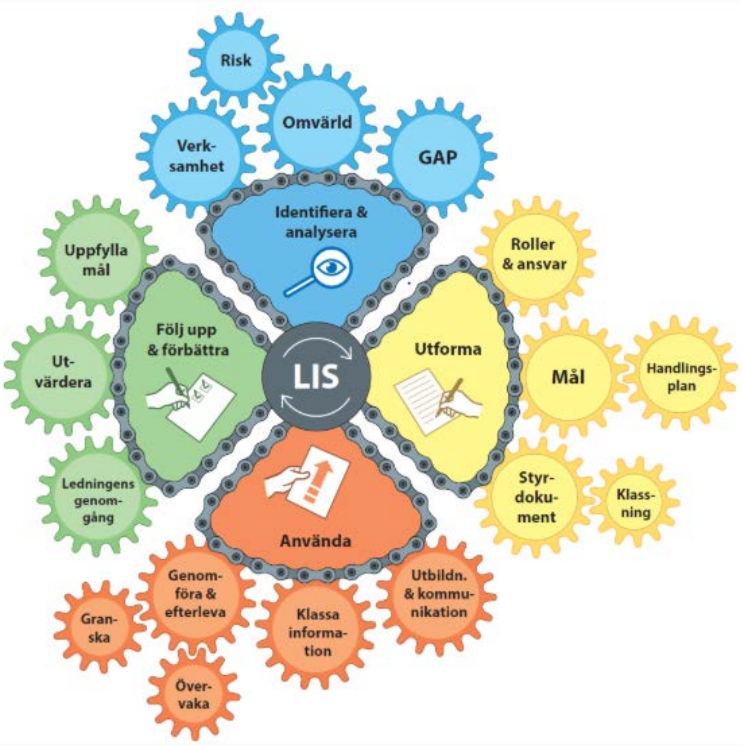
Vi har med utgångspunkt i MSB:s metodstöd för informationssäkerhet och gällande standard inom området granskat om arbetet i Falu kommunkoncern är strukturerat och ändamålsenligt. Inkluderade i granskningen är Falu kommun, Falu Stadshus AB som moderbolag bestående av bolagen Kopparstaden AB, Lugnet i Falun AB samt Falu Energi & Vatten AB med dotterbolaget Falu Elnät AB.

Falu Stadshus AB och Lugnet i Falun AB omfattas av de styrdokument som är beslutade av kommunen. I övrigt har bolagen egna styrdokument som vi redogör för under avsnitten för respektive bolag.

3.1 MSB:s metodstöd för systematiskt informationssäkerhetsarbete

MSB 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. Certifiering sker mot standarden ISO 27001 vilken styr krav för informationssäkerhet.

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



Metodstödet och de fyra metodstegen med underliggande metoddelar.

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

Ledningens förståelse för och engagemang i informationssäkerhet är grundläggande för att lyckas. Med andra ord måste ledningen få kunskap om hur de kan leda och styra verksamheten på ett effektivt sätt för att åstadkomma god informationssäkerhet. Ledningens stöd är också oumbärlig för att frågan ska få acceptans och ett engagemang från andra roller i organisationen.

Det bör finnas en person inom organisationen med ansvar för att samordna informationssäkerhetsarbetet. Grundprincipen är att ansvaret för informationssäkerhetsarbete ska följa det ordinarie verksamhetsansvaret från ledning ner till enskilda medarbetare. Informationssäkerhetssamordnaren 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 informationssäkerhetssamordnarens roll och vilket mandat och rapporteringsplikt som ska ingå i rollen.

Var i organisationen informationssäkerhetssamordnaren eller motsvarande är placerad beror på organisationens struktur men bör generellt vara placerad nära ledningen, exempelvis i ledningsstaben. Vanliga organisatoriska placeringar, enligt MSB:s metodstöd är exempelvis:

- Säkerhet
- Kvalitet
- Juridik

I de fall rollen är placerad i en strategisk IT-funktion såsom CIO[3]-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] Titel för person på direktörsnivå som svarar för ett företags interna informationssystem

4 Resultat av granskningen avseende Falu kommun

4.1 Styrdokument

I Falu kommun finns styrdokument för informationssäkerhet i form av en policy och tillhörande säkerhetsinstruktioner. Nedan följer en kort beskrivning av informationssäkerhetspolicy och tillhörande informationssäkerhetsinstruktioner.

Det framkommer i intervjuer en enig bild att beslutade styrdokument inte har implementerats i kommunens verksamhet. De är inte kända och används inte för att styra kommunens arbete med informationssäkerhet. Delar av innehållet används i introduktionsutbildning för nyanställda. Av intervjupersonerna så känner någon till att det finns policydokument, andra har eftersökt dessa inför denna granskning och därigenom fått kännedom om vad dessa innehåller.

Det framgår vidare att styrdokumenten är föråldrade och inte aktuella att implementera. Det ingår i det kommande utvecklingsarbetet för informationssäkerhet att säkerställa att nya och aktuella styrdokument finns som tydliggör ansvar och hur arbetet ska bedrivas.

Policy för Informationssäkerhet

I policyn anges den övergripande politiska inriktningen för Informationssäkerhet. Falu kommuns policy för informationssäkerhet är beslutad av kommunfullmäktige 2010-10-07. Den bygger till stora delar på den för tiden gällande utformningen och rekommendation från MSB.

I dokumentet framgår av en organisationsbild hur styrdokument för informationssäkerhet förhåller sig till varandra. I den framgår att policyns viljeriktning tydliggörs i ett antal informationssäkerhetsinstruktioner som är målgruppsanpassade för att styra arbetet.

I intervjuer framkommer att policy och instruktioner utformades av kommunens nuvarande informationssäkerhetssamordnare under ett sommarjobb på Falu kommun under studietiden vid högskolan.

Det framgår bland annat i policyn att:

> ”Informationssäkerheten är en integrerad del av Falu Kommuns verksamhet. Alla som hanterar informationstillgångar har ett ansvar att upprätthålla informationssäkerheten. Det är också ett ansvar för chefer på alla nivåer att aktivt verka för en positiv attityd till informationssäkerheten samt att informationssäkerhetspolicyn med tillhörande instruktioner efterlevs”.

Följande strategier finns beskrivna i dokumentet för att uppnå målen att säkerställa informationens tillgänglighet, riktighet och konfidentialitet. Det framgår även som mål att ”säkerhetsarbetet får inom rimliga gränser inte underordnas funktionalitet och ekonomi”.

3.2. Strategier för att nå målen

- All personal måste ha **kunskap** om gällande informationssäkerhetsregler.
- All personal ska vara förvissade om att **informationsförsörjningen** är säker och effektiv samt bidrar till ökat skydd och stöd för medarbetare, samverkande parter och tredje man.
- Ingångna **avtal** ska vara kända och följas av de som berörs av avtalen.
- Alla investeringar både i form av **informationshantering** och **teknisk utrustning** ska skyddas i tillräcklig grad, exempelvis genom brandskydd, skalskydd, IT-säkerhetssystem, serviceavtal och garantier.
- Det ska finnas en gemensam, säker och väl definierad **infrastruktur** för extern och intern datakommunikation.
- **Hotbilden** för varje enskilt informationssystem som är av vikt för vår verksamhet ska analyseras fortlöpande.
- **Händelser** i informationssystemen som kan leda till negativa konsekvenser förebyggs. Incidenter av betydelse för informationssäkerheten ska loggas.
- Det är viktigt att **krishanteringsförmågan** upprätthålls.

Det framgår vidare att årliga mål för informationssäkerhetsarbetet ska formuleras i kommunens övergripande informationssäkerhetsplan. Någon informationssäkerhetsplan har dock inte upprättats sedan policyn beslutades.

Informationssäkerhetsinstruktion för förvaltning

Denna informationssäkerhetsinstruktion beskriver hur systemägare och systemansvariga ska hantera informationssystem i kommunen. Den beskriver bland annat roller och ansvar, regler och rutiner för system och generella regler.

Informationssäkerhetsinstruktion för användare

Personal och förtroendevalda

Informationssäkerhetsinstruktionen som riktar sig till personal och förtroendevalda beskriver hur medarbetare och förtroendevalda inom Falu Kommun ska hantera information samt använda IT-stöd och datorsystem på ett säkert sätt med Falu Kommuns informationssäkerhetspolicy som grund.

Information i styrdokumentet ligger till grund för den del i introduktionsutbildning som erbjuds nyanställda avseende IT-användning och informationssäkerhet. Det ska även undertecknas en ansvarsförbindelse efter att medarbetaren tagit del av policy och säkerhetsinstruktion. Det är chefernas ansvar att säkerställa att detta genomförs. Det finns ingen övergripande uppföljning över hur stor del av de anställda som tagit del av informationen.

Elev

Det finns även informationssäkerhetsinstruktioner för elev som ska signeras när dessa får ett konto i kommunens nätverk. Av dokumentet framgår hur elever inom bildningsförvaltningen ska använda IT-stöd och datorsystem på ett säkert sätt med Falu Kommuns informationssäkerhetspolicy som grund.

Kund

Informationssäkerhetsinstruktion för kunder beskriver hur kunder till Falu kommun ska använda ”Min sida” på ett säkert sätt med Falu Kommuns informationssäkerhetspolicy som grund. Instruktionen bygger på ett antal principer från erfarenheter av användandet av e-tjänster inom kommunen.

Informationssäkerhetsinstruktion för kontinuitet, drift och utveckling

Informationssäkerhetsinstruktion Kontinuitet, drift och utveckling gäller för IT/Organisation. I instruktionen finns avsnitt som beskriver organisation och ansvar, interna nätverk och krav samt löpande åtgärder. Det finns även avsnitt som beskriver kommunens kontinuitetsplanering vid händelser av kris eller katastrof. Grunden till kontinuitetsplanen ska enligt instruktionen utgöras av en riskanalys av informationssystemens sårbarheter samt vilka hot som kan finnas mot verksamheten. Regelbundna tester av kontinuitetsplaneringen ska genomföras och uppdateras vid förändringar.

Kommunens incidenthantering beskrivs i informationssäkerhetsinstruktionen men då dokumentet är föråldrat stämmer inte informationen med nuvarande rutiner som beslutats för incidenthantering. Gällande rutin finns publicerad på intranätet. I intervjuer ges exempel på förvaltningar som har informerat anställda om rutinen. Antal incidenter som rapporteras är lågt vilket kan vara en indikation på att rutinen inte är tillräckligt känd i verksamheten. En förklaring som ges i intervjuer är också att det har varit svårt att få medarbetare att se rapportering av incidenter som en del i ett ständigt förbättringsarbete och lärande. Det uppfattas som ett angiveri där någon utpekas i att brista i sin hantering av personuppgifter eller informationssäkerhet.

4.1.1 Bedömning

Det finns beslutade styrdokument för kommunens informationssäkerhetsarbete. Dessa är dock inte implementerade i verksamheten för att kunna efterlevas. De är i nuläget inte styrande för hur roller och ansvar ser ut eller för hur arbetet ska bedrivas.

Då de är föråldrade och därigenom inte aktuella behöver samtliga dokument i form av policy och säkerhetsinstruktionen revideras. En plan för hur dessa ska implementeras i samtliga verksamheter bör tas fram för att berörda inom kommunen ska ha tydliga instruktioner över ansvar och vad som förväntas för att säkerställa en god informationssäkerhet.

Det framgår inte av dokumenten att dessa även är styrande för kommunala bolag. Två av de kommunala bolagen (Lugnet i Falun AB samt Falu Stadshus AB) anser sig enligt uppgift i intervjuer omfattas av kommunens beslutade policys och riktlinjer för informationssäkerhet. Därför behöver man i arbetet tillse att även deras behov och

förutsättningar beaktas i utformningen av nya styrdokument så att de är tillämpbara även för verksamhet som bedrivs av kommunala bolag.

4.2 Organisation för informationssäkerhet

I Falu kommun är säkerhetsarbetet organiserat i kommunstyrelseförvaltningen på ett risk- och säkerhetskontor. En säkerhetschef leder gruppen och rapporterar direkt till kommundirektören. Inom verksamheten finns även beredskapssamordnare, säkerhetssamordnare, ansvarig för Brottsförebyggande rådet, och samordnare för olycksfall och vattensamordning. I nuläget är inte informationssäkerhetsarbetet organiserat med övrigt säkerhetsarbete men kan vara en tänkbar placering när arbetet övergår i mer förvaltning än uppbyggnad.

I samband med att styrdokument beslutades år 2010 fanns planer på att inrätta en roll som informationssäkerhetskoordinator vilket är en roll som beskrivs i styrdokument. Den var då tänkt att vara placerad på IT-avdelningen. I intervjuer beskrivs det att arbetet aldrig kom igång på ett strukturerat sätt. Det ansvar som var tilldelat avsades på grund av tidsbrist då det inte skedde någon omprioritering av arbetsuppgifter som gav förutsättningar att driva informationssäkerhetsarbetet.

I december 2019 tillsatte kommunen en informationssäkerhetssamordnare som ansvarar för att driva utvecklingen av kommunens arbete med informationssäkerhet. Tjänsten är nyinrättad i kommunen och arbetet är under uppstart. Man har gjort bedömningen att den bästa placeringen i nuläget för informationssäkerhets-samordnaren är på stadskansliet men att detta kan ändras när formerna för arbetet har fastställts. Närmaste chef är i nuläget kanslichef på stadskansliet vilken rapporterar till kommunstyrelsens ledningsutskott.

I samband med anställning tydliggjordes vad uppdraget som samordnare innefattar. I intervjuer upplever både samordnaren själv och övriga i verksamheterna att det finns en tydlighet över samordnarens roll och uppdrag i informationssäkerhetsarbetet. Ett flertal av intervjupersonerna uttrycker att de ser fram emot det arbete som ska påbörjas då det tidigare saknats någon som håller ihop arbetet och säkerställer att det sker på ett systematiskt och likartat sätt i hela kommunen. Det framhålls dock att man ser risker med att det inte finns någon organisation för informationssäkerhetsarbetet och att det t byggs upp kring en person. Det medför att det blir både personberoende och sårbart. Rollerna behöver förtydligas så all personal vet vad man har ansvar för, var man kan få stöd och hur arbetet ska genomföras. Det framkommer en bild av att ingen direkt har tagit tag i frågorna tidigare och att det inte har funnits ett strukturerat arbete med informationssäkerhet i kommunen.

Det finns i nuläget inga utsedda personer från förvaltningarna som ska driva informationssäkerhetsarbetet inom respektive verksamhet. I förstudie som genomförts har representation funnits från förvaltningarna.

För GDPR-arbetet har samordnare utsetts som är organiserade i en GDPR-grupp vilket upplevs ha fungerat bra för informationsspridning och samarbete för att hjälpa varandra i GDPR-relaterade frågor. Tankar finns att organisera även arbetet med

informationssäkerhet på ett liknande sätt men det är i nuläget oklart om samordnarna för GDPR ska få ett utökat uppdrag som även inkluderar informationssäkerhet i stort eller om andra funktioner också ska ingå. I intervjuer beskrivs att det är otydligt vilket mandat man som samordnare har. Uppdraget är att säkerställa att det sker ett aktivt arbete med GDPR på förvaltningen men samordnare upplever inte att de har mandat att ge chefer i uppdrag att vidta de åtgärder som behövs.

Ansvar för informationssäkerheten följer det ordinarie verksamhetsansvaret för kommunens chefer. Förvaltningscheferna är informationsägare och i vissa fall systemägare och därigenom ansvariga för verksamhetens hantering av information. Det är också chefernas ansvar att säkerställa att alla medarbetare har kunskap och kännedom om sitt ansvar för informationshantering. Det framkommer i intervjuer att det fortfarande lever kvar en bild att det är IT-avdelningen som har ansvar inom området, det beskrivs därför att det behöver förtydligas vad verksamheterna själva ansvarar för och hur gränsdragningen mellan informationssäkerhet och IT-säkerhet ser ut. Under granskningen har vi noterat att det finns en stor vilja att arbeta med informationssäkerhet inom kommunen och dess betydelse för verksamheten är förankrat i förvaltningarna men att den kompetens och resurser som krävs för att driva arbetet har saknats.

Även IT-avdelningen har en betydande roll i informationssäkerhetsarbetet även om det till stor del innebär att vara mottagare av beställningar från verksamheterna. Även om inte styrdokumenten är implementerade så framgår detta ansvar tydligt i informationssäkerhetsinstruktionen för kontinuitet och drift. IT-avdelningen uppger att de i sin utförarroll utgår från denna instruktion och informationssäkerhetspolicyn även om de inte är aktuella, då det inte finns någon annan styrning att rätta sig efter.

Vi uppfattar i intervjuer att det finns förvaltningar där man upplever en tydlighet i hur ansvaret för de olika delarna av informationssäkerhet är fördelat mellan förvaltningarna och IT-avdelningen. Samtidigt framkommer från andra en bild att detta fortfarande är otydligt, främst för att IT-avdelningen tidigare varit drivande i arbetet och verksamheterna inte har kommit igång i sitt arbete och tagit det ansvar som de har.

Även om samarbetet uppges ha blivit bättre de senaste åren upplever man från IT-avdelningens sida att det i stora delar saknats en dialogpart och tydlig beställare för att kunna leverera till verksamheten. Från vissa av intervjupersonerna från förvaltningarna framkommer att det historiskt funnits en uppfattning att IT-avdelningen bestämmer över förvaltningarnas system och IT-tjänster. Samtidigt beskrivs att man är medveten att man varit dåliga på att styra och beställa det stöd och åtgärder som man är i behov av vilket i sin tur har lett till att IT-avdelningen tvingats ta beslut utifrån sitt perspektiv och kunskap.

Det nämns av flera intervjupersoner att både arbetet med informationssäkerhet och systemförvaltning behöver bli mer strukturerat och vikten av att hela kommunen arbetar på ett likartat sätt. Idag saknas ansvariga för vissa system och därigenom någon för IT-avdelningen att ha en dialog med för hanteringen av system och säkerhetsåtgärder.

I Falu kommun saknas i nuläget en beslutad systemförvaltningsmodell. Ett arbete pågår som utgår från den vedertagna modellen pm3 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 och utgår i grunden från ett verksamhetsperspektiv. Planen i Falu kommun är att införa modellen i en lite mindre skala utifrån lokala förutsättningar och behov. 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.

En inventering har genomförts på förvaltningarna för att alla system ska bli kända. IT-avdelningen har en systemförteckning som de utför driftåtgärder utifrån. I inventeringen framkom system som inte fanns på denna lista. När uppdateringar eller åtgärder inte vidtas för system kan detta utgöra en risk i skyddet för de tillgångar som finns i detta system. I planeringen ingår att införa och tydliggöra systemförvaltningsroller och att arbetssätt och roller implementeras i samtliga verksamheter. Detta är något som flera intervjupersoner har lyft i granskningen och som efterfrågas som en del i informationssäkerhetsarbetet.

4.2.1 Bedömning

Vår bedömning är att kommunstyrelsen inte har säkerställt att det finns en ändamålsenlig organisation för informationssäkerhetsarbetet i kommunen. Trots att det beslutats om styrdokument för närmare tio år sedan där en organisering beskrivs har inte kommunstyrelse eller nämnder gett verksamheten i uppdrag att verkställa en organisation i enlighet med dessa styrdokument. Det har inte heller efterfrågats någon rapportering över arbetet med kommunens informationssäkerhet.

Vi ser positivt på att kommunen nu infört en funktion för informationssäkerhet med en central placering i organisationen. Det är dock av stor vikt att kommunen säkerställer att det byggs upp en hållbar organisation som inte är alltför personberoende och sårbar i det kommande utvecklingsarbetet. Funktionen informationssäkerhetssamordnare är ny i kommunen och det är viktigt att det finns en tydlighet i ansvarsfördelning mellan samordnaren, förvaltningarna och IT-avdelningen som är kommunicerad och uppfattad. Informationssäkerhetssamordnaren har inget formellt ansvar för kommunens informationssäkerhet utan ska ha en stödjande roll och till viss del granskande för att ledning, chefer och medarbetare tar sitt ansvar för informationssäkerhet i verksamheten.

Vår bedömning är att ansvariga för informationen i förvaltningarna inte har tagit sitt ansvar för att säkerställa en god informationssäkerhet för kommunens informationstillgångar. Roller och ansvar behöver därför tydliggöras samt uppdrag beskrivas så att det finns en tydlighet i vad detta ansvar innebär och vilka åtgärder som behöver vidtas. Alla medarbetare och förtroendevalda har ett ansvar för sin hantering av information och sitt IT-användande, i det arbete som hittills bedrivits så har inte utbildning- och informationsinsatser genomförts för att säkerställa detta och det finns inte aktuella och implementerade styrdokument som beskriver ansvaret för var och en.

4.3 Informationssäkerhetsarbetet i praktiken

I intervjuer framkommer en enad bild om att det inte har funnits något aktivt och strukturerat informationssäkerhetsarbete i kommunen förrän informationssäkerhetssamordnare anställdes i slutet av 2019. Det finns exempel från verksamheter där ett mer strukturerat arbete har genomförts och man kommit lite längre. Av material vi har tagit del av är Arbetsmarknad och integrationskontoret ett sådant exempel.

På övergripande nivå var det inte förrän arbetet med GDPR startade som man på allvar påbörjade ett arbete kring personuppgifter och informationssäkerhet. De flesta intervjupersoner beskriver kommunens informationssäkerhet utifrån det GDPR-arbete som genomförts.

Det finns inte något Ledningssystem för informationssäkerhet, LIS, i nuläget men det beskrivs att ett sådant är grunden i det påbörjade utvecklingsarbetet för informationssäkerhet. Arbetet ska enligt intervjupersoner bygga på MSB:s rekommendationer och metodstöd för LIS och följa ISO27001-standarden. Det finns i nuläget inga planer på att certifiera kommunen i enlighet med ISO 27001.

Då en intern medarbetare rekryterades till tjänsten som informationssäkerhetssamordnare fanns redan från starten en god kännedom om kommunens struktur och system då tidigare anställning varit på IT-avdelningen med uppdrag inom både IT-relaterade frågor och som projektledare för kommunens samordnade GDPR-arbete.

Arbetet med GDPR strukturerades som ett projekt där nuvarande informationssäkerhetssamordnare var projektledare. I projektet ingick representanter från de olika förvaltningarna och sektorerna genom utsedda GDPR-samordnare. De insåg i det arbetet att det fanns otroliga brister i hantering av information i helhet men också gällande personuppgifter. De bestämde då att bygga upp arbetet kring personuppgifter i första hand. Ett likande upplägg finns med i planeringen för det kommande informationssäkerhetsarbetet. Att skapa nätverk av personer som har detta som ansvar och vara kontakt i verksamheterna.

Uppdrag för informationssäkerhetsarbetet ges av kommunledningsgruppen som där även återrapportering sker. Det arbete som har genomförts hittills har utgått från det första steget i metodstödet för informationssäkerhet där kommunen identifierar och analysera nuläget. Informationssäkerhetssamordnaren har i arbetet genomfört en förstudie kring informationshantering och förvaltning. I projektet har representanter från förvaltningarna deltagit.

I maj 2020 deltog informationssäkerhetssamordnaren på kommunledningsgruppen och presenterade ett förslag till plan för det kommande arbetet. I planen fanns ett förslag att koppla ihop åtgärder för informationssäkerhet med det arbete som kommunen genomför med processkartläggning och styrning i effektiva processer. Det innebär i stort att arbetet med informationssäkerhet blir en stödprocess till identifierade huvudprocesser i verksamheterna. I projektet med effektiva processer har verksamhetsutvecklarna fått i uppdrag att dokumentera vilken information som hanteras i varje process, som en del i informationssäkerhetsarbetet.

Kommunledningsgruppen beslutade i enlighet med förslaget och arbetet ska nu påbörjas tillsammans med projektledare för effektiva processer.

Informationshanteringen förändras konstant beroende på organisatoriska förändringar, teknisk utveckling eller förändrade hotbilder och ställer därför krav på ständiga anpassningar och förbättring av det systematiska informationssäkerhetsarbetet. Genom en strukturerad övervakning och mätning ges förutsättningar för att utvärdera i vilken grad informationssäkerheten är ändamålsenligt utformad, har avsedd verkan, samt att säkerhetsåtgärder existerar och fungerar tillfredsställande. En viktig del i arbetet framgår av metodstödets avsnitt för att följa upp och förbättra. En del i detta arbete är ”ledningens genomgång” där kommunstyrelse och kommunledning får information om arbetet och får möjlighet att vara delaktiga samt bedöma vilka förbättringsåtgärder som behöver prioriteras för att säkerställa arbetet med informationssäkerhet.

Enligt information i intervjuer saknas tydliga rapporteringsvägar för informationssäkerhet men detta ingår i arbetet som nu är påbörjat i kommunen. I nuläget sker en rapportering till kommunledningsgruppen. Det har inte skett någon regelbunden rapportering till styrelse eller nämnder avseende informationssäkerhet, främst på grund av att inget aktivt arbete har bedrivits i kommunen. Presentation har genomförts gällande GDPR och ansvaret som personuppgiftsansvariga och personuppgiftsincidenter delges styrelse och nämnder löpande. I vissa nämnder har även viss information om informationssäkerhet getts men det framkommer att det är svårt att få tillräckligt med tid för att hinna gå igenom det på ett tillräckligt sätt.

Behörighetshantering

I intervjuer beskrivs att det finns rutiner för tilldelning av behörigheter för applikationer som används inom organisationen. Dessa är verksamhetsspecifika och behörigheter utgår inte från någon kommunövergripande hantering.

Ansvarig chef beställer den behörighet som användaren behöver baserat på den anställdes roll respektive arbetsuppgifter. Detta sker genom en e-tjänst för beställning på intranätet. Systemförvaltare eller utsedd administratör tilldelar sedan behörigheten för avsett system.

Det framgår i intervjuer att det främst är inom socialförvaltningen och omsorgsförvaltningen som det finns rutiner och lagkrav vad gäller åtkomst till information. Där sker loggkontroll och stickprov kvartalsvis för att upptäcka eventuella avvikelser.

Det beskrivs vidare att rutiner behöver utvecklas generellt vad gäller ändringar eller avslut av behörigheter då det händer att det missas och behörigheter finns kvar hos medarbetare som inte längre ska kunna ha åtkomst i vissa system. Det finns även sårbarheter i hanteringen av kommunens mappstruktur och vissa system där det inte finns stöd eller rutiner för hanteringen av åtkomst och ansvaret därför ligger helt på att inte någon medarbetare tar del av information som den inte ska ha behörighet och åtkomst till.

Säkerhetsklassningar och riskanalyser

För att tydliggöra att olika typer av information har olika värde för verksamheten bör en klassning av information och system genomföras. Kommunen kan därefter skapa förutsättningar för lämpliga skyddsnivåer.

Detta görs oftast med en systemöversikt där ansvar och roller är definierade och dels med stöd av någon metod för informationsklassning. I Falu kommun har ett inledande arbetet skett med stöd i metoden KLASSA, som är en metod framtagen av SKR[4].

Enligt KLASSA ska tre aspekter bedömas i en informationsklassning:

- Konfidentialitet
- Riktighet
- Tillgänglighet

Utifrån varje aspekt ska informationen klassas utifrån följande nivåer:

- 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. Åtgärdsplanerna handlar om olika saker där IT-säkerhetsåtgärder rent tekniskt är en del. Det kan även vara att göra mer utförliga risk- och konsekvensanalyser, förbättra rutiner eller andra åtgärder som bedöms nödvändiga för att säkerställa säkerheten för informationstillgångarna.

Enligt intervjuer har klassning av system inte genomförts mer än på ett fåtal system och arbetet är inte systematiserat. I samband med införande av ett nytt verksamhetssystem inom omvårdnadsförvaltningen, socialförvaltningen och sektor arbetsmarknad och integration skedde en informationsklassning av samtliga tillgångar. Informationssäkerhetssamordnaren ledde arbetet och i nuläget ansvarar projektledaren för implementeringen av verksamhetssystemet för de åtgärder som framkom efter klassningen. Vissa av dessa har redan åtgärdats medan andra planerats in som en del i genomförandet. Kommunens medicinskt ansvariga sjuksköterska har gjort bedömningen att kommunens verksamhet inom hälso- och sjukvården omfattas av NIS-direktivet. Då det nya verksamhetssystemet kommer innehålla journaluppgifter var informationsklassningen en viktig del för att efterleva NIS-direktivet. Intervjupersoner

[4] Sveriges Kommuner och Regioner

säger att det planerade utvecklingsarbetet för informationssäkerhet blir viktigt för att kommunen ska upprätthålla en efterlevnad av de lagar som styr verksamheten.

Informationsklassning är enligt den planering vi har tagit del av en av aktiviteterna som ska påbörjas under 2020 tillsammans med riskanalyser. De förvaltningar som påbörjat klassning av sin information och system har tagit stöd av informationssäkerhetssamordnaren. Intervjupersoner beskriver att det är ett tidskrävande arbete att gå igenom allt men att resultatet och att få en bra överblick över sin information och säkerhet är värt mödan de behöver lägga ner. Och att det arbetet är direkt nödvändigt för att dokumentera och kunna vidta åtgärder för att förbättra informationssäkerheten. I de åtgärdsplaner som hittills upprättats i samband med informationsklassning har ansvariga utsetts för olika uppgifter men endast ett fåtal åtgärder har hunnit påbörjas.

Det har inte skett något systematiskt arbete med riskanalyser för kommunens informationssäkerhet. Viss riskhantering har skett i de personuppgiftsbehandlingar som registrerats i GDPR-arbetet. I kommunens internkontrollplan för 2020 finns kontrollmål för GDPR där samtliga behandlingar ska gås igenom och revideras.

I intervju med IT-säkerhetskoordinator framkommer att bristen av tydlighet i verksamheternas ansvar inom informationssäkerhet och systemförvaltning leder till att IT-avdelningen får göra egna bedömningar av vilka IT-säkerhetsåtgärder som behövs. Exempelvis finns inte systemförvaltare utsedda för alla system eller så är ansvaret för dessa otydligt. Att genomföra en klassning föder krav på verksamheten att åtgärda de brister som eventuellt framkommer vilket kan medföra kostnader för nya systemlösningar. Nya hot och risker leder till att kommunen kontinuerligt behöver arbeta med sina säkerhetsåtgärder. I många delar väljer verksamheterna att nå upp till den lägsta möjliga nivån för sina säkerhetslösningar för att det inte ska bli för höga kostnader.

Informationssäkerhetssamordnaren bekräftar också otydligheten men säger samtidigt att det funnits ett välfungerande säkerhetsarbete inom IT med ett stort intresse för dessa frågor. Genom det finns en god säkerhetskultur i kommunens IT-miljö vilket ger en grundtrygghet. Säkerheten är däremot inte baserad på informationsklassning och det går därför inte att säkerställa att vidtagna åtgärder står i relation till hur skyddsvärd informationen är. Det har inte genomförts några tester för att utvärdera att nuvarande IT-säkerhetsåtgärder är tillräckliga. Det har dock inte skett några intrång som lett till konsekvenser eller incidenter för kommunens informationstillgångar.

I intervjuer framkommer en medvetenhet om att det i nuläget finns sårbarheter i informationshanteringen. Vissa av dessa kommer inom kort att avhjälpas genom att nya system implementeras där en kravställning har skett kring inbyggd säkerhet i upphandlingsförfarandet. Exempel som lyfts i intervjuer är gemensamma mappar på server där det inte finns någon behörighetsstyrning, användning av kommunikationsvägar via sociala medier där verksamhetsinformation delas samt andra faktorer där medarbetare utgör en risk på grund av att de inte har tillräcklig kunskap om informationssäkerhet eller dataskyddsarbete.

4.3.1 Bedömning

Vår bedömning är att det inte finns ett ändamålsenligt arbetssätt för att uppnå god informationssäkerhet. Det har inte skett något strukturerat och systematiskt arbete med detta inom förvaltningarna förutom de delar som hör till efterlevnad av GDPR. Arbetet med informationsklassning är precis påbörjat och det är endast ett fåtal av kommunens informationssystem som har säkerhetsklassats. När det kommer till åtgärdsplaner utifrån KLASSA har det arbetet påbörjats och vissa åtgärder föreslagits. Det är dock ett nyligen påbörjat arbete och det återstår en stor del innan detta är fullt ut genomfört.

Vår bedömning är därmed att en del uppföljning har genomförts men att stora delar av arbetet är nyligen påbörjat och sker inte på ett systematiskt sätt. Detsamma gäller för riskanalyser där detta endast har genomförts i samband med inköp av nya systemlösningar eller för de system där arbetet med KLASSA har gjorts.

Hot och risker är därför inte identifierade så att verksamheten kan beställa de IT-säkerhetslösningar som står i relation till hur skyddsvärd informationen är. De IT-säkerhetsåtgärder som finns idag utgår i stort utifrån den kunskap och erfarenhet som IT-avdelningens medarbetare besitter kring de tekniska lösningar som finns tillgängliga.

Verksamheten är kravställare gentemot IT och vi bedömer det därför ej som ändamålsenligt att IT i stora delar saknar dialogpart på grund av att ansvariga i verksamheten brustit i ett strukturerat arbete med sin informationssäkerhet. Vi bedömer det som en risk då det är verksamheten som tar skada om säkerheten i systemen inte är tillräcklig.

Vår bedömning är att hanteringen av behörigheter och åtkomst till system och information behöver utvecklas då det i nuläget endast finns ett strukturerat arbete med åtkomsthantering inom vissa system och verksamheter.

Det saknas utbildningsinsatser och informationstillfällen har varit få för att skapa en tillräcklig medvetenhet hos medarbetarna i kommunen över ansvar för informationssäkerhet. De insatser som skett har främst varit inriktade mot efterlevnad av GDPR. Detta är en del i informationssäkerhet men långt ifrån tillräckligt för att säkerställa en god säkerhet för informationstillgångarna. Medarbetare, förtroendevalda och andra samarbetspartners med tillgång till kommunens informationstillgångar är en stor säkerhetsrisk om inte en tillräcklig kunskap finns över var och ens ansvar för informationssäkerheten och hantering av IT-system och utrustning. Det låga antal incidenter som rapporteras riskerar att vara en konsekvens av att det inte är tillräckligt känt vad som är en informationssäkerhetsincident och att dessa behöver rapporteras för att ett systematiskt förbättringsarbete kan ske. I Falu kommuns fall är vår bild att det låga antalet incidenter inte står i relation till att det inte sker några incidenter utan främst på att kunskapsnivåerna och medvetenheten kring informationssäkerhet är låg.

5 Resultat av granskning avseende de kommunala bolagen

5.1 Falu Stadshus AB

Falu Stadshus AB ägs helt av Falu kommun. Bolaget har i sin roll som moderbolag endast förvaltande uppgifter och inga anställda eller egna verksamhetssystem. Det informationssäkerhetsarbete som genomförs är därigenom helt styrt av de rutiner och åtgärder som vidtas av Falu kommun.

Bedömning

Utifrån de iakttagelser vi gjort över informationssäkerhetsarbetet i Falu kommun som även omfattar Falu Stadshus AB är vår bedömning att det saknas styrande dokument som tydliggör ansvar och hur arbetet ska bedrivas. Det framgår inte i styrdokument om och vilka av de kommunala bolagen som omfattas av policy och riktlinjer.

Vi anser att det behöver förtydligas på koncernnivå hur de kommunala bolagen ska underställa sig de av kommunen beslutade styrdokumenten, hur arbetet ska bedrivas samt hur rapporteringsvägarna ska se ut.

För Falu Stadshus AB:s del så finns inga egna verksamhetssystem där en informationsklassning behöver genomföras och inte heller någon egen personal som behöver medvetandegöras över ansvar för informationssäkerhet.

Det behöver därigenom förtydligas hur de inom kommunen som ansvarar för informationssäkerhetsarbetet ska inkludera och beakta behov som finns hos de kommunala bolagen som ingår i deras ansvar.

5.2 Lugnet i Falun AB

Lugnet i Falun AB (LUFAB) äger och förvaltar fastigheter och anläggningar inom området Lugnet i Falu kommun samt är en aktiv aktör i utvecklings- och exploateringsfrågor inom Lugnet-området.

I intervju beskrivs läget för bolaget. Lugnet i Falun AB är mitt i ett utvecklingsarbete och har implementerat ett flertal policys under året. En utredning av bolaget har tidigare visat brister i styrning och ledning varpå en tf. VD tillträdde i augusti 2019 med uppdrag att skapa ordning och reda. Det anställdes även en ansvarig för ekonomi och administration. Förutom att implementera nya policys så har det även funnits behov att utveckla arbetet med intern kontroll som helt saknats tidigare. De tillämpar nu kommunens riktlinjer för intern kontroll.

I intervjun framkommer även att bolaget enligt ägardirektiv omfattas av kommunens policys och de har en skyldighet att följa det som kommunen beslutar. De nyttjar i så stor utsträckning som möjligt de funktioner som kommunen tillhandahåller, exempelvis ekonomifunktion, jurist, IT mm. Det skapar en effektivitet att som litet bolag inte behöva

organisera en egen verksamhet för detta. Ägardirektiven ses för närvarande över och de nya ska förhoppningsvis vara förtydligade gällande mål för bolaget.

Det sker en formell ägardialog fyra gånger per år. Rapportering sker till moderbolaget Falu Stadshus AB. De får även uppdrag och direktiv därifrån. Intervjupersonerna beskriver att det har skett en utveckling av koncerntänket och att mer gemensamma frågor hanteras. Bland annat har det skett ett gemensamt arbete inom GDPR där en kartläggning av känslig information har skett. Bolaget ska också använda sig av ett nytt fastighetssystem som implementeras inom sektor service i kommunen, de kommer även att vara informationsägare för systemet. Bolaget litar på att kommunen gör säkerhetsklassning och andra åtgärder som är nödvändiga för att upprätthålla en god informationssäkerhet.

Det framkommer i intervjuer att bolaget ibland glöms bort och de måste till stor del själva vara på tå och visa att de finns och de behov de har. Bolaget inte har varit involverade i det arbete som hittills har påbörjats avseende informationssäkerhet och det har inte skett något internt arbete för att säkerställa en god informationssäkerhet för Lugnet i Faluns informationstillgångar. De äger i nuläget ett eget system som inte delas med Falu kommun vilket är ett övervakningssystem för driften av anläggningarna på Lugnet. IT-avdelningen ansvarar inte för uppdateringar och säkerhet för systemet men däremot kommunikationen som sker i systemet. I nuläget finns ingen support om det sker något utanför kontorstid när IT-avdelningen inte är i tjänst. De har påtalat det vid ett flertal tillfällen att de har andra behov då anläggningarna är öppna på andra tider. Enligt intervjupersoner har IT-avdelningen startat en utredning för att se över om det går att skriva serviceöverenskommelser som även kan tillämpas utanför kontorstid.

Det har enligt intervjupersonerna inte skett någon utbildning för bolagets medarbetare kring informationssäkerhet och var ens ansvar i arbetet. Det har skett en mer informell dialog om att låsa sin dator och mer användarinriktade tips över hantering av telefon och de bärbara datorerna som medarbetare på bolaget använder.

5.2.1 Bedömning

Utifrån de iakttagelser vi gjort över informationssäkerhetsarbetet i Falu kommun som även omfattar Lugnet i Falun AB är vår bedömning att det saknas styrande dokument som tydliggör ansvar och hur arbetet ska bedrivas. Det framgår inte i styrdokument om och vilka av de kommunala bolagen som omfattas av policy och riktlinjer.

Vi anser vidare att det behöver förtydligas på koncernnivå hur de kommunala bolagen ska underställa sig de av kommunen beslutade styrdokumentet, vad som förväntas och hur rapporteringsvägarna ska se ut.

Då nuvarande styrdokument är föråldrade och i behov av revidering är vår bedömning att bolaget bör säkerställa att nya styrdokument även kan fungera för deras verksamhet och vara ett stöd för hur arbetet ska bedrivas.

För Lugnet i Falun AB:s del så delar de ett flertal system med kommunen och tar därigenom del av de aktiviteter och åtgärder som genomförs för dessa system av ansvariga inom kommunen. Inom bolaget finns ett eget verksamhetssystem där en informationsklassning behöver genomföras vilket inte är gjort. Bolaget har visserligen få anställda men vi anser att ändå vara av vikt att dessa har fått grundläggande

kunskaper om informationssäkerhet och IT-användande för att kunna ta sitt ansvar för att bolagets informationstillgångar hanteras på ett säkert sätt.

Vi har fått bilden att Falu kommuns medarbetare inte känner till att Lugnet i Falun AB ska likställas med en förvaltning gällande bolagets IT och därigenom omfattas av de styrdokument och den organisering av informationssäkerhetsarbetet som beslutas av kommunen. Det behöver därför förtydligas på vilka sätt kommunen ska inkludera och beakta behov som finns hos det kommunala bolaget samt säkerställa att en samordning och dialog sker. Vi ser vidare att bolaget bör ta ansvar för sitt eget deltagande i det kommunövergripande arbetet för att ta del av information och kunskap som finns hos informationssäkerhetssamordnare och andra representanter inom Falu kommun.

5.3 Falu Energi och Vatten AB/Falu Elnät AB

Falu Energi & Vatten, FEV är en kommunal energibolagskoncern med ansvar för el, elnät, fjärrvärme, fjärrkyla, kraftproduktion, stadsnät, återvinning samt vatten och avlopp i Falu kommun. Falu Elnät AB ingår som dotterbolag i den kommunala energibolags-koncernen och är ett renodlat nätbolag för distribution av elkraft. Falu Elnät AB har ingen egen organisation utan omfattas i sin helhet av styrning hos FEV vad gäller informationssäkerhetsarbetet.

Bolaget har ca 200 medarbetare.

5.3.1 Styrdokument

I inledningen av bolagets informationssäkerhetspolicy framgår att:
”Informationssäkerhet är den del i organisationens ledningssystem som avser hantering av verksamhetens information. Informationssäkerhetspolicyn och särskilda instruktioner styr Falu Energi & Vattens informationssäkerhetsarbete”.

Av dokumentet framgår att nuvarande policy gäller från 2017-12-01. Informationssäkerhetspolicyn redovisar FEV:s inriktning och mål för informations-säkerhetsarbetet och konkretiseras i tre informationssäkerhetsinstruktioner:

- Informationssäkerhetsinstruktion Avdelning
- Informationssäkerhetsinstruktion Kontinuitet och Drift
- Informationssäkerhetsinstruktion användare

I intervjuer framkommer att policy och instruktioner har utgått från Falu kommuns styrdokument och tagits fram i samarbete med kommunen. Dessa utgår från det koncept som MSB rekommenderade vid tiden för framtagandet. Bolagets policy och riktlinjer är dock anpassade utifrån bolagets organisation och funktioner. Dokumenten används som stöd trots de är föråldrade och en omarbetning av styrdokument är initierad.

5.3.2 Roller och ansvar

I policyn redogörs för bolagets roller inom informationssäkerhetsarbetet. VD är ansvarig för bolagets övergripande arbete och inom verksamhetsstöd har en informationssäkerhetsansvarig utsetts som har det operativa ansvaret för arbetet.

I intervjuer framkommer dock att det inte finns någon ansvarig för det samlade säkerhetsarbetet utan säkerhetsskyddsarbetet och riskanalyser sker per verksamhetsområde. IT-relaterat säkerhetsarbete är organiserat inom avdelningen Utveckling och IT.

5.3.3 Informationssäkerhetsarbetet i praktiken

Det finns inget ledningssystem för informationssäkerhet implementerat i nuläget men vid en intern genomgång under 2018–2019 framkom behovet av ett sådant. Det finns idag ett tekniskt stödsystem för ledningssystem som de kallar för dokumentbanken på intranätet. Där finns styrdokument för informationssäkerhet vilket är en del av ledningssystemet. Ledningssystemet för informationssäkerhet ska enligt intervjupersoner bygga på MSB:s rekommendationer och metodstöd för LIS och följa ISO27001-standarden.

Bolaget är inkluderade i Falu kommuns informationssäkerhetsarbete efter att kommunens informationssäkerhetssamordnare initierat ett samarbete där Falu Energi och Vatten och även det kommunala bolaget Kopparstaden ingår. Arbetet är i uppstarten och hittills har man genomfört en analys av nuläget och ska gå vidare med en GAP-analys för att se vilka delar som saknas i jämförelse med ISO27001-standarden. Det framgår i intervjuer att det är mycket arbete men att det är nödvändigt då hela systematiken ligger i att göra arbetet grundligt från början. Det har inte skett något praktiskt arbete med åtgärder ännu men man ser från bolagets sida att det kan bli ett bra samarbete där man kan dra nytta av både kommunens kompetens och arbete och även övriga bolags delaktighet.

Alla nyanställda följer ett introduktionsprogram där IT-säkerhet ingår. I checklistan finns en punkt där chefer har i uppdrag att säkerställa att nyanställda får en genomgång av IT-användande. Exempelvis hur man ska hantera datorer, system och lösenord. Genomgången som de har med IT är ca 2–3 timmar och tar sin utgångspunkt i informationssäkerhetspolicyn. De omsätter innehållet i ett samtal med utgångspunkt utifrån rubrikerna för att det ska vara lätt att ta till sig och omsätta i sunt förnuft. De går även igenom informationssäkerhetsinstruktion för respektive målgrupp, se 5.3.1.

Alla anställda har fått information om GDPR genom en grundutbildning och vissa utsedda medarbetare har fått en fördjupad utbildning. Bolaget har även köpt in en utbildning för informationssäkerhet via verktyget Junglemap som är en webbaserad utbildning men man har ännu inte genomfört utbildningen för samtliga medarbetare.

Bolaget har inte utsett ett dataskyddsombud. Enligt gällande ”Riktlinje för hantering av personuppgifter” framgår att bolagen inom FEV juridiskt är personuppgiftsansvariga. I intervjuer framkommer att det innebär att det är VD som är ansvarig för att säkerställa att bolaget efterlever de lagkrav som finns i enlighet med dataskyddsförordningen. I riktlinjerna står dessutom att ansvaret för den praktiska hanteringen av personuppgifter

innehas av systemansvarig för de system där uppgifterna hanteras. För övriga behandlingar ligger ansvaret på den person som ansvarar för att behandlingen utförs.

I riktlinjen för hantering av personuppgifter framgår en beskrivning för hantering av incidenter och vem som ansvarar för anmälan och rapportering av dessa. I intervjuer framhålls att det finns styrdokument men att det inte finns någon tydlig organisering av frågor för GDPR då ingen person har ett uttalat ansvar för detta. Det finns en person inom bolaget som hanterar frågor idag men som inte vill ha det formella ansvaret då inte arbetet är organiserat i nuläget.

Säkerhetsklassning och riskanalys

Bolaget har inte genomfört informationsklassning enligt någon specifik metod men riskanalyser har upprättats för bolagets driftssystem utan att en klassning av informationen har skett. Arbetet med riskanalyser sker löpande och ansvariga för detta är avdelningscheferna då arbetet sker verksamhetsspecifikt.

I det kommande arbetet kommer en samverkan att ske med kommunen för att genomföra informationsklassning. Detta då det är en förutsättning att de använder samma klassningsmodell så att bolaget ska kunna nyttja det digitala arkivsystem som kommunen implementerar.

Systemförvaltning

De har identifierat närmare 100 system som behöver ha utsedda systemansvariga, några är för närvarande vakanta, men ordningen då är att avdelningschefen står som ansvarig för systemet.

Systemägarskap utses av avdelningscheferna och de som är systemansvariga har andra huvudsakliga arbetsuppgifter inom bolaget. I intervjuer beskrivs att systemägarna upprättar drift och underhållsdokumentation för de system och information som de är ansvariga för. I det ingår även hantering av personuppgifter och förteckningar för det.

Bedömning av systemen sker i samarbete mellan systemansvariga och IT och det ser olika ut hur aktivt arbetet är. Det är dock inget som hanteras till vardags och dessa frågor skulle enligt intervjupersoner kunna vara högre upp på agendan. De har informerat verksamheterna om systemägaransvaret och om systemansvarigs ansvar för informationen inom systemet. Det behöver även förtydligas i ledningsgruppen hur ansvaret ser ut och hur arbetet behöver bedrivas för att ske på ett mer systematiskt sätt.

När de gör förändringar i systemmiljön så sker en genomgång av säkerhet och om det finns behov av åtgärder, men de har inte kommit så långt som IT-funktionen skulle vilja. De gör själva bedömningen i intervjun att det inte skulle uppfylla krav gällande systematiskt arbete i enlighet med ISO 27000-standarden.

NIS-direktivet

Som anpassning och åtgärder för NIS-direktivet har ett aktivt arbete inom informationssäkerhet skett. Detta har varit ett uppdrag från bolagets styrelse som uttryckt att detta är ett viktigt arbete som bolaget behöver ta sig an. Man har även haft extern konsulthjälp.

I arbetet har åtgärdsplaner för elnät och vatten som i dagsläget omfattas av NIS tagits fram. De arbetar även löpande med de nya direktiv som kommer från MSB, Livsmedelsverket mm. Arbetet är pågående och kommer att ta några år att färdigställa. Exempel på åtgärder som vidtagits är förstärkt tillträdesskydd och skalskydd samt infört lokala brandväggar. De har ingen samlad bild över hur långt arbetet har kommit då respektive avdelningschef ansvarar för sina delar av arbetet. I intervjuerna framkommer en bild att det sker ett bättre praktiskt arbete än vad som dokumenteras och att det är ett förbättringsområde inom bolaget.

5.3.4 Bedömning

Det finns inom bolaget styrdokument som beskriver ansvar och till viss del hur arbetet ska bedrivas. Styrdokumenten är i vissa delar föråldrade trots att en revidering skett 2017. FEV har initierat ett förbättringsarbete i samarbete med Falu kommun där även revidering av styrdokument ingår som en uppgift i det kommande arbetet.

Vi upplever att det finns en uppfattad ansvarsfördelning mellan avdelningschefer och IT-avdelningen men att vissa uppgifter och aktiviteter kan utvecklas som behöver ingå i ett systematiskt informationssäkerhetsarbete. Det sker i nuläget ingen informationsklassning vilket är grundläggande för att bedöma risker så att vidtagna säkerhetsåtgärder står i relation till hur skyddsvärd informationen är. En annan väsentlig del är att utbildning i informationssäkerhet erbjuds och genomförs för samtliga medarbetare för att säkerställa att alla med ansvar för informationssäkerhet har tillräcklig kunskap och kännedom om detta. Vi uppfattar att det inte har genomförts någon utbildning men att detta planeras.

Styrelsen har gett verksamheten i uppdrag att det ska ske ett aktivt åtgärdsarbete inom bolaget för att säkerställa informationssäkerheten i enlighet med NIS-direktivet. Ett antal åtgärder har vidtagits i det arbetet även om det är ett omfattande arbete som förväntas ta några år till att genomföra samt att det är ett ständigt pågående arbete utifrån att risk och hot förändras kontinuerligt.

Riskanalyser och bedömningar av system har genomförts med regelbundenhet. Ansvar för åtgärder finns hos avdelningscheferna men det finns idag ingen heltäckande bild över status för arbetet. Vi anser därför att bolaget bör strukturera sitt arbete så att det kan följas upp och prioriteras utifrån hot och risker. Det finns dessutom en risk att arbetet blir alltför personberonde och sårbart vid personella eller organisatoriska förändringar om dokumentation saknas.

Vår bild är att intentionerna i det utvecklingsarbete som är planerat i samarbete med Falu kommun för bolagets informationssäkerhet har goda förutsättningar att ge den systematik och struktur som i nuläget saknas. Arbetet bör därför säkerställas genom att

förankras i bolagsstyrelse och företagsledningen för att ledningens engagemang ska finnas, rapporteras och följas upp löpande samt att tillräckliga resurser finns för att genomföra de åtgärder som krävs för att uppnå en god informationssäkerhet.

5.4 Kopparstaden AB

Kopparstaden AB är Falun kommuns allmännyttiga bostadsbolag. Bolaget äger och förvaltar ca 6 000 lägenheter, 280 lokaler och 610 uthyrningsförråd i Falun.

Bolaget har närmare 120 anställda.

5.4.1 Styrdokument

Kopparstaden AB saknar informationssäkerhetspolicy och instruktioner för arbetet. IT-chef har fått i uppdrag att ta fram nya styrdokument och vi har i granskningen tagit del av ett första utkast till policy som kommer omfatta både informationssäkerhet och dataskydd.

Av utkastet till policy framgår att bolagets arbete ska utgå från ISO27001-standarden.

Policyn ska enligt utkastet antas av bolagets styrelse och revideras årligen vid årets första styrelsemöte. Samtliga medarbetare ska få introduktion i policyn, ansvar för att så sker ligger på närmsta chef.

I intervju framkommer att säkerhetsinstruktionerna inte är strukturerade mer än på övergripande nivå och vi har därför inte tagit del av dessa.

5.4.2 Roller och ansvar

I utkastet till policy beskrivs att ansvaret följer det ordinarie verksamhetsansvaret och all personal fortlöpande ska få information och utbildning för att ha förutsättningar för ett högt säkerhetsmedvetande.

IT-chef har uppdraget att utveckla bolagets arbete med informationssäkerhet.

5.4.3 Informationssäkerhetsarbetet i praktiken

Det finns inte en organisation eller tydlig struktur för informationssäkerhetsarbetet i nuläget. Detta är en brist som har identifierats av Kopparstaden själva och mynnat ut i att bolaget upprättat en IT-organisation. En IT-chef tillsattes i januari 2020 och i dennes uppdragsbeskrivning framgår ett ansvar för informationssäkerheten och att stötta övriga i verksamheten.

Inom IT-organisationen finns förutom IT-chef även IT-samordnare, IT-administratör och en ansvarig för Fastighetsnära IT. IT-driften köps in av extern part där säkerhetslösningar ingår.

Det pågår ett utvecklingsarbete med ett flertal delar inom IT och systemförvaltning för att förtydliga roller och ansvar men som även förbättrar säkerheten för hanteringen av

bolagets informationstillgångar. Det sker i nuläget inga utbildningsinsatser för informationssäkerhet för att säkerställa att medarbetarna har den kunskap och medvetenhet som krävs för att upprätthålla en god informationssäkerhet.

Under 2020 har bolaget försökt att hitta samarbete och samverkan med kommunens IT-avdelning och informationssäkerhetssamordnare. Man ska påbörja informationsklassning med hjälp av KLASSA. Arbetet har påbörjats där mellan 30–40 system har identifierats. En avstämning ska ske med samtliga områdeschefer för att genomföra klassningen. Utifrån resultatet i klassningen är planen sedan att börja åtgärder med de system och information som är mest skyddsvärt tills en genomgång har kunnat göras för samtliga system.

Det har till viss del genomförts riskanalyser för extraordinära händelser. I de analyserna har man kommit fram till att mycket kan ske manuellt utan större påverkan på verksamheten under en tid. Ett övergripande risk- och säkerhetsarbete har påbörjats inom bolaget men pga. rådande pandemi har det satts på paus under våren. Kontinuitetsplanering finns för ett av bolagets viktigaste system då det ingått i kravställning för systemet som köps in som en tjänst.

Det finns en rutin och process för incidenthantering och rapportering. Det har skett incidenter både gällande personuppgifter och informationssäkerhet. Efter att incidenthantering varit en återkommande punkt på veckomöten med medarbetarna har det börjat ske en mer frekvent incidentrapportering.

Det finns sårbarheter som är identifierade där åtgärder pågår för att förbättra säkerheten. För några år sedan skedde ett intrång som ledde till konsekvenser för bolagets informationstillgångar. Det har inte skett efter att de åtgärder som bedömdes nödvändiga då genomfördes. Intrångsförsök sker dock hela tiden och i intervju framkommer att man inte har så stor kontroll över dessa mer än de grundläggande säkerhetsåtgärder i form av brandväggar, antivirusskydd mm som bolaget har. Det har inte genomförts några penetrationstest eller andra revisioner för att säkerställa att vidtagna IT-säkerhetsåtgärder är tillräckliga för att skydda informationstillgångarna.

GDPR

För bolagets GDPR-arbete finns en organisation där representanter träffas en gång per månad. Bolaget har inte utsett något dataskyddsombud men det finns en utsedd GDPR-ansvarig som är sakkunnig i GDPR. GDPR-ansvarig sammankallar gruppen till möten med utsedda operativt GDPR-ansvariga. Dessa är utsedda från olika avdelningar inom bolaget och ansvarar för att hantera samtliga processer, rutiner och system inom den egna organisationen gällande GDPR och hur GDPR praktiskt ska hanteras inom det egna ansvarområdet. De har i uppgift att lyfta GDPR-frågor från de egna leden till gruppen av operativt ansvariga.

I intervjuer beskrivs att det finns en relativt låg mognad för frågor inom informationssäkerhet men att det har skett en utveckling som kommit på köpet genom det gemensamma arbetet med GDPR. Intervjupersonerna beskriver samtidigt att informationssäkerheten behöver angripas i ett bredare perspektiv.

Alla nyanställda får en utbildning i GDPR och det pågår en diskussion hur de anställda som redan gått utbildningen ska hållas uppdaterade och få information eller utbildning mer kontinuerligt. Information sker löpande på veckomöten där samtliga medarbetare deltar.

5.4.4 Bedömning

Kopparstaden AB saknar i nuläget styrdokument för Informationssäkerhet. Det pågår ett arbete med att ta fram en policy som kommer omfatta både informationssäkerhet och dataskydd. Efter att den är fastställd ska säkerhetsinstruktioner tas fram. Vår bedömning är att dessa dokument är väsentliga att ha på plats för att det ska finnas en tydlighet i ansvar och roller samt hur arbetet ska bedrivas.

Arbetet utgår i nuläget till stora delar från bolagets IT-funktion vilket kan medföra vissa risker då upplevelsen i verksamheten kan bli att det är IT:s ansvar att bedriva informationssäkerhetsarbetet. Det behöver därför tydliggöras hur ansvaret ser ut för verksamhetens avdelningschefer/systemansvariga som kravställare och beställare till IT-funktionen avseende drift och IT-säkerhet.

Vi ser det som positivt att det har påbörjats ett arbete med bolagets informationssäkerhet som ska utgå från gällande standard ISO 27001. Informationsklassning är grundläggande för ett systematiskt arbete med informationssäkerhet som utgår från att bedöma risker så att vidtagna säkerhetsåtgärder står i relation till hur skyddsvärd informationen är. En annan väsentlig del är att utbildning i informationssäkerhet erbjuds och genomförs för samtliga medarbetare för att säkerställa att alla med ansvar för informationssäkerhet har tillräcklig kunskap och kännedom om detta.

Vår bedömning är att det finns ett strukturerat arbete för åtgärder och efterlevnad i enlighet med GDPR som är en del i informationssäkerhetsarbetet. En organisation har upprättats med representanter från olika avdelningar där ett informationsutbyte och kunskapsöverföring sker. Det finns beslutade rutiner för hantering av personuppgifts- och informationssäkerhetsincidenter som används och det sker löpande informationstillfällen för att hålla frågan aktuell för medarbetarna.

Vi uppfattar att intentionerna i det utvecklingsarbete som är planerat för bolagets informationssäkerhet har goda förutsättningar att ge den systematik och struktur som i nuläget saknas. Arbetet bör därför säkerställas genom att förankras i bolagsstyrelse och företagsledningen för att ledningens engagemang ska finnas och att övriga roller och ansvar i bolaget förtydligas. Resurser behöver tillsättas så att arbetet kan ske på ett systematiskt sätt så att de åtgärder som krävs för att uppnå en god informationssäkerhet kan genomföras. Arbetet bör följas upp och rapporteras löpande för att hållas aktuellt och inte stanna av.

5.5 Koncerngemensamt arbete med Informationssäkerhet

Det sker i nuläget inget systematiskt koncerngemensamt arbete inom informationssäkerhet. Det är endast ett fåtal av bolagen som har inkluderats i det påbörjade arbetet som initierats av Falu kommun.

Falu Energi och Vatten har varit delaktiga i den nulägesanalys som genomförts och anger att de går vidare med en GAP-analys i jämförelse med krav i enlighet med ISO 27001-standarden som är nästa steg i enlighet med MSB:s metodstöd för ett systematiskt informationssäkerhetsarbete.

Kopparstaden har inlett ett samarbete med kommunen gällande informationsklassning där kontakt tagits med kommunens informationssäkerhetssamordnare.

I intervjuer framkommer att Lugnet i Falun AB inte känner sig uppdaterade och inkluderade i vad som är på gång i kommunen trots att de delar system och organisation med kommunen och därigenom är beroende av det arbete och den säkerhetsorganisation som Falu kommun inrättar.

Vad gäller Falu Stadshus så är bolaget helt beroende av det arbetet som bedrivs inom kommunen då de inte har en egen organisation eller verksamhetssystem och därigenom inte genomför något administrativt arbete i egen regi.

5.5.1 Bedömning

Vår bedömning är att det inte sker en ändamålsenlig samordning mellan kommunen och de kommunala bolagen när det gäller informationssäkerhetsarbetet. Vår bild är att det främst beror på att det inte har pågått ett systematiskt arbete med informationssäkerhet varken i kommunen eller bolagen. Det har inte heller funnits någon utsedd ansvarig för informationssäkerhet som skulle kunna vara sammanhållande i arbetet. Sedan funktionen informationssäkerhetssamordnare tillsatts i kommunen har inledande samarbete och dialog genomförts mellan bolag och kommunen. Även Falu Energi och Vatten AB och Kopparstaden AB har på senare tid inrättat nya funktioner med tydligare ansvar för informationssäkerhetsfrågorna.

Vad gäller Falu Stadshus AB och Lugnet i Falun AB så behöver ansvaret för informationssäkerhetsarbetet tydliggöras för dessa då det i nuläget är otydligt. Om bolagen ska inkluderas i kommunens löpande arbete utan egna åtgärder och organisation behöver även de behov och förutsättningar som finns hos dessa tillgodoses av den kommunala verksamheten för att upprätthålla en god informationssäkerhet.

Kommunkoncernen har ett stort behov av att utveckla sitt informationssäkerhetsarbete. Genom att ta vara på de resurser som finns och inte bygga upp kompetens och egna organisationer inom kommunen respektive bolagen kan synergier erhållas. Vår uppfattning är att kommunkoncernen både säkerhetsmässigt och ekonomiskt skulle vinna på en tydligare samordning av dessa frågor där samtliga bolag inkluderas i arbetet och det kan ske genom en utvecklad koncernsamverkan.

6 Slutsats och rekommendationer

Vår sammanfattande bedömning utifrån granskningens syfte är att kommunstyrelsen och bolagen inte har säkerställt ett ändamålsenligt och systematiskt arbete med sin informationssäkerhet.

Det finns beslutade styrdokument för kommunens informationssäkerhetsarbete men det finns en otydlighet vilka av bolagen som omfattas av dessa. Styrdokumenten är inte implementerade i verksamheten för att kunna efterlevas och är i nuläget inte styrande för hur roller och ansvar ser ut eller för hur arbetet ska bedrivas. De är även i stora delar föråldrade och i behov av revidering. Falu Energi och vatten har styrdokument för arbetet som är reviderade 2017, dessa utgår till stor del från kommunens styrdokument men med vissa anpassningar till bolagets förutsättningar. Även dessa är i behov av revidering utifrån gällande rekommendationer. Kopparstaden AB saknar styrdokument men dessa är under framtagande.

Vi bedömer det som positivt att ett utvecklingsarbete har påbörjats för informationssäkerhet både i kommunen och i bolagen. Det har tillsatts en informationssäkerhetssamordnare i Falu kommun och i bolagen har ett tydligare ansvar tilldelats inom IT-funktionen för informationssäkerhetsfrågorna. För både kommunen och bolagen framgår att det strategiska utvecklingsarbetet ska ske med utgångspunkt i ett ledningssystem för informationssäkerhet i enlighet med rekommendationerna från MSB som i sin tur utgår från ISO27001-standarden.

Vi vill poängtera vikten av ledningens engagemang och verksamheternas ansvar i informationssäkerhetsarbetet då det är avgörande för genomförandet och att säkerhetsåtgärder vidtas utifrån en riskbedömning där åtgärden kan sättas i relation till hur skyddsvärd informationen är. Fram tills nu har IT-funktionen i kommunen tagit en stor roll i arbetet utifrån sin tekniska kompetens och de lösningar som är tillgängliga utifrån resurser. I de kommunala bolagen är det till stor del IT-funktionen som leder det strategiska arbetet avseende informationssäkerhet. Vi bedömer det som en risk då ansvarig för det strategiska informationssäkerhetsarbetet ska vara kravställare gentemot IT. Det arbetet riskerar att försvåras om arbetet leds från samma organisation. Vi rekommenderar därför att avdelningschefer eller systemansvariga utses att vara del i det aktiva arbetet för att ta ansvar för de informationstillgångar som de hanterar och att gränsdragning mellan dessa ansvar tydliggörs.

Vi uppfattar att intentionerna i det utvecklingsarbete som är planerat för kommunen och bolagens informationssäkerhet har goda förutsättningar att ge den systematik och struktur som i nuläget saknas. Arbetet bör därför säkerställas genom att förankras i styrelser, nämnder och tjänstemannaledning för att ledningens engagemang ska finnas och att övriga roller och ansvar i bolaget förtydligas. Resurser behöver tillsättas så att arbetet kan ske på ett systematiskt sätt så att de åtgärder som krävs för att uppnå en god informationssäkerhet kan genomföras. Arbetet bör följas upp och rapporteras löpande för att hållas aktuellt och inte stanna av.

Slutligen är vår bedömning att samordning i arbetet för informationssäkerhet mellan kommunen och de kommunala bolagen kan utvecklas. Synergier kan uppnås genom att tillsammans nyttja kompetens och erfarenhet när metodstödet som det systematiska

informationssäkerhetsarbetet ska utgå från ska genomföras då alla är överens om det som plattform för utvecklingsarbetet.

6.1 Rekommendationer

Utifrån vår bedömning och slutsats rekommenderar vi kommunstyrelsen, kommunens samtliga nämnder samt bolag att:

- Säkerställa att det finns aktuella och implementerade styrdokument avseende informationssäkerhet
- Säkerställa att det finns en hållbar organisation för att driva ett systematiskt informationssäkerhetsarbete och beakta på vilka sätt en samordning mellan kommun och kommunala bolag kan ske
- Säkerställa att roller och ansvar mellan Informationssäkerhetssamordnare, IT och verksamhet tydliggörs
- Säkerställa att tillräcklig utbildning ges för att medvetandegöra informationssäkerhetsansvaret för alla inom Falu kommun och dess kommunala bolag
- Säkerställa att arbetet med informationssäkerhetsklassning implementeras fullt ut i kommunen och de kommunala bolagen
- Tydliggöra rapporteringsvägar för informationssäkerhet och säkerställa att ledningens genomgång blir en årlig rapportering till berörda

Vidare rekommenderar vi kommunstyrelsen att:

- Tydliggöra i vilken utsträckning de kommunala bolagen omfattas av kommunens styrdokument avseende informationssäkerhet
- Tydliggöra roll och uppdrag för informationssäkerhetssamordnaren så att det framgår hur detta ansvar ser ut internt i kommunen och i förhållande till de kommunala bolagen

Datum som ovan

KPMG AB

Magnus Larsson *Certifierad kommunal yrkesrevisor*	Jenny Thörn *Kommunal revisor*	Linnéa Grönvold *Kommunal revisor*

Falu kommun och kommunala bolag
Granskning av Informationssäkerhet

2020-06-10