LUNDS UNIVERSITET
Ekonomihögskolan

Institutionen för informatik

Informationssäkerhetspolicyer inom Sveriges kommuner

-En kvalitativ studie utifrån fyra aspekter

Kandidatuppsats 15 hp, kurs SYSK16 i Informatik

Författare: Viktor Fresk
Martin Petrelius

Handledare: Magnus Wärja

Rättande lärare: Christina Keller
Paul Pierce

Informationssäkerhetspolicyer inom Sveriges kommuner - En kvalitativ studie utifrån fyra aspekter.

ENGELSK TITEL: Information Security Policies within Swedish municipalities - A qualitative study based on four aspects.

FÖRFATTARE: Viktor Fresk, Martin Petrelius

UTGIVARE: Institutionen för informatik, Ekonomihögskolan, Lunds universitet

EXAMINATOR: Christina Keller, Professor

FRAMLAGD: maj, 2021

DOKUMENTTYP: Kandidatuppsats

ANTAL SIDOR: 78

NYCKELORD: Information Security Policies, Informationssäkerhet, Kommuner, Roller & ansvar, Styrning, Datahantering, Riskhantering

SAMMANFATTNING (MAX. 200 ORD): Informationssäkerhet är en viktig faktor i nästintill alla organisationer idag. Många verksamheter hanterar information som är känslig och det finns ett behov att upprätta regelverk för hur en organisation ska skydda sig. Information Security Policies är ett fundamentalt regelverk för hur en organisation hanterar den information som man besitter inom verksamheten. Denna studie ämnar åt att undersöka dessa policies inom Sveriges kommuner för att kartlägga hur verksamheterna arbetar med policies utifrån fyra aspekter. Dessa inkluderar Styrning, Roller & Ansvar, Data samt Riskhantering. Undersökningen har baserats på teori samt en kvalitativ undersökning på fem diverse kommuner i Sverige, där samtliga tillfrågade skiljer sig åt i både geografisk plats samt storlek. Studien visar att samtliga aspekter är relevanta för kommunerna i arbetet med policies, och att arbetet med policies såväl som informationssäkerhet är något som kommunerna måste fortsätta utveckla inom sina inbördes verksamheter.

Innehåll

Figurer

Tabeller

1 Introduktion

1.1 Bakgrund

År 2015 genomförde Myndigheten för samhällsskydd och beredskap (hädanefter refererat som MSB) en undersökning i samverkan med Sveriges kommuner och landsting (SKL). En undersökning av informationssäkerheten i Sveriges kommuner vid namn *En bild av kommunernas informationssäkerhetsarbete 2015*. Grunden för rapporten las av en enkätundersökning gällande flera olika aspekter angående informationssäkerhet utskickad till samtliga kommuner i Sverige. Rapporten visade på flertalet brister hos svenska kommuner när det gäller informationssäkerhet. 170 av de 232 kommuner som var med i enkätundersökningen visade sig inte ha något systematiskt säkerhetstänk i sin behandling av information. Samtidigt fanns det i 129 av 232 kommuner inte en process för rapportering eller incidenthantering med anknytning till informationshantering inom kommunen. Vidare så gjordes samma år ytterligare en rapport vid namn *Informationssäkerheten i Sveriges kommuner* vilken syftar till att ge ytterligare analys och rekommendationer till kommunerna utifrån MSB:s tidigare enkät. Den första rapporten var en undersökning av säkerhetsläget hos kommunerna medan den senare rapporten syftade till att ge stöd för kommunerna till framtida förbättringar och utveckling i att bli mer säkra i sin informationshantering (MSB, 2015).

"Kommunerna har ett av det svenska samhällets mest komplexa uppdrag. Det omfattar allt från den dagliga omsorgen av äldre till att säkerställa att känslig infrastruktur fungerar. En stor del av den samhällsviktiga verksamheten räknas till kommunernas ansvar. Säker informationshantering spelar en central roll i detta uppdrag" (MSB, 2015, p.7).

År 2015 fanns det alltså i en majoritet av svenska kommuner inte ett systematiskt arbetssätt med informationssäkerhet. Trots att kommunerna har en samhällsfunktion där en stor mängd uppgifter behandlas så las år 2015 inte tillräckligt med resurser på informationssäkerhet.

1.2 Problemområde

Enligt MSB:s hemsida för informationssäkerhet (2021) så delas vikten av att skydda sin information in i tre kategorier, tillgänglighet, riktighet och konfidentialitet. Tillgänglighet för att informationen ska finnas tillgänglig när den behövs, riktighet att informationen inte är manipulerad och sist konfidentialitet att endast personer med rätt behörighet kan ta del av informationen. Enligt MSB behövs ett säkerhetstänk i alla delar och skikt av samhället i alltifrån organisationer i offentlig sektor till företag och privatpersoner (MSB, 2021).

Von Solms beskrev i sin artikel *Information Security Management (1): Why Information Security is so important* redan år 1998 hur information är i fara överallt där organisationer

använder sig av datakapacitet uppkopplad till nätverk och hur organisationer därmed behöver standarder och regelverk för att skydda sig. Von Solms gör i sin artikel en liknelse vid hur det behövs standarder för att hantera säkerheten i nätverk av datorer på samma sätt som det behövs säkerhetsföreskrifter för vägnätverk där bilar körs. På samma sätt som det finns föreskrifter om körkort, trafikpoliser, kontroller att bilar är kördugliga och rödljus så menar Von solms att det på samma sätt behövs föreskrifter och regler att förhålla sig till i nätverk av datorer, föreskrifter såsom information security policies (1998).

Hoten som organisationer ställs inför sammanfattas av Peltier till att kunna varieras från att vara både externa och interna, hoten kan variera från att vara hackare som kommer från utsidan till internt där anställda slarvar med integriteten. Det huvudsakliga syftet med att upprätta ett dokument eller ett regelverk av säkerhetsstandarder är enligt Peltier att skydda en organisations tillgångar från hoten som exempelvis nämns ovan. Peltier menar att genom ett noggrant val och studering av policies, standarder och riktlinjer för att skydda en organisations tillgångar så skyddar man även de huvudsakliga målen och syften som organisationen jobbar för (2001).

Enligt MSB:s undersökning år fanns det i 67 av 230 kommuner inte en Information Security Policy eller ett styrande dokument för informationssäkerhet, i mer än en fjärdedel av kommunerna saknas alltså ett styrande dokument för informationssäkerhet. Samtidigt svarade 77 av 175 kommuner att det för tillfället vid år 2015 pågick en process att upprätta en information security policy. Som MSB också belyser är policyn i form av ett styrande dokument den centrala delen för att en kommun skall kunna arbeta med informationssäkerhet (MSB, 2015). Det kan därför tyckas oroväckande att en fjärdedel av Sveriges kommuner saknar en grund i informationssäkerhet. I relation till den avsaknad som år 2015 fanns av Information Security Policies tillsammans med den roll som svenska kommuner utgör i samhället i sin hantering av informationstillgångar så kan frågan ställas ifall information security policies idag är en avgörande del i kommunernas arbete (MSB,2015). I arbetet med policies för informationssäkerhet så har diverse aspekter identifierats. De teorier och litteratur vi presenterar framhäver fyra aspekter av ISP, nämligen styrning, roller & ansvar, data samt riskhantering. I den första MSB rapporten *En bild av Kommunernas Informationssäkerhetsarbete 2015* (2015) beskrivs policy och riktlinjer som en central del i upprättandet av en informationssäker organisation. Vidare nämner MSB att en sådan policy skall innehålla hantering av risk, vilka som ansvarar för vilka områden samt att förstå vilken information som behöver hanteras. Liknande hur MSB definierar informationssäkerhetspolicy har motsvarande aspekter skildrats i den litteratur som vi vidare belyser i denna studie.

1.3 Forskningsfråga

Utefter bakgrunden och problemområdet ovan ställer vi oss frågan:

På vilket sätt förhåller sig svenska kommuner till fyra aspekter av informationssäkerhets policies?

1.4 Syfte

Studien syftar till att kartlägga svenska kommuners policies utifrån fyra aspekter av informationssäkerhet.

2 Litteraturgenomgång

Uppsatsens litteraturgenomgång kommer att innefatta en redogörelse för fyra väsentliga delar utav Information Security Policies som en organisation kan jobba med för att säkra informationssäkerhet. Genomgången börjar med att förklara just begreppet policies för att sedan ge en beskrivning av vad policies är inom ämnet informationssäkerhet. De olika begreppen som är Information Security Policies redogörs och vikten av dess roll som en del av en policy för att arbeta informationssäkert redogörs. I följande teoriavsnitt avser vi att undersöka och utvärdera fyra fundamentala delar av säkerhetspolicies i behandlingen av informationssäkerhet hos organisationer, styrning, roller & ansvar samt data och riskhantering.

2.1 Policies

Begreppet *Policy* förklaras i *The Cambridge Dictionary (2021)* som en uppsättning regler eller bestämmelser för hur man ska hantera specifika situationer, och som blivit överenskomna av en grupp, såsom en organisation, regering eller politiskt parti. Ordet *Policy* är på svenska också översatt till bestämmelser eller regelverk. Policies finns att hitta överallt i samhället och varierar i form. Det kan variera från att man inte får röka på svenska uteserveringar, till bestämmelser hur ett bolag tillsätter en ny vice direktör (VD). Inom informationssäkerhet, visar sig policies i form av ett styrande dokument för hur organisationen i fråga skall hantera, behandla samt skydda behörig information (Peltier, 2001).

2.2 Information Security Policies

Information security policies (hädanefter refererat som ISP) är ett begrepp för ett typ av dokument till för att samla en mängd olika policies/regler som tillsammans skapar riktlinjer för hur en verksamhet bygger en informationssäker organisation. Reglerna och riktlinjerna för ett sådant dokument skapas och kan sättas ihop utifrån en mängd olika teoretiska modeller eller certifieringar (Höne et al, 2002). Dessa regler eller förhållningssätt är i mångt skiljaktiga beroende på vilken typ av organisation som undersöks men kan sammanfattas till att behandla de lagar och regler som är till för att skapa ett informationssäkert arbetssätt inom en organisation. Huvudmålet med upprättandet policies inom en organisation är att definiera skyldigheter och rättigheter för de som använder information inom en organisation (Karin Höne and J.H.P. Eloff, 2002).

2.3 Styrning

Att organisationen har en genomtänkt och omfattande styrning är vitalt för att en ISP skall kunna bildas. En lyckad styrning bygger på att hela verksamheten förstår betydelsen av information och dess värde, från ledningen till de enskilda anställda. Genom att ha en tydlig strategi och kommunikation kan organisationer enklare hantera sina respektive informationsprocesser, och hur man skall skydda dem (Kane & Koppel, 2013). Detta gör att styrningen blir komplett och en del av organisationens arbete med upprättandet av ett ISP. Nedan

förklaras strategi samt kommunikation, två vitala delar för styrning inom en information security policy.

2.3.2 Kommunikation

En ytterligare bestämmelse som organisationen måste förhålla sig till och styra är värdet av kommunikation som styrs från ledningen av organisationen. Denna bestämmelse fokuserar på vikten av kontinuerlig återkoppling och kommunikation för att säkerställa att informationssäkerhet förekommer i alla delar av verksamheten. Kane och Koppel menar vidare att riskhantering och specifika säkerhetsfunktioner inte bör ske i det tysta, utan skall uppträda i alla delar av organisationen, för att lättare kunna kommunicera och därefter hantera eventuella felaktigheter såsom läckor eller intrång (Kane & Koppel, 2013).

Vidare hävdar Höne och Eloff (2002) att det i slutändan är användarna själva som beslutar huruvida säker informationshanteringen blir. Detta belyser att kommunikationen genom verksamheten måste vara koncis då användarna ofta är de anställda som hanterar känslig data. Den politik som omfattar informationssäkerhet brukar generellt sett vara att information skall ses som en tillgång och skall behandlas därtill. Kritisk information måste behandlas med säkerhet, och detta är något som hela verksamheten bör och skall känna till. Det är därför viktigt att kommunikation sker från toppen av organisationen till de anställda för att förhindra eventuellt läckage, spridning, förstöring eller modifiering av information (Kane & Koppel, 2013).

2.3.3 Strategi

En informationssäker styrning behandlar ett flertal perspektiv. Den belyser b. la vikten av att förstå samt implementera strategiskt grundande beslut. För att kunna skapa en strategi inom informationssäkerhet menar Kane och Koppel (2013) att organisationen först måste förstå sin nuvarande position gällande informationssäkerhet. Detta består i att uppfatta de resurser och förmågor som organisationen har att arbeta med gällande implementationen av en informationssäker strategi. Vidare tar författarna upp tre element som tillsammans bildar en fullständig strategisk styrning. Att först av allt kunna analysera sin strategiska position, för att vidare kunna välja ett adekvat tillvägagångssätt samt att slutligen implementera detta. Analys-elementet består i att bilda sig en uppfattning om var organisationen befinner sig i nuläget gällande informationssäkerhet. Detta för att enklare kunna besluta om var målsättningen skall resultera i. Att jämföra s.k *best practices* såsom ISO 27000 serien ger verksamheten en indikation på vad man skall fokusera på. Att kunna besluta om eventuella tillvägagångssätt förutsätter att analysen har varit välgrundad. Detta för att enklare förstå vilka alternativ som finns och vad som passar organisationen bäst. Slutligen måste en genomtänkt strategi bildas, som bör vara en kombination av de tidigare elementen (Kane & Koppel, 2013).

Vidare måste den strategi som implementeras vara skapad utifrån det landskap och den kultur som existerar inom verksamheten menar Krag Brotby (2009). För att kunna skapa korrekta och användbara bestämmelser att förhålla sig till inom organisationen så måste det finnas en tydlig kontext för informationssäkerhet i verksamheten, och strategin måste utformas utifrån dess förutsättningar. Kontexten kommer att visa vad som är möjligt inom verksamheten att utföra gällande potentiella lösningar (Brotby, 2009).

Att utforma en genomtänkt strategi utifrån den position som organisationen befinner sig i gör det sedan enklare för verksamheten att kunna fatta grundande beslut vid implementering av eventuella verktyg för informationssäkerhet (Volchkov, 2019). Andrej Volchkov (2019) menar också i sin bok *Information Security Governance* att skapandet av en gemensam strategi inom verksamheten är vitalt för att organisationen skall kunna uppnå en välgrundad styrning.

2.4 Roller & Ansvar

Roller & Ansvar är delen av Policyn som belyser hur de anställda integreras i arbetet mot informationssäkerhet. Nedan förklaras hur de anställda kan utbildas samt det ansvar som kan och ska finnas inom en informationssäker organisation.

2.4.1 Utbildning

Både Bulgurcu et al (2010) samt Sohrabi Safa et al (2016) benämner att det är just personalen som hanterar data som är ett av de större säkerhetsmässiga hoten mot en verksamhet vilket gör att det är just utbildning som kan nyttjas för att hjälpa en organisation att säkert behandla data. Enligt Bulgurcu et al (2010) är aspekten av roller och ansvar regeln eller policyn som talar om hur sammanhängande personers ansvar är i relation till den information som delas inom en organisation. Personer som är på insidan av ett informationssystem kallas för insiders, det är de personerna som opererar och är auktoriserade att behandla informationen inom ett visst system. Den faktiska användarens bruk och missbruk av informationstillgångar är ett av de största hoten i samband med insiders hantering av data (Bulgurcu et al, 2010). Även Hu et al (2012) diskuterar i inledningen av sin rapport *Managing Employee Compliance with information Security Policies:The critical role of Top Management and Organizational Culture* att det är de interna användarnas och de anställdas hantering av data som ofta är inblandade i säkerhetsincidenter.

Tsohou et al (2015) belyser i sin artikel *Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs* vikten av att utbilda sin personal med så kallade *Awareness programs* i sammanhanget av sin information security policy. Utbildningar som är till för att ge riktlinjer till de anställda för vikten av informationssäkerhet tillsammans med kontentan av organisationens säkerhetspolicys (2015). Enligt Peltier så kan inte en strategi eller policy för informationssäkerhet bli implementerad utan ett program för utbildning hos de anställda, en utbildning med fokus på just policy samt vad den innefattar för procedurer och verktyg (2007). Peltier uttrycker att ett awareness program ska innefatta 3 aspekter nämligen medvetenhet, träning samt utbildning. Medvetenhet för att tydliggöra och lära ut vad som förväntas av de anställda, träning och utbildning för att bemästra de verktyg som innefattas av säkerhetspolicyn. Enligt Peltier så spelar det inte någon roll hur solid och stark säkerhetsarbetet som utförts kring policyn är om det inte finns någon process för att förankra denne med att utbilda de anställda inför sina skyldigheter och rättigheter (2007).

2.4.2 Ansvar

I boken *Information Protection Playbook* behandlas betydelsen av att utforma tydliga roller genom verksamheten som också besitter specifika ansvarsområde. Vidare föreslås en specifik kommité som skall bestå av ansvariga personer från flera delar av organisationen. Kommittén skall kunna fatta exekutiva beslut och på så sätt få en bättre styrning över verksamhetens områden och informationssäkerhets bestämmelser (Kane & Koppel, 2013). Thomas R Peltier beskriver hur det är toppskiktet av organisationen som har huvudansvaret och i slutändan styr hur kapitalet av information hanteras. Han menar att det är de styrandes uppgift att delegera ut ansvarsområden och tilldela positioner såsom en corporate information officer (CIO). En CIO som bär huvudansvaret för det dagliga arbetet med informationstillgångar inom organisationen. Vidare nämner Peltier hur en CIO också kan ha delegerade roller under sig såsom en Information Systems Security officer som bär ansvaret för säkerheten och rapporterar direkt till CIO:n (2001). Paul Williams belyser i sin artikel *Executive and board roles in information security* beskriver att ju mer informationsintensiv en organisation är, desto fler roller behövs det med involveringen av informationssäkerhet. Vidare belyser Williams att det är av vikt att roller och ansvar är definierade tillsammans med att organisatoriska strukturer finns inom verksamheter för informationssäkerhet (Williams, 2012).

2.5 Datahantering

Informationssäkerhet bygger på att veta vilken information som man ska skydda, därför är det viktigt för organisationer att veta vilken data som verksamheten behandlar. För att en organisation skall veta hur deras policies för informationssäkerhet skall se ut, måste det finnas bestämmelser för klassificeringar, konfidentialitet, integritet samt tillgänglighet beträffande den data man hanterar inom verksamheten (Volchkov, 2019).

2.5.1 Klassificering

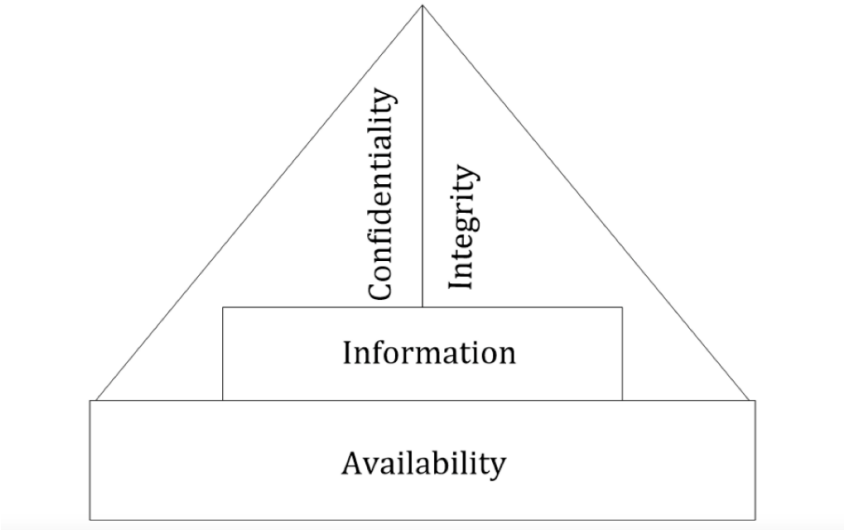
En del i att skapa riktlinjer och bestämmelser inom informationssäkerhet är hur verksamheten behandlar den data som existerar till dess förfogande. Att klassificera den data som innefattar information gör att organisationen enklare kan organisera samt prioritera hanteringen av data inom verksamheten. Organisationen bör implementera verktyg för att kunna applicera klassificering som en del av sina riktlinjer för informationssäkerhet, menar Colin Tankard (2015). Verktygen skall variera i funktion som i slutändan skall ge en helhetsbild för klassificeringen av data. Tankard menar att verktygen skall först av allt kunna identifiera vilken data som är aktuell för organisationen, för att senare kunna värdera informationen i förhållande till dess risk. Att klassificera den data som organisationen hanterar menar Tankard (2015) resulterar i ett bättre förhållande till datasäkerhet genom hela organisationen. De anställda kan enklare förstå värdet i informationen de hanterar och kommer lättare kunna förhålla sig till de regelverk som existerar kring hanterandet av information. Att klassificera data gör det även enklare för organisationen att identifiera de risker som finns (Tankard, 2015).

När organisationen har identifierat riskerna så föreslår Kane och Koppel (2013) att verksamheten bör arbeta med att prioritera de risker man urskiljt. Detta för att enklare förstå bredden

samt graden av de konsekvenser den aktuella risken innebär. Vidare skall riskerna delas upp i förhållande till varandra och till andra affärsrisker, för att på så sätt kunna förhindra dem med lämpliga resurser.

2.5.2 CIA (Confidentiality, Integrity, Availability)

Ett begrepp som ofta ses som grunden i policies för informationssäkerhet är den s.k CIA modellen. De tre förkortningarna behandlar konfidentialitet, integritet samt tillgänglighet och skapades som ett verktyg för behandlingen av informationssäkerhet och datahantering. CIA modellen används för att enklare förstå hur data skall hanteras inom en organisation (Samonas och Coss, 2014). Den första aspekten i CIA behandlar konfidentialitet, hur en organisation förhindrar att information sprids till icke auktoriserade parter. Data måste hållas skyddad och endast öppen för dem med tillgång till den, för att förhindra eventuellt läckage och spridning (Samonas och Cos, 2014). Den andra aspekten är integritet, och fokuserar på att försäkra sig om att datan som man hanterar är korrekt och inte har blivit manipulerad. Detta för att kunna försäkra sig om att datan och informationen är korrekt. Organisationen kan försäkra sig om detta genom att implementera verktyg som kan förhindra eventuella intrång, manipulering och extrahering (Samonas och Cos, 2014). Den sista delen i CIA triaden är tillgänglighet och behandlar just att data skall vara åtkomlig till de användare med rätt till dess information. Qadir och Quadri beskriver i *Information Availability: An Insight into the Most Important Attribute of Information Security* (2016) att tillgängligheten är viktig då de tidigare nämnda delarna är beroende av att tillgänglighet finns. Det kan inte finnas konfidentialitet och integritet utan att ha tillgänglighet (Qadir och Quadri, 2016). Detta har även gjort att den traditionella CIA modellen har uppdaterats där tillgängligheten har fått en större roll.



Figur 1:1 *Uppdaterad CIA modell*

Beroende på typen av organisation kan CIA modellen te sig olika. Olika verksamheter värderar de diverse aspekter annorlunda vilket resulterar i en varierande tillämpning. Qadir och Quadri (2016) menar därför att den klassiska CIA modellen inte är optimal då den värderar alla aspekter som lika, vilket de menar inte fungerar i praktiken.

2.6 Riskhantering

Arbetet med datahantering innebär också att hantera de eventuella risker som kan tänkas existera i förhållande till den information organisationen behandlar. Nedan presenteras teori relevant till riskhantering samt ISO 27000 serien.

2.6.1 Informationssäkerhetsrisker

De regelverk samt bestämmelser som organisationer har behandlar ofta hur man hanterar de risker som verksamheten utsätts för. De hot som existerar riskerar att utnyttja de eventuella svagheter som förekommer i organisationen, externa hot såsom hackare och virus, men även interna som t. ex anställda. Kane & Koppel (2013) menar att organisationen bör arbeta efter ett ramverk för att på ett effektivt sätt kunna reducera risk. Vidare menar författarna att de anställda och de ansvariga för speciella positioner såsom IT säkerhet och IT support måste ha kunskapen och de verktyg som krävs för att kunna identifiera möjliga risker. Detta för att kunna lokalisera och verifiera risken samt kunna hantera den, om så möjligt. Riskhantering behandlar identifiering, bedömning samt kontroll och är en vital del i en organisations fullständiga regelverk och bestämmelser gällande informationssäkerhet (Volchkov, 2019). Att primärt kunna identifiera de risker som organisationen utsätts för är ett krav för att senare kunna bedöma hur stor risken är att de inträffar. Först efter detta kommer organisationen kunna arbeta mot att kontrollera samt reducera risk (Peltier, 2007). Vidare nämner Andrej Volchkov (2019) att de nämnda principerna för riskhantering också är viktiga för att senare kunna tillämpa standarder såsom ISO 27000-serien inom organisationen. För att kunna optimera de rekommendationer som ISO tillför behövs det ett system för att hantera de risker som finns.

2.6.2 ISO 27000 serien

Enligt Diesterer (2013) finns det inget perfekt tillvägagångssätt för att hantera risker men att upprätta ett Risk Management System är ett verktyg för att hantera säkerhetsaspekterna. ISO-certifieringarna ger organisationen ett slags mätvärde och en verifikation för hur långt säkerhetsaspekter och riskhantering är integrerade inom en organisation (Diesterer, 2013). ISO-27000 är den första och övergripliga certifieringen som behandlar standarderna och grunderna för hela 27k serien som sedan fortsätter med ett flertalet specifika certifieringar (Diesterer, 2013).

ISO 27000 bygger på att upprätta ett ISMS (Information security management system) med hjälp av ett ramverk bestående av följande fyra cyklar: plan-do-check-act (PDCA-cycle). *Plan* stadiet i cykeln börjar med att identifiera tillgångarna av information och deras associerade risker, tillsammans med att utforma och välja alternativ för att kontrollera de specifika associerade riskerna skapas en bild av hur ett information security management system skall upprättas. Stadie nummer två i cykeln är *do* vilket behandlar hur det ska gås tillväga med att implementera lösningarna för att kontrollera och hantera säkerhetsriskerna inom sitt ISMS. Stadie nummer tre i PDCA-cykeln behandlar *check* som är till för att övervaka ISMS-systemet i drift, monitorera samt utvärdera prestandan av systemet. Sista steget i cykeln är *act*

vilket innefattar att underhålla och i mån förbättra systemet som ligger i drift samt granska att systemet sköts korrekt (Diesterer, 2013).

En sådan certifiering är beskrivs av Diesterer med vad som nu uppfattas som "*common language of organizations around the world*" och att en verifiering är en bekräftelse från en tredje part, att en organisation uppfyller säkerhetskrav och hanterar sina risker på ett korrekt sätt (2013).

2.7 Sammanfattning av Litteraturgenomgång

Den litteratur vi presenterat ovan är ämnad att öka förståelsen samt kunskapen kring vilka faktorer som kan anses av särskild betydelse i arbetet med policies inom informationssäkerhet. Dessa faktorer har sammanfattats nedan och är indelade i områden baserat på deras inbördes ämnen.

Styrning - Kane och Koppel (2013) benämner vikten i att ha en fullständig och tydlig strategi för styrningen genom hela organisationen. Detta inleds med att kunna uppfatta verksamhetens resurser och nuvarande strategiska position. Vidare benämns kommunikationen som en faktor till god styrning där Höne och Eloff (2002) belyser att god ISP ofta kretsar kring användarna, och hur kommunikationen mellan dessa måste vara koncis och tydlig.

Ansvar & Roller – Både Peltier (2001) och Williams (2012) säger att det är viktigt att en organisation att ha delegerade roller och organisatoriska strukturer inom informationssäkerhet. Både Bulgucru et al (2010) samt Sohrabi Safa et al (2016) benämner att det oftast är anställda som är inblandade de största säkerhetsmässiga hoten, något som kan motverkas av utbildning. Peltier uttrycker att ett så kallad awareness program ska skapa medvetenhet, träna samt utbilda de anställda. Peltier menar även att en strategi för informationssäkerhet inte kan bli implementerad utan att personalen utbildas rätt (2007).

Datahantering - En stor del av den information som riskerar att exponeras finns i form av data. Det är därför viktigt för organisationen att veta hur data ska hanteras. Detta arbete inleds med att identifiera datan man behandlar, som i sin tur leder till en möjlighet att klassificera information i förhållande till dess risk, menar Colin Tankard (2015). Ett begrepp som ofta benämns som grunden i informationssäkerhet är CIA. Begreppet behandlar konfidentialitet, integritet samt tillgänglighet, och beskrivs av Samonas och Coss (2014) som en modell för hur data skall hanteras inom en verksamhet.

Riskhantering - Genom verktyg, identifiering, bedömning samt kontroll menar Kane och Koppel (2013) att en organisation skall kunna hantera de eventuella risker som existerar. Att minimera de hot som riskerna medför är kärnan i informationssäkerhet, där standarder som den framstående ISO 27000 serien finns (Volchkov, 2019). Verktyg som ISO 27000 ger organisationen en indikation på hur väl deras arbete med riskhanteringen är (Diestrer, 2013).

3 Metod

Nedan följer en beskrivning för den metod som utformat arbetet som resulterar i denna uppsats. Litteraturen som används för metodkapitlet är *Den kvalitativa forskningsintervjun* av Steinar Kvale tillsammans med *Från stoff till studie* av Rennstam & Wästerfors. Syftet med metodkapitlet är att visa hur arbetet och tillvägagångssättet studien gått till och hur denne kom till stånd från början.

3.1 Metodval

I boken *Den kvalitativa forskningsintervjun* av Steinar Kvale beskrivs valet av att genomföra en kvalitativ forskningsintervju som grunden i att försöka förstå världen från det utvalda undersökningsobjektets synvinkel. Meningen är att utbytet ska bli ett sådant där objektet som undersöks ger en nyanserad bild grundad på deras erfarenhet och upplevelser av det diskuterade ämnet (2015). Bakgrunden till vår undersökning baseras på den kvantitativa undersökningen som MSB genomförde på 232 svenska kommuner runt om i landet år 2015. MSBs arbete syftar till att kartlägga det systematiska informationssäkerhetsarbetet som genomförs i svenska kommuner. Undersökningen som gjordes av MSB syftade till att kvantitativt insamla konkret data och till vilken utsträckning systematiskt informationssäkerhetsarbete sker ute hos de svenska kommunerna (MSB,2015). Vår studie ämnar att utifrån det som MSB undersökte gällande systematiskt informationssäkerhet, fokusera på specifika policies som utgör styrande riktlinjer i hur kommunerna jobbar informationssäkert. Vi anser då att vår kvalitativa studie kan bidra till en mer nyanserad bild av ämnet. Boken *Från stoff till studie* belyser att en kvalitativ undersökning syftar till att förstå och undersöka betydelser, processer och kvaliteter, snarare än kvantitativ data (Rennstam & Wästerfors, 2015). Vi ämnar till att ge en mer kvalitativ förståelse med fokus på policies gällande informationssäkerhet.

Likt vad som beskrivs i syftet i början av uppsatsen så ämnar arbetet byggas på genomförandet av kvalitativa intervjuer för att skapa en förståelse kring hur arbetet kring policies sker hos kommunerna. En av de aspekter som Kvale (2015) benämner är av vikt för att säkra kvaliteten på intervjun är den intervjuades kvalifikationer. Kvale belyser vikten av att intervjuobjektet har omfattande kunskap kring ämnet och vidare kan föra ett kvalificerat samtal(2015). I vårt fall innebär det en person med god inblick i organisationens verksamhet inom informationssäkerhet. Vidare finns det flera intervjuformer som belyser olika forskningssyften, däribland faktaintervjuer, som inte enbart baseras på objektets enskilda uppfattningar och åsikter, utan främst på korrekt och trovärdig fakta (Kvale, 2015).

Kvale (2015) tar även upp generalisering gällande kvalitativa studier och belyser problematiken kring att de resultat som införskaffas inte nödvändigtvis är korrekta. Detta belyser vikten av att intervjuobjekten skall ha god kunskap och inblick i det sagda ämnet. Vi anser att den kvalitativa studien kommer att göra detta då vi syftar till att både undersöka personliga erfarenheter i kombination med faktiskt information, för att resultatet skall skapa en mer nyanserad bild än den kvantitativa studien som genomfördes av MSB.

4 Studie

I detta kapitel presenteras metoderna för den studie som genomförts. Vi tar nedan hänsyn till de urval som gjorts, hur dessa formats samt beskriver de relevanta faktorerna reliabilitet, validitet samt etiska aspekter och hur dessa är aktuella för studiens resultat samt utförande.

4.1 Urval

Vi har genomfört fem intervjuer med fem diverse ansvariga för informationssäkerhet inom respektive kommun. I vårt arbete med valet av dessa personer har vi utgått från Alan Bryman som i sin bok *Samhällsvetenskapliga Metoder* (2018) beskriver begreppet målstyrda urval. Målstyrda urval grundas i att de kvalitativa objekten för studien skall vara valda utifrån det mål som forskningen skall resultera i. I vårt fall innebär detta att de fem objekten vi intervjuat är kvalificerande samt kunniga inom informationssäkerheten på deras kommun. Vi har även valt särskilja de olika kommunerna på deras storlek baserat på antal invånare, samt geografisk plats. Detta för att uppnå ett så pass balanserat resultat som möjligt.

4.1.1 Val av Respondenter

Då vår studie innefattar en kvalitativ undersökning är det av relevans att de objekt som är föremål för intervju är kvalificerade samt erfarna inom ämnet informationssäkerhet i deras respektive kommun. MSB (2015) nämner i sin undersökning att deras kvantitativa studie är baserad på enkätsvar från anställda inom "IT-funktionen" av kommunen, vilket gjort att svaren från enkäten har formats utifrån denna synvinkel. I vår undersökning var det därför av betydelse att objekten hade god uppfattning om arbetet med informationssäkerheten inom kommunen. Grunden för denna studie innefattar som tidigare nämnt fem diverse intervjuobjekt. Samtliga bedöms vara kvalificerade då de alla har betydande roller inom sin respektive kommun, såsom informationssäkerhetsansvarig och IT-säkerhetsansvarig. Nedan presenteras en tabell över de tillfrågade objekten och deras respektive omständigheter. Uppdelningen av kommunernas storlek har gjorts genom invånarantal, där 1000 - 25 000 invånare setts som liten kommun, 25 000 - 50 000 setts som mellan, samt 50 000 - 150 000 som klassificerats som en stor kommun. Denna indelning har skett med hänsyn till kommunindelningen gjord av *Sveriges Kommuner och Regioner* (2021).

Namn	Förkortning	Storlek (Invånare)
Stor Kommun 1	SK1	ca 100 000
Stor Kommun 2	SK2	ca 100 000
Mellan Kommun 1	MK1	ca 30 000
Liten Kommun 1	LK1	ca 8000
Liten Kommun 2	LK2	ca 20 000

Tabell 1: *Tillfrågade Kommuner*

4.1.2 Utformning & Plats

Den geografiska uppdelningen av intervjuobjekten har omöjliggjort potentialen i att genomföra studien på plats. Detta faktum i kombination med den nuvarande situationen med Covid-19, som gjort att flera branscher tvingats omorganisera sitt arbete utifrån smittorisken har gjort att tre av fem intervjuer har genomförts via programmet Zoom. Programmet tillåter att informanten samt intervjuaren kan se varandra via videokamera, vilket bidrar till en social miljö. I vårt fall är också programmet vitalt då det möjliggör hela studien. Resterande två har gjorts via telefon. Steinar Kvale (2015) beskriver i boken *Den kvalitativa forskningsintervjun* att datorstyrda intervjuer möjliggjort studier som tidigare varit begränsade av geografiska faktorer. Det finns också negativa aspekter med att genomföra en intervju på distans, såsom att avsaknaden av den fysiska aspekten kan resultera i svårigheter gällande uttryck av kroppsspråk (Kvale, 2015). Detta blir däremot enklare att uppnå genom användandet av videokamera.

4.2 Validitet

Validitet som begrepp beskrivs av Steinar Kvale hänga samman med ord såsom riktighet, giltighet och till sanning. För att vidare belysa vikten och definitionen av validitet benämner Kvale ifall den metod som läggs fram verkligen undersöker det den ämnar att undersöka(2014). Vidare skriver Kvale att frågan om validitet kan sammanfattas med frågeställningen ifall man mäter du vad du tror att du mäter (Kvale, 2014). Likt vad som framgår ur syftet av uppsatsen är syftet att kartlägga svenska kommuners informationssäkerhets policies utifrån fyra kategorier, vilket görs i en kvalitativ intervju där urvalet informanter har en huvudsaklig roll gällande styrandet av informationssäkerhet. Validiteten i respondenternas svar bekräftas av att de alla har just en huvudsaklig roll för informationssäkerheten inom kommunen.

4.3 Reliabilitet

I nationalencyklopedin (2021) beskrivs reliabilitet som tillförlitlighet till de värden som blivit uppmätta genom studien. Då reliabiliteten traditionellt sett varit betydande i den kvantitativa forskningen, måste den även nämnas som betydande för den kvalitativa (Kvale, 2015). Kvale menar vidare att reliabiliteten inom den kvalitativa forskningen behandlar huruvida ett resultat är konsistent och som tidigare nämnt tillförlitligt. I intervjusammanhang ter sig detta i form av intervjuobjektens nivå av pålitlighet i sina svar. Kommer en person t. ex svara detsamma på en fråga om den ställs vid olika tillfällen (Kvale, 2015)? Vår studie visar på reliabilitet då samtliga tillfrågade besitter samma eller likartade positioner, samt att transkriberingen och resultatet komponerats inom en kort tidsram vilket bidrar till en sanningsenlig tolkning av studien.

4.4 Etiska Aspekter

I utförandet av kvalitativa undersökningar måste det tas hänsyn till vilka moraliska samt etiska aspekter som är relevanta för studien. Till att börja med fick samtliga intervjuobjekt information om oss som intervjuare, uppsatsens syfte samt hur objektets medverkan användes för studiens resultat. Via telefon var de även informerade om vad intervjun skulle behandla för att minska eventuella osäkerheter. Vidare informerades samtliga intervjuobjekt om att de skulle förbli anonyma om de så önskade, samt att vi innan varje enskild intervju bad om lov för att få spela in samtalet.

5 Empiri

I detta kapitel presenteras vår empiri och resultatet från den kvalitativa undersökning vi genomfört. Nedan presenteras resultatet utifrån varje genomförd intervju och presenteras utifrån de fyra aspekterna vi introducerat i litteraturgenomgången. Varje intervju presenteras utifrån denna dess aspekter.

5.1 Allmänt om Kommunerna

5.1.1 Stor kommun 1 (SK1)

Den första av de två stora kommunerna vi undersökt har ett invånarantal med mer än 100 000 personer. Vårt intervjuobjekt arbetar på den aktuella kommunen och innehar rollen som IT-säkerhetsansvarig. Intervjuobjektet menar att kommunen har en hel avdelning som behandlar informationssäkerhet och bekräftar även att arbetet sker med hänsyn till ett styrande dokument. Mer specifikt finns en samordnar-roll som hanterar arbetet med detta. Vidare anser informanten att det styrande dokumentet blev uppdaterat förra året, samt att kommunen började arbeta med informationssäkerhet i större utsträckning i samband med GDPR införandet 2018 och menar att informationssäkerhet har en betydande roll i kommunens arbete.

5.1.2 Stor kommun 2 (SK2)

Den andra tillfrågade kommunen i undersökningen har ett invånarantal på strax under 100 000. Den tillfrågade jobbar i rollen som biträdande informationssäkerhetsansvarig och har beskrivit sin roll som den personen som jobbar hundra procent med informationssäkerhet inom kommunkoncernen. Intervjuobjektet berättar att en ny strategi om trygghet och säkerhet togs fram för ett år sedan där just informationssäkerheten inom kommunen spelat en stor roll i strategin. Informanten menar att man under senare år pratat och mer och mer om informationssäkerhet, att det för bara något år sen låg mer i bakgrunden men att det blivit större fokus på ämnet de senare åren.

5.1.3 Mellan kommun 1 (MK1)

Den tredje kommunen som tillfrågades i undersökningen har ett invånarantal mitt emellan de två stora och två små kommunerna med omkring 30 000 invånare. Den tillfrågade respondenten till för att representera kommunen innehar rollen som informationssäkerhetssamordnare. En roll som respondenten själv sammanfattar likt att ha det strategiska ansvaret inom kommunen för informationssäkerhet. Respondenten berättar att kommunen har en Policy samt några styrande dokument för att hantera informationssäkerhet. Respondenten tycker att informationssäkerhet är en stor del av kommunens arbete men tycker också att det inte har lyckats anammas rätt riktigt än.

5.1.4 Liten kommun 1 (LK1)

Den fjärde kommunen som intervjuas är en mindre kommun med färre än 15 000 invånare. Den tillfrågade berättar att denne kan titulera sig rollen som informationssäkerhetssamordnare. Samtidigt har den tillfrågade flera andra ansvarsområden på sitt bord, personen innehar bland informationssäkerheten också ansvaret för brottsförebyggande och säkerhetsskydd. Den tillfrågade förklarar att ansvaret är ett av många som hamnat på dennes bord. Den tillfrågade berättar att det finns styrande dokument för kommunen, ett som kallas riktlinjer för informationssäkerhet och ett annat som benämns som policys för informationssäkerhet. Respondenten berättar att kommunen i dagsläget inte riktigt jobbar utifrån de styrande dokumenten och att detta beror på att dessa inte riktigt är bearbetade att bli begripliga och lätta att hantera ännu.

5.1.5 Liten kommun 2 (LK2)

Den sista tillfrågade kommunen benämns som liten och har ett invånarantal med färre än 20 000. Respondenten är kanslichef och är ytterst ansvarig som säkerhetschef. Denne är då chef över information säkerhetssamordnaren, en roll där tidigare sittande precis avgått för någon vecka sen. Respondenten berättar att det för tillfället inte finns någon informationssäkerhetspolicy utan snarare specifika styrdokument för specifika områden av kommunen.

5.2 Styrning

Nedan presenteras de svar som kommunerna uppvisat beträffande styrningen inom kommunen. Svaren presenteras inom sina de aspekter vi tidigare presenterat i uppsatsens litteraturgenomgång.

Beträffande de stora kommuner som vi i detta resultat benämner som SK1 respektive SK2, anser båda intervjuobjekt att styrningen utgår från ledningen och att de har det slutgiltiga besultsfattandet angående kommunens arbete med informationssäkerhet (SK1:48, SK2:58). SK1 uttrycker även att de har en informationssamordnare som också deltar aktivt i de beslut som fattas (SK1:49). SK2 menar vidare att de i beslutsfattandet försöker arbeta utifrån ISO 27000 serien, och att det arbetas aktivt för att få fram riktlinjer för ett s.k “ledningens genomgång” (SK2:58). Detta skall göra det enklare för ledningen att arbeta med informationssäkerhet inom kommunen, där verktyg såsom en årscykel presenteras som en lösning mot att arbeta mer systematiskt inom informationssäkerhet (SK2:59).

Gällande den mellanstora kommunen, så menar informanten att MK1 inte har en liknande styrning som de stora kommunerna har, där ledningen har det slutgiltiga beslutsfattandet (MK1:62). Det saknas i nuläget och informanten beskriver detta som en brist i kommunens arbete med informationssäkerhet (MK1:52). Istället är det informanten själv i sin roll som informationssäkerhetssamordnare som behandlar diverse styrdokument som kommun hanterar (MK1:62). Vidare menar informanten att det även är de enskilda förvaltningarna som beslutar i sin egna verksamhet (MK1:65).

De två små kommunerna LK1 samt LK2 menar att det finns bestämmelser kring beslutsfattandet, där LK1 menar att med hänvisning till deras riktlinjer att det övergripande beslutsfattandet utgår från den politiska ledningen, dvs kommunfullmäktige och kommunstyrelsen. LK2 uttrycker likvärdigt, att det är ledningen i form av kommunfullmäktige som ansvarar för informationssäkerheten inom kommunen (LK2:60). Detta ansvar bryts sedan ner till respektive

förvaltning samt nämnd som i den egna verksamheten ansvarar för sin respektive informationssäkerhet (LK2:61). Kommunstyrelsen i LK2 har även en roll som samordnare, för att behandla ansvaret genom kommunen (LK2:64).

Sammanfattningsvis så tyder resultaten på att de stora kommunernas beslutsfattande utgår från ledningen, och att den mellanstora kommunen, MK1 i detta fall, inte tydliggjort precist hur beslutsfattandet genomförs. De två små kommunerna, LK1 och LK2 har även de har ett beslutsfattande som utgår från ledningen, och att det även finns specifika riktlinjer kring detta.

5.2.1 Kommunikation

I de frågor som rör kommunernas kommunikation inom informationssäkerhet skiljer sig de olika exemplena åt. I kommun SK1 så förmedlas kommunikationen genom ledningsgrupperna samt hos den informationssäkerhetssamordnare som informanten nämner (SK1:49). SK2 förklarar att dennes kommun behandlar kommunikationen inom ett specifikt nätverk, som samtliga representanter från alla kommunens bolag använder. Detta nätverk grundar sig i ett äldre PUL-nätverk, som syftar på personuppgiftslagen (SK2:72). Informanten menar vidare att detta nätverk har omorganiserats, och nu benämns som "Informationssäkerhets och Dataskyddsnätverket" (SK2:74). Detta nätverk används av de ansvariga inom dataskydd samt informationssäkerhet (SK2:76). Utöver arbetet genom nätverket, träffas även alla representanter en gång i månaden där de arbetar med att förmedla information, uppdatering kring verksamheterna, samt arbeta med diverse e-tjänster, rutiner och utbildningar (SK2:77). Detta med målet att få ut dessa aspekter i de respektive verksamheterna (SK2:79).

MK1, den representerade mellanstora kommunen, beskriver att kommunikationen inom deras arbete med styrningen grundar sig i dennes roll som informationssäkerhetssamordnare (MK1:72). Informanten beskriver att de diverse verksamheterna kommunicerar till dennes post när de har funderingar eller dylikt gällande deras information och hanterandet av den (MK1:72). Informanten beskriver även att detta görs allt mer oftare, med verksamheter som hanterar personuppgifter inom t. ex vården i framkant, som gör det mer frekvent (MK1:79).

De mindre kommunerna, LK1 respektive LK2 beskriver kommunikationen inom kommunen på ett liknande sätt som MK1. Informanten representerande LK1 beskriver att det blivit vanligare att frågor från verksamheterna ställs mot denne samt mot kommunens dataskyddsombud (LK1:153). Detta ser informanten som positivt och menar att det tyder på en ökad medvetenhet inom de diverse verksamheterna (LK1:154). I kommun LK2 arbetas det likvärdigt, där informanten i sin roll som informationssäkerhetssamordnare får arbeta utifrån de verksamheter som finns och se till att kommunikation är enhetlig genom alla verksamheter (LK2:74). Som samordnare är detta en huvuduppgift, och informanten beskriver detta som ett viktigt steg i att se till att kommunen arbetar systematiskt med informationssäkerhet genom kommunens alla verksamheter och delar (LK2:75).

Sammanfattningsvis så utgår kommunikationen genom samtliga kommuner från en samordnare som är insatt inom informationssäkerhet. Denna roll arbetar med att sammanställa de diverse verksamheterna som kommunen hanterar, samt göra deras arbete enhetligt. Vidare så menar också en av de stora kommunerna, SK2, att de använder ett nätverk där kommunikation förmedlas och utgår från.

5.2.2 Strategi

Informanten representerande kommun SK1 uttrycker att denne inte vet om det finns någon specifik strategi som styrningen inom informationssäkerhet utgår ifrån, till dennes vetskap (SK1:54). Däremot menar informanten att kommunen har utformade strategier till andra aspekter inom verksamheten, och nämner digitaliseringsstrategi som ett exempel (SK1:55). Den strategi som SK2 arbetar utifrån är den tidigare nämnda strategin gällande ISO 27000, där kommunen skall arbeta mot att bli "certifieringsbara" (SK2:55), för att därefter kunna forma riktlinjer och regler för att kunna nå mot det som informanten beskriver som "ledningens genomgång" (SK2:56). Detta är ett arbete som pågår, och som informanten nämner inte är helt färdigställt (SK2:60). SK2 menar också att kommunen har ett väldigt stort fokus på digitaliseringen inom de olika verksamheterna, och menar vidare att arbetet med informationssäkerhet har en stor roll i digitaliseringen av kommunen och dess resultat (SK2:45). Informanten beskriver också att dennes roll som biträdande informationssäkerhetsansvarig har placerats vid avdelningen för digitalisering och innovation, istället för vid en traditionell plats vid en säkerhetsavdelning (SK2:46).

I den mellanstora kommunen, MK1, är den strategiska styrningen grundat i informantens roll som informationssäkerhetssamordnare (MK1:63). Den tillfrågade beskriver att de styrdokument som denne skapar fungerar som strategisk grund, då de är övergripande för kommunen och dess verksamheter (MK1:64).

Beträffande de mindre kommunerna som undersökts, LK1 och LK2, så beskrivs det som att den strategi som finns även den grundar sig i den informationssäkerhetssamordnare som finns. LK1 beskriver att det saknas en specifik mall eller instruktioner för strategin inom kommunen, men menar vidare att medvetenheten har ökat, och att det är informanten själv i sin roll som får ta emot frågor från de diverse verksamheterna (LK1:153). LK2 beskriver på liknande sätt, där rollen som informationssäkerhetssamordnare får ansvara för att strategin mellan de diverse verksamheterna är enhetlig (LK2:74). Däremot nämner informanten att deras samordnare avgick för en tid sedan, vilket gjort att informanten fått en betydande del i arbetet med informationssäkerhet inom kommunen (LK2:17).

Sammanfattningsvis så visar resultaten att strategin för styrningen av informationssäkerhet i de olika kommunerna ser annorlunda ut. I de två stora kommunerna, så har SK1 i nuläget ingen vetskap om det finns en specifik strategi gällande styrningen, medan SK2 i sitt arbete mycket utgår från aspekterna inom ISO 27 000-serien. I de mindre kommunerna, MK1, LK1 samt LK2 så utgår strategin från rollen som samordnare, som de alla besitter i någon form.

5.3 Roller & Ansvar

Nedan presenteras de svar som kommunerna uppvisat beträffande roller och ansvar inom kommunen. Svaren presenteras inom sina de aspekter vi tidigare presenterat i uppsatsens litteraturgenomgång.

5.3.1 Utbildning

Respondenten som representerar SK1 besvarar att arbetet och frågan kring just utbildning för informationssäkerhet är något som denne har försökt driva framåt i kommunen. Respondenten för SK1 har i sin roll som IT-säkerhetsansarig efterfrågat utbildningar men inte fått gehör från

en ledningsnivå (SK1:69). Respondenten för SK1 belyser att hen skulle vilja ha E-learning utbildningar och att anställda genomför ett proof of conduct test för informationssäkerhet. Respondenten från SK1 vill se att nyanställda får göra denna typ av prov och besvara ett antal frågor för att sedan bli godkända (SK1:79). Dessa typer av utbildningar har eftersträvats av ett par stycken utan gehör från ledningsnivå (SK1:86).

I den andra största kommunen SK2 berättar respondenten att det funnits en del utbildningar i föreläsningsform hos kommunen(SK2:114). SK2 berättar vidare att de utbildningar som skett för personalen varit användningen av MSB:s utbildningsprogram för informationssäkerhet DISA. Vidare benämner respondenten från SK2 att det saknats uppföljning av utbildningarna som har genomförts, att det är på väg in i dagarna som intervjun sker(SK2:116). Respondenten från SK2 avslutar med att förklara att kommunen i framtiden gärna vill se bättre uppföljning och att det i dagsläget byggs upp en plan för att ge nyanställda en obligatorisk utbildning kring informationssäkerhet (SK2:118).

I MK1 svarar respondenten att det för tillfället har genomförts två stycken utbildningar för informationssäkerhet. Den första är en kommunövergripande utbildning som behandlar hur användarna ska hantera information i sin vardag (MK1:98). Vidare svarar respondenten från MK1 att den andra utbildningen är framtagen av arbetsrättsjuristen och utbildar hur en användare ska behandla sekretess i sitt arbete (MK1:101). Respondenten från MK1 berättar att hen har en målsättning att denna utbildning om sekretess ska genomföras av alla arbetande inom kommunen, att den inte riktigt är implementerad i hela organisationen riktigt ännu(MK1:103).

Informanten från LK1 berättar att det innan Coronapandemin fanns en tanke att sätta upp och utbilda verksamhetschefer med instruktioner utifrån MSBs:s riktlinjer vid arbetsplatsträffar (LK1:206). Coronapandemin ställde till den planen och istället har det genomförts så kallade Nano utbildningar för de anställda inom kommunen (LK1:211). Utbildningar som inte tar mer än tre till fyra minuter per tillfälle vilket enligt respondenten möjliggör att utbildningen ska kunna ske oavsett hur mycket tid den anställde har (LK1:219). Nano utbildningen har enligt respondenten från LK1 varit på en grundlig nivå och innehåller alltifrån instruktioner att man inte ska klicka på obehöriga länkar till hur man skall spara ner sin information. Respondenten menar att detta har höjt lägstanivån kring informationssäkerheten hos kommunen (LK1:223). Avslutningsvis förklarar respondenten att det finns just utbildning men att det fortfarande finns en förbättringspotential samt att det är en kamp för att få just sin frågor hörda (LK1:223).

Informanten från LK2 berättar att det för tillfället inte finns någon övergripande utbildning för de anställda inom kommunen. Informanten berättar att detta arbete var något som informations säkerhetssamordnaren hade på sitt bord innan hen slutade för ett litet tag sedan (LK2:99). Respondenten från LK2 berättar att det för tillfället finns en plan för utbildning men ingen som kan genomföra den för tillfället (LK2:101). Avslutningsvis berättar LK2 att det visserligen sker utbildning inom informationssäkerhet enskilt inom respektive verksamhet (LK2:103).

5.3.2 Ansvar

Informanten från SK1 har själv titeln och ansvaret som IT-säkerhetsansvarig (SK1:15).Respondenten från SK1 besvarar att det i riktlinjerna för informationssäkerhet finns satta rollansvar som är till för den enskilde anställde att följa (SK1:63). Respondenten arbetar som IT-säkerhetsansvarig och berättar att det finns en hel avdelning tillägnad informationssäkerhet som hanterar ämnet, till exempel finns det en satt roll med en informationssäkerhetssamordnare (SK1:15). Den tillfrågade från SK1 berättar att rollen som informationssäkerhetssamordnare blev tillsatt år 2018 i samband med att GDPR trädde i kraft (SK1:31).

Informanten som representerar vår andra stora kommun, SK2, har själv rollen som biträdande informationssäkerhetsansvarig och beskriver sig vara den i kommunkoncernen som arbetar med informationssäkerhet till hundra procent (SK2:15). Vidare berättar informant från SK2 att huvudansvaret för informationssäkerhet ligger på förvaltningschefen som kan ses som informationsägare för verksamheten (SK2:91). Ytterligare säger respondenten att det finns en informationssäkerhetsansvarig som också är IT-direktör (SK2:93). Vidare finns det roller med ansvar såsom IT-Säkerhetsansvarig, dataskyddsombud samt informationssäkerhetssamordnare som enligt informanten från SK2 är till för att stötta verksamheterna (SK2:96).

Informanten från MK1 har rollen som informationssäkerhetssamordnare, vilket den tillfrågade berättar sig ha det strategiska ansvaret för informationssäkerhet inom kommunen (MK1:17). Informanten från MK1 påpekar att hen blev tillsatt för 3 år sedan och att det innan dess inte fanns någon på heltid som satt i tjänsten och hade det strategiska ansvaret för informationssäkerheten (MK1:19). Vidare beskriver informanten från MK1 att det är förvaltningscheferna som är informationsägare och att det är förvaltningarna som vidare ska ha sina egna handläggare för området informationssäkerhet (MK1:86). Respondenten från MK1:s ansvar är att strategiskt stötta handläggarna på förvaltningarna med sitt arbete för informationssäkerhet (MK1:88).

Informanten från LK1 har rollen som trygghetstrateg på kommunen, vilket den intervjuade benämner som ett tämligen brett ansvar (LK1:82). I den rollen är denne också informationssäkerhetssamordnare. Bland annat ansvarar informanten i rollen som trygghetstrateg också för områden såsom brottsförebyggande och säkerhetskydd (LK1:83). Informanten från LK1 berättar att arbetet med informationssäkerhet var likt en puck som hamnade på dennes bord för 4 år sedan och beskriver sig fortfarande befinna sig i lärande fasen av ämnet (LK1:36). Vidare berättar respondenten att det utöver hens roll finns ett dataskyddsombud som enbart jobbar och ansvarar med behandlingen av person uppgifter (LK1:198).

Respondenten har för LK2 har ansvaret som kanslichef och chef över en roll som benämns informationssäkerhetssamorndaren. Personen som satt i den senast nämnda rollen har precis varit slutat men informanten beskriver att dennes roll som kanslichef chefar över informationssäkerhetssamordnaren (LK2:18). Vidare beskriver respondenten att hen är säkerhetsskyddschef enligt säkerhersskyddslagstiftningen(LK2:19) Respondenten beskriver att det är kommunfullmäktige som har det övergripande ansvaret för informationssäkerheten (LK2:60). Sedan beskriver respondenten för LK2 att respektive nämnd ansvarar enskilt för informationssäkerhetsarbetet som sker i de olika nämnderna (LK2:62).

5.4 Datahantering

Nedan presenteras de svar som kommunerna uppvisat beträffande datahanteringen inom kommunen. Svaren presenteras inom sina de aspekter vi tidigare presenterat i uppsatsens litteraturgenomgång.

5.4.1 Klassificering

På de frågor som beträffar klassificering av den data som respektive kommuner hanterar kan det konstateras att samtliga kommuner arbetar utifrån detta, men på olika sätt och utvecklingsnivåer. De stora kommunerna, SK1 och SK2 arbetar båda med att klassificera den datan dem hanterar. SK1 belyser att klassificeringen av t. ex dokument görs inom kommunen (SK1:112) . Vidare menar informanten att kommunen klassificerar både manuellt samt via speciella program, som då klassificerar informationen utifrån dess nivå av sekretess b. la (SK1:112). Vidare uttrycker informanten att detta är något som man borde göra i större utsträckning genom sveriges kommuner och menar också att han inte tror att det är så vanligt (SK1:114). Informanten som representerar SK2 menar också att den egna kommunen klassificerar, och förklarar att klassificeringen grundar sig den informationshanteringsplan som är upprättad utifrån arkivlagen (SK2:136) . Den informationshanteringsplan tar sig i form av omfattande worddokument, som samlar mängder av information, menar informanten (SK2:138). Vidare arbetar även SK2 med klassificering av system, för att kunna konstatera vilken information som är ämnat till vilket system (SK2:141). Även SK2 menar som SK1 också uttrycker att klassificering är något som kommunen måste arbeta med ytterligare, och fortsätta utveckla samt utvärdera för varje år (SK2:143).

Även kommun MK1 arbetar med att klassificera den data som hanteras och beskriver arbetet som "högt och lågt" där klassificering sker men inte på ett tillräckligt systematiskt sätt (MK1:139). Informanten menar vidare att klassificering pågick innan den tid som denne tillsattes som informationssäkerhetssamordnare, och att de verksamheter i kommunen som hanterade skyddsvärd information gjort det som en del i deras arbete (MK1:140).

Beträffande de små kommunerna, LK2 och LK2, så är arbetet med klassificering bara påbörjat. Informanten för LK1 beskriver att kommunen i sitt arbete använder Office 365, och sparar arbetet utifrån dess verktyg (LK1:260). Det är därför svårt att alltid veta var informationen tar vägen efter att användaren sparat dokumentet (LK1:261). Dessutom sparas allting i programmets moln, och där finns det särskilda bestämmelser hur information lagras där, menar informanten (LK1:247). Vidare beskriver informanten att det bästa hade varit att kunna klassificera ett dokument när det skapas, för att sedan kunna placera det på lämplig plats utifrån dess risk och innehåll (LK1:276). Arbetet med klassificeringen inom kommun LK1 har på grund av diskussioner om molnlagring gentemot server-lagring stannat upp arbetet, och informanten uttrycker även att de väntar på att Sverige skall bestämma sig kring de regelverken som påverkar dessa faktorer (LK1:282). Informanten menar dessutom att klassificering sker inom specifika verksamheter inom kommunen som arbetar utifrån specifika program, som har egna lösningar på klassificering av data (LK1:283). Slutligen sammanfattar informanten att klassificering sker inom kommunen, men inte hos den enskilde anställde (LK1:291). LK2 och dess arbete med klassificering av data är också pågående, där informanten menar att kommunen arbetar utifrån ett program vid namn "KLASSA" som sveriges kommuner och regioner har tagit

fram (LK2:126). Detta arbete har inte slutförts ännu, då kommunen inte hunnit gå igenom all informationsmängd som de ansvarar över (LK2:128).

Sammanfattningsvis så arbetar de större kommunerna, SK1 och SK2 med klassificering av data. Den mellanstora kommunen MK1 hävdar att klassificering också görs inom kommunen, men inte på ett tillräckligt systematiskt sätt. Slutligen så har arbetet med klassificering även påbörjats inom de små kommunerna LK1 samt LK2, men där båda representerade informanter hävdar att de har en lång väg att gå innan arbetet är färdigställt.

5.4.2 CIA (Confidentiality, Intergrity, Availability)

Hur kommunerna i fråga förhåller sig till CIA triaden är olika. Ett arbete med klassificering innebär att behandla frågor som konfidentialitet, integritet samt tillgänglighet. Samtliga kommuner hävdar att detta arbete pågår. Den klassificering som sker utifrån informationen och dess sekretess gör att CIA triaden behandlas, men till olika grader.

5.5 Riskhantering

Nedan presenteras de svar som kommunerna uppvisat beträffande riskhanteringen inom kommunen. Svaren presenteras inom sina de aspekter vi tidigare presenterat i uppsatsens litteraturgenomgång.

5.5.1 Informationssäkerhetsrisker

I de frågor i intervjun som omfattat riskhanteringen inom informationssäkerhet, så menar samtliga informanter att hanteringen av informationen är en risk. Inom de stora kommunerna, SK1 samt SK2, så menar båda informanter att riskerna finns på användarnivå (SK1:99, SK2:126). Informanten som representerar SK1 belyser detta genom att förklara att det inte finns tillräckligt med kunskap inom hanteringen av information hos användarna, och informanten ser detta som den största risken som existerar i förhållande till informationssäkerheten inom kommunen (SK1:99). I kommun SK2 resoneras det likartat, där informanten hävdar att det saknas kompetens hos medarbetarna gällande hanteringen av information och data (SK2:126).

Beträffande den mellanstora kommunen MK1, så menar informanten att en stor fråga som angår riskhanteringen är vilka resurser som finns till hands för kommunen att arbeta utifrån (MK1:123). Informanten menar att det inte finns tillräckligt med resurser för att hantera alla de risker som existerar i samband med informationshanteringen, vilket gör att särskilda hot som t. ex cyber-säkerhetshot blir allt mer uppenbara (MK1:127). Vidare beskrivs det att statliga verk som kommuner har andra krav att arbeta med informationssäkerhet, krav som också blir allt mer svåra i.o.m den budget som ges (MK1:130). Detta visar sig t. ex i införskaffandet av nya system (MK1:126). Personal blir också en risk med tanke på kraven och budgeten, och informanten menar att detta då blir en påtaglig risk (MK1:134). Vidare uttrycker denne önskningar om att regeringen borde ställa högre krav för kommuner, då de ansvarar för hanteringen av samhällsviktiga tjänster (MK1:129). Informanten menar att detta är något som många kommuner får arbeta med, och talar inte specifikt utifrån dennes egna kommun (MK1:123).

När det gäller de mindre kommunerna i undersökningen, LK1 och LK2, så finns riskerna också i hanterandet av den information man arbetar med (LK1:257, LK2:109). I samband med resonemanget kring LK1s arbete med Office 365 och dess molnlagring, menar informanten att risker uppkommer i denna procedur (LK1:257). Informanten beskriver vidare att risker uppkommer när man sparar information på diverse ställen, då det inte är självklart att man vet var informationen hamnar (LK1:260). Risker uppkommer då det finns flertal sätt att spara den information man hanterar, menar informanten, och att det därför blir svårt att spåra data (LK1:261). LK2 nämner vikten av förtroendet som finns för kommuner kan skadas när hanteringen av information är bristfällig (LK2:116). Informanten nämner att det finns en rad exempel där det finns brister hos kommunerna inom informationssäkerhet, och att detta i sin tur påverkar allmänhetens förtroende för dem (LK2:115). Informanten nämner vidare ett exempel som hanterandet av patientjournaler, där riskerna kan resultera i en liv och död fråga, om tillgången till sådana uppgifter är bristfällig (LK2:117).

Sammanfattningsvis så anser alla kommuner att den största risken inom hanteringen av information är just i arbetet med data samt information. Detta med undantag för MK1 som främst uttrycker att risker uppkommer i.o.m resursbrister.

5.5.2 ISO 27000

Samtliga av de tillfrågade kommunerna fick svara på frågan huruvida de använder ISO i sitt arbete. Resultatet visar att samtliga kommuner arbetar utifrån ISO och främst ISO 27000 serien, men att de har utvecklats olika i det arbetet. SK1 menar att de hänvisar till ISO i sitt arbete med informationssäkerhet, och menar vidare att de även hänvisar till standarder när det gäller annat arbete, och nämner hanteringen av s.k datahallar som exempel (SK1:137). Informanten menar vidare arbetet med ISO är något de försöker hänvisa till. (SK1:137). SK2 arbetar även dem utifrån ISO, och informanten beskriver att det beslutades i den strategi som tidigare nämnts i resultatet för styrning, att kommunen skall arbeta utifrån ISO 27000 (SK2:55). Informanten beskriver att kommunen arbetar mot att bli "certifieringsbara" men inte att de skall certifiera sig (SK2:56). Vidare så beskrivs det att kommunen i nuläget arbetar med att få fram de riktlinjer som hör till ISO 27000, detta arbete har dessvärre stannat upp då den pågående covid-19 pandemin krävt att kommunen behövt prioritera om (SK2:150-153). Vidare arbetas det även med utbildning i förhållande till ISO 27000 och sedan skall också arbetet slutföras med det s.k "ledningens genomgång" som tidigare nämnt i detta resultat (SK2:154). Den undersökta medelstora kommunen, MK1, arbetar också enligt ISO 27000 menar informanten (MK1:146).

Beträffande de mindre kommunerna, så hävdar båda informanter att deras respektive kommuner försöker arbeta utifrån ISO. Informanten för LK1 förklarar arbetet med ISO som att kommunen försöker, och menar att kommunen inte lyckas arbeta utifrån alla delar av ISO standarden, såsom riktlinjerna för klassificering, som informanten nämner som exempel (LK1:299). Vidare så menar informanten att det framgår i LK1s riktlinjer för informationssäkerhet att de skall arbeta utifrån ISO standarder, men påstår som sagt att detta inte görs tillräckligt (LK1:304). Informanten för LK2 menar att kommunen arbetar med ISO på sätt och vis, men beskriver att kommunen inte har som mål att bli certifierade, men att arbetet skall vara grundat i de standarder som ISO belyser (LK2:138). Vidare menar informanten att i arbetet med

att ta fram en handlingsplan för informationssäkerhet inom kommunen, så har informationssäkerhetssamordnaren utgått från ISO standarder (LK2:139).

Sammanfattningsvis så arbetar samtliga av de tillfrågade kommunerna med ISO standarder till en viss grad. De större kommunerna försöker hänvisa till ISO frekvent, där SK2 också arbetar aktivt med att få fram specifika riktlinjer att arbeta utifrån. MK1 hävdar också att de arbetar utifrån ISO och belyser ISO 27000-serien. Beträffande de mindre kommunerna beskrivs arbetet som pågående, där både LK1 samt LK2 försöker arbeta utifrån ISO, men har mycket kvar att göra innan detta kan göras fullt ut.

6 Diskussion

Nedan diskuteras samt analyseras vårt resultat i förhållande till den teori vi tidigare presenterat i denna uppsats. Diskussionen är uppdelad utifrån de fyra aspekter vi tidigare presenterat.

6.1 Styrning

6.1.1 Kommunikation

I den teori som presenterats i litteraturgenomgången belyser Kane och Koppel (2013) vikten av att styrningen inom en organisation skall ske från ledningen och genom alla de diverse verksamheterna. Detta för att kunna säkerställa att ett arbete med informationssäkerhet förekommer enhetligt genom organisationen i fråga. Då vi i vår undersökning har fokuserat på svenska kommuner så måste teorin också behandlas utifrån den uppbyggnad som kommunerna har. Kommuner har ett oerhört ansvar för landets välmående och är uppbyggt av flera diverse verksamheter som alla ansvarar för olika aspekter av kommunen övergripande arbete. Det är därför av stort intresse att undersöka hur kommunikationen mellan dessa olika verksamheter inom kommunen är uppbyggda gällande ämnet informationssäkerhet, samt hur dessa kan bli behandlade i kommunens riktlinjer och regler, s.k policies.

Som tidigare nämnt så belyser teorin att det är viktigt att kommunikationen gällande informationssäkerhet utgår från ledningen, för att sedan kunna genomföras inom respektive verksamhet. Detta för att få kommunikationen så pass enhetlig och koncis som möjligt. Teorin belyser även att information skall ses som en tillgång, och resultatet visar att samtliga av de tillfrågade kommunerna anser att informationssäkerhet har en mycket betydande roll i kommunens arbete. Det belyses även i empirin att samtliga av de fem kommuner vi undersökt arbetar med kommunikation gällande informationssäkerhet, men gör det på ett flertal olika vis. I kommun SK1 så belyser empirin tydligt att kommunikationen gällande informationssäkerhet inom kommunen utgår från kommunens ledning. Detta tillsammans med en specifik informationssamordnare som också har en del i de beslut som tas. Att kommunen har en samordnare gällande informationssäkerhet tyder på att denne också ser till att kommunikationen gällande informationssäkerhet är enhetlig genom kommunens alla led och verksamheter, vilket bidrar till en koncis styrning.

Höne och Eloff (2002) belyser också att det i slutändan är användarna själva som beslutar huruvida starkt en organisations informationssäkerhetsarbete är. I kommunernas fall så är det mångt och mycket de anställda som är ansvändarna, då det är dem som arbetar och hanterar den information som kan ses som värdefull. Det är därför vitalt att kommunikationen genom organisationen är enhetlig. I kommun SK2 så visar resultatet att de utgår från ett speciellt nätverk i deras arbete med kommunikation för informationssäkerhet. Nätverket används av alla representanter från de olika verksamheterna inom kommunen, och bidrar då till att kommunikationen är enhetlig. Utöver detta, så träffas dessa representanter en gång i månaden för att se till att informera, uppdatera samt förmedla information som kan vara av värde för de olika verksamheterna. Kommunen benämner nätverket som “Informationssäkerhet och

dataskyddsnätverket" och behandlar frågor utifrån hanteringen av information. Att använda verktyg som dessa gör det enklare för kommunen att kommunicera styrningen från ledningen genom alla de inblandade verksamheterna.

Den mellanstora kommunen som vi undersökt framhäver inte likartade verktyg, men menar att kommunikationen utgår från den roll som den tillfrågade har som informationssäkerhetssamordnare. Informanten beskriver att de olika verksamheterna kommunicerar frågor och funderingar till denne vid behov. Via de svar som vi fått så framgick det inte huruvida enhetligt kommunikationen är, och om den är grundad i ledningen. Informanten menar vidare att frågor som rör informationssäkerhet är något som informanten får ta emot allt mer ofta, och ser detta som något positivt. Det går att konstatera att informanten därför har en vital roll i kommunens arbete med informationssäkerhet, och att det också är viktigt att denne förmedlar likvärdig och koncis information till alla verksamheter, för att säkerställa att arbetet sker likartat. Det framgår i teorin att det är viktigt att informationsarbete såsom riskhantering och specifika säkerhetsfunktioner inte skall ske i det tysta. det är därför ett bra tecken att informanten för MK1 hävdar att dennes kontakt och kommunikation med verksamheterna blivit allt mer frekvent.

De mindre kommunerna som framgår i empirin, LK1 samt LK2, menar att deras kommunikation behandlas på ett likartat sätt som beskrivet i MK1. Informanten som representerar LK1 menar att det blivit mer vanligare att det ställs frågor mot denne eller kommunens dataskyddsombud. Detta kan som nämnt gällande MK1 också ses som en positiv trend, då det visar att kommunens verksamheter behandlar informationssäkerhet och dess värde. Däremot kan det också belysas som ett problem att de diverse verksamheterna har mer frekventa funderingar kring informationssäkerhet, vilket kan tyda på att kommunens styrning samt kommunikation behöver förbättras. Att de olika verksamheterna visar att de inte har full kunskap gällande hanteringen av information gör att eventuella risker kan uppkomma hos de användare som använder den, i kommunens fall medarbetarna. Empirins resultat gällande kommun LK2 tyder på likvärdigt hanterande av kommunikation. Det är informationssäkerhetssamordnaren som i sitt arbete ansvarar för att kommunikationen genom de olika verksamheterna sker på ett enhetligt vis. Detta beskrivs av informanten som samordnarens huvudsakliga uppgift, att se till att kommunens alla delar arbetar informationssäkert. Det framgår som sagt genom teorin att det är av betydelse att kommunikationen utgår från organisationens ledning. Även fast de svar vi fått gällande kommunikationen inom de mindre kommunerna inte belyser detta, så är detta inget garanti för att det inte sker. Det som är viktigt är att kommunikationen är enhetlig och koncis genom hela kommunen för att säkerställa att informationssäkerhet behandlas och arbetas med inom samtliga delar av kommunen.

6.1.2 Strategi

En ytterligare del i att en organisation skall kunna uppnå en välgrundad styrning finns i att ha en tydlig strategi för verksamhetens informationssäkerhet. Teorin som vi presenterat i uppsatsens litteraturgenomgång belyser detta. Kane och Koppel (2013) belyser vikten av att organisationen måste kunna förstå den nuvarande position som verksamheten befinner sig i gällande informationssäkerhet, för att sedan kunna införa och bestämma lämpliga förändringar i arbetet. Detta består b. la i att kunna uppfatta de resurser som organisationen har tillgång till. Då vi i denna studie undersökt svenska kommuner, så kan detta se väldigt annorlunda ut genom de olika kommunerna.

Man kan anta att större kommuner har större resurser att tillgå, och att deras inbördes strategier skiljer sig åt, vilket vår empiri också visar. Kane och Koppel (2013) menar att en grundad strategi skall vara gjord utifrån de tre aspekterna som belyser analys, val av tillvägagångssätt samt slutligen en implementation. Krag Brotby (2009) menar liknande tidigare teori att organisationens strategi måste vara skapad utifrån det landskap och kultur som organisationen befinner sig i, vilket förklarar att kommunernas strategi har förmedlats på diverse sätt genom vår undersökning, då samtliga visar på ett annorlunda informationssäkerhetsarbete.

Informanten som representerar SK1 förmedlar att denne inte riktigt vet om det finns en specifik strategi som är byggd utifrån arbetet med informationssäkerhet, däremot uttrycker informanten att det finns andra strategier inom kommunen som rör andra aspekter av verksamheten, och nämner en digitaliseringsstrategi som exempel. Om man jämför detta med SK2, den andra tillfrågade stora kommunen, så skiljer sig svaren avsevärt. Informanten för SK2 uttrycker att mycket av den strategi som kommunen arbetar utifrån grundar sig i standarden ISO 27000-serien. Detta arbete sker utifrån de riktlinjer som ISO hanterar och kommunen arbetar för att kunna nå det som informanten beskriver som "ledningens genomgång" som skall resultera i en komplett styrning som utgår från ledningen. Vidare påstår informanten även att detta är ett arbete som kommunen arbetar successivt med, och att det är en pågående process. Kane och Koppel (2013) nämner just att organisationer kan arbeta med vad de benämner som "best practices" för att kunna ge verksamheten en indikation på hur deras position gällande informationssäkerhet ser ut. Det kan därför ses som positivt att SK2 arbetar aktivt med ISO 27000 i utformandet av sin strategi, för att då enklare förstå vad som behöver arbetas vidare med. Vidare så menar informanten att dennes roll som biträdande informationssäkerhetsansvarig har placerats vid avdelningen för digitalisering och innovation, då informanten påstår att kommunen har ett stort fokus på digitaliseringen. Brotby (2009) menar genom teorin att det är viktigt att det finns en tydlig kontext inom organisationens arbete med informationssäkerhet, vilket gör att placeringen av informantens roll belyser att informationssäkerhet är en viktig del av digitaliseringen inom kommunen. Inom den mellanstora kommunen är strategin grundad i informantens roll som informationssäkerhetssamordnare, vilket gör att dennes position får väldigt mycket ansvar.

Beträffande de mindre kommunerna, LK1 samt LK2, ser situationen liknande ut. LK1 och dess informant uttrycker att det är denne i sin roll som samordnare som ansvarar för att vägleda samt handleda verksamheterna utifrån deras funderingar inom informationssäkerhet. Informanten menar att medvetenheten inom kommunen har ökat, vilket gör att denne får frågor från de olika verksamheterna mer frekvent. Även detta gör att informanten får ett oerhört ansvar i kommunens strategi kring informationssäkerhet. I den andra mindre kommunen, LK2, visar sig situationen vara liknande, där det är informationssäkerhetssamordnaren som får ta emot frågor och funderingar från verksamheterna. Informanten uttrycker också att den samordnare som gjorde detta också avgick för en tid sedan, vilket resulterat i att informanten i sin roll som kanslichef fått ta över under tiden. Detta kan tyda på att det inte finns tillräckligt med resurser att hantera informationssäkerhet och strategin kring det, då det inte finns personal med högre spetskompetens kring ämnet som kan arbeta under tiden en ny samordnare sökes. Även om informanten nämner att denne är säkerhetsskyddschef och att informationssäkerhet är en del av det arbetet.

6.2 Roller & Ansvar

6.2.1 Utbildning

Utifrån svaren som redovisas i empirin så är utbildning en faktor som varierar kraftigt hos de olika kommunerna. Det verkar inte finnas några tydliga övergripande krav på att en kommun måste bedriva utbildning inom informationssäkerhet och svaren har resulterat i att det i vissa kommuner knappt finns någon utbildning alls samtidigt som det i andra hela tiden pågår utbildning för informationssäkerhet. Peltier beskriver hur en strategi för informationssäkerhet inte kan bli implementerad utan just rätt träning för de anställda. Utbildning ska grunda sig i att ge de anställda träning och utbildning inför en Information Security Policy (2007).

Den största kommunen SK1 besvarar frågan kring utbildning att det finns en avsaknad och att det i dagsläget är just utbildningar som hen i sin roll som IT-säkerhetschef efterfrågat utan att få tillräcklig gehör från kommunens ledning. Nästa stora kommun, SK2, berättar att det har funnits en del utbildningar i föreläsningsform hos kommunen, utbildningarna som skett för personalen i SK2 har varit förankrade i just MSB:s utbildningsprogram. SK2 belyser att trots att det faktiskt funnits utbildning för de anställda så har det fallerat i uppföljningen av utbildningarna, något som enligt respondenten säger vara på väg in under dagarna. Hos en annan kommun, MK1, fanns det istället två konkreta utbildningar, en som skedde på en kommunövergripande nivå kring hur användare hanterar sin data och en annan som behandlar sekretess i sitt arbete. Målsättningen som respondenten från MK1 la fram att var att utbildningen för sekretess inte är genomförd av hela kommunen men att den står i begrepp att bli det. I bägge fallen för de två mindre kommunerna, LK1 och LK2, så har viss utbildning bedrivits. I LK1:s fall har man höjt lägstanivån med grundliga nanoutbildningar i informationssäkerhet. I LK2:s fall så bedrivs inte utbildningar på en kommunövergripande nivå utan utbildning är utlagt på de enskilda verksamheterna. I bägge fallen av de mindre kommunerna, LK1 och LK2, så fanns och finns det planer på att utveckla aspekten av utbildning, i LK1:s fall havererade planerna på grund av coronapandemin och i LK2:s fall så låg planerna på bordet av en informationssäkerhetssamordnare som aldrig kom till skott på grund av att denne slutade.

För samtliga kommunerna medverkande i undersökningen har det alltså funnits eller finns utbildningar, om än i vissa fall en begränsad upplaga. Samtliga 5 respondenter har på ett eller annat sätt belyst att det finns förbättringspotential för sin respektive kommun när det kommer till utbildning. Anledningarna till att det kan tyckas finnas och ses en förbättringspotential skiljer sig åt mellan kommunerna. För SK1 fanns en önskan att utbildning ska tas fram, för SK2 skulle denne följas upp bättre samt MK1 som hade en vision att implementera utbildningar i en större utsträckning. Även LK1 och LK2 tycks sig ha en potential att utveckla spektret av utbildning men att detta inte kunnat genomföras på grund av diverse anledningar som nämns ovan, coronapandemin samt avgående positioner.

Peltier menar att det slutligen inte spelar någon roll hur starkt säkerhetsarbetet är för informationssäkerhetspolicies inom en organisation om det inte finns ett tydligt sätt att förankra den hos de anställda (2007). Det är alltså av vikt att kommunerna fortsätter att förankra utbildningar och kunskap hos de anställda för att lyckas jobba informationssäkert inom sina organisationer. Mot vad som står i teoriavsnittet så är det just de anställda som utgör ett stort informationsmässigt säkerhetshot mot organisationer, det är oftast de anställda som oftast är inblandade i säkerhetsincidenter, detta benämns av både Bulgurcu et al(2010) samt Sohrabi Safa(2016). Arbetet är inte riktigt slutfört och det kan tyckas behövas förbättringar där utbildning får en större plats i de policys som kommunerna jobbar fram.

6.2.2 Ansvar

I teorikapitlet beskrivs det av Kane & Koppel vikten av att det finns tydliga satta roller med befattningar som har ansvar inom organisationen (2013). I våra fem kommuner som använts i undersökningen har samtliga respondenter just en ansvarsgrund i arbetet mot informationssäkerhet. De olika rollerna som respondenterna har är IT-säkerhetsansvarig,informationssäkerhetsansvarig, informationssäkerhetssamordnare, trygghetsstrateg samt kanslichef. Det som skiljer de olika kommunerna åt är hur stort ansvarsområdet är fördelat på personalen hos de olika kommunerna. En jämförelse är att det i den stora kommunen SK1 finns en hel avdelning för informationssäkerhet samtidigt som informationssäkerhetsarbetet i LK1 är tillordnad rollen trygghetsstrateg, en roll som utöver informationssäkerhet också är ansvarig för brottsförebyggande och säkerhetsskydd. SK1, SK2 samt MK1 har enligt empirin en person med tillsatt ansvar som jobbar heltid med att samordna informationssäkerheten inom kommunen. För LK1 delas detta ansvar av en heltidsanställd som samtidigt har hand om andra aspekter av verksamheten, för LK2 har det funnits en position arbetat med en med ämnet men som precis avslutat sin tjänst. Det som benämns i teorikapitlet av Williams(2012) är att det skall finnas organisatoriska strukturer inom verksamheten, vilket finns samtidigt som dessa skiljer sig åt i storlek och omfattning mellan kommunerna. I teorikapitlet tas det upp hur det är de styrandes uppgift att delegera ut roller, roller som bär just ansvaret för det dagliga arbetet med informationstillgångar, ansvar som kan likställas med en chief information officer för att sen fördelas ner till en vad författaren benämner som en Systems Security Officer (Peltier, 2001). Liknande roller finns etablerade för samtliga kommuner, det finns positioner med ansvar för informationssäkerheten. Det som skiljer kommunerna åt är just att respondenten från LK1 inte enbart kan fokusera på att jobba med just informationssäkerhet då dennes positionen som trygghetsstrateg även innefattar andra delar av kommunens verksamhet.

6.3 Datahantering

6.3.1 Klassificering

Klassificering av data har en omfattande roll i hur en organisation hanterar sin information. Genom att klassificera, kan organisationer enklare förstå vikten av den information som existerar, såväl som dess tillhörande risk. I vår studie av de fem kommunerna vi tidigare presenterat så har vi som del i arbetet undersökt huruvida kommunerna förhåller sig till klassificering inom verksamheten. De svar vi fick tyder på att samtliga av de tillfrågade kommuner på något vis arbetar med klassificering, men till olika grad. De större kommunerna visar utifrån vår undersökning att deras arbete med klassificering av data har kommit längre än de mindre kommunerna, där informanterna uttrycker att arbetet bara börjat.

SK1 och dess representant menar att dennes kommun aktivt arbetar med klassificering av data, och nämner specifikt klassificeringen av dokument som ett exempel. Teorin belyser att organisationer bör implementera verktyg för att kunna klassificera sin data och utveckla sina riktlinjer angående ämnet (Tankard, 2015). Detta uttrycker informanten för SK1 att kommunen arbetar med, och menar att verksamheterna arbetar både manuellt och via speciella program, som klassificerar datan utifrån dess nivå av sekretess och risk. Detta gör att kommunen

enklare kan dela in den information som de hanterar, för att då också förstå vilken grad av skydd som informationen bör ha. Att kunna värdera informationen utifrån dess risk är ett krav för klassificering, och då kan speciella verktyg vara till hands (Tankard, 2015). Informanten menar att arbetet sker utifrån specifika program, och att klassificeringen även sker manuellt. Slutligen så uttrycker också informanten att klassificering är något som bör göras i större utsträckning, och att denne inte heller tror att det pågår ett arbete med klassificering på många av Sveriges kommuner.

Beträffande den andra stora kommunen som vi undersökt, SK2, så menar även dennes informant att kommunen arbetar med klassificering av den data man hanterar. Informanten uttrycker att deras arbete med klassificering inom kommunen grundar sig i en informationshanteringsplan, som är upprättad utifrån arkivlagen. Vidare beskriver informanten att informationshanteringsplanen visar sig i form av omfattande word-dokument, där mängder av information sparas. Tankard (2015) belyser vikten av att använda verktyg som varierar i funktion för att på så sätt få en så bred helhetsbild av klassificeringen inom organisationen. Att samla all information i ett word-dokument kan göra det svårt för kommunen i sitt arbete, då det kan vara problematiskt att bilda sig en uppfattning kring all mängd av information genom ett dokument som skall samla mycket av kommunens data. Kane och Koppel (2013) menar att en del i klassificeringen är att urskilja riskerna som informationen har, vilket kan bli komplicerat om man skall utgå från ett omfattande dokument. Vidare uttrycker informanten att SK2 också arbetar med klassificering av system, vilket tyder på att arbetet sker på flera sätt genom verksamheten. Informanten uttrycker slutligen också som SK1 menar, att arbetet med klassificering är något som kommunen måste fortsätta och utveckla vidare. Den mellanstora kommunen, MK1, menar att klassificering av data också sker inom kommunen, men informanten uttrycker att detta inte sker på ett tillräckligt systematiskt vis.

Beträffande de två mindre kommunerna, så menar båda informanter att arbetet med klassificering inom kommunen har påbörjats, men att de både har mycket arbete kvar för att det skall bli färdigställt. Informanten som representerar LK1 menar att de arbetar utifrån Office 365, och att informationen sparas där via molntjänsten som programmet besitter.

Vidare uttrycker också informanten att arbetet med klassificering inom kommunen har stannat upp, då diskussioner pågår angående moln eller serverlagring. Som Tankard (2015) uttrycker, så måste verksamheten använda rätt verktyg för att kunna nå en fulländad klassificering. Kommunen måste då arbeta med detta ytterligare, för att bestämma sig om vilket verktyg som är lämpligt att använda sett till kontexten av den information de skall klassificera. LK2 uttrycker att de använder sig av programmet "KLASSA" för att klassificera system med avseende för informationssäkerhet. Informanten uttrycker också att detta arbete också bara är påbörjat, och att det finns mycket kvar att arbeta med.

Sammanfattningsvis kan man konstatera att de större kommunerna har kommit längre i sitt arbete med klassificering gentemot de mindre som bara påbörjat processen. Detta kan vara på grund av resurs samt personal aspekter, då man kan anta att de större kommunerna har mer att tillgå i frågor beträffande informationssäkerhet samt klassificering.

6.3.2 CIA (Confidentiality, Integrity, Availability)

När en organisation arbetar med hantering av data så måste det göras med hänsyn till CIA triaden. De tre aspekterna behandlar konfidentialitet, integritet samt tillgänglighet. Konfidentialiteten behandlar hur organisationen gör att information och data endast behandlas av de med

tillgång till den, för att förhindra att data inte manipuleras eller extraheras till fel parter. Integritet behandlar att data och information skall vara korrekt medan tillgänglighet belyser vikten av att data skall vara tillgänglig för dem som hanterar den. En del i att arbeta utifrån CIA är att klassificera den data och information man hanterar. Då samtliga kommuner hävdar att de arbetar med klassificering till viss grad så behandlar man åtminstone en del av CIA. Att klassificera data utifrån sekretess och risk gör att man skapar konfidentialitet. Den risk som information för med sig blir också enklare att hantera om organisationen arbetar med klassificering, då man enklare kan värdera och skydda information utifrån dess sekretess. Detta i sin tur bidrar med integritet. Då samtliga kommuner även har tillsatta roller som behandlar informationssäkerhet och vilka användare som hanterar den, så kan det antas att kommunerna också arbetar med tillgänglighet, då de genom roller, utbildning, ansvar samt styrning belyser vilka på kommunen som får hantera information. Att även implementera verktyg som kan hjälpa kommunerna att skydda information, såsom exemplet "KLASSA" gör även att verksamheten kan arbeta mot att förhindra eventuella risker (Samonas och Coss, 2014). Qadir och Quadri (2016) nämner även att den uppdaterade CIA triaden också fungerar bättre i praktiken, då de menar att det främst måste finnas tillgänglighet inom datahantering, för att sedan kunna arbeta med konfidentialiteten samt integriteten. Detta visar sig också på kommunerna, då det inte går att tillämpa de två nämnda aspekterna utan att veta vilka som skall ha tillgång till informationen, i kommunens fall medarbetarna.

6.4 Riskhantering

6.4.1 Informationssäkerhetsrisker

En aspekt i arbetet med en informationssäker organisation är att kunna hantera de risker som verksamheten kan utsättas för, i förhållande till den information som förekommer. Samtliga av de tillfrågade informanterna menar att just hanteringen av information är det som bidrar med högst risk inom kommunens arbete. Kane och Koppel (2013) menar att risk förekommer i flera former inom informationssäkerhet, däribland externa hot såsom hackare och virus, men också hos de anställda som hanterar informationen. Detta stämmer väl in på de två stora kommunerna som vi undersökt, där båda menar att den största risken finns hos användarna. I kommunens fall är detta ofta de medarbetare som verkar inom kommunen.

Informanten för SK1 menar att det inte finns tillräckligt med kunskap hos de användare som arbetar med information inom kommunen. Detta gör då att risker uppkommer i arbetet då användarna inte vet hur de ska hantera de olika typerna av information och data som förekommer i kommunens arbete. Liknande resonemang visar sig i SK2, där informanten också belyser att det saknas kunskap i hanteringen av information. Detta kan bero på att de stora kommunerna har fler anställda och fler som använder den information som existerar, och att inte tillräcklig utbildning, roller samt verktyg för hanteringen finns att tillgå i arbetet med kommunens informationssäkerhet. Som båda kommuner uttryckte i resultatet angående roller och ansvar, så visade båda informanter att det finns en avsaknad av utbildning inom kommunerna samt att det inte finns tillräckligt med uppföljning i det arbetet. Detta kan tyda på varför de båda kommunerna menar att riskerna ligger hos användarna.

Beträffande den mellanstora kommunen, , MK1, så menar informanten att det inte finns tillräckligt med resurser att tillgå och detta bildar i sin tur risker inom kommunen. Andrej Volchkov (2019) menar att riskhantering bör ingå i en organisations fullständiga regelverk angående informationssäkerhet. Om inte det finns tillräckligt med resurser att tillgå för att färdigställa sådana regelverk, kan risker lätt uppkomma. De mindre kommunerna som undersökts menar också att hanteringen av information är den primära risken inom informationssäkerheten på kommunen. LK1 uttrycker att risker uppkommer i deras arbete med Office 365 och hur de sparar information. Informanten uttrycker att det finns risker när man sparar information på flertal ställen. Detta belyses även i teorin, där det framkommer att man primärt måste kunna identifiera den aktuella risken för att sedan kunna hantera den. Detta är något som kan bli komplicerat då information är sparad på diverse platser och är svår att spåra. Peltier (2007) belyser att man inte kan reducera risk innan man identifierat den. Det kan därför argumenteras för att kommunen behöver ett mer utvecklat regelverk och system för hur de sparar information. Om de risker som finns i organisationen inträffar, riskerar det att både skada allmänheten samt verksamheten. Detta är något som LK2 uttrycker. Informanten menar att hanteringen av informationen leder till minskat förtroende för kommuner, vilket i sin tur kan skada ett flertal delar av samhället. Det är därför oerhört viktigt att kommunerna har ett satt regelverk för hur de skall identifiera, hantera samt reducera risk, då de har en markant roll i samhället gällande informationshantering, personlig såväl som allmän.

6.4.2 ISO 27000

Samtliga fem kommuner redogjorde för att de på ett eller annat sätt arbetar eller försöker arbeta utifrån ISO certifieringar och då 27 000 serien. Samtidigt ser det olika ut för kommunerna kring hur långt ISO certifieringarna är integrerade i verksamheten. För SK2 har man i en strategi för informationssäkerhet beslutat att ISO 27 000 serien ska användas och SK2 arbetar med att bli just certifieringsbara. Målet för SK2 att bli certifieringsbara finns kvar men arbetet stannade upp på grund av corona pandemin. För SK1 så hänvisar man till ISO i sitt arbete med informationssäkerhet och benämner att detta exempelvis görs i hanteringen av datahallar. De mindre kommunerna , MK1, LK1 samt LK2 arbetar också utifrån ISO samtidigt som LK1 benämner att det inte görs tillräckligt. LK2 berättar att man försöker hänvisa till ISO men säger också att kommunen inte arbetar med att bli certifierade. Det är tydligt att samtliga fem kommuner försöker jobba utifrån de klassificeringar och krav som ställs utifrån ISO serien samtidigt som ingen av dem söker efter att bli specifikt certifierade. Det är tydligt att ISO:s ramverk kan behandlas av kommunerna utan att de sätter upp målsättningen att bli just certifierade. SK2 berättar just att de har en målsättning att bli certifieringsbara men inte att de ska certifiera sig. Såsom nämns i teorin så kan en ISO certifiering vara en just bekräftelse för att en organisation hanterar sina risker och uppfyller säkerhetskrav (Diestrer,2013). Certifieringar som för tillfället inte finns i någon av de kommuner som är med i studien. Om än försöker samtliga fem kommuner arbeta utifrån ramverken trots att ingen av dem har ett konkret mål att på något sätt certifiera sig utifrån 27 000 serien.

6.5 Policies utifrån de fyra aspekterna

Utifrån den rapport som MSB (Myndigheten för samhällsskydd och beredskap) genomförde år 2015, visade det sig att i 67 av 230 undersökta kommuner inte fanns en typ av information security policy eller ett styrande dokument att förhålla sig till (MSB, 2015). Det var alltså vid tidpunkten för denna undersökning drygt en fjärdedel av Sveriges kommuner som inte hade

ett sådant regelverk att arbeta utifrån. I de fem kommuner som vi i denna studie undersökt, visar det sig att fyra av fem påstår sig ha en informationssäkerhetspolicy. Den sista av de fem, LK2, menar att det inte finns ett övergripande styrande dokument, utan snarare specifika styrande dokument för de diverse verksamheterna och områdena inom kommunen.

MSB nämner vidare i samma rapport att en policy för informationssäkerhet skall behandla hantering av risk, vilka som ansvarar för vilka områden samt att förstå vilken information som behöver hanteras. Våra fyra valda aspekter inom denna studie korresponderar med de som MSB nämner som essentiella i arbetet med policies, och då dessa utav resultatet samt teorin visat sig vara relevanta för kommunerna i dess arbete med informationssäkerhet, kan man konstatera att de också är relevanta i just arbetet med ett styrande dokument eller policies. Det kan därför anses vara troligt att dessa fyra aspekter bör behandlas i kommunernas styrande dokument eller policies.

6.6 Sammanfattning av diskussion

I diskussionen ovan har vi analyserat samt undersökt hur de fem diverse kommunerna i vår studie förhåller sig till de fyra aspekter vi ämnat att undersöka. Vi kan först av allt konstatera att fyra utav fem kommuner arbetar med en policy som skall funktionera som grund i deras arbete med informationssäkerhet. Samtliga kommuner behandlar också de fyra aspekterna styrning, roller och ansvar, data samt riskhantering i sitt arbete, men till olika grader och utvecklingsnivåer. Beträffande styrningen så visar resultatet att åtminstone en stor kommun uttrycker att styrningen utgår från ledningen, medan de mindre syftar till deras informationssamordnare som en betydande del i det arbetet. Vidare nämner också SK2 att de inom kommunen implementerat ett större nätverk för kommunikation, något som inte visar sig hos de mindre. Detta tyder på att de större kommunerna har en mer centraliserad styrning som utgår från ledningen och att detta sedan förmedlas ned genom organisationen. Detta till skillnad från de mindre där samordnaren har en mycket betydande roll för hela kommunens informationssäkerhet.

Sett till roller och ansvar så visar de större kommunerna på ett bredare spektrum av roller. Detta tyder på att de större kommunerna har fler personer som ansvarar för informationssäkerheten, vilket korresponderar med deras övergripande storlek i jämförelse med de mindre. Beträffande utbildning så hävdar samtliga kommuner att det är något som måste utvecklas. Utbildning måste ses som en grund i arbetet med policies då det är relevant för det övergripande arbetet kring informationssäkerhet. Att samtliga kommuner inte har tillräckligt med utbildning för anställda kan vara svaret på varför resultatet även visar att det saknas kunskap inom de andra aspekterna.

Beträffande datahantering så menar kommunerna att det sker en klassificering av information, men även detta på olika vis. Att de inte uttrycker likvärdiga svar kan tyda på flera skillnader i kunskap men även resurser. Utifrån klassificeringen kan man också härleda CIA triaden. De olika graderna av klassificering kan tyda på att kommunerna skiljer sig i förhållande till begreppen konfidentialitet, integritet samt tillgänglighet. Det finns flertal exempel bortsett från de kommuner vi undersökt, där kommuner spridit, manipulerat samt av misstag extraherat fel information, vilket tyder på att CIA inte behandlas så pass mycket som det bör inom de

Svenska kommunerna. I behandlandet av data så uppkommer även risk. Det är därför positivt att samtliga kommuner menar att det förhåller sig till standarder såsom ISO, där t. ex SK2 uttryckte att standarden ISO 27000 ingår i kommunens övergripande strategi för informationssäkerhet. Något att notera är att även om de alla använde sig utav ISO, så uttryckte ingen att de var certifierade. Några kommuner menar att de arbetar mot att bli "certifieringsbara" men att arbetet inte kommit längre. Detta tyder också på att arbetet med informationssäkerhet och dess policies måste fortsätta att utvecklas genom samtliga kommuner.

7 Slutsats

Informationssäkerhet Policies eller styrande dokument är det huvudsakliga styrmedlet som är användbart för organisationer att arbeta informationssäkert med sina informationstillgångar. Det är dessa policies som styr hur en organisation jobbar informationssäkert och därmed redogör för hur en organisation hanterar risk, vilka roller som finns samt vilken information som behöver hanteras, likt vad MSB framfört i sin rapport presenterad i inledningen. I relation till den avsaknad som år 2015 fanns av Information Security Policies i Sveriges kommuner tillsammans med den viktiga roll som de har i samhället att hantera viktiga informationstillgångar, har denna uppsats ämnat till att undersöka hur svenska kommuner förhåller sig till fyra aspekter av Information Security Policies.

De fem kommunerna som undersökts skiljer sig åt i både invånarantal och geografisk position. Av resultatet visat så skiljer sig kommunerna även åt i mängden resurser som kan läggas på arbetet med informationssäkerhet. Samtidigt skiljer sig inte vikten av att hålla sin information säker, samtliga kommuner hanterar information som behöver hållas just säker och berättar att informationssäkerhet är en betydande del i kommunens arbete. Däremot skiljs den känsliga datan åt i mängd och kvantitet, de större kommunerna har mer information att hantera och kan lägga fler resurser på säkerheten än de små.

Studien vi har genomfört på fem kommuner har visat att nästan samtliga, fyra av fem, påstår att de inom verksamheten arbetar utifrån ett styrande dokument eller policy. Undersökningen visar att de fyra aspekterna styrning, roller och ansvar, data samt riskhantering alla har en viktig del i kommunens arbete med informationssäkerhet. Utöver detta visar studien även att dessa fyra aspekter alla är relevanta i relation till varandra. Det kan inte skapas en utbildning utan att ha en tydlig styrning kring kommunens informationsarbete. Det kan inte heller existera korrekt datahantering i organisationen utan att användarna inom verksamheten är utbildade inom ämnet samt att det finns tydliga roller. Slutligen så kan inte hanteringen av risk behandlas om inte organisationen i fråga är medvetna om informationen och den data man hanterar. Det kan därför konstateras att de fyra aspekter som vi i denna uppsats har belyst, bör ingå i kommunernas arbete med policies för informationssäkerhet.

Slutligen, så kan det konstateras att de fyra aspekterna som denna studie undersökt alla är relevanta i upprättandet av policies för informationssäkerhet, och att dessa således bör behandlas i arbetet med styrande dokument för kommunen. Informationen som kommunerna behandlar är i många fall känslig, och oavsett hur pass stor kommunen är och vilka tillgångar som finns att tillgå, så finns det i samtliga kommuner potential att utveckla sitt arbete med informationssäkerhet. Detta arbete grundar sig i att ha en enhetlig och övergripande policy för kommunen att förhålla sig till. Detta gör att organisationen får en stadig grund att arbeta utifrån, vilket är ett krav för att informationssäkerhetsarbetet skall kunna utvecklas genom kommunen och alla dess inbördes verksamheter.

7.1 Vidare forskning

I denna studie har vi undersökt huruvida svenska kommuner förhåller sig till fyra aspekter av policies inom informationssäkerhet. Vi har valt att avgränsa oss till dessa fyra aspekter. Det kan således vara av intresse att undersöka flera betydande faktorer för arbetet med policies.

8 Bilagor

8.1 Frågeformulär

Övergripande frågor

Vad har du för roll inom kommunen och hur samspelar den med informationssäkerhet?

Finns det något/några övergripande styrande dokument för hur kommunen hanterar informationssäkerhet i nuläget, s.k policies?

Om nej:

har ni något liknande?

När blev denna senast uppdaterad?

Hur länge har ni inom kommunen arbetat med informationssäkerhet?

Anser du att informationssäkerhet är en betydande del i kommunens arbete?

Styrning

Finns det inom kommunen bestämmelser gällande beslutsfattande och styrning för informationssäkerhet?

Om ja:

Finns det någon strategi som detta beslutsfattande utgår från?

Hur sker kommunikationen inom kommunen gällande informationssäkerhet?

Om nej:

Tror du att ett gemensam styrning och beslutsfattande är något som kommunen kan ha användning för?

Roller & Ansvar

Hur ser ansvars och rollfördelning ut inom kommunen gällande informationssäkerhet?

Finns det satta rollansvar som den enskilde anställde ska följa?

Hur ser arbetet med utbildning ut för anställda inom kommunen gällande informationssäkerhet?

Data & Riskhantering

Som kommun ansvarar ni för mycket information och data, vilka risker ser ni med hanteringen av sådan information

Arbetar ni med att klassificera den data ni hanterar?

Hur identifierar ni de aktuella riskerna som finns?

Har kommunen bestämmelser kring riskerna och hur man motverkar dem?

Använder sig kommunerna av standarder såsom ISO i arbetet med informationssäkerhet?

8.2 Transkriberingar

8.2.1 Transkribering SK1

1 Kommun SK1.

2 Informant: Anonym.

3 Intervjuare: Viktor Fresk.

4 Yrkestitel: IT-säkerhetsansvarig.

5 Datum: 10 maj 2021, Kl 10:07

6

7 Intervjuledare= X

8 Informant= Y

9

10 Informanten godkänner att samtalet spelas in.

11

12 X- Vad har du för roll inom kommunen och hur den samspelar med

13 informationssäkerhet?

14

15 Y- Precis, min roll är ju IT- Säkerhetsansvarig är jag. Så att egentligen har vi ju andra

16 roller som hanterar informationssäkerhet, vi har en hel avdelning där det finns en

17 informationssäkerhetssamordnarroll. Och det är dom som också ansvarar för de här
18 dokumenten som jag tror att ni är ute efter lite grann.
19
20 X- Precis, det leder väl vidare till nästa fråga då: Finns det något övergripande
21 styrande dokument för hur kommunen hanterar informationsäkerhet i nuläget?
22
23 Y- Ja, det gör det.
24
25 X- Och när blev den senast uppdaterad eller reviderad?
26
27 Y- Jag har för mig att det var förra året, reviderades den.
28
29 X. Och hur länge har ni i kommunen arbetat med informationssäkerhet?
30
31 Y- Jag skulle vilja påstå att det var lite i samband med GDPR införandet egentligen, i
32 en större utsträckning iallafall, att man tillsatte just den här
33 informationssäkerhetssamordnare rollen dåråå. Så strax efter 2018 skulle jag säga då.
34
35 X- Okej. Och slutligen då på övergripande frågor, anser du att
36 informationsäkerheten är en betydande del i kommunens arbete idag?
37
38 Y- Det är det absolut.
39
40 X- Kanon.
41
42 Y- Det är det.

43

44 X- Okej om vi går in på lite mer styrnings delen av allting så vill jag fråga om
45 det inom kommunen finns bestämmelser gällande beslutsfattande och hur
46 styrningen sker genom kommunen för informationssäkerhet?

47

48 Y. Beslutsfattande ligger ju egentligen på ledningsgruppsnivå, gör det ju, absolut,
49 slutgiltiga beslutsfattandet. Sen har jag för mig att den här informationssäkerhets
50 samordnaren rollen har en hel del att kunna besluta om också.

51

52 X- Finns det någon strategi som detta beslutsfattande utgår ifrån?

53

54 Y- Vi har nåt som kallas digitalisering men det har inte riktigt med det att göra
55 egentligen. Strategi för digitalisering men hur mycket informationssäkerhet som
56 kommer in där det vet jag faktiskt inte.

57

58 X- Jag förstår, okej. Om vi går in på lite mer roller och ansvar då. Finns det
59 några satta rollansvar som den enskilde anställde ska följa. Alltså att det finns
60 ett något typ av dokument som representerar den enskilde anställdes
61 skyldigheter?

62

63 Y- Ja det är ju det här, vad hette det, riktlinjer eller programmet heter det väl numera
64 som styr det. Så det är egentligen samma dokument som vi pratade om tidigare.

65

66 X- Mm och hur ser arbetet med utbildning ut för anställda inom kommunen
67 gällande informationssäkerhet? Finns det något?

68

69 Y-Mm det är en mycket intressant fråga. Det är ju sånt här som jag i min roll och

70 även andra då roller har efterfrågat att vi ska ha utbildningar men man är inte så
71 mycket för det på en ledningsnivå om man säger så.
72
73 X- Vad för typ av utbildning?
74
75 Y- Ja som vi skulle vilja genomföra?
76
77 X- Ja.
78
79 Y- Ja vi skulle ju vilja genomföra någon form av E-learning och sådana saker där du
80 egentligen gör en form av proof of concept, eller nej vad heter det proof of conduct
81 heter det. Som egentligen tillexempel som nyanställd får göra prov eller genomgång
82 och svara på lite frågor och sen utifrån det bli godkänd då.
83
84 X- Mm.
85
86 Y- Så det är det vi har eftersträvat några stycken. Men vi får inte så mycket gehör för
87 det tyvärr.
88
89 X- Vad tror du det beror på då?
90
91 Y- Ja det är en jättebra fråga faktiskt. Jag tycker inte man riktigt är vaken att man vill
92 införa det och på andra företag brukar det vara en HR avdelning som liksom styr sånt
93 där men dom har inte riktigt nappat på det här ännu.
94
95 X- Okej jag förstår. Om vi går in på lite det här sista, data och riskhanteringen.

96 Som kommun så ansvarar ni för väldigt mycket information såväl personlig

97 som allmän. Vilka risker ser ni med hanteringen av den informationen?

98

99 Y- Riskerna är då tycker jag på användarnivå att man inte har kunskapen helt enkelt.

100 Sen är det ju även att man behöver en klassning av dokument för att förstå vad det är

101 för dokument man hanterar.

102

103 X- Jag förstår det leder nog in på min nästa fråga här hur ni arbetar med att

104 klassificera den datan ni hanterar.

105

106 Y- Mm precis. Det är just det här med klassningen som vi kommer in på som du

107 säger.

108

109 X- Aa jag förstår men hur fungerar det rent praktiskt när man klassificerar

110 data?

111

112 Y- Det kan man göra både manuellt och via vissa program som klassar ett dokument

113 vad det är för någonting om det är sekretessbelagt eller om det är en allmän handling

114 och såna saker. Så att det här skulle man ju som kommun göra i en mycket större

115 utsträckning och jag tror att det inte är jättevanligt heller tyvärr.

116

117

118

119

120 X- Okej och du har svarat på nog rätt många frågor här som vi hade nedskrivna

121 här men specifika bestämmelser kring riskerna och hur man motverkar dom.

122 Har ni någon plan för när väl en risk uppkommer och hur ni ska hantera det

123 beroende på vilken risk det är?

124

125 Y- Tänker du på incidenter nu eller?

126

127 X- Aa lite mer så.

128

129 Y-Aa det finns ju en, vad heter det, personuppgiftsincident hantering inom

130 kommunen. Där bland annat vårt dataskyddsombud blir inblandad helt enkelt.

131

132 X- Jag förstår.

133

134 X- Okej tack så jättemycket, men slutligen då, använder sig kommunerna av

135 standarder såsom ISO?

136

137 Y- Aa man försöker hänvisa till det, ISO-27000, och vissa fall när det gäller datahallar

138 och sånt där och man hänvisar till standarder kring det, absolut det försöker vi göra.

139

140 X- Bra. Ja det var alla frågor vi hade.

141

142 Samtalet avslutas.

143

8.2.2 Transkribering SK2

1 Kommun: SK2.

2 Informant: Anonym.

3 Intervjuare: Martin Petrelius.

4 Yrkestitel: Biträdande informationssäkerhetsansvarig.

5 Datum: 12 maj 2021, kl 10:00

6

7 Intervjuledare= X

8 Informant= Y

9

10 Informanten godkänner att samtalet spelas in.

11

12 X: Vad har du för roll inom kommunen och hur samspelar den med

13 informationssäkerhet?

14

15 Y: Min roll är biträdande informationssäkerhetsansvarig. Så jag jobbar ju med

16 informationssäkerhet till 100%, i kommunkoncernen kan vi ju säga, för det är ju även

17 över bolagen till viss del, de kommunala bolagen.

18

19 X: Finns det något eller några övergripande styrande dokument för hur

20 kommunen hanterar informationssäkerhet i nuläget?

21

22 Y: Ja vi tog ju en ny strategi, beslutade om en ny strategi för ett år sedan drygt, som

23 heter "strategi för trygghet och säkerhet i kommunen", och där i finns ett avsnitt om

24 informationssäkerhet och dataskydd.

25

26 X: Så det hanterar policies i informationssäkerhet, dem dokumenten?

27

28 Y: Ja, vi har inga policies utan hos oss heter det "strategi".

29

X: När blev denna senast uppdaterad?

Y: Den är beslutad för ett år sedan drygt, 2020-01-27 och den ligger på sundsvall.se om ni vill ta del av den.

X: Hur länge har ni inom kommunen arbetat med informationssäkerhet?

Y: Ja det är svårt att säga, det är väl ett par år som man liksom har pratat utifrån informationssäkerhet mer. Tidigare har det väl legat lite mer i bakgrunden, men det har funnits med en längre tid, men det har inte varit fokus på samma sätt som det har blivit de senaste åren.

X: Anser du att informationssäkerhet är en betydande del i kommunens arbete, och varför är de det?

Y: Ja det tycker jag nog utifrån att, vi har ju en väldigt stor fokus på digitaliseringen här i kommunen och min roll har man valt att placera i avdelningen för digitalisering och innovation, och det är ju utifrån att om man ska digitalisera på ett bra sätt så är informationssäkerheten en väldigt viktig del att få med. Utifrån det så känns det som vi har ett bra fokus på informationssäkerhet, bättre skulle jag säga än om min roll låg på en traditionell säkerhetsavdelning eller på IT-avdelningen.

X: Finns det specifika bestämmelser när det gäller beslutsfattande och vilken riktning kommunen skall gå i sitt arbete med informationssäkerhet?

Y: Ja i den här strategin som blev beslutad för ett år sedan så beslutade vi också att vi skulle arbeta utifrån ISO 27 000 och att vi skulle bli certifieringsbara, vi ska inte certifiera oss men vi ska bli certifieringsbara, och utifrån det arbetet så håller vi på för fullt att ta fram alla typer av riktlinjer och vi ska ta fram det här ledningens genomgång så du får en årscykel i hur du arbetar systematiskt med informationssäkerhet. Så vi är liksom på gång och jobbar med den processen, det är inte helt klart än hur alla delar då.

X: Finns det någon specifik strategi som beslutsfattandet utgår ifrån, men du var ju lite inne på det här innan med den strategin som ni nämnde.

Y: Ja, precis.

X: Hur sker kommunikationen mellan dem här olika delarna, du nämnde att du sitter på innovation och digitaliseringsdelen av kommunen, hur sker kommunikationen mellan alla delar beträffande informationssäkerhet?

Y: Ja vi har ju ett nätverk i kommunen där vi har representanter från alla förvaltningar och bolag som egentligen grundar sig i PUL-nätverk på personuppgiftslagens tid när vi hade PUL-ombud, och då har vi gjort om det nätverket så idag kallar vi det för informationssäkerhets och dataskyddsnätverket. Så där sitter både människor som jobbar med informationssäkerhet och dataskydd av personuppgifter ut i organisationen och då har vi träffar en gång i månaden där vi försöker förmedla information, ta till oss vad som händer ute i verksamheterna och jobbar fram olika e-tjänster, rutiner och utbildningar b.la då. För att få ut det i verksamheterna.

X: Hur ser ansvars och rollfördelning ut genom kommunen gällande

82 informationssäkerhet?

83

84 Y: Ja, det var en bra fråga. I den här strategin, kopplat till strategin så finns det något
85 som heter verksamhetsplan och där har vi beskrivit de olika rollerna inom egentligen
86 alla säkerhetsområden, men det finns ju även då för informationssäkerhet och
87 dataskydd, och då är det ju kommunfullmäktige som fastställer den här strategin för
88 den ska ju beslutas politiskt, och sen är det ju varje nämnd och styrelse som
89 ansvarar för att strategin i sin tur ska efterlevas i sin förvaltning eller bolag. Sen under
90 det så kommer kommundirektör, så har du trygghets och säkerhetschefen som har
91 ett övergripande ansvar. Du har förvaltningsdirektören och VD som har ansvar för
92 informationen och är ju liksom informationsägare, och har ju då också ett ansvar för
93 informationssäkerheten. Sen är det ju informationssäkerhetsansvarig som är samma
94 person som också är IT-direktör och så är det jag då som är biträdande, sen har du
95 ju IT-säkerhetsansvarig, du har dataskyddsombud och sen i verksamheterna så har
96 du informationssäkerhetssamordnare, som ska liksom stötta verksamheterna och
97 göra rätt.

98

99 X: Inom de enskilda verksamheterna?

100

101 Y: Ja, för inom förvaltningen av bolagen, och det är ju dem som är med i det här
102 nätverket som jag pratade om, men det är inte samma typ som en CISO, för ofta så
103 kan det ju, många kallar det ju för informationssäkerhetssamordnare för den
104 övergripande rollen, men det här mer människor som har det vid av sitt ordinarie
105 arbete om man säger så. En del av sin tjänst. Och dataskyddssamordnare som är
106 också dem som är med i det här nätverket. Sen har du ju informationsägare,
107 informationsförvaltare där har vi inte riktigt fått dem rollerna etablerade än, utan det

jobbar vi med i.o.m det här ISO införandet, och så systemägare, systemförvaltare, systemadministratör och sådana typer av roller finns ju också då.

X: Hur ser med utbildning ut för anställda inom kommunen gällande informationssäkerhet?

Y: Ja, vi har tagit fram en del utbildningar både som att vi haft i föreläsningsform, vi har haft någon, vi har byggt en e-tjänst med utbildningar, vi ska använda oss av DISA, som är MSBs utbildning i informationssäkerhet. Vi har inte haft någon jättebra uppföljning utifrån att vi inte har haft ett bra system där vi kunnat följa upp utbildningarna, men det kommer, det är på väg in i dagarna faktiskt. Så vi skall kunna ha en bättre uppföljning och likväl se till att nyanställda och nya roller ska kunna få utbildningar som kommer vara obligatoriska. Det håller vi på att bygga upp.

X: Som kommun så ansvarar ni för väldigt mycket information och data, såväl personlig som allmän, vilka risker ser du med hanteringen av sådan data och information inom kommunen?

Y: Ja den största risken nästan, om man ska ärlig tänkte jag säga, är ju medarbetarna utifrån kompetens helt enkelt.

X: Att det inte finns tillräckligt med kunskap?

Y: Ja.

X: Arbetar ni med att klassificera den data ni hanterar?

Y: Ja, det gör vi ju också. Det finns ju mycket olika lagar som vi måste efterleva i kommunen och en stor del i klassificeringen är ju i informationshanteringsplanen utifrån arkivlagen. Så det är ju ett jättestort arbete och sen ofta ligger ju den här informationshanteringsplanen i stora, tunga word-dokument. Så du gör ju det där jobbet en gång och sen använder du inte resultatet i din dagliga verksamhet, för det går ju inte att söka i ett dokument som är 140 sidor långt på ett smart sätt. Sen gör vi klassificering också av system, så att vi skall kunna veta vilken typ av information som är okej och lägga i just det systemet. Så vi gör ju både klassificering av information och av system då. Men det är ett jättestort jobb och det är jättemycket kvar att göra och det behöver ju göras liksom och utvärderas varje år egentligen, att ligger vi kvar på den här nivån? Är det något som har förändrats och så vidare.

X: Hur arbetar ni med ISO 27000, hur hanterar ni den helt enkelt?

Y: Ja men just nu så är vi ju inne i den här perioden eftersom vi inte hållit på med det här så länge, så är vi ju inne i den här perioden och försöker få fram dem här riktlinjerna då som hör till 27000, och det är ju ganska mycket riktlinjer. Sedan hände det ju såklart, vi fick ju prioritera om lite utifrån pandemin då och fokusera på att ta fram styrande dokument och hjälp med distansarbete och sådana delar. Sedan jobbar vi ju med utbildningsinsatser men som sagt det är ju, vi ska ju få in ett system så att vi skall kunna ha bättre uppföljning där, och sen håller vi ju på så att vi ska ta fram en "ledningens genomgång" för första gången i höst då förhoppningsvis då, som skall upp till kommunstyrelsen, till nämnden.

X: Det var alla frågor vi hade. Tack för dina svar.

161 Y: Ja men vad bra.

162

163 Samtalet avslutas.

164

8.2.3 Transkribering MK1

1 Kommun: MK1

2 Informant: Anonym.

3 Intervjuare: Viktor Fresk.

4 Yrkestitel: Informationssäkerhetssamordnare.

5 Datum: 12 maj 2021, kl 9:00

6

7 Intervjuledare= X

8 Informant= Y

9

10 Informanten godkänner att samtalet spelas in.

11

12 X-Då kan vi börja inleda med att vi har fått godkännande av Y att spela in samt

13 att vi har lovat att radera materialet när uppsatsen är färdigställd. Och att det

14 kommer vara helt anonymt. Då kör vi igång med första frågan då. Vad har du

15 för roll inom kommunen och hur samspelar den med informationssäkerhet?

16

17 Y- Min roll är informationssäkerhetssamordnare, det betyder då i våran kommun att

18 jag har det strategiska ansvaret inom kommunen för informationssäkerhet. Jag

19 jobbar då på heltid sedan 3 år tillbaka. Och innan det hade dom väl inte någon riktig

20 utpekad på heltid utan det var en som hade det på sidan av.

21

22 X-Tack.

23

24 X-Finns det något eller några övergripande styrande dokument för hur

25 kommunen hanterar informationssäkerhet i nuläget, s.k policies?

26

27 Y- Jo vi har några styrande dokument. Policies är ju den övergripande så den har vi.

28 Vi har också några andra styrande dokument tillexempel hur informationssäkerhets

29 klassningen ska se ut inom kommunen. Det finns ju ingen nationell sådan. Vi har

30 även hur vi ska hantera, hur vi ska göra våran informationssäkerhetsklassning. Vi har

31 även rutin på hur vi ska göra riskanalyser. Vi har även ett styrande dokument vad

32 förvaltningarna ska tänka på när det gäller skyddade personuppgifter som är väldigt

33 väldigt skyddsvärt. Bland annat. Så vi har några styrande dokument.

34

35 X- Och en följd fråga då, när blev denne senast uppdaterad?

36

37 Y-Den blev skapad och beslutad i december 2018.

38

39 X- Och sen så en lite övergripande fråga, anser du att informationssäkerhet är

40 en betydande del i kommunens arbete?

41

42 Y- Ja det var en svår fråga. Den är ju superviktig i kommunens arbete men sen så

43 kanske man inte har lyckats anamma det riktigt än. Men det börjar smått komma

44 igång.

45

46 X- Kanon, och som vi nämnde lite kort där innan så har vi dom fyra aspekterna

47 som vi nämnde innan som vi utgår ifrån. Jag tänkte börja lite med styrningen

48 helt enkelt och ledningen av informationssäkerhet inom kommunen. Och finns

det då inom kommunen särskilda bestämmelser gällande hur beslutsfattandet och styrningen för informationssäkerhet ska gå till.

Y- inte just nu.

X- Inte just nu?

Y- Inte just nu nä och det är en stor brist men inte just nu.

X- Tror du det är någonting som kommunen skulle kunna ha användning för i senare tillfällen?

Y- Ja. Asså styrningen det finns ju på det sättet att jag är den strategiska, och dom kommunövergripande styrdokument jag skapar gäller ju för hela kommunen så på det sättet ja. Men om du menar mandat och beslutsgångar så är det i mångt och mycket förvaltningarna själva som styr upp. Men jag börjar märka att dom tar mer och mer råd av mig iallafall. Men inget såhär dokumenterat.

X- Och hur ser kommunikationen ut mellan dom här förvaltningarna? Som hanterar informationssäkerhet på sina vardera aspekter. Är det du som sitter i styrningen där som informationssamordnare?

Y-Ja dom kontaktar mig om jag har tur eller om dom har tur. För det är ju deras information.

X- Ja jag förstår.

Y- Och dom börjar få in det, vissa av dom. Få in att kontakta mig så fort det är någonting som dom funderar över. Men det finns ju ingen sådan här process för det än. Naturligtvis den förvaltningen som jobbar med personuppgifter med vård och sånt dom har ju det lite det i ryggmärgen men det finns ändå en hel del att jobba med där också.

X- Mm okej. Då går vi in lite på roller och ansvar då. Hur ser ansvars och rollfördelingen ut inom kommunen gällande informationssäkerhet?

Y- Ja det är ju förvaltningscheferna som är informationsägare. Dom har det övergripande ansvaret. Dom gör ju ingenting operativt mer än att dom tar beslut och får information. Jag är ju den strategiska som ska stötta då i min roll. Och ge styrande dokument som gäller för hela kommunen. Sen är ju tanken att förvaltningarna ska ha sina handläggare för det här området. Som är duktiga på att få igång det systematiska arbetet och utbilda och ja. Jobba med informationssäkerhet och utbilda.

X-Ja det leder in på min nästa fråga. Och den är just. Hur ser arbetet med utbildning ut för anställda inom kommunen för informationssäkerhet, finns det någon utbildning för de anställda?

Y- Ja det finns en utbildning som gjorts som är kommunövergripande eller egentligen finns det två utbildningar. Som jag har varit drivande i. En är ju en sån här kommunövergripande när det gäller användare. Hur dom ska hantera informationen i sin vardag och vad som ska tänka på. Och sen så finns det en utbildning som

arbetsrättsjuristen har gjort i uppdrag av mig och det handlar om sekretess som vi inte riktigt har implementerat i hela organisationen än men på vissa delar. Min vision är ju att hela den utbildningen ska genomföras av alla oavsett om man jobbar med sekretess eller inte för man kan ju faktiskt komma i kontakt med det ändå. Så det finns två utbildningar inom det här området just nu.

X- Mm tack. Och du kom in lite på det här, du guidade oss igenom det här själv nästan. Men lite mer data och riskhantering. Som kommun så ansvarar ni för väldigt mycket information och data såväl som personlig som allmän. Vilka risker tror du finns med hantering av sån här känslig data?

Y- Asså vilka risker det finns?

X-Ja ganska övergripande fråga jag förstår. Sett från kommunens perspektiv.

Y- Ja men om jag ska generellt utan att prata om våran kommun så kan jag generellt skönja att kommuner, jag har ju jobbat på statlig myndighet att kommuner har inte nog med resurser för att jobba aktivt med riskfrågorna ur alla aspekter. Och då tänker jag mig även aspekten utifrån upphandlandet av nya system. Att man hanterar i vardagen eller att man hittar nya hot, Cybersäkerhet hot till exempel. Asså resursfrågan tror jag är den största risken i alla kommuner. Statliga verk dom har ju

ett helt annat krav från regeringen att att jobba med informationssäkerhet. Och därigenom så lägger dom ju budget på det också. Så det är två helt olika världar, tyvärr. Det är som att jag hade önskat att regeringen ställde samma höga krav på kommunerna för att kommunerna hanterar väldigt väldigt mycket samhällsviktiga tjänster nära människorna. Men så att så ser det inte ut idag. Jag skulle säga att den största risken är personal, alltså resursfrågan i kommunen.

X- Jag förstår. Du nämnde det lite innan här att med sekretessbelagd information och sådant. Arbetar ni med att klassificera den data ni hanterar?

Y- Vi arbetar högt och lågt. Inte systematiskt än men dom som har väldigt skyddsvärdig information dom har ju gjort det innan jag kom in även om det finns hela tiden förbättringar att göra.

X- Och använder sig kommunerna någonting av standarder såsom ISO till exempel?

Y- Jag jobbar med ISO- 27000.

X- Hela den serien?

Y- Mm. Ja.

X- Ja det var det vi hade.

Konversationen avslutas.

155

8.2.4 Transkribering LK1

1 Kommun: LK1

2 Informant: Anonym.

3 Intervjuare: Viktor Fresk.

4 Yrkestitel: Informationssäkerhetssamordnare

5 Datum: 11 maj 2021, kl 10:00

6

7 Intervjuledare= X

8 Informant= Y

9

10 Informanten godkänner att samtalet spelas in.

11

12 X-Vi skriver då en kandidatuppsats om informationssäkerhet och fokuserar på

13 de styrande dokumenten som kommuner kan använda för

14 informationssäkerhet. Och då har vi identifierat fyra aspekter som anses

15 viktiga i ett sånt dokument och det är dels styrning och sen roller & ansvar,

16 datahantering samt riskhantering. Och dom här aspekterna kommer då med

17 bakgrund av MSB som gjorde en undersökning 2015 som var rätt vid på

18 svenska kommuner. Och just för policy arbetet hos kommuner så visade sig de

19 här fyra aspekterna verkade vara högst relevanta för att kunna starta ett

20 välgrundat styrande dokument. Så att vi tänker helt enkelt intervjua fem

21 stycken kommuner och se hur deras arbete går till. Det är därför vi har

22 kontaktat dig.

23

24 Y- Aa jag skrattar för det är rätt fascinerande, om vi bara ska ta min bakgrund i det

25 här, så ni får inte tro att ni har hamnat hos någon form av superproffs. Jag har varit

på räddningstjänsten eller kommunen i, vad blir det, 4 år. Och anledningen kan man säga, eller grunden till att jag började där är att jag skulle jobba med trygghet och säkerhet. Men kommuner som ni säkert har förstått när ni sitter med såna här arbeten är ju väldigt olika, i vissa kommuner kanske det sitter en person som gör en specifik sak, typ informationssäkerhet eller säkerhetskydd eller vad det nu kan tänkas va. Men ju mindre kommunerna är ju fler puckar får ju respektive tjänsteman ta hand om.

X- Ja jag förstår.

Y- Och den här pucken med informationssäkerhet den hamnade liksom i min ryggsäck också från jag började för några år sen. Och det va helt nytt för mig. Jag har aldrig någonsin jobbat med dom frågorna överhuvudtaget och var lite, grinig, är nog fel ord för jag hade inget val men jag tog på mig den sen har skjutit den som en stor jävla snövall framför mig så länge det bara gick. Men jag inser ju själv att det där är någonting som man måste jobba med och som hänger ihop med allt arbete som vi gör på kommun och framförallt jag som sitter med lite säkerhetsskydd, fungerar inte det ena så fungerar inte det andra. Så det är en punkt som liksom har ramlat på mig och som jag faktiskt kan tycka är ganska intressant när man läser om den. Sen ibland när jag håller på med den så är den så jävla stor att man får liksom nästan ta en paus.

X- Ja.

Y- För man reder inte ut det, för, jag vet inte hur ni, ni kommer säkert fram till det tänker jag. Men kommuner det är nog väldigt olika hur man jobbar, en del har kommit väldigt långt och vi har väl kommit kanske en liten bit, vi är inte sämst i klassen som

man brukar säga men vi är inte bäst heller.

X- Mm ja jag förstår.

Y- Men bara för att ni ska förstå ifall ni får lite flummiga svar så beror det på att jag fortfarande är i lärandefasen kan man väl säga av det här.

X- Ja jag förstår det är det som blir intressant ju. Just med att intervjua olika kommuner att det är så olika. Men får jag fråga dig om det är okej för dig att spela in det här så transkriberar vi sen och använder?

Y-Ja för jag satt och tänkte på det innan jag kopplade upp mig, vad fasen ska dom spela in för men det underlättar ju ert arbete.

X- Ja och vi håller det helt anonymt också. Så att ditt namn eller kommunens namn kommer inte vara med eller något.

Y- Nä juste och det är ingen film, för först när du sa att ni skulle intervjua mig så tänkte jag att det ska spelas in och liksom, men jag förstår det är ju ert arbete.

X- Ja det är bara material för att vi ska kunna transkribera det sen och skriva det så.

Y-Det blir nog bra.

X- Men vi kan börja med frågan, du kanske svarade lite på det, men vad har du för roll inom kommunen och hur samspelar den med informationssäkerhet.

79 Men det svarade du lite på kanske.

80

81 Y- Ja det gjorde jag ju även om det inte var frågan jag fick så. Men om vi ska börja
82 med min titel när jag presenterade vad jag jobbar med på kommunen då är det
83 trygghetsstrateg och det är ju tämligen brett. Men i den rollen så jobbar jag med
84 alltifrån brottsförebyggande, säkerhetskydd, informationssäkerhet. Så att
85 informationssäkerhetssamordnare kan jag också titulera mig. Det är ju bara titlar det
86 här det är lite fånigt. Men som informationssäkerhetsamordnare.

87

88 X- Jag förstår och sen nästa fråga, finns det något eller några övergripande
89 styrande dokument för hur kommunen hanterar informationssäkerhet i
90 nuläget?

91

92 Y- Ja det gör det. Vi har något som vi kallar för riktlinjer för informationssäkerhet. Ett
93 ganska tungt dokument får man nog säga men vi kan komma till det kanske, och sen
94 har vi ett dokument som vi kallar för policy för informationssäkerhet. Så det är väl
95 dom två grunddokumenten kan man säga. Sen är tanken och vi, om jag säger att vi
96 jobbar med det nu så ljuger jag, men tanken är att vi ska bygga upp under policies
97 och riktlinjer ska det finnas instruktioner som då ska vara lätthanterliga och
98 användbara för dom andra två dokumenten är ju inte användbara utan det är ju bara
99 en tillvävnad. Men där är vi inte riktigt än.

100

101 X-Ja okej tack. Och när blev denna senast uppdaterad?

102

103 Y- Ja du, nu ska vi se. Uppdaterad och uppdaterad. Vi jobbar ju med dom här dom är
104 ganska färska som dokument men nu ska vi se, 2017, dom måste ha varit klara 2018

sen har vi nog tittat på dom men om jag skulle säga att dom är uppdaterade det kan jag nog inte säga att dom är men säg 2018 dårå är dom ju sen.

X- Aa och sen nästa fråga tror jag att du svarade också på lite innan men anser du att informationssäkerhet är en betydande del i kommunens arbete?

Y-Det var en sån där stor fråga. Men om jag svarar hur jag tycker då så tycker jag självklart att det är en jättestor fråga. För det är oerhört viktigt att all information som hanteras på rätt sätt och att folk förstår vad det är för information man hanterar. Men jag tror tyvärr även om vi har jobbat med frågan så är det ju så att vi som jobbar med den frågeställningen tycker det är viktigt. Sen när det ska sippra ner i alla verksamheter så är man väldigt olika kunnig. Om man tillexempel tar socialtjänsten som ett exempel så är dom väldigt väldigt duktiga på att hantera sin information. För dom är vana med sånt vid sekretess och det är hemliga grejer som dom jobbar med. Så dom är väldigt duktiga med det. Men tittar vi på andra verksamheter där jag sitter tillexempel själv på räddningstjänsten så kanske vi är mindre bra. Så att informationssäkerheten den är jätteviktig men den är väldigt olika utifrån verksamheterna och vi försöker då med tanke på att vi kört lite utbildning och så att höja lägsta nivån. För att kan vi höja lägsta nivån litegrann så tror jag att det kommer att bli mycket bättre men vi har en lång väg kvar har vi.

X- Ja kanon, som vi nämnde lite innan där så har vi fyra aspekter som vi utgår ifrån med dom här styrande dokumenten som vi anser vara av vikt. Och om vi börjar då med styrningen av kommunen då för informationssäkerhet. Finns det inom kommunen bestämmande gällande beslutsfattande och styrning för vad informationssäkerhetsarbetet ska gå någonstans och hur det ska arbetas med?

Y-Ja den enkla frågan på det är ja. Sen tror jag inte att jag vill trassla in mig så mycket mer utan då kan jag ju säga såhär som hade jag kunnat skicka till er. Dom både riktlinjerna och policyerna vi har för det är ju inga konstigheter utan det är öppna dokument och där står allting med styrning och roller och ansvar i den.

X- Ja det skulle vara hjälpsamt. Men det leder vidare till nästa då finns det någon strategi som ni utgår ifrån med det här beslutsfattande arbetet? Finns det någon mall eller liknande?

Y- Ja det är också en sån där svår fråga för alltihop det blir så, när man pratar eller när jag har varit och försökt informera olika verksamheter och verksamhetschefer om just informationssäkerhet så är ju det ordet. Bara ordet. Ställer ju, alltså folk det blir ju frågetecken i huvudet på dom för folk vet inte vad det är. Så egentligen kan jag tycka att hela ordet är fel. Jag brukar dra en jämförelse med mobbning i skolan. När man pratar om mobbning. Man kan tro att man vet vad mobbning är men det vet man ju inte det finns massa saker i mobbning och det är lite samma här. För i informationssäkerhet så har vi ju allt i form av hanteringen av personuppgifter tillexempel och GDPR kommer in. Vi har då det som jag har suttit mycket med nudå. Hemliga handlingar och hantering av sån information. Vi har ju informationer som idag, ja tekniken har ju sprungit ifrån oss lite med appar och olika program och så vidare. Så att det finns nog egentligen inte någon, vad ska jag säga, det har blivit mer och mer vanligt att man ställer frågor till mig eller till vårt dataskyddsombud kring just de här frågorna och det ser jag som positivt. Sen vet jag inte om jag har bra svar. Men jag tror att medvetenheten har ökat. Så att det finns en kunskap där ute hos cheferna framförallt att jobba med frågan och att man inte bara kan köra hej vilt. Men det finns inga direkta instruktioner eller någon mall så det gör det inte. För det var väl

158 det som var frågan egentligen.

159

160 X-Mm tack om vi går vidare, om roller och ansvar.

161

162 Y-Mm.

163

164 X-Hur ser roller och ansvarsfördelningen ut inom kommunen gällande

165 informationssäkerhet?

166

167 Y- Det ska jag ju kunna egentligen känner jag men det är samma där, när ni får den
168 policyn där så står det i den, kan ni få vilka ansvar och roller. Så det är bättre att ni
169 får läsa det tänker jag. Bättre än att jag svamlar till det här nu. För det står, det finns
170 ju en rubrik jag antar att den här. För den här riktlinjen och policyn vi har den
171 skapades ju i egentligen precis när jag började och då är dom ju uppställda i ett visst
172 mönster. Och tanken från början var att det här skulle bli ett gemensamt dokument
173 för flera kommuner. Så det var väl någon, jag tror att det var någon firma som skulle
174 hjälpa oss med det här. Sen havererade det på vägen någonstans så fick varje
175 kommun ta sitt egna svar och då nu när ni pratar om styrning, roller och ansvar det
176 här då är det uppspaltat på det viset.

177

178 X- Mm.

179

180 Y- Så att om jag mailar de här till er så kan ni kika själva exakt vad det står på roller
181 och ansvar.

182

183 X- Ja men du sa innan att det fanns ett dataskyddsombud eller vad var det?

184

Y- Ja GDPR med personuppgiftshantering, den lagstiftningen är ju spännande. Jag tänkte väl nåt vid nåt tillfälle, när jag kom, när jag fick mycket såna här frågor att det kanske jag kan sätta mig in i lite men gdpr om ni har nosat på den, det måste man jobba heltid med om man ska kunna ro ut det.

X-Mm

Y-Men då är det så att i vissa kommuner och det kommer ni säkert stöta på så är informationssäkerhetssamordnaren och dataskyddsombudet samma person. Men så är det inte hos oss utan vi har ett specifikt dataskyddsombud som då ska jobba med GDPR frågor eller egentligen är hon som en polis kan man säga alltså när någon verksamhet ska hantera personuppgifter så ska man prata med henne och så ska hon komma med olika råd och stöd kring hur dom kan göra och inte kan göra. Så dataskyddsombudet jobbar ju egentligen enbart med person uppgifter kan man säga, och hur vi hanterar det. Men det krockar ju med informationssäkerheten för allting blir ju som en enda kaka egentligen när det inte är enskilda frågor så att det. Mm.

X-Tack. Och hur ser arbetet med utbildning ut för anställda inom kommunen gällande informationssäkerhet? Finns det någon utbildning kring informationssäkerhetspolicies?

Y- Ja det gör det faktiskt vi har jobbat sen, det måste ju va, 2 år tillbaka med, ja tanken var att vi skulle skapa instruktioner och att varje verksamhetschef skulle få ett arbetsområde kan man säga och vi skulle följa MSB där dom har ju olika, ja det finns någon bra film som MSB har gjort som vi skulle ha då som grund sen skulle vi låta cheferna få följa det mönstret på sin arbetsplatsträffar som va grundtanken men sen

kom Coronan och ställde till det. Och sen la vi det lite på is men då har vi istället kört nanoutbildningar i informationssäkerhet och jag vet inte om ni har hört talats om det överhuvudtaget?

X- Nej det har vi inte.

Y-Det är ju ett, ja vi köper den tjänsten men det är en man får då som medarbetare ett mail med jämna mellanrum med en kort utbildning.Den tar inte mer än en 3 / 4 minuter att genomföra. Och då ska man liksom ha tid för det oavsett hur mycket mail man har och så vidare så ska man göra den där utbildningen och så hos oss har vi kört varannan vecka har man fått ett mail om den här nanoutbildningen. Och då har vi haft, det har funnits en massa olika utbildningar, men då har vi haft en med informationssäkerhet då. Och det har varit verkligen basic. Alltifrån att man inte ska klicka på länkar till att man ska fundera på hur man sparar sin info. Så det är ganska bred utbildning men ganska basic och den tror jag har varit väldigt bra den har höjt lägstanivån men tyvärr är det ju så med alla våra medarbetare vi är ju 15 hundra ungefär, det är ju inte så många. Men det är ju ändå 15 hundra. Så är det ju kanske inte, säg, kanske 60 procent som gör utbildningen så trots att man då vet att man ska göra den så blir det ett manfall. Så alla har ju inte genomfört den. Men vi har kört en utbildning och den ska rulla ett hjul för vi har ju ett enormt. En enorm rotation på människor så att vi kör det, så har man blivit anställd nu i Januari så kommer man påbörja den i sommar och sen rullar det på så att alla liksom ska få den då så att så är planen. Utbildning har vi men det kunde också bli mycket bättre men det är en kamp där ute att få just sina frågor att bli viktiga.

X- Ja, ja. Tack.

238 Y-Så det finns.

239

240 X-Om vi går vidare lite till data och riskerna som finns med den. Och som
241 kommun så ansvarar ni för väldigt mycket information såväl som personlig och
242 allmän. Vilka risker ser du med behandligen av denna information?

243

244 Y- Ja. Det är stora frågor ska ni veta. Hur ska jag svara kort på det här. Jag känner
245 att jag blajjar för mycket. Men man kan säga såhär att vi har haft många och långa
246 diskussioner i vår lilla kommun för det ligger nämligen i Office 365 i molnet. Och då
247 har man ju i EU bestämt att man inte får spara saker som är av känslig betydelse i
248 molnet om molnet finns i USA. Så där är vi just nu och då ska man ju sätta det i
249 relation till alternativet som i vårt fall skulle va att ha en server stående i någon
250 korridor eller något rum. Och sen att man sen då ska bygga den säkerheten för hur
251 man än gör så måste man ju ha en säker hantering av informationen. Och då just nu
252 så resonerar vi så att molnet är trots allt säkrare för oss än att ha den i en server. För
253 då måste vi ju ha mängder av säkerhetsåtgärder på den informationen där. Så att
254 som det ser ut just nu ligger vi kvar i office 365 och kommer göra. Det sista jag hörde
255 nu var ju att Microsoft också inser nu att om dom ska kunna ha kvar sin kunder i
256 Europa så måste dom ha sitt moln i Europa, så det kommer förändras. Men där är ju
257 inte vi riktigt den enda kommunen som kämpar med de här frågorna. Men risken är
258 ju, för det var det som var frågan, med all information som man hanterar som
259 kommun är ju att man sparar på så många olika ställen och idag med den tekninken
260 som är med Office365 tillexempel så kanske man inte ens har koll på var min
261 inforamtion hamnade för jag har bara tryckt på spara. Och det funkar ju, men vart
262 hamnade den och är det originalet som hamnade där eller är det en kopia som
263 hamnade där. Så risken är att möjligheterna att spara idag är så många så att man till

264 sist inte vet vilket papper eller vilket dokument som är det rätta.

265

266 X- Mm.

267

268 Y-För i kopior på kopior sen så mailar man kanske sen har något förändrats. Så att

269 det är den stora risken men det är ju både en utbildningssak och en teknik sak

270 egentligen. Så det vart ett långt svar på den frågan.

271

272 X-Det är bra. Det leder vidare till min nästa och du nämnde lite kort hur man

273 klassificerar datan och arbetet med att klassificiera den datan ni har på

274 Office365?

275

276 Y- Ja det är också ett pågående arbete för det är inte så enkelt. I den bästa av

277 världar så skulle man när man börjar med ett dokument, sätta en klassificering på

278 den. För att då veta hur man ska spara den. Så att nu då om det är ett öppet

279 dokument då kan jag spara den på den platsen, är det ett känsligt dokument då kan

280 jag inte spara det på samma plats som det andra utan jag får spara det på ett annat

281 sätt. Och det där håller vi på med och försöker strukturera upp men just nu med

282 tanke på hela Office365 diskussionen om molnet så har den stannat av litegrann och

283 vi får nog vänta till landet sverige har bestämt sig för hur vi får göra. Sen hör ju till

284 saken att det är många verksamheter som jobbar i verksamhetssystem så att man

285 har inte Office365 eller man sparar det inte bara i sin dator utan man kör ju i

286 verksamhetssystem. För då har man en helt annan säker hantering om vi säger som

287 socialtjänsten dom jobbar ju i särskilda system som dom har köpt in. Och då blir det

288 ju en annan hantering av deras information med inloggningar och så vidare. Så det

289 är en blanding av de här olika sätten att hantera information ju. Och vi på

290 räddningstjänsten vi har ju vissa system som vi sparar i och då är det ju ett

kontrollerat system som bara vissa kommer in i. Man kan ju säga att man klassar informationen men inte som enskild medarbetare gör man inte det. Utan det är mer att man jobbar i ett system då och då är den informationen, kan man säga, klassad från början ju.

X-Mm jag förstår. Okej om vi går vidare då. Använder sig kommunerna av standarder idag såsom ISO i sitt arbete?

Y-Ja. Det där ISO. Det finns ju ett, ja det kan man väl säga att vi försöker. För det är ju. Jag vet ju att det finns ett klassar system och att man ska klassificiera alla sina system och det ska bli ISO, så. Men jag kan nog inte riktigt svara på den. För vi, nej det gör vi nog egentligen inte om jag ska vara ärlig. För det köps in system från höger och vänster och det är appar och det är inget ISO så. Men grunden är ju att det ska vara så. För det står ju i riktlinjerna då i våra informationssäkerhetsriktlinjer att man ska jobba uteefter ISO. Men Ja, Nja får jag nog svara på den.

X-Ja men bra! Det var alla frågor vi hade. Jättebra svar.

Y- haha ja, långa om inte annat.

X- Ja men det är bra. Jag var lite nyfiken där om man får återvända där till tidigare det du nämnde om dom här riktlinjerna och policys att ni hade två olika dokument. Där det ena är riktlinjer och det andra lite mer Policy. Vad är innehållet där skiljer dom åt?

Y-Ja jag är inte så duktigt på just policy och riktlinjer jag är mer en praktiker. Jag är

inte så mycket för det här med dokument. Ser man. Nu kanske jag säger något som är dumt men pratar man generellt om vår kommun så skulle jag säga att hela kommunen är mer praktisk än teoretisk. Ja vi kör mycket. Ja vi kör. Och när man pratar med andra kommuner så är det ju. Man har väldigt fina dokument i pärmar och man är skitnöjd. Men man kan inte köra, för man har inte riktigt den förmågan. Hos oss är det om man tar mer generellt tvärtom, vi kör och så kanske man måste producera ett vackert dokument som ska stå i bokhyllan. Och om man tar då policy och riktlinjer här då så är policyrna egentligen det stora övergripande dokumentet kan man säga. Det är där det riktigt flummiga som då talar om vad politikerna tycker dom har det ansvaret och så vidare. Sen pinnar man ner det till riktlinjer och då är det lite lite mer i detalj vem som ska göra vad chefen har för ansvar och så vidare. Och sen är ju tanken att det ska mynna ut, man kan se det som en pyramid egentligen. Det kommer ni se i det där dokumentet. Policys är ju det överst i pyramiden och sen kommer riktlinjerna och sen kommer instruktionerna. Så basen längst ner där alla medarbetare ska vara med. För en medarbetare kommer kräkas om han eller hon ska läsa riktlinjerna. Det funkar ju inte. Det är så fina ord och så mycket konstiga saker så dom begriper inte det, och det gör inte jag heller knappt. Utan då är det instruktionerna där och den basen är vi ju inte riktigt klara med kan man ju säga då. Utbildningen finns där och kunskapen i den nanoutbildningen då. Det finns inga dokument skrivna i den där baspyramiden då kan man säga. Så att det var väl en enkel förklaring då.

X- Tack så jättemycket.

Konversationen avslutas.

8.2.5 Transkribering LK2

1 Kommun: LK2.

2 Informant: Anonym.

3 Intervjuare: Martin Petrelius.

4 Yrkestitel: Kanslichef

5 Datum: 11 maj 2021. Kl 16:00

6

7 Intervjuledare= X

8 Informant= Y

9

10 Informanten godkänner att samtalet spelas in.

11

12

13 X: Vad har du för roll inom kommunen och hur samspelar den med

14 informationssäkerhet?

15

16 Y: Någon informationssäkerhetschef har vi inte, däremot har vi haft en

17 informationssäkerhetssamordnare som precis har slutat för två veckor sedan. Jag är

18 idag kanslichef och jag är chef för informations säkerhetssamordnaren, när det finns

19 en sådan på plats. Jag är också säkerhetsskyddschef enligt

20 säkerhetsskyddslagstiftningen och en del av säkerhetsskyddsarbetet är ju då

21 informationssäkerhet, så utifrån det så har jag ju den sidan av informationssäkerhets

22 arbetet också.

23

24 X: Finns det något eller några övergripande styrande dokument för hur

25 kommunen hanterar informationssäkerhet i nuläget, s.k policies?

Y: Nej, det finns det inte, vi har inte någon informationssäkerhets policy, som det brukar kallas. Det finns specifika styrdokument kan finnas, men då är det mer i form av riktlinjer eller rutiner för hur vi hanterar informationssäkerhet inom ett specifikt område, t. ex socialtjänsten, rutiner för hur man hanterar informationssäkerhet inom den verksamheten. Vi har inget kommunövergripande som kommunfullmäktige har antagit.

X: Hur länge har ni inom kommunen arbetat med informationssäkerhet?

Y: Det är en jättesvår fråga att besvara egentligen, vi har inte haft en informationssäkerhetssamordnare mer än ett år, det innebär ju inte att vi inte tidigare har arbetat med informationssäkerhet, såklart, men då har det varit personer som haft det som sin ordinarie tjänst, t. ex återigen genom socialtjänsten. Där finns det ju regleringar inom patientdatalagen och inom socialstyrelsens föreskrifter om informationssäkerhet, men då har det ingått i det ordinarie arbetet, men det samordnade arbetet, det kommunövergripande, om vi pratar om det systematiska informationssäkerhetsarbetet så är det ett år ungefär.

X: Anser du att informationssäkerhet är en betydande del i kommunens arbete?

Y: Det är det absolut. Jag brukar säga att när jag pratar om informationssäkerhet så brukar jag säga som så att: Den viktigaste och den största tillgången för kommunen är personalen, människorna som arbetar inom kommunen, men den näst största tillgången är informationen, och utan information så kan vi inte genomföra vårt arbete. så arbeta på ett säkert sätt med hur vi hanterar den informationen, hur vi

skyddar den osv, är en jätteviktig fråga.

X: Finns det någon bestämmelse gällande beslutsfattande och hur det skall gå genom kommunen för just informationssäkerhet, du nämnde den här samordnaren innan och lite så, men finns det några vidare bestämmelser kring det?

Y: Man kan väl säga som att kommunfullmäktige har ju egentligen det övergripande ansvaret för informationssäkerhetsarbetet generellt i hela kommunen, och sen ansvarar respektive nämnd eller styrelse för informationssäkerhetsarbetet i den egna verksamheten, oavsett om det då inom skola, förskola eller inom socialtjänsten. Kommunstyrelsen har ett särskilt samordningsuppdrag, och allt det här regleras ju t. ex av det kommunala men även av nämndernas reglementen. När det gäller på förvaltningsnivå så är det ju då jag som kanslichef, eller egentligen förvaltningschefen då som är kommundirektören, i mitt fall, som har det övergripande samordnande ansvaret, och sen jag då som kanslichef och säkerhetsskyddschef. Det är så ansvarsgången går kan man väl säga.

X: Hur ser kommunikationen ut mellan dem här olika delarna, finns det någon kommunikation mellan dem eller är det lite att alla kör sitt egna "race"?

Y: Det är det man har en informationssäkerhetssamordnare till. Mycket i det uppdraget är att se till att vi arbetar på ett systematiskt sätt och i den systematiken innebär det ju också att man tar fram metoder, att man arbetar enhetligt med dem här frågorna. Och sen är det ju vissa frågor som rent naturligt berör fler olika nämnder och förvaltningar.

79

80 X: Hur ser ansvars och rollfördelningen ut inom kommunen gällande

81 informationssäkerhet?

82

83 Y: Ja det beskrev jag ju i princip i mitt förra svar.

84

85 X: Finns det satta rollansvar som den enskilde anställda ska följa?

86

87 Y: Säg frågan igen.

88

89 X: Finns det satta rollansvar som den enskilde anställda ska följa, alltså t. ex

90 finns det policies riktade till de specifika anställda i deras hantering av

91 information?

92

93 Y: Det finns det ju inom respektive verksamheter, och då pratar vi ju om det jag

94 tidigare nämnde som rutiner eller riktlinjer.

95

96 X: Hur ser arbetet med utbildning ut för anställda inom kommunen gällande

97 informationssäkerhet? Finns det någon utbildning?

98

99 Y: Inte övergripande, utan det var en utav dem sakerna som vår

100 informationssäkerhetssamordnare hade på sitt bord innan hen slutade, så att just nu

101 har vi inget. Vi har en plan men ingen som kan genomföra det just för tillfället.

102 Påbörjad information till alla chefer inom kommunen, sen så pågår det naturligtvis

103 hela tiden utbildning inom informationssäkerhet återigen inom respektive

104 verksamhet.

105

X: Vilka risker ser du med hanteringen av sådan information, vad finns det för risker att arbeta utifrån?

Y: Ja det är ju väldigt mycket, det är en väldigt vid fråga. Som du nämner så b.la hanterar vi ju väldigt mycket information som rör den enskilda medborgaren och där finns ju kritiska beroenden, t. ex om man inte kan ha tillgång till patientjournaler, så kan ju det vara väldigt allvarligt, då kan det ju handla om liv och död. Sedan handlar vi det ju också om väldigt stora värden, både ekonomiska värden men även förtroende förlust, t. ex. Det ser vi ju på kommuner eller organisationer och myndigheter där det har funnits brister inom informationssäkerheten, att det påverkar allmänhetens förtroende för den organisationen väldigt mycket, så det är ju en stor risk. Den största risken naturligtvis är ju liv och hälsa för befolkningen men även förtroende. Sen så kan det ju finnas information hos en myndighet som handlar om sveriges säkerhet och då pratar vi ju risker på ett helt annat plan.

X: Arbetar ni med att klassificera den datan ni hanterar på olika sätt i förhållan de till risk t. ex?

Y: Mm, vi har påbörjat det arbetet, vi har tidigare haft ett system för detta som heter "Ifacts", som används av flera andra kommuner, b.la Malmö stad vet jag. Vi har lämnat det systemet, vi var inte riktigt nöjda och har gått över till "KLASSA", som sveriges kommuner och regioner tagit fram. Men vi har ju en rätt lång väg att gå innan vi liksom har gått igenom all informationsmängd vi har, men det pågår.

X: Finns det något ramverk eller bestämmelser för att hantera sådana uppgifter?

132

133 Y: I en del av GDPR så har vi då förutom naturligtvis dataskyddsförodningen, så har
134 vi ju rutiner och riktlinjer kring det också, hur vi hanterar personuppgifter.

135

136 X: Använder ni er utav standarder såsom ISO i arbetet?

137

138 Y: Ja, på sätt och vis, men inte helt, det är inte så att vi siktar på att bli certifierade
139 inom ISO men i arbetet med att ta fram en handlingsplan för informationssäkerhet så
140 har vår tidigare informationssäkerhetssamordnare utgått från ISO standarder, så man
141 kan säga att arbetet bygger på det men kanske inte 100%, inte fullt ut som sagt.

142

143 X: Kanon, det var allt vi hade.

144

145 Samtalet avslutas.

146

9. Referenser

Brotby, Krag. 2009. *Information Security Governance.* Hoboken: John Wiley & Sons Inc. https://eds.b.ebscohost.com/eds/detail/detail?vid=2&sid=8b69819c-ba0f-42c1-9402-43c51dee02f2%40sessionmgr103&bdata=JnNpdGU9ZWRzLWxpd-mUmc2NvcGU9c2l0ZQ%3d%3d#AN=lub.6138452&db=cat07147a (Hämtad: 2021-04-21)

Bryman, Alan. 2018. *Samhälls-vetenskapliga metoder.* 3. uppl. Oxford: Oxford University Press.

Bulgurcu, Burcu. Cavusoglu, Hasan. Benbasat, Izak. 2010. *Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness.* Tillgänglig online: https://www.jstor.org/stable/25750690?seq=1#metadata_info_tab_contents (Hämtad 2021-04-04)

Diesterer, Georg. 2013. *ISO/IEC 27000, 27001 and 27002 for Information Security Management.* Tillgänglig online: *https://serwiss.bib.hs-hannover.de/frontdoor/deliver/index/docId/938/file/ISOIEC_27000_27001_and_27002_for_Information_Security_Management.pdf* (Hämtad 2021-04-14)

Hu, Qing. Dinev, Tamara. Hart, Paul. Cooke, Donna. 2012. Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. Tillgänglig online: https://onlinelibrary.wiley.com/doi/epdf/10.1111/j.1540-5915.2012.00361.x (Hämtad 2021-05-03)

Höne, Karin och J.H.P, Eloff. 2002. *Information Security Policy - what do international information security standards say?. Computers and Security 21(5): 402-410. https://eds.b.ebscohost.com/eds/detail/detail?vid=4&sid=8b69819c-ba0f-42c1-9402-43c51dee02f2%40sessionmgr103&bdata=JnNpdGU9ZWRzLWxpd-mUmc2NvcGU9c2l0ZQ%3d%3d#db=bth&AN=7850713 (Hämtad 2021-04-26)*

Kane, Greg och Koppel, Lorna. 2013. *Information Protection Playbook.* Oxford: Elsevier. https://books.google.se/books?id=Do3Sivwfk58C&pg=PP1&dq=kane+%26+koppel&hl=sv&sa=X&ved=2ahUKEwjAx4C6pMHwAhVOi-IsKHTxCCvAQ6AEwAHoECAYQAg#v=onepage&q=kane%20%26%20koppel&f=false (Hämtad: 2021-04-02)

Kvale, Steinar. 2015. *Den kvalitativa forskningsintervjun.* 3. uppl. Lund: Studentlitteratur AB.

MSB. 2015. *En bild av kommunernas informationssäkerhetsarbete* 2015. Tillgänglig online: https://www.msb.se/sv/publikationer/en-bild-av-kommunernas-informationssakerhetsarbete-2015/ (p.7) (Hämtad 2021-04-14)

MSB. 2021. *Detta är informationssäkerhet.* Tillgänglig online: https://www.informationssakerhet.se/om-informationssakerhet2/vad-ar-informationssakerhet/ (Hämtad 2021-04-14)

Nationalencyklopedin. [u.å.]. https://www.ne.se/info/ (Hämtad 2021-05-04).

Peltier, Thomas.R. 2007. *Implementing an Information Security Awareness Program.* Tillgänglig online: https://www.tandfonline.com/doi/pdf/10.1201/1086/45241.14.2.20050501/88292.6 (Hämtad 2021-04-07)

Peltier, Thomas. 2001. *Information Security Policies, Procedures, and standards. Guideline for effective security management.* Tillgänglig online: **https://books.google.se/books?hl=sv&lr=&id=mM_LsS-W4f4C&oi=fnd&pg=PP1&dq=information+security+policies+&ots=WhRXnZevhg&sig=SvGecuQIdpz9aziqiriLwjZaTtQ&redir_esc=y#v=onepage&q=information%20security%20policies&f=false** (Hämtad 2021-04-22)

Qadir, Suhail och Quadri, S.M.K. 2016. *Information Availability: An Insight into the Most Important Attribute of Information Security. Journal of Information Security, 7, 185-194* http://dx.doi.org/10.4236/jis.2016.73014 (Hämtad: 2021-05-02)

Rennstam, Jens och Wästerfors, David. 2015. *Från Stoff till Studie: Om analysarbete i kvalitativ forskning.* 1. uppl. Lund: Studentlitteratur AB.

Samonas, Spyridon och Coss, David. 2014. *The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. Journal of Information System Security* 10(3): 21-45. http://www.proso.com/dl/Samonas.pdf (Hämtad 2021-04-23)

Sohrabi Safa, Nader. Von Solms, Rossouw. Furnell, Steven. 2016.Information security policy compliance model in organisations. Tillgänglig online: https://www.researchgate.net/publication/309045498_Information_security_policy_compliance_model_in_organisations (Hämtad 2021-05-03)

Sveriges kommuner och regioner. 2021. *Kommungruppsindelning.* *https://skr.se/skr/tjanster/kommunerochregioner/faktakommunerochregioner/kommungruppsindelning.2051.html* (Hämtad: 2021-04-26)

Tankard, Colin. 2015. *Data classification - the foundation of information security. Network Securty 2015(5): 8-11.* *https://www.sciencedirect.com/science/article/pii/S1353485815300386?casa_token=IbPhRJCqNpoAAAAA:-dCiw0AIyw2z1mjOA77KHj0AljRhrrim82Wg42Js7Vh_YxspQLNZ4cmTD3EoKYpH4XoLr_552_Y (Hämtad: 2021-04-16)*

Tsohou, Aggeliki. Karyda, Maria. Kokolakis, Spyros. 2015. Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. Tillgänglig online:

https://www.sciencedirect.com/science/article/pii/S0167404815000565
(Hämtad 2021-04-14)

Volchkov, Andrej. 2019. *Information Security Governance: Framework and Toolset for CISOs and Decision Makers.* Boca Raton: Taylor & Francis Group. https://books.google.se/books?hl=sv&lr=&id=O_Z1DwAAQBAJ&oi=fnd&pg=PP1&dq=information+security+governance+volchkov&ots=rwV5sKs-6f&sig=KM_ru0TwLYbJgtqg-f2fGq5fLU8&redir_esc=y#v=onepage&q=information%20security%20governance%20volchkov&f=false (Hämtad: 2021-04-12)

Von Solms, R. 1998. *Information security management (1): why information security is so important, Information Management & Computer Security, Vol. 6 No.4,pp.174-177.* Tillgänglig online: **https://www.emerald.com/insight/content/doi/10.1108/EUM0000000004533/full/pdf?title=information-security-management-1-why-information-security-is-so-important**
(Hämtad 2021-04-06)

Williams, Paul. 2012. Executive and board roles in information security. Tillgänglig online: *https://reader.elsevier.com/reader/sd/pii/S1353485807700739?token=40CE058E92761361CE766965214EA61096490EEF8EBD5E24DFB6E7B64ED4D566F18698790798C9E89623DB43B509D5EA&originRegion=eu-west-1&originCreation=20210516150247*
(Hämtad 2021-04-17)