Bachelor Degree Project

UNIVERSITY OF SKÖVDE

HUR SER ANVÄNDNINGEN UT AV MOLNBASERADE LÖSNINGAR FÖR LAGRING AV SÄKERHETSKOPIOR HOS KOMMUNER I SVERIGE?

HOW IS THE USE OF CLOUDBASED SOLUTIONS FOR STORAGE OF BACKUP HANDLED BY MUNICIPALITIES IN SWEDEN?

Examensarbete inom huvudområdet informationsteknologi
Grundnivå 22,5 högskolepoäng
Vårtermin 2018

Andreas Lindén
e13andli@student.his.se

Handledare: Joakim Kävrestad
Examinator: Marcus Nohlberg

Sammanfattning

Att säkerhetskopiera innebär att försäkra sig om att det alltid finns en eller flera säkerhetskopior ifall originalfilen skulle gå förlorad. Säkerhetskopiering är ett koncept som har funnits länge. Från den enskilda hemanvändaren, till företag, till organisationer: alla kan nyttja säkerhetskopiering för att skydda sina data som finns lagrade på olika system.

Denna studie har för avsikt att studera hur användningen av molnbaserade lösningar för säkerhetskopiering ser ut hos kommuner i Sverige. Säkerhetskopiering kan hanteras på många olika sätt och det finns flera olika implementationer att välja mellan. Molnbaserade lösningar och de funktioner som de tillhandahåller har potentialen att föra med sig många nya möjligheter för kommuner. Med de funktioner som tillhandahålls av en molnbaserad lösning däribland möjligheten till lagring av säkerhetskopior, är det intressant att se hur dessa funktioner har kunnat utveckla ett koncept som ändå är så centralt inom kommuner som säkerhetskopiering är. Säkerhetskopiering är en viktig arbetsuppgift hos kommuner och omfattande arbete som bedrivs varje dag.

En enkät skickades ut där Sveriges kommuner fick besvara frågor angående deras användning av molnbaserade lösningar för säkerhetskopiering. Av 290 kommuner var det totalt 67 kommuner som svarade. Underlaget från enkäten analyserades och de som studien kom fram till var att en mindre del av Sveriges kommuner har implementerat en molnbaserad lösning för säkerhetskopiering. Dock är de som använder sig av denna implementation kommuner som har gjort det under en längre tid. Hanteringen av säkerhetskopieringen ser ut som så att det sker minst en gång per dygn där kommunen oftast tar hjälp av en privat outsourcingleverantör. Det finns många effektivitetsfaktorer som kan uppnås vid användandet av denna implementation av säkerhetskopiering, vilket återspeglar ett stort användbarhetsområde. Molnbaserade lösningar för säkerhetskopiering anses vara en fullgod lösning i avseende på säkerhets och integritetsfrågor.

De kommuner som inte använder sig av en molnbaserad lösning för säkerhetskopiering använder sig av en egen lösning och detta sköts på plats hos kommunen genom en implementation som oftast tagits fram utefter kommunens behov. De kommuner som bedriver egen lösning gör det främst på grund av kostnadsskäl och säkerhetsfrågor.

Oavsett lösning är kommunerna överens om att dataintegritet är något som bör prioriteras högt och att resurser bör läggas på att säkerställa att detta område håller en hög kvalité.

Nyckelord: molnbaserade lösningar, säkerhetskopiering, kommuner, enkätstudie.

English summary

Managing backups to ensure that one has a backup copy if an original file is lost, deleted, or corrupted is a concept that has existed for a while. Ranging from the home user to companies and organizations, everyone can utilize backups to protect data that have been saved on different systems.

This study is being conducted to explore how cloud-based solutions for backup are being used in municipalities in Sweden. Backup can be handled in many different ways and there are several implementations to choose from. Cloud-based solutions provide new functions to municipalities and offer them novel opportunities. With the functions brought by a cloud-based solution including the opportunity of storing backups makes it interesting to see how these functions could have developed a concept that backup is, which is a procedure of importance regarding the work at municipalities. Backup is a thorough process that is being conducted every day.

A survey was sent out to Sweden's municipalities, and they were asked to answer questions regarding their usage of cloud-based solutions for backup. Out of a total of 290 municipalities, 67 responded. The answers from the survey were analyzed, and the results from the study are explained below.

A small part of Sweden's municipalities has implemented a cloud-based solution for backup, but the ones who employ it have been doing so for some time. Backup is being completed at least once per day in cases where the municipalities often make use of a private outsourcing provider. There are several effectivity factors regarding the use of cloud-based solutions for backup which reflects a big area of usability. Cloud-based solutions for backup are viewed as safe solutions when it comes to managing integrity.

Furthermore, most of the municipalities implement their own solution for backup and manage it as an on-premise solution which have been implemented according to the municipalities needs. The foremost reasons for this method are cost and security concerns.

Regardless of the solution, the municipalities agree that data integrity is a matter that should be highly prioritized and that resources should be focused on ensuring that this area holds a high quality.

Innehållsförteckning

1 Introduktion

Digitaliseringen av samhället fortskrider kontinuerligt. Samhällsfunktioner och arbetssätt omvandlas och ersätts av tekniska lösningar. Flertalet samhällsfunktioner och tillhandahållandet av stora mängder information är något Sveriges kommuner har hand om. För att utveckla kommunernas verksamhet krävs det att utdaterade lösningar ersätts med fungerande lösningar. Något som har fått fotfäste för olika samhällsfunktioner är molnbaserade lösningar. Dessa kan användas för flera ändamål, bland annat för att lagra stora mängder information, något som kommuner är i behov av eftersom de agerar som en så pass stor samhällelig funktion.

Tidigare studier inom området av Ali m. fl. (2015) kom fram till att implementeringen av molnbaserade lösningar inom australiensiska kommuner bland annat bidrog till en positiv funktion av katastrofåterställning samt backup av säkerhetskopior. En stabil lösning för databackup ansågs kunna vara ett verktyg för snabb återställning vid oväntade situationer. Molnbaserade lösningar har funnits på marknaden sedan en tid tillbaka och det finns studier tillgängliga gällande just användningen av molnbaserade lösningar samt studier gjorda på dem och deras implementation i olika organisationer. Det som gör denna studie unik är att den fokuserar på en specifik komponent, säkerhetskopiering, inom området kring molnbaserade lösningar och hur detta tillämpas inom kommuner. Studien inkluderar även de kommuner som använder sig av en annan lösning vilket ställer molnbaserade lösningar i kontrast mot andra alternativ. Detta medför att studien ger en helhetsbild över hur säkerhetskopiering hanteras ute hos kommuner i Sverige.

Många organisationer behandlar data som kräver speciell hantering då de data som lagras kan kopplas till individer (Ali & Soar, 2014). Säkerhetskopior som görs på data som lagras inom kommuner innehåller ofta sekretessbelagd information. Därav kommer studien även utforska hanteringen av personuppgifter vad gäller de data som säkerhetskopieras. Studien kommer även omfatta vilka effekter som kan ha uppnåtts av att arbeta med molnbaserade lösningar och vilka positiva och negativa aspekter som erhållits av en implementation av dessa för säkerhetskopior.

Studien är baserad på en enkät som skickades ut till samtliga kommuner i Sverige. Kontaktpersoner med en ledande roll avseende IT-infrastruktur inom kommunen var respondenter för enkäten och deras svar är det som ligger till grund för studien.

Strukturen på rapporten är enligt följande: kapitel 2 innehåller en bakgrundsförklaring om ämnet. I kapitel 3 presenteras problemdefinitionen. Vidare i kapitel 4 förklaras metoden som använts i arbetet samt validitetshot applicerbara för studien. I kapitel 5 kommer resultat presenteras och analyseras. I kapitel 6 behandlas slutsatser för studien. I det avslutande kapitel 7 återfinns diskussion om ämnet och studien.

2 Bakgrund

I detta kapitel kommer följande ämnen belysas: molnlagring, säkerhetskopiering, användningen av molnbaserade lösningar inom kommuner samt relaterad forskning. Studien kommer att utforska hur utbredd användningen av molnbaserade lösningar för säkerhetskopiering är inom kommuner. Därav är det viktigt att definiera molnmodellen för att få en förklaring till hur denna fungerar och vilka olika sorters lösningar som finns tillgängliga. Kapitlet innehåller även en definition av säkerhetskopiering då detta är centralt för studien. Lagar och regler för kommuner som planerar att använda sig av molnbaserade lösningar presenteras, hur en kommun ska förhålla sig till behandlingen av informationssäkerhet och vidare tar kapitlet även upp vad som gäller för personuppgifter när molnbaserade lösningar ska användas. Kapitlet avslutas med ett avsnitt om relaterad forskning inom området.

2.1 Molnlagring

Molnlagring definieras som en metod att köra applikationsmjukvara och att lagra data i centrala datorsystem, vilket användare sedan kan få tillgång till genom internet (Carr, 2013).

Molnmodellen är en modell som används för att förklara hur molnbaserade lösningar fungerar. Molnmodellen och begreppen som molnbaserade lösningar innefattar kommer att förklaras med hjälp av National Institute of Standards and Technologys (NIST) definition av molnmodellen. NIST definierar molnmodellen med hjälp av fem nödvändiga karaktäristiska egenskaper, tre olika servicemodeller samt fyra distributionsmodeller. Molnmodellen från NIST används för att förklara hur molnbaserade lösningar kan utnyttjas av kommuner med vilka möjligheter som finns till olika sorts topologier och sammansättningar (Sinanc m.fl., 2013).

Enligt Sinanc m. fl. (2013) är de fem nödvändiga karaktäristiska egenskaperna för molnmodellen enligt följande.

1. Direkt begärd självservice: Användare av molnbaserade lösningar ska kunna kontrollera egenskaper som till exempel lagringskapacitet vid behov, och detta utan att behöva involvera andra människor.

2. Bred nätverksåtkomst: Användare ska kunna nyttja tjänstens resurser genom en standardiserad nätverksåtkomst och kunna nå tjänsten via flertalet enheter såsom stationära datorer, smartphones och surfplattor.

3. Resurskonsolidering: Både olika fysiska och virtuella resurser som finns dynamiskt i en leverantörs resurspool ska kunna erbjudas baserat på användarens behov, samt även betjäna flertalet användare samtidigt.

4. Snabb elasticitet: Resurser som en användare använder ska kunna bli anpassade efter behov. Resurser, funktioner samt moduler ska kunna skalas upp och ned utifrån användarens behov. På detta sätt upplevs resurserna som oändliga, men användaren betalar endast för de resurser som nyttjas.

5. Mätbar service: Med hjälp av mätbar service ska både leverantör samt användare kunna övervaka, kontrollera och rapportera resursanvändning. Resurser ska kunna fördelas efter användares behov för att användaren endast ska behöva betala för de resurser som används. För att möjliggöra detta krävs det att möjligheten finns att mäta till exempel användning av bandbredd och lagring.

De tre servicemodeller som existerar inom molnmodellen är följande:

1. Software as a Service (SaaS): Denna form används av användare för att använda leverantörens mjukvara och associerade data som återfinns på en molninfrastruktur som användaren kan interagera med genom ett gränssnitt. Några exempel på detta är Flickr, Google Docs och VMWare Cetas.

2. Platform as a Service (PaaS): Användaren kan driva applikationer via den här sortens service genom att använda sig av verktyg som finns tillgängliga via leverantören, exempelvis uthyrning av hårdvara, operativsystem, lagring och även nätverkskapacitet. Några exempel på detta är Google App Engine, Windows Azure och VMware Cloud Foundry.

3. Infrastructure as a Service (IaaS): Med detta menas nödvändiga datorresurser som tillhandahålls användarna för att distribuera och köra mjukvara. En användare kan alltså bygga upp en infrastruktur utan inköp av hårdvara och kan i stället nyttja detta som en utkontrakterad service. Exempel som återfinns är Amazon Web Services, OpenStack och VMware vCloud Suite.

De fyra olika distributionsmodeller som finns är följande:

1. Privat moln: Den här sortens infrastruktur tillhandahåller ett exklusivt användande för bara en enda organisation med flera användare.

2. Gemenskapsmoln: Denna sort är delad av konsumenter från flera olika organisationer med samma intressen.

3. Publikt moln: Ett publikt moln är gjord för öppet användande och tillåter användare att få tillgång till det genom att använda sig av ett gränssnitt som återfinns i webbläsare.

4. Hybridmoln: Hybridmoln är en modell som använder sig av två eller flera distinkta molndistributionsmodeller (Sinanc m.fl., 2013).

Förutom de egenskaper och molnmodeller som finns tillgängliga och som presenteras från NIST kan kommuner komma att anpassa sin verksamhet just utefter vilka resurser som behövs för den aktuella lösningen som kommunen har. Många olika privata outsourcingleverantörer existerar på marknaden. En kommun kan också göra valet att låta lagra sina säkerhetskopior på ett annat sätt som ej involverar en privat outsourcingleverantör som till exempel ett statligt ägt alternativ. Kombinationer finns också tillgängliga med att viss information sparas med en lösning och andra data med en annan lösning.

2.2 Säkerhetskopiering

Att säkerhetskopiera eller göra en backup definieras som en process som kopierar data till ett alternativt ställe på så vis att dessa data kan användas för att återställa originalversionen utifall denna skulle ha gått förlorad eller blivit skadad. Faktorer som påverkar hur ofta en säkerhetskopia bör skapas inkluderar hur ofta data ändras, hur värdefulla de är samt hur lång tid det tar att göra säkerhetskopieringen. Det finns många olika sätt och flera olika lagringsmedier att använda sig av. Exempel på dessa är CD-R, DVD-R, USB, externa hårddiskar samt molnbaserade lösningar (Computerhope, 2017).

Enligt Symantec (2003) beskrivs det att göra en säkerhetskopia på sina filer som privatperson, företag eller myndighet är en nödvändighet utifall en oförutsedd händelse, datorkrasch eller en yttre påverkan skulle göra att data blir obrukbara eller skulle försvinna. När en säkerhetskopia görs av data är detta en process där alla eller en del av de data som finns på en lagringsenhet sparas på ett annat lagringsmedium som en säkerhetskopia. Det går även att göra en säkerhetskopia och lagra denna utan att använda sig av något externt lagringsmedium som att exempelvis spara säkerhetskopian på en annan partition av hårddisken. Men om hela hårddisken skulle fallera skulle detta inte vara att föredra då både originalfilerna samt säkerhetskopian skulle gå förlorade. Det är därför mest optimalt att skapa

en säkerhetskopia som lagras på ett externt lagringsmedium och att denna säkerhetskopia inte har samma fysiska plats som originalkopian om till exempel en brand skulle inträffa och leda till att både original och säkerhetskopia skulle förloras (Symantec, 2003).

2.3 Användningen av molnbaserade lösningar inom kommuner

Vad gäller utövandet av integritet inom en organisation krävs det att lagar, policyer och standarder följs korrekt för att hantera och skydda information som kan bindas till individer. Detta är något en organisation måste prioritera vid planering och införskaffande av en molnbaserad lösning (Ali & Soar, 2014).

I ett mejl från en jurist på Datainspektionen (E. Marcus, mejlkontakt, 30 april 2018) tillgodoses information och dokument över vad som applicerar för de kommuner som vill använda sig av molnbaserade lösningar samt hur de ska förhålla sig till dataskyddsförordningen (GDPR) vad gäller detta. Det är denna information och dokument förmedlade via juristen som vidare användes för att färdigställa ett fullgott bakgrundskapitel i denna studie. Ett av dokumenten som juristen bifogar kommer från den juridiska analys som Pensionsmyndigheten (2016) har gjort angående användning av molntjänster vilket ligger till underlag för att förklara vilka lagar och regler som kommuner måste förhålla sig utifrån gällande GDPR. Juristen bifogar även rapporten som heter ”Molntjänster i staten – En ny generation av outsourcing” som Pensionsmyndigheten (2016) har gjort genom ett regeringsuppdrag där de fått i uppdrag att analysera och värdera potentialen för användning av molntjänster hos myndigheter i Sverige. I rapporten återfinns vilka risker och hinder som anses vara applicerbara vid en potentiell implementation av användning av molntjänster. Rapporten går även den igenom vilka lagar och regler som är nödvändiga att fastställa för att en myndighet ska kunna använda sig av en molntjänst. Rapporten har publicerats på Pensionsmyndighetens webbplats, men har även publicerats på Samrådsgruppens webbplats för kommunala arkivfrågor. Samrådsgruppen fungerar som ett beredande samarbetsorgan mellan det statliga arkivväsendet och de primära och landstingskommunala sektorerna. Samrådsgruppen har till uppdrag att arbeta med frågor som rör stat, kommuner och landsting inom arkivområdet för att se till att utvecklingen av arkivfrågor fortskrider för den offentliga sektorn. Samrådsgruppen (2016) skriver att även om rapporten om molntjänster är fokuserad för statlig verksamhet är informationen som återfinns i rapporten även relevant för hur kommunala verksamheter ska hantera molnbaserade lösningar. Därav har även denna rapport publicerats på Samrådsgruppens webbplats. Rapporterna används som källor då de är rekommenderade som styrdokument från juristen på Datainspektionen för vad som gäller för GDPR och lagar och regler som appliceras för kommuner angående deras användning av molnbaserade lösningar. Rapporterna har från Pensionsmyndighetens sida tagits fram i samarbete med MSB och Datainspektionen. Datainspektionens egen webbplats kommer även att användas som kompletterande källa, detta för att Datainspektionen har den fullgoda versionen av GDPR. Genom att tillgodose den information som finns om GDPR där kan det valideras att informationen som återfinns i rapporterna från Pensionsmyndigheten stämmer. Bakgrundskapitlet är alltså till för att validera de lagar, regler och bestämmelser som är förutsatta för att en kommun ska få använda sig av en molnbaserad lösning enligt GDPR-direktiven. Genom att använda Datainspektionen som källa kan kapitlen även utökas på så sätt att de inte missar några viktiga delar som kan ha utelämnats i rapporterna då GDPR är en omfattande lagstyrning.

2.3.1 Laglighetskontroll

I rapporten Molntjänster i staten från Pensionsmyndigheten (2016) beskrivs det hur svenska kommunala myndigheter ska förhålla sig till implementationen av molntjänster. Före implementationen av en molnbaserad lösning måste en kommun utföra en laglighetskontroll. En laglighetskontroll innefattar offentlighets- och sekretesslagen, hantering av personuppgifter samt arkivlagen men kan också innefatta en analys av speciallagstiftningar. En kommun behöver kunna göra tillräckliga juridiska bedömningar; detta genom att ha kännedom om vilka molntjänstleverantörer som kommer att hantera kommunens information, hur informationen kommer att hanteras samt var informationen lagras rent geografiskt. Utan dessa faktorer är det omöjligt att kunna bedöma lagligheten av informationshanteringen hos en molntjänstleverantör.

Gällande vilka legala krav som tillämpas när uppgifter från kommuner ska hanteras av en molntjänstleverantör beror detta på vilken typ av information som ska lagras. När laglighetskontrollen ska göras bör kommunen ha arbetat fram syftet med att hantera informationen i den planerade lösningen samt vilka funktioner som myndigheten vill nyttja med tjänsten. Laglighetskontrollen kan göras som en del av kommunens informationsklassning och riskanalys. Utöver laglighetskontrollen är det viktigt att kartlägga informationens känslighet ur ett individ-, verksamhets- och samhällsperspektiv för att kunna göra en tillräckligt bra bedömning om informationen ens kan hanteras i en molnbaserad lösning. Laglighetskontrollen ska innefatta om uppgifterna som kommunen ska lämna ut till molntjänstleverantören är sekretessbelagda, om det är allmänna handlingar och utifall informationen innehåller personuppgifter. När kommunen har klarlagt vilken typ av information som ska behandlas är nästa steg att ta reda på regler som återfinns i till exempel tryckfrihetsförordningen, offentlighets- och sekretesslagen, arkivlagen, samt vad som behöver appliceras för hantering av personuppgifter eller vad som gäller sin egen registerförfattning. Med hjälp av det sammanvägda regelverket som är tillämpligt på den planerade hanteringen ska kommunen sammanställa de krav som molntjänstleverantören måste uppfylla för att hanteringen ska vara godkänd enligt lag (Pensionsmyndigheten, 2016).

2.3.2 Offentlighets och sekretesslagstiftningen

Pensionsmyndigheten (2016) beskriver vad gäller offentlighets- och sekretesslagen att efter kommunen har klarlagt innehållet i informationen är nästa steg att göra klart ifall den innehåller uppgifter som är sekretessreglerade samt ifall informationen omfattas av säkerhetsskyddslagen. Om säkerhetsskyddslagen skulle vara aktuell måste kommunen, utöver sekretessprövningen, se om det är möjligt att uppfylla de lagliga krav som ställs på god informationssäkerhet, säkerhetsskyddsavtal och säkerhetsprövning av personal. Det är oftast problematiskt att teckna säkerhetsskyddsavtal med en global molntjänstleverantör och göra en säkerhetsprövning av dess anställda som kan vara utländska medborgare då de oftast har sin arbetsplats utanför Sveriges gränser. I realiteten är det väldigt få fall där information som säkerhetsskyddslagen tillämpas på kan hanteras i en molntjänst. Därav bör det vara helt uteslutet att hantera information där säkerhetsskyddslagen är tillämplig.

Ifall säkerhetsskyddslagen inte kan tillämpas kan en kommun lämna ut information till en molntjänstleverantör utifall informationen inte skulle ha sekretesskydd. Ifall den skulle vara sekretessbelagd ska kommunen göra en prövning ifall informationen kan lämnas ut till molntjänstleverantören enligt offentlighets- och sekretesslagen. När sekretessprövningen görs måste kommunen fastställa att prövningen görs i förhållande till molntjänstleverantören men även i förhållande till om det skulle finnas underleverantörer till molntjänstleverantören som kan komma att ha hand om kommunens information. Det kan förekomma förhållanden där en avtalsreglerad tystnadsplikt kan medföra att informationen utan förhinder av sekretessvillkor kan lämnas ut till molntjänstleverantören. Detta omfattar dock inte i normalfall information som är integritetskänslig eller information med speciellt skyddsbehov med hänsyn till Sveriges internationella relationer eller rikets säkerhet (enligt säkerhetsskyddslagen). Andra omständigheter som kommunen måste beakta är ifall informationen kan bli exponerad för andra länders rättsordningar och ifall den skulle lagras utanför Sveriges gränser eftersom den då möjligtvis skulle kunna bli tillgänglig för andra länders myndigheter. Kommunen bör inte förlita sig på en avtalsreglerad tystnadsplikt oavsett känsligheten

hos informationen, detta ifall molntjänstleverantören skulle anlita mer än enstaka underleverantörer samt ifall underleverantörer byts ut med jämna intervall. Kommunen måste ha möjlighet att kontrollera och följa upp att leverantörerna följer avtalen och villkoren i dessa. När molntjänstleverantören anlitar många underleverantörer eller om underleverantörer regelbundet byts ut blir det svårt för kommunen att se till att avtal efterlevs, särskilt då underleverantörerna är utom Sveriges gränser.

Information som har bedömts vara sekretesskyddad i förhållande till leverantören kan inte hanteras i en molntjänst, detta även om tystnadsplikt kan bestämmas i olika avtal (Pensionsmyndigheten, 2016).

2.3.3 Arkivlagen

När kommunen har kontrollerat att integritetsskyddslagstiftningen inte omöjliggör hanteringen av information hos en molntjänstleverantör så kan kommunen gå vidare med att kontrollera om allmänna handlingar kommer att hanteras i tjänsten (Pensionsmyndigheten, 2016). Ifall kommunen ej kommer hantera allmänna handlingar är nästa steg att ta reda på om leverantörens uppdrag kommer innefatta endast teknisk lagring eller teknisk bearbetning. Ifall molntjänstleverantörens uppdrag är sådant kan det ske att handlingarna kan komma att ändra status gällande tryckfrihetsförordningen. Avseende de handlingar som ännu ej är allmänna och som kommunen lämnar ut till molntjänstleverantören kommer dessa att betraktas som expedierade och tolkas som allmänna enligt tryckfrihetsförordningen.

Ifall molntjänstleverantören ska hantera allmänna handlingar på uppdrag av en kommun behöver kommunen se till att krav uppfylls enligt offentlighets- och sekretesslagens krav på en god offentlighetsstruktur och arkivlagens krav på bevarande och gallring. Det som kommuner ska utgå ifrån är att allmänna handlingar ska bevaras. Gallring får endast ske om det stämmer överens med riksarkivets föreskrifter eller beslut, ifall inte särskilda villkor finns att tillämpa från lag eller förordning. Kommunen behöver säkerställa att leverantören utför radering av uppgifter som har valts att gallras av myndigheten. Ifall beslut tas att handlingar ska bevaras behöver det kontrolleras att leverantören kan långtidsbevara handlingar, att det finns möjligheter att överföra handlingar till annan leverantör eller hämta hem handlingar.

När allmänna handlingar lagras i en molnbaserad tjänst ställs krav på tillförlitlighet och autenticitet. Kommuner med skyldigheter att bevara allmänna handlingar måste kunna garantera handlingarnas autenticitet över tid och detta oberoende av formen handlingarna lagras i. Där handlingarna lagras ska det finnas ständig tillgång till dem men även möjlighet att oåterkalleligt kunna gallra allmänna handlingar som lagras hos en molntjänstleverantör. Innan en upphandling måste bestämmelserna i arkivlagen med tillhörande föreskrifter och eventuella registerförfattningar vara klarlagda samt risker med att lagra allmänna handlingar i molnet tas i beaktande.

Gällande handlingar som har ett speciellt integritetskänsligt slag får dessa inte lämnas ut till utomstående aktör, undantaget är ifall det finns en lagreglerad tystnadsplikt.

Det är av yttersta signifikans att det finns tillämpningsbara legala förutsättningar att just den molntjänstleverantör som är tänkt att anlitas kan uppfylla kraven en kommun har klarlagt. Detta för att hanteringen av en molnbaserad lösning ska kunna tillåtas i sin helhet (Pensionsmyndigheten, 2016).

2.3.4 Informationssäkerhet

Enligt Pensionsmyndigheten (2016) är informationssäkerhet ett viktigt område gällande användningen av molntjänster hos kommuner. Vilken nivå av säkerhet som behöver appliceras bestäms utefter konfidentialitet, riktighet, tillgänglighet och spårbarhet. Vilka skyddsåtgärder som behöver antas ska beaktas utefter hur skyddsvärd informationen är men även vilka speciella risker som finns relaterade till hanteringen av informationen. Informationen som ska hanteras behöver ha skydd emot obehörig åtkomst, avbrott i önskad tillgänglighet samt förlust, förstörelse eller manipulation. Andra faktorer som kan vara viktiga är att ha möjlighet att spåra hur och av vem som informationen har hanterats, detta för att kunna klarlägga vem som har hanterat informationen. För att få rätt nivå av säkerhet

behöver en kommun ta utgångspunkt i sin informationsklassificering men också göra en specifik riskanalys som relaterar till informationen som är tänkt att behandlas i en tilltänkt molntjänst.

Gällande upprätthållandet av en god informationssäkerhet är det lämpligt att en organisation som en kommun inför ett ledningssystem för informationssäkerhet (LIS). Enligt Myndigheten för samhällsskydd och beredskap ska informationssäkerhet införas och tillämpas enligt ett ledningssystem i enlighet med den svenska och internationella standarden för informationssäkerhet SS-ISO/IEC 27001 och 27002. För att göra detta ska följande steg utföras:

1. Ta fram styrande dokument	Upprätta en informationssäkerhetspolicy och andra styrande dokument som behövs för kommunens informationssäkerhet.
2. Utse informationssäkerhetsansvariga	Utse en eller flera personer som leder och samordnar arbetet med informationssäkerhet.
3. Genomföra informationsklassificering	Klassificera myndighetens information med utgångspunkt i krav på konfidentialitet, riktighet, och tillgänglighet.
4. Genomföra risk-och-sårbarhetsanalys	Utifrån risk-och-sårbarhetsanalyser och inträffade incidenter avgöra hur risker ska hanteras samt besluta om åtgärder.
5. Dokumentera	Dokumentera granskningar och säkerhetsåtgärder av större betydelse som vidtagits.

Tabell 1: Införande av informationssäkerhet (Pensionsmyndigheten, 2016).

Enligt säkerhetsskyddslagen (1996:627) finns det särskilda skyddsåtgärder som ska tillämpas för information som kan komma att påverka rikets säkerhet. Lagen säger att verksamhetsutövarna själva ska bedöma om de driver någon form av säkerhetskänslig verksamhet. Är fallet sådant får de bestämma om vad som ska betraktas som skyddsvärt enligt säkerhetsskyddslagstiftningen. Verksamhetsutövare behöver alltså göra en kvalificerad säkerhetsanalys enligt säkerhetsskyddsförordningen.

Gällande de privata leverantörer av molntjänster som finns kan dessa anlitas på flera olika sätt och i olika omfattningar. Detta medför olika sorters styrning av informationssäkerhet men även olika risker. Under de flesta omständigheter utgjuts ett juridiskt bindande avtal gentemot när myndigheter erbjuder varandra tjänster. För privata leverantörer gäller inte lagen Myndigheten för samhällsskydd och beredskap 2009:10 föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet, vilket medför att kunden inte kan vara säker på att leverantören utför ett systematiskt informationssäkerhetsarbete. Hur informationssäkerheten hos leverantören gällande tjänsterna är utformad är svårt att veta jämfört med om det skulle vara i egen drift och förvaltning men även jämfört med en offentlig aktör som molntjänstleverantör åt andra myndigheter. På grund av detta är det ett stort behov av att redan i underlaget för anskaffningen av en molntjänst från en molntjänsteleverantör tydliggöra krav på villkor för uppföljning och efterlevnad av satta krav. Eftersom det även finns en bristande insyn kan detta försvåra att vid en incident snabbt kunna skapa en samlad bild över hur samhällsviktig verksamhet blivit drabbad av incidentens konsekvenser (Pensionsmyndigheten, 2016).

2.5 Personuppgifter

I detta kapitel kommer personuppgifter och hanteringen utefter GDPR att förklaras.

Datainspektionen (2018) skriver att behandling av personuppgifter ska ske på så vis att det säkerställs en lämplig säkerhet för personuppgifterna. Detta omfattar skydd mot obehörig eller otillåten behandling samt att personuppgifter ska behandlas mot förlust, förstöring eller skada som är åsamkad genom olyckshändelse genom att behandlingen ska använda sig av tekniska eller organisatoriska verktyg för att motverka detta.

Om en kommun använder sig av en molntjänst för att lagra personuppgifter förlorar kommunen den faktiska kontrollen över dessa personuppgifter där de lagras. Det kan även förekomma att molntjänstleverantörer använder standardavtal med fördefinierade användarvillkor och anlitar underleverantörer. Det är kritiskt att kommuner har god kännedom om de krav som ställs.

Det som definieras enligt Datainspektionen (2018) gällande GDPR och hur personuppgifter ska hanteras i en molntjänst samt vilka lagar och regler en organisation måste förhålla sig utefter så anges följande.

Om en myndighet eller kommun använder sig av en molntjänst för sin personuppgiftsbehandling är det myndigheten eller kommunen som är personuppgiftsansvarig för behandlingen även om denna utförs av molntjänstleverantören eller någon underleverantör. Leverantören och potentiella underleverantörer blir då den personuppgiftsansvariges personuppgiftsbiträden. Det är alltså myndigheten eller kommunen i detta fall som ansvarar för att lagar för personuppgifter och andra lagar följs, dessa kan vara exempelvis myndighetsspecifika registerförfattningar och offentlighets- och sekretesslagen.

Datainspektionen (2018) skriver vidare att den personuppgiftsansvarige måste göra en bedömning utifall den personuppgiftsbehandling som molntjänstleverantören planeras utföra kommer vara i enlighet med hur personuppgifter ska hanteras, alltså en laglighetskontroll. Personuppgiftshanteringen anger att personuppgiftsbiträden bara får behandla personuppgifter i enlighet med instruktioner från den personuppgiftsansvarige. Personuppgiftsbiträdet måste ge tillräckliga garantier vad gäller tekniska och organisatoriska åtgärder för att behandlingen ska uppfylla GDPR. Detta för att säkerställa att den registrerades rättigheter skyddas korrekt. Utifall en myndighet skulle anlita en molntjänstleverantör händer det dock ofta att myndigheten blir hänvisad till villkoren som har satts upp av leverantörens standardavtal. När detta är aktuellt måste den personuppgiftsansvariga granska avtalsvillkor och riktlinjer från leverantören och sedan utifrån dessa göra en bedömning. Denna bedömning innefattar personuppgiftshanteringens bestämmelser och slutsatserna från den personuppgiftsansvariges egen risk- och sårbarhetsanalys. I enlighet med GDPR måste den personuppgiftsansvarige beakta följande aspekter:

- om det finns en risk för att personuppgifter kan komma att användas för några andra ändamål än de ursprungliga,
- om det finns en risk att molntjänstleverantören skulle kunna lämna över personuppgifter till ett utomstående land, alltså ett land utanför EU/EES och utifall detta stödjs av hur personuppgifter får behandlas enligt dokumenterade instruktioner samt
- om det finns säkerhetsåtgärder som måste appliceras för att kunna skydda personuppgifterna som ska behandlas, exempelvis att säkerställa att personer som har rätt att behandla personuppgifterna ska omfattas av tystnadsplikt och beakta konfidentialitet.

Utöver detta måste den personuppgiftsansvarige även:

- initiera ett personuppgiftsbiträdesavtal med molntjänstleverantören där det framgår att de skyldigheter som fastställs enligt GDPR har fullgjorts och möjliggöra till granskningar av detta,

- ta hänsyn till annan lagstiftning såsom sekretesslagstiftningen,

- fastslå att personuppgiftsbiträdet inte får anlita ett annat personuppgiftsbiträde om detta inte har godkänts enligt specifika tillstånd av den personuppgiftsansvarige, samt

- etablera rutiner för agerande om en personuppgiftsincident inträffar.

Vidare måste den personuppgiftsansvarige genomföra en risk- och sårbarhetsanalys med avseende att bedöma om det finns en möjlighet att anlita tänkt molntjänstleverantör för att behandla personuppgifterna samt även vilken säkerhetsnivå som är lämplig och vilka åtgärder som ska vidtas. Desto högre integritetsrisk en personuppgiftsbehandling har desto större blir även kraven på säkerhetsåtgärder. Åtgärder som även bör övervägas är de vad gäller autentisering, behörighetsstyrning, behörighetskontroll, kommunikationssäkerhet, rutiner för säkerhetskopiering och utplåning samt skydd mot obehörig åtkomst och skadlig programvara. Det ska kunna säkerställas konfidentialitet, integritet, tillgänglighet och motståndskraft. Möjligheten ska finnas att återställa personuppgifter vid en incident och det ska även vara möjligt att testa behandlingen av personuppgifter och hur denna säkerhet ser ut. När känsliga personuppgifter ska behandlas krävs det att autentisering ska användas vid överföring av uppgifter i öppet nät samt att dessa uppgifter ska vara skyddade med kryptering. Vidare måste åtkomstkontroller utföras regelbundet och systematiskt för att kunna följa upp vem som har haft åtkomst till vilka uppgifter. Den personuppgiftsansvarige ska se till att för varje person som utför något arbete under den personuppgiftsansvarige och som har tillgång till personuppgifter bara behandlar dessa och utför detta arbete utifrån instruktioner från den personuppgiftsansvarige.

Det finns flera etablerade metoder för risk- och sårbarhetsanalys och de måste utarbetas specifikt för den molntjänstleverantör kommunen ämnar anlita. En av metoderna innefattar att använda sig av en checklista som tagits fram av EU:s nätverks- och informationssäkerhetsbyrå ENISA; Cloud Computing, Information Assurance Framework som används för att bedöma risken att använda sig av molnbaserade lösningar.

Den personuppgiftsansvarige ska även se till att ett personuppgiftsbiträdesavtal upprättas som återspeglar kraven i personuppgiftshanteringen enligt GDPR. De villkor som upprättas i personuppgiftsbiträdesavtalet ska kunna skiljas från övriga villkor som gäller mellan dessa parter och det som upprättas ska ej kunna ändras av personuppgiftsbiträdet. Personuppgiftsbiträdesavtal ska:

- ålägga att personuppgiftsbiträdet har skyldighet att tillämpa svensk lagstiftning avseende personuppgifter,

- ålägga att personuppgiftsbiträdet har skyldighet att vidta lämpliga säkerhetsåtgärder såsom vad gäller vid överföring av personuppgifter till tredjeländer,

- säkerställa att personuppgiftsbiträdet endast har rätten att behandla personuppgifter i enlighet med den personuppgiftsansvariges instruktioner,

- säkra vetskapen om att den personuppgiftsansvarige känner till vilka andra personuppgiftsbiträden som möjligtvis ska komma att behandla den personuppgiftsansvariges personuppgifter,

- säkra vetskapen att den personuppgiftsansvarige på ett korrekt sätt ska kunna följa upp att personuppgiftsbiträden lever upp till de krav som den personuppgiftsansvarige ställer på personuppgiftsbehandlingen,

- säkerställa att tekniska och praktiska förutsättningar existerar för att kunna utreda misstankar om någon hos den personuppgiftsansvarige eller hos något personuppgiftsbiträde haft obehörig åtkomst till personuppgifterna samt

- säkerställa att det är klarlagt vad som händer när avtal hos en leverantör avslutas och vilka åtgärder som då ska vidtas (Datainspektionen, 2018).

2.6 Relaterad forskning

Ali, Soar, Yong, McClymont och Angus (2015) studerar och identifierar faktorer som skulle inverka ifall kommuner i Australien skulle börja användandet av molnbaserade lösningar. Studien använde sig av ramverket technology-organization-environment (TOE) samt modellen diffusion of innovation (DOI) för att tillsammans skapa en modell för att förstå IT-/IS-antagandet och i detta fall antagandet av molnbaserade lösningar. Utifrån detta genomfördes fördjupade intervjuer med australiensiska kommunfullmäktiges IT-chefer. Studien kom fram till att områden som innovationsegenskaper, teknologiska, organisatoriska och miljöfaktorer som skulle påverka ett potentiellt användande av molnbaserade lösningar. Inom dessa områden finns det många faktorer som de har identifierat som behöver utforskas ytterligare för att få en mer djupgående förklaring på varje faktors potentiella inverkan på implementationen av en molnbaserad lösning.

Wyld (2010) presenterar i sin forskning hur molnbaserade lösningar används i olika stater runt om i världen från USA till Europa och Asien. Genom att studera hur molnbaserade lösningar skulle fungera gentemot en annan lösning presenteras komplikationer som skulle kunna uppstå och detta i kontexten för den publika eller privata sektorn. Dessa baseras på åtta kriterier som återfinns i molnmodellen. För att kunna övergå till ett molnkoncept behöver dessa uppnås. Kriterierna är: Universal Connectivity, Open Access, Reliability, Interoperability and User Choice, Security, Privacy, Economic Value samt Sustainability. Förutom dessa tekniska bitar är en stor del av att byta till molnbaserade lösningar från en annan lösning sprungna ur de som ska använda den ersättande teknologin. För att en person ska vilja börja använda sig av en ny teknologi krävs det att denne kan ha tillgång till samma utbud av IT-resurser som de tidigare haft. Studiens slutsatser presenterar hur den offentliga sektorn anses komma att utvecklas på grund av molnbaserade lösningar. Studien anger att molnbaserade lösningar förhoppningsvis kommer att ändra hur den offentliga sektorn beräknar, fungerar, kommunicerar och hur de samarbetar. Men att molnbaserade lösningar även kommer påverka de företag som tillhandahåller IT infrastruktur, mjukvara, support och andra services för detta ändamål och att nya sorts industrier kommer att uppkomma för att kunna förflytta sig till lösningar orienterade runt molnbaserade lösningar.

Sakurai och Kokuryo (2016) studerar hur flera kommuner i Japan förlorade alla sina invånares data inklusive säkerhetskopiorna på grund av en jordbävning år 2011. Studien presenterar alternativ till hur säkerhetskopiorna hade kunnat lagras och hur den japanska staten försökte introducera en molnbaserad lösning för lagring av säkerhetskopiorna.

Ali, Soar och Yong (2017) undersöker utmaningar och problem som kan påverka användandet av cloud computing hos lokala regeringskanslier i Australien. Totalt 480 IT-personal från 47 kanslier deltog i studien. Studien är en kvantitativ enkätstudie där fokus ligger på olika områden som skulle kunna påverka användandet av cloud computing. Resultaten visar att flera aspekter påverkade varför kanslierna var osäkra på att börja använda cloud computing och studien konkluderar att innan detta har fått en lösning kommer inte användandet och spridningen av cloud computing att vara lika omfattande.

3 Problemdefinition

Denna studie är avsedd att utforska kommuners användning av molnbaserade lösningar för säkerhetskopiering och huruvida en sådan implementation har kunnat skapa möjligheter för att utveckla kommuners arbete och hur en sådan implementation fungerar. Eftersom studien kretsar kring molnbaserade lösningar och säkerhetskopiering samt att det är data som lagras på säkerhetskopiorna är det av stor vikt hur personuppgifter hanteras. Därav kommer studien omfatta detta området om personuppgiftshantering. Flera områden är för studien relevanta att få svar på såsom om kommuner har kunnat uppnå besparingar och ifall säkerheten kring data har fungerat. Det är även intressant resultatmässigt att klarlägga hur effektivt en molnbaserad lösning har inverkat på att lagra säkerhetskopior samt vilka effektiviseringsområden som kommuner har kunnat observera. Frågor kring presenterade områden kommer studien fokusera på att besvara.

Sveriges kommuner har ett komplext uppdrag vad gäller funktionaliteten av vårt samhälle. Kommuner har hand om samhällsservice som innefattar förskola, skola, socialtjänst och äldreomsorg. Enligt lag måste kommuner upprätthålla vissa verksamheter. Kommuner har ett ansvar för den samhällsviktiga verksamheten. För att kommuner ska kunna upprätthålla sin samhällsservice ingår att informationshantering fungerar på ett korrekt sätt (Sveriges kommuner och landsting, 2017).

En kommun är en omfattande och komplex organisation där det är viktigt att stöd i form av resurser, kompetens och budget fokuseras för att upprätthålla en välfungerande informationssäkerhet. Myndigheten för samhällsskydd och beredskap (MSB) genomförde på uppdrag av regeringen och i samverkan med Sveriges kommuner och landsting (SKL) en undersökning av informationssäkerheten 2015 där över 230 kommuner medverkade och svarade på enkätfrågor som handlade om systematiskt informationssäkerhetsarbete. Enligt MSB är det positivt att många kommuner har en utpekad funktion för informationssäkerheten. Mindre positivt är dock att denna utpekade funktion förlägger så lite tid på att arbeta med vad som är tänkt att vara dess huvuduppgift. Vid analys av tiden som kommunerna lägger på informationssäkerhet hamnar arbetet med informationssäkerhet under andra arbetsuppgifter. Gällande samhällets beroende av både informationssäkerhet samt teknik och att kommuner har hand om så pass mycket känslig information bör informationssäkerhetsarbetet vara värderat högre, menar MSB. MSB förklarar att 40 % av kommunerna inte har någon definierad funktion alls för deras informationssäkerhet (Myndigheten för samhällsskydd och beredskap, 2015).

Information står ofta i centrum vid en krishantering och utvärderingar har visat att information är en av de största komponenterna vad gäller hantering av en kris. Vid en krissituation är tillgången till korrekt information i rätt tid avgörande (Myndigheten för samhällsskydd och beredskap, 2015). Kommuner har ett viktigt jobb med att ha en fungerande lösning för tillgång till information vid en krissituation.

Under den stora östjapanska jordbävningen år 2011 förlorade flera kommuner sina invånares sparade data, inklusive deras backuper. Detta eftersom backuperna hade sparats på samma ställe som originalfilerna. Eftersom kommunerna inte hade planerat för att potentiellt förlora alla sina data på samma gång stod de nu inför en stor uppgift hur de skulle agera i en krissituation utan tillgång till data om sina invånare (Sakurai m.fl., 2016).

Att kommuner alltid har tillgång till deras information i form av säkerhetskopior är av yttersta signifikans. Användningen av molntjänster för säkerhetskopiering inom kommuner presenterar ett spännande område att utforska. Enligt Datainspektionen (2018) används molnbaserade lösningar i allt större utsträckning inom kommuner, myndigheter och företag.

Vad gäller molnbaserade lösningar för kommuner finns det ett flertal aspekter att nyttja. Genom användning av molnbaserade lösningar kan drift och underhåll överlåtas till molntjänstleverantören och denne ansvarar då för hårdvara och lokaler. Detta medför även att besparingar kan möjliggöras avseende kostnader att tillhandahålla egna system. Genom att inte lagra sina säkerhetskopior på en annan fysisk plats utan att i stället lagra dem hos en molntjänstleverantör kan katastrofskador som till exempel brand eller jordbävning motverkas. Genom att använda en molnbaserad lösning från en molntjänstleverantör finns möjligheten att skala upp eller ned gällande resurser utefter behovet från

verksamheten. Om denna implementation inte används är detta något som är mer svåruppnåeligt då en organisation måste ha hand om sin egen utrustning där information lagras (Velte m.fl., 2010). Dessa aspekter är endast några exempel som en kommun kan nyttja från en molntjänstleverantör genom att överlåta arbetsuppgifter till molntjänstleverantören för att minimera och effektivisera arbetsuppgifter.

Den fråga som kommer att besvaras i denna studie är följande forskningsfråga:

Hur ser användningen av molnbaserade lösningar för lagring av säkerhetskopior ut hos kommuner i Sverige?

Följande underfrågor kommer att komplettera forskningsfrågan:

Vilka fördelar samt nackdelar finns för kommuner med molnbaserade lösningar för säkerhetskopiering?

Hur ser hanteringen ut av personuppgifter gällande molnbaserade lösningar för säkerhetskopiering i kommuner?

Vilka effekter har kommuner som använder molnbaserade lösningar som implementation för säkerhetskopiering kunnat se?

3.1 Förväntade resultat

Målet med denna studie är att kunna presentera hur användningen av molnbaserade lösningar ser ut för säkerhetskopiering och hur detta hanteras i Sveriges kommuner. Genom insamlade data kommer studien att tillgodose hur situationen gällande användning av molnbaserade lösningar för säkerhetskopiering ser ut i dagsläget. Genom slutsatserna och resultaten från studien kommer denna studie att kunna användas som en indikation på om en kommun skulle se fördelar eller nackdelar med att använda sig av en molnbaserad lösning för säkerhetskopiering. Studien kan ses som ett dokument som kommuner kan läsa igenom för att få en övergripande bild över hur användningen av molnbaserade lösningar för säkerhetskopiering ser ut hos kommuner i Sverige i dag. Utifrån detta skulle nästa steg kunna vara att undersöka om kommunen skulle vara aktuell för en sådan implementation.

4 Metod

I följande kapitel diskuteras forskningsmetoden som låg till grund för studien.

4.1 Enkätstudie

För att kunna besvara studiens frågeställning användes en enkätstudie. Enligt Berndtsson m. fl. (2002) innefattar metoden enkätstudie att använda sig av en enkät och vidare statistiska tekniker för att kunna analysera de data som har samlats in. En enkätstudie används för att utforska ett relativt välkänt ämne där det finns tillgång till en stor bas av respondenter som har vetskap ämnet som studeras. Fördelar med enkätstudie är att med hjälp av begränsade verktyg kan enkäten få en stor spridning och nå ut till många respondenter och på detta sätt kan många informanter fångas upp. En enkätstudie går oftast även att utföra under en kort tidsperiod. Detta gjorde metoden lämplig för denna studie då den skulle utföras under ett relativt kort tidsspektrum. Vidare beskriver Berndtsson m. fl. (2002) att andra positiva egenskaper med enkätstudier innefattar möjligheten att kontrollera enkätstudien med hjälp av en väl utformad enkät för att minimera oklarheter som till exempel otydliga frågor. Denna studie nyttjade ett kvantitativt angreppssätt i utvecklingen av enkäten, detta för att utefter studiens frågeställning kunna presentera resultat statistiskt med grafer (Berndtsson m.fl., 2002).

Genom att säkerställa att frågorna i en enkät är så tydliga som möjligt och inte kan missuppfattas kan svaren på frågorna bli så utförliga som möjligt, vilket resulterar i att kvalitén på studien höjs (Wohlin m.fl., 2012).

Några negativa aspekter med en enkätstudie är att det inte går att förtydliga frågor eftersom ingen tvåvägskommunikation sker mellan den ansvariga och respondenten. Fält som tillåter löpande text kan användas för att förtydliga vissa frågor (Berndtsson m.fl., 2002). Huvuddelen av enkäten bestod av frågor av det kvantitativa slaget men kvalitativa frågor förekom även, detta för att få ett förtydligande till varför respondenten valde att svara så som de gjorde. Vidare användes även kvalitativa öppna frågor i enkäten.

Enkäter kan skapas både i pappersform och i elektronisk form. Den vanliga metoden är att skicka ut en enkät och tillsammans med den bifoga instruktioner för tillvägagångssätt för att fylla i den. Respondenten går igenom enkäten, svarar på frågorna och skickar sedan in den (Wohlin m.fl., 2012). För att denna studie skulle vara genomförbar och för att enkäten skulle kunna spridas till alla kommuner i Sverige skapades en elektronisk enkät som skickades ut via mejl.

Det finns flera olika alternativ när det kommer till elektroniska enkäter. För att konfidentialitetskravet ska uppfyllas gällande etik för denna studie är det viktigt att ingen personlig information samlas in. Detta är ett problem med flera olika elektroniska enkäter. Limesurvey är ett enkätverktyg som är ett projekt byggt på öppen källkod och kan administreras av enkätskaparen. Genom att använda Limesurvey uppfylls konfidentialitetskravet då ingen personlig information samlas in av enkätverktyget (Schmitz, 2018).

4.2 Urval

Kommuner är urvalet som har gjorts i denna studie då alla Sveriges kommuner erbjöds att medverka. Alla kommuner kunde besvara enkäten då studien avsåg att utforska både de kommuner som använder molnbaserade lösningar för säkerhetskopiering men även de som inte gör det. Sveriges kommuner varierar i storlek vad gäller invånarantal och anställda inom kommunen. Detta återspeglar såklart hur en kommun är uppbyggd efter resurser och vilka möjligheter som finns utifrån detta. Hade en viss typ av kommuner inkluderats hade troligen en viss sorts resultat uppnåtts. Men då hade möjligtvis studien blivit väldigt styrd och hade antagligen fått problem med validitetshot. Att inte avgränsa studien till att enbart inkludera till exempel kommuner med ett visst antal invånare eller anställda inom en kommun och att inkludera alla kommuner innebär att resultaten från studien blir av högre kvalité och mer generella, vilket gör studien mer användbar.

Innan enkäten kunde skickas ut till kommunerna behövdes kontaktuppgifter till personer inom kommunerna som hade en ledande roll inom tillhandahavandet av IT-infrastrukturen. Kommunerna kontaktades via mejl där de fick ett kort meddelande om en förfrågan att tillgodose ovannämnda kontaktuppgifter till vederbörande inom deras kommun. Denna kontaktuppgift användes sedan för att sprida enkäten till de som var ämnade som respondenter.

4.3 Validitetshot

Validitetshot är något som behöver beaktas för en studie. De validitetshot som kommer att diskuteras och kan vara applicerbara för denna studie faller inom fyra områden. Dessa områden är slutsatsvaliditet, internvaliditet, konstruktionsvaliditet samt externvaliditet Wohlin m. fl. (2012).

Inom *slutsatsvaliditet* finns det två validitetshot som är tillämpningsbara, dessa två är *Low statistical power* och *Fishing and the error rate*. För att få en så god svarsfrekvens som möjligt bjöds alla Sveriges kommuner in till att delta i studien, detta för att motverka *Low statistical power* vilket betyder att ifall det finns ett för litet underlag kan fel slutsatser fås. *Fishing and the error rate* betyder att forskaren försöker fånga upp ett specifikt svar från respondenterna och därmed få ut ett resultat som forskaren vill uppnå, genom att inte vinkla några frågor i enkäten kan detta validitetshot motverkas.

Vad gäller internvaliditet är *Instrumentation* och *Maturation* applicerbara. *Instrumentation* betyder att ifall de medel som används för att samla in data för studien är dåligt designade så kan detta påverka studien negativt. Genom att designa en enkel och lättfattlig enkät motverkas detta validitetshot. *Maturation* handlar om att de som deltar i enkäten blir trötta eller uttråkade, detta validitetshot kan motverkas genom att skapa en kort enkät där endast de väsentligaste frågorna inkluderas så att respondenten utför enkäten till sin bästa förmåga.

För validitetshoten inom konstruktionsvaliditet är det I*nadequate preoperational explication of construct* och *Evaluation apprehension* som är applicerbara. Genom att definiera eventuella koncept tillräckligt väl i enkätfrågorna motverkas *Inadequate preoperational explication of construct* genom att tydliggöra vad det är enkätfrågorna efterfrågar. Gällande *Evaluation apprehension* som betyder att deltagare kan försöka framstå som bättre än de i själva verket är när de blir utvärderade kan detta hot motverkas till viss grad genom att inte vinkla några frågor som skulle försöka få en kommun att framstå som bättre än en annan kommun.

Det validitetshot som är applicerbart gällande externvaliditet är *Interaction of selection and treatment*. Med detta menas att fel personer deltar i en undersökning. Detta hot kan inte motverkas helt men till stor del. I denna studie motverkades detta genom att delge information om att studien ämnade att få in svar från respondenter som har en ledande roll på kommunerna angående deras IT-infrastruktur samt att de mejladresser som samlades in är faktiska mejladresser till dessa personer.

4.4 Etik

Gällande denna studie och de etiska krav som finns baserades dessa på Vetenskapsrådet (2002) som ställer upp fyra etiska krav: informationskravet, samtyckeskravet, konfidentialitetskravet och nyttjandekravet. För att denna studie ska uppfylla dessa fyra krav vidtogs ett flertal åtgärder, vilka beskrivs nedan.

I och med deltagande i studien fick respondenterna information i början av enkäten om studiens och enkätens syfte. På så vis uppfylls informationskravet. Samtyckeskravet kan uppnås genom att de som tillfrågas vara med i enkäten inte på något sätt ska känna sig tvingade att deltaga i enkäten och informeras om att deltagandet är frivilligt. Vad gäller konfidentialitetskravet och nyttjandekravet kan dessa två uppfyllas genom att undvika att samla in personliga data genom enkäten. De data som samlades in var endast de som var nödvändiga för att besvara studiens forskningsfråga.

4.5 Dataanalys

En likertskala är en summationsskala där resultatet från flera frågor tas och dessa sedan sammanställs. Meningen med en likertskala är att respondenterna inte ska svara ”Ja” eller ”Nej” utan att de i stället ska få välja hur mycket de instämmer eller håller med om påståendet i varje fråga (Statistiska centralbyrån, 2016).

Vad gäller analys av data från en likertskala är alternativen kraftigt begränsade. Förklarande mått och statistik som till exempel medelvärde och standardavvikelse är svåra att applicera vid analys av data från en likertskala. Till exempel är det svårt att förklara vad genomsnittet av ”Aldrig” eller ”Sällan” verkligen betyder. Exempelvis blir ”Sällan och en halv” inget som går att räkna på då det inte har någon användbar betydelse. Ifall svaren från likertskala-frågorna är överrepresenterade på extremnivåerna av högt och lågt skulle medelvärdet beräknas vara enligt det neutrala eller mittensvaret på likertskalan, detta är ännu en anledning till varför medelvärde och standardavvikelse inte kan tillämpas för att representera data. På grund av detta var det i denna studie inte möjligt att räkna på medelvärde eller standardavvikelse för analysen av likertskala-data då dessa värden inte skulle vara ett statistiskt korrekt sätt att beräkna central tendens. Övriga data-analyser som kräver att ett medelvärde har räknats ut exkluderas därför också (Journal of Graduate Medical Education, 2013).

Enkätfrågorna skapades på så vis att de kunde besvaras genom att tillämpa en likertskala. Genom att ha en likertskala kunde resultat från frågorna enkelt presenteras och sedan analyseras. Vissa av frågorna ställdes som öppna frågor där resultatet vägdes ihop, sammanställdes och sedan analyserades.

Stapeldiagram användes för att visualisera resultatet från frågorna som var av kvantitativt slag och för att vidare sen analysera svaren. Detta för att skapa en lättbegriplig bild över respondenternas svar på enkätfrågorna. Den vertikala axeln i stapeldiagrammen redogör antal svar och den horisontella presenterar svarsalternativen för enkätfrågan. De flesta enkätverktyg har fördefinierade funktioner för att räkna ut andelar av alla svar för varje fråga och sedan möjlighet att exportera de färdiga diagrammen.

Wahlin (2011) återger att för enkäter där helt öppna frågor återfinns kan inte dessa analyseras statistiskt, i stället görs en sammanställning av resultaten från frågan för att de mest centrala delarna ska kunna utvinnas. Detta tillvägagångssätt valdes för analysen av de öppna frågorna som återfinns i studiens resultat. Analys av frågor sinsemellan applicerades också för att se om det fanns samband eller olikheter mellan frågorna.

4.6 Design av enkät

Wahlin (2011) skriver att vid skapandet av en enkät finns vissa saker som forskaren behöver ha i åtanke. Det är rekommenderat att inleda enkäten med följeinformation som innehåller: vad undersökningen handlar om, vem som har skickat enkäten, när enkäten senast ska besvaras, hur respondenten kan ta del av resultaten från undersökningen samt hur respondenten ska gå tillväga om de behöver hjälp angående enkäten.

Anonymitet ska aldrig utlovas eftersom detta aldrig kan garanteras, dock är det viktigt att enkäterna behandlas konfidentiellt. Detta bör framgå i följeinformationen.

Genom att eftersträva enkelhet i frågorna och hålla dem korta, koncisa och ha ett enkelt språk minskar detta risken för feltolkning. Frågorna i enkäten bör formuleras neutralt och inte vara ledande, detta för att åsikter från den som skapar enkäten ej får förekomma på så sätt att det på något sätt skulle påverka respondenterna.
Antalet frågor bör vara relativt få genom att endast ställa frågor som konkretiserar problemställningen. Om det är lämpligt kan enkäten avslutas med en öppen fråga. Även om den inte kan analyseras med statistiska metoder kan en öppen fråga ge intressant information som ytterligare belyser problemställningen (Wahlin, 2011).

Enkäten avslutades med ett tack till respondenten för deras deltagande samt kontaktuppgifter som kunde användas ifall frågor kring enkäten eller studien skulle uppstå.

4.8 Enkätfrågor

Frågorna i enkäten baserades på tidigare studier inom området av Ali m. fl. (2015) samt Ali. m.fl. (2017). Detta för att kunna utforma frågor relevanta för denna studies problemformulering. Då tidigare forskning behandlade området om molnbaserade lösningar fanns det flera områden och frågor som ansågs tillämpliga att basera och utforma frågor för i denna studies enkät för att kunna besvara forskningsfrågorna.

4.9 Sökning efter relaterad forskning

Sökningen efter relaterad forskning genomfördes genom att söka i databaser efter forskningsartiklar som har blivit peer reviewed. De söktermer som användes i sökningarna var: *cloud computing municipalities*, *cloud computing backup municipalities*, *cloud computing data backup municipalities*, *cloud computing*, *molnlagring* samt *molnlagringstjänster*.

4.10 Pilottest av enkät

Innan den slutgiltiga enkäten skickades ut till respondenterna på kommunerna utfördes ett pilottest av enkäten. Genom att utföra ett pilottest kan detta användas för att reda ut ifall det är några frågor som är otydliga, kan missuppfattas eller om några frågor saknas. Ytterligare aspekter som kan undersökas är exempelvis hur lång tid det tog att slutföra enkäten. Detta kan sedan tas i beaktande och frågor kan behöva arbetas om och andra delar av enkäten justeras, detta för att få en så bra och förståelig enkät som möjligt. Ett pilottest är tänkt att utföras av utomstående personer då den som utför studien oftast själv missar viktiga saker som andra personer uppfattar.

Fyra studenter från högskolan i Skövde fick utföra pilottestet av enkäten och fick efteråt besvara nedanstående frågor.

- Tycker du det saknas någon fråga?
- Var alla frågor förståeliga?
- Finns det några frågor som upprepas eller någon onödig fråga?
- Behöver något i enkäten förtydligas?
- Är svarsalternativen för frågorna rimliga?
- Hur lång tid tog enkäten att utföra?

Studenterna som utförde pilottestet ansåg att frågorna verkade tillräckliga, att de var förståeliga och ej otydliga. Den feedback som erhölls från de studenter som utförde pilottestet var att svarsformen för två av frågorna behövde ändra karaktär för att frågan skulle kunna besvaras korrekt samt att enkäten tog cirka 5 minuter att slutföra.

5 Resultat och analys

I detta kapitel kommer resultat och analys från studien att presenteras.

5.1 Godtycklig svarsfrekvens

Att veta att resultaten från en studie är godtyckliga för att representera en population är ett viktigt verktyg för att försäkra sig om studiens validitet. För att kunna beräkna en godtycklig representation av en population kan Cochrans formel tillämpas. Cochrans formel användes i denna studie då den ansågs lämplig att använda eftersom studien använde likertskalor samt eftersom den räknar ut vad som eftersöks och om studien har uppnått en godtycklig svarsfrekvens eller ej. Cochrans formel används normalt sett i situationer för att räkna på större populationer. Då denna studie har ett mindre omfång att förhålla sig till användes den modifierade versionen av Cochrans formel framtagen för mindre populationsberäkningar. För Cochrans formel krävs en konfidensnivå (generellt 95 %), vilket innebär att i 95 % av fallen kommer studien att producera liknande resultat. Förutom detta kräver formeln även ett konfidensintervall. Detta kan vara ett exakt värde (Z-index) eller ett bestämt värde, i vanliga fall 5 % vilket betyder att resultatet kan variera 5 % (positivt och negativt). Det observerade deltagandet i studien behöver vara större eller lika med resultatet från Cochrans formel för att räknas som en godtycklig svarsfrekvens.

Cochrans formel:

$$n_0 = \frac{Z^2 pq}{e^2}$$

Modifierad version av Cochrans formel för uträkning vid mindre populationer:

$$n = \frac{n_0}{1 + \frac{(n_0 - 1)}{N}}$$

Populationen av Sveriges kommuner är 290 och antalet medverkande kommuner var 67. Med dessa siffror fanns tillräckliga data för att utföra beräkningen.

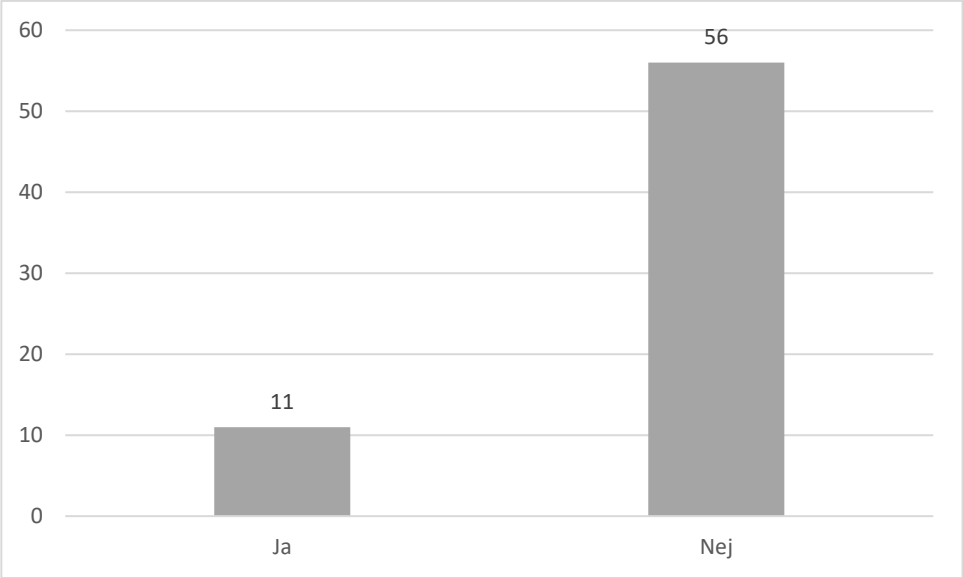
Beräkning enligt nedan:
67 / (1+(66/290)) = 54,58 ≈ 55

Efter att ha utfört beräkningen blev svaret att det totala antalet svar som behövdes var 55. Detta är det minimala antalet respondenter som behövdes för att uppfylla konfidensnivån på 95 % tillsammans med konfidensintervallet på 5 %. Då studien fick 67 totalt svarande uppnår studien en godtycklig svarsfrekvens (Israel, 2018).

5.2 Introduktionsfrågor

Den första frågan i enkäten var ”Vilken kommun representerar du?” Denna fråga var till för att säkerställa att inga dubbla svar samlades in från en och samma kommun, och därav kommer resultaten från denna fråga ej att presenteras. Vid sammanställningen av svaren framgick att två svar ej var användbara. Detta innebar i sin tur att det totala deltagarantalet blev 67 kommuner av totalt 290.

Den andra introduktionsfrågan var ”Använder er kommun molnbaserade lösningar för säkerhetskopiering?” Hur kommunerna svarade presenteras i tabellen nedan. Resultatet visar att den största delen kommuner i Sverige, 84 % av de tillfrågade kommunerna inte använder sig av molnbaserade lösningar för säkerhetskopiering och att en mindre mängd, 16 % använder sig av detta.

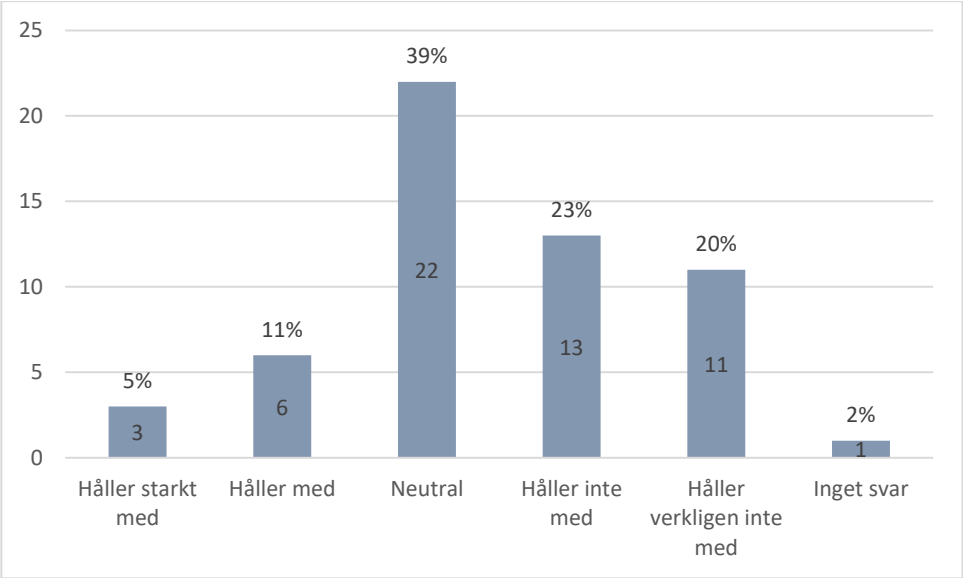


Figur 1. Resultat om användning av molnbaserade lösningar för säkerhetskopiering hos svarande kommuner.

5.3 Följdfrågor

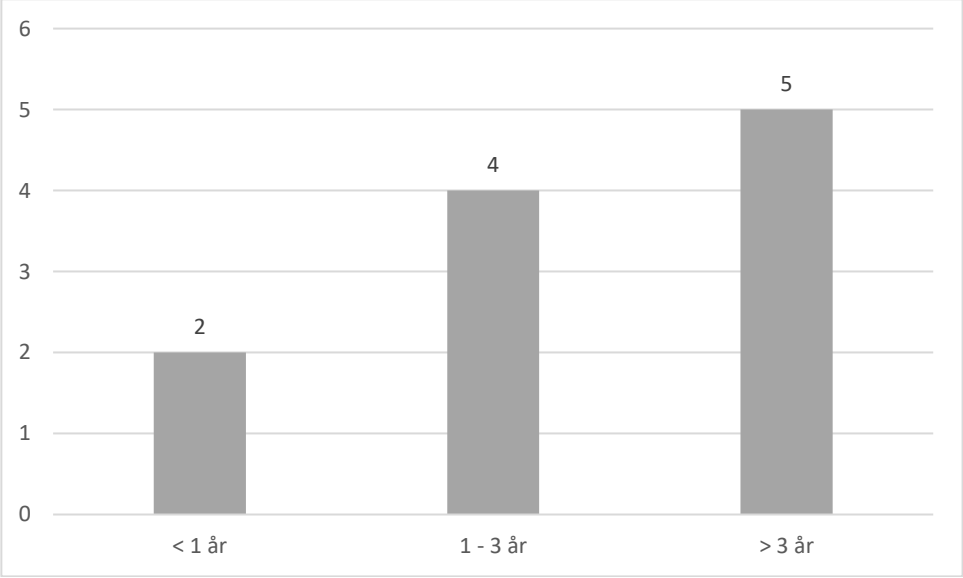
Varför använder sig er kommun ej av molnbaserade lösningar för säkerhetskopiering?

Kommuner som ej använder sig av molnbaserade lösningar för säkerhetskopiering grundade sig i att de i stor utsträckning har en egen väl fungerande infrastruktur för säkerhetskopiering. Detta i en egen serverhall eller genom lagring på annan fysisk plats och. Denna lösning ej kommer att bytas ut så länge den fungerar. En kommun motiverade detta med ”Återläsning och skrivning till backup går snabbare med 10gb i backbonet än att överföra data på en internetlina med betydligt långsammare överföring.” En annan kommun nämnde att vad gäller säkerhetskopiering är lokal lagring både kostnads- och platseffektivt vid tillhandahållande av egen serverhall. Kommuner nämnde att det i stor utsträckning är kostnadsskäl som ligger till grund för varför kommuner inte använder sig av en molnbaserad lösning; det anses billigare att ha drift på plats. Vad som även nämndes omfattande var juridiska överväganden, säkerhet och integritet och vad dessa faktorer spelar för roll när en kommun har planerat att använda sig av molnbaserade lösningar just eftersom kommuner hanterar information som anses känslig såsom personuppgifter. Kommuner uppgav att de inte känner sig säkra med att överlåta hantering av personuppgifter till extern part. Många kommuner återgav att de vill ha sina data ”inom egna väggar”, detta för att det medför större kontroll samt även tillgänglighet för dem. Vidare har flera kommuner policyer som begränsar användning av molnbaserade lösningar. Dock uppgav vissa kommuner att de kommer att testa en molnbaserad lagring men kommer att behålla den befintliga lösningen under tiden. Det framkom även av frågan att när avtal går ut eller när kommunen avser ersätta existerande lösning kommer övervägandet om molnbaserad lösning att vara aktuellt. Då kommer de två stora faktorerna för eventuellt införande vara informationssäkerhetsaspekter och kostnadsaspekter. Det som även omnämndes var att kapacitet i nätverk har begränsat deras möjlighet till att implementera en molnbaserad lösning för säkerhetskopiering. Analys av detta visar att det är oftast mer än en faktor som ligger till grund för beslutet av en kommun att inte använda en molnbaserad lösning för säkerhetskopiering.



Figur 2. Vår kommun har planer på att införskaffa molnbaserade lösningar för säkerhetskopiering i framtiden.

När kommunerna som inte använder en molnbaserad lösning för säkerhetskopiering skulle svara på påståendet om de hade planer på att införskaffa detta i framtiden uppgav 16 % att de höll med om detta påstående till någon grad och har planer på detta. Resultaten visar att 43 % inte håller med till någon grad. Detta överensstämmer med resultaten från föregående fråga där kommunerna uppgav ett flertal anledningar till varför det inte anses aktuellt att använda eller införskaffa detta. Dock ställde 39 % sig neutrala till frågan. Detta kan relateras till att vissa kommuner har en lösning som de är nöjda med för tillfället men de kan tänka sig att testa en molnbaserad lösning, vilket uppgavs som svar på de öppna frågorna.



Figur 3. Hur länge har er kommun använt sig av molnbaserade lösningar för säkerhetskopiering?

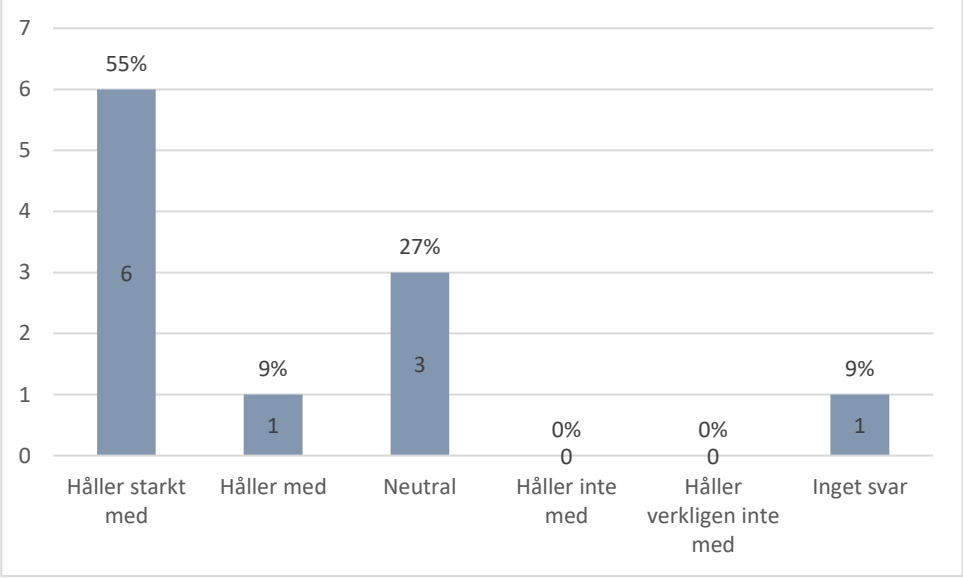
Av de 11 kommuner som använder sig av molnbaserade lösningar för säkerhetskopiering framgår av resultaten att 46 % har använt det mer än 3 år, 36 % mellan 1–3 år samt 18 % i mindre än ett år. Cirka hälften av de tillfrågade kommunerna som använder molnbaserad lösning för säkerhetskopiering har haft denna implementation en längre tid. Dock uppgav mer än hälften av kommunerna att de haft denna implementation mellan 1–3 år och mindre än ett år, vilket får anses som en kort tid. Detta kan än en gång relateras till frågan som ställdes till de kommuner som ej använder sig av molnbaserade lösningar där det framkom många hinder som påverkar användningen. Detta är i linje med tidigare forskning, exempelvis Ali m.fl. (2015), där resultaten visar att användningen av en ny teknologi påverkas av hur tekniskt redo en organisation är. De hinder som omnämndes av kommuner som inte använder molnbaserade lösningar stämmer överens med att de inte känner sig tekniskt redo. Detta återspeglas i resultaten att kommuner på grund av dessa hinder inte använt sig av en molnbaserad lösning en längre tid, detta på grund av att hinder har satt stopp för en tidigare implementation.

Hur ofta görs säkerhetskopior hos er kommun som sedan lagras hos en molnleverantör?

De kommuner som har implementerat en molnbaserad lösning för säkerhetskopior tar säkerhetskopior minst en gång per dygn som sedan lagras hos molnleverantören. Kommunerna beskrev att det kan vara varierande inkrementellt till månatligt och att det sker olika beroende på system. Vissa kommuner har backup som görs direkt i och med en ändring i ett dokument eller liknande. Vidare har vissa kommuner implementerat en kontinuerlig cykel med vecko-, månad- och årsbackuper. Det generella användningsområdet visar sig alltså vara att använda en molnbaserad lösning för att ta säkerhetskopior minst en gång per dygn, men att lösningen oftast inkluderar scheman eller implementationer som varierar vad gäller specifika resurser.

Hur ofta görs säkerhetskopior hos er kommun?

De kommuner som ej använder sig av molnbaserade lösningar för säkerhetskopior utför säkerhetskopior övervägande minst en gång per dygn. Även här gäller specifika säkerhetskopierings-scheman gällande vad det är för informationsinnehåll, känslighet av data samt att de implementerar snapshot. Kommunerna uppgav även att säkerhetskopiering styrs utifrån policyer. Oavsett lösning skiljer sig inte själva säkerhetskopieringen åt något nämnvärt.



Figur 4. Användningen av molnbaserade lösningar för säkerhetskopiering har fungerat bättre än föregående lösningar.

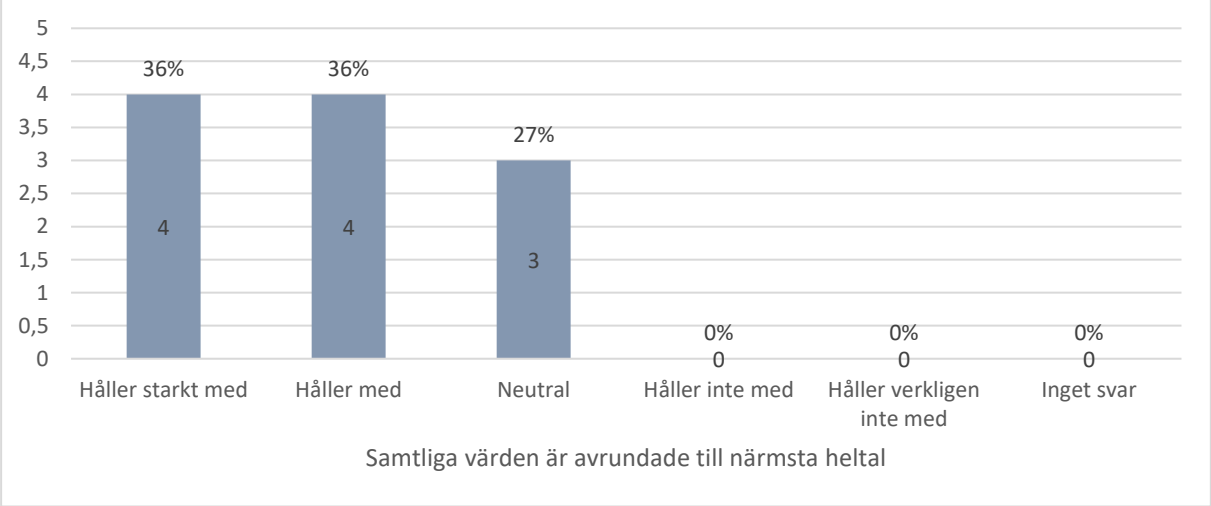
I tidigare studier gjorda av Ali m. fl. (2017) fick respondenterna likt denna studie svara på en skala. I studien fick respondenterna indikera med alternativen starkt oviktigt, oviktigt, lätt oviktigt, neutral, lätt viktigt, viktigt och starkt viktigt med hur mycket de höll med om frågans påstående. Gällande var data befinner sig vad gäller lagringsställe och hur en molnbaserad lösning fungerar med tanke på policyer och hur information hanteras framgår det av studien gjord av Ali m. fl. (2017) att 32 % anser detta vara starkt viktigt, 23 % att det är viktigt och 38 % att det är lätt viktigt. Hela 93 % anser detta vara viktigt till någon grad. Då informationshantering och lagring är den stora aspekten gällande säkerhetskopiering fångar denna fråga i denna studie upp om de som använder molnbaserade lösningar för säkerhetskopiering anser att detta har fungerat bättre än deras tidigare lösning. Jämförs studien gjord av Ali m. fl. (2017) med denna studie är det totalt 64 % i denna studie som anser att en molnbaserad lösning har fungerat bättre än tidigare lösning. Tidigare studie av Ali m. fl. (2017) påvisar hur viktigt detta området anses vara och det bekräftas av denna studie med att validera att de som implementerat en molnbaserad lösning för säkerhetskopiering anser att den har fungerat bättre än föregående lösningar.

Vad för sorts molnbaserad lösning för säkerhetskopiering använder sig er kommun av?

De molnbaserade lösningar som kommuner nämnde är bland annat en hybridlösning och att de skickar iväg en kopia till en plats utanför kommunen. Privata outsourcingleverantörer dominerade respondenternas svar, exempelvis Atea och Azure Storage omnämndes. Många kommuner ser enkelheten med privata outsourcingleverantörer och det är därför detta är mest förekommande.

Vilken eller vilka lösningar för säkerhetskopiering använde er kommun sig av innan?

Innan kommuner använde sig av en molnbaserad lösning hade de oftast en så kallad på plats-lösning där allt fanns lokalt i kommunen med till exempel bandrobot eller liknande. En leverantör som nämndes är Microsoft DPM.



Figur 5. Lagringen av säkerhetskopior med hjälp av molnbaserade lösningar har effektiviserat verksamheten för vår kommun.

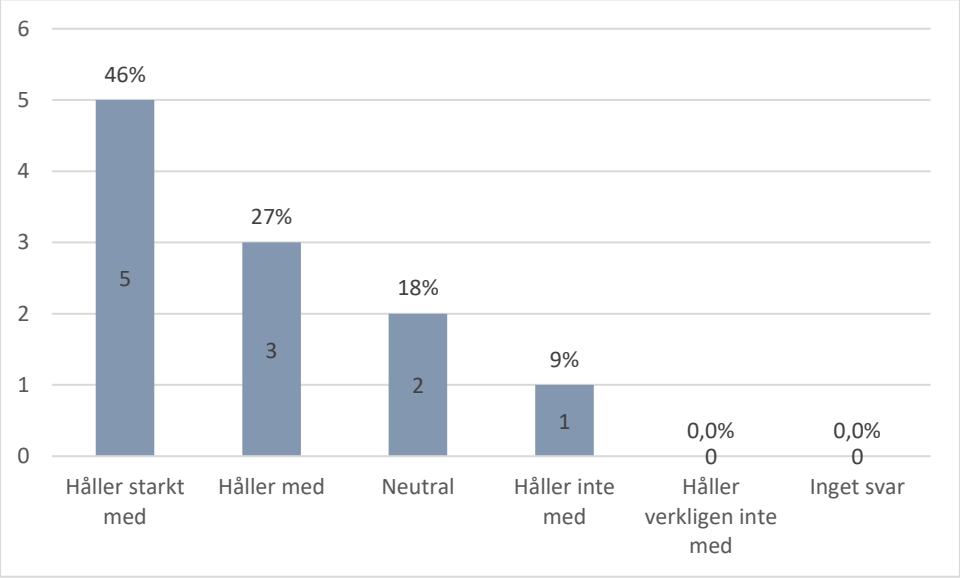
Resultatet av denna fråga visar att 27 % ställde sig neutrala till påståendet ifall molnbaserade lösningar har effektiviserat kommunens verksamhet. Dock uppgav 72 % att de höll med eller starkt höll med om påståendet. Resultaten påvisar alltså att kommunerna har kunnat effektivisera sin verksamhet till följd av en implementation av molnbaserade lösningar. Effektivitet var en av forskningsfrågorna till denna studie, samt att se till vilka för -eller nackdelar som molnbaserade lösningar har kunnat tillföra. Vilka effekter som kunnat uppnås presenteras i nedanstående fråga.

Vilka sorts effekter hos er verksamhet har er kommun kunnat se till följd av implementationen av molnbaserade lösningar för säkerhetskopiering?

Effekter som kommuner har kunnat uppnå är minskad datalagring och kostnad för säkerhetskopiering. Detta har kunnat uppnås eftersom arbetskostnad, lagringskostnad samt mjukvarukostnad och hantering av underhåll för infrastruktur har minskat i den interna miljön. Kommuner har även uppnått tidsbesparingar för deras personal vilket har lett till ökad kvalitet. Kommunerna beskrev att deras molnbaserade lösning är ett effektivare samt säkrare alternativ gentemot andra lösningar. Kommunerna nämnde även att de nu har ett snabbare och enklare sätt att återställa sina säkerhetskopior och att de inte behöver vara beroende av bandtyper. Vad som även togs upp är aspekten att eliminera hotet att byggnaden med säkerhetskopior brinner ned eller liknande. I tidigare forskning av Sakurai m. fl. (2016) återfinns exemplet där en jordbävning orsakade att flera kommuner i Japan förlorade alla sina data samt säkerhetskopior om sina invånare. Hade en molnbaserad lösning varit implementerad hade detta kunnat undvikas. Vad gäller denna studie bekräftas detta med att en molnbaserad lösning gör att kommuner inte behöver oroa sig för vad som händer med deras data vid en naturkatastrof och att de kan vara säkra på att kunna återställa dessa data trots omständigheter. Vad som även nämndes är aspekter såsom funktionalitet och hög tillgänglighet. Förutom rent fysiska principer som elimineras handlar det därmed även om att kommunerna anser sig kunna spara in både kostnaden för säkerhetskopieringslösningar men även kostnader för anställda och tidsbesparingar inom organisationen. Tidigare forskning gjord av Ali m. fl. (2015) presenterar att effekterna av att använda molnbaserade lösningar bland annat är: ökad produktivitet, effektivitet, pålitlighet och möjlighet till att reducera infrastruktur. De andra stora aspekterna som Ali m. fl. (2015) konkluderar är kostnadsbesparingar som organisation genom att inte behöva tillhandahålla infrastruktur och möjligheter till katastrofåterställning samt snabb återställning för oväntade situationer. De resultat som återfinns från studien av Ali m. fl. (2015) och denna studie överensstämmer utefter vilka effekter som har tillkommit utefter en implementation av en molnbaserad lösning.

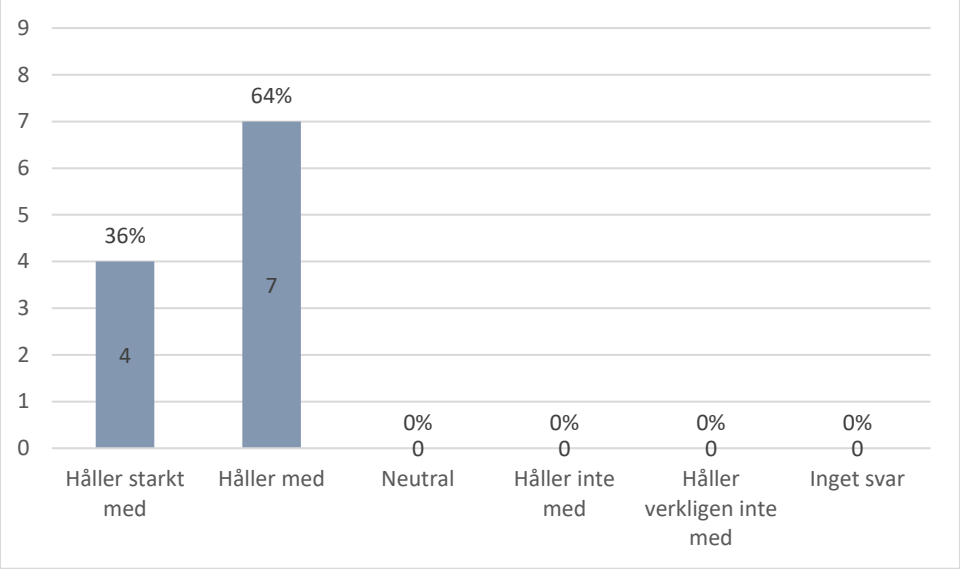
Vad för data är det er kommun sparar på era säkerhetskopior?

De kommuner som använder sig av molnbaserade lösningar för säkerhetskopiering angav att de sparar alla data som hanteras av kommunen, vilket inkluderar offentliga data och handlingar samt systemdata. En kommun nämnde att ”Vi sparar all data som produceras, dock krypteras denna vid både sändning, lagring och nedtagning. Vår backup ligger i enskilt kluster där ingen annan data finns än vår.”



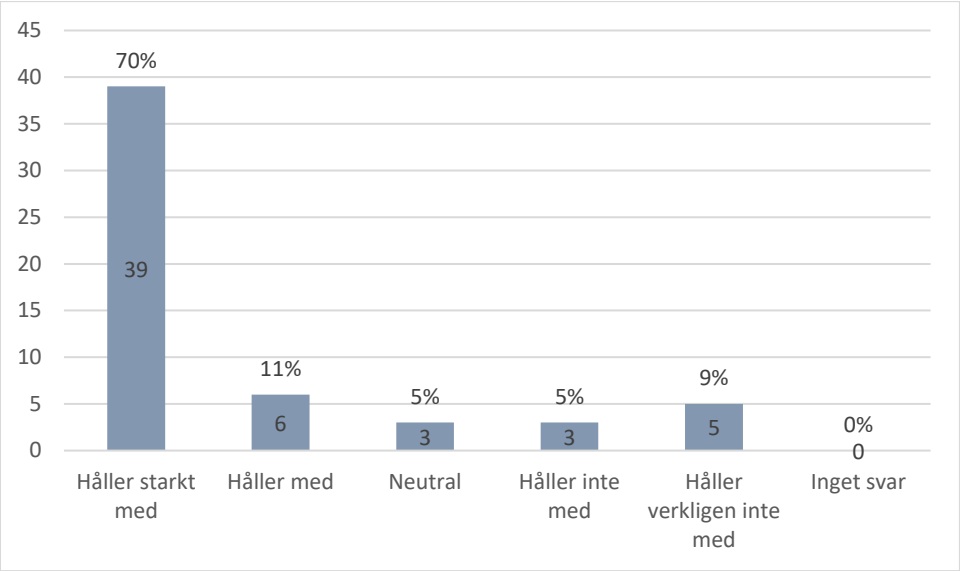
Figur 6. Molnbaserade lösningar för säkerhetskopiering är en stabil lösning vad gäller säkerhetskopiering samt återställning av data.

Utifrån resultaten på denna fråga framgår att en övervägande del av respondenterna anser att molnbaserade lösningar är en stabil lösning vad gäller säkerhetskopiering. Endast en respondent, motsvarande 9 %, höll inte med om att det är en stabil lösning. Tidigare forskning från Ali m. fl. (2015) beskriver att molnbaserade lösningar ger organisationer bättre service vilket innefattar reducerade risker för organisationen men även möjligheten till att ha data lättillgängliga och åtkomliga. Studiernas resultat överensstämmer då reducerade risker som Ali m. fl. (2015) nämner även är något denna studie påvisar då de flesta respondenter instämde om att molnbaserade lösningar skapar stabilitet för kommunen i deras arbete.



Figur 7. Vi känner förtroende till att lagra vår kommuns säkerhetskopior hos en molnleverantör.

Resultaten från denna fråga är övervägande positiva. Samtliga höll starkt med eller höll med om att de känner förtroende för att lagra sina säkerhetskopior hos en molnleverantör. Tidigare studier gjorda av Ali m. fl. (2017) belyser aspekten att en myndighet förlorar kontrollen över sina data när den överlåts att hanteras och lagras hos en molnleverantör. I studien av Ali m. fl. (2017) uppgav 68 % av respondenterna att denna fråga är starkt viktig samt 22 % att detta är viktigt med kommentaren att ifall detta inte sköts korrekt kan det leda till stora negativa konsekvenser. Tidigare forskning tyder alltså på att förtroendet för molnleverantörer inte är stort på grund av säkerhetsfrågor. Detta skiljer sig från vad denna studies resultat visar. Denna studie utfördes hos svenska kommuner och den tidigare studien utfördes hos australiensiska lokala statliga kanslier. Resultaten från de olika studierna gällande detta område kan ha att göra med olika faktorer. Det kan vara så att svenska kommuner har ett större förtroende än australiensiska lokala statliga kanslier med att överlåta förtroende till en molnleverantör. En faktor som kan tala för att svenska kommuner känner sig trygga med att överlåta sina data till en molnleverantör kan vara att de uppgav i enkäten att de upplevt många positiva effekter vid användningen av molnbaserade lösningar för säkerhetskopiering samt att de stött på få problem.



Figur 8. Vår kommuns lösning för säkerhetskopiering är en stabil lösning vad gäller säkerhetskopiering samt återställning av data.

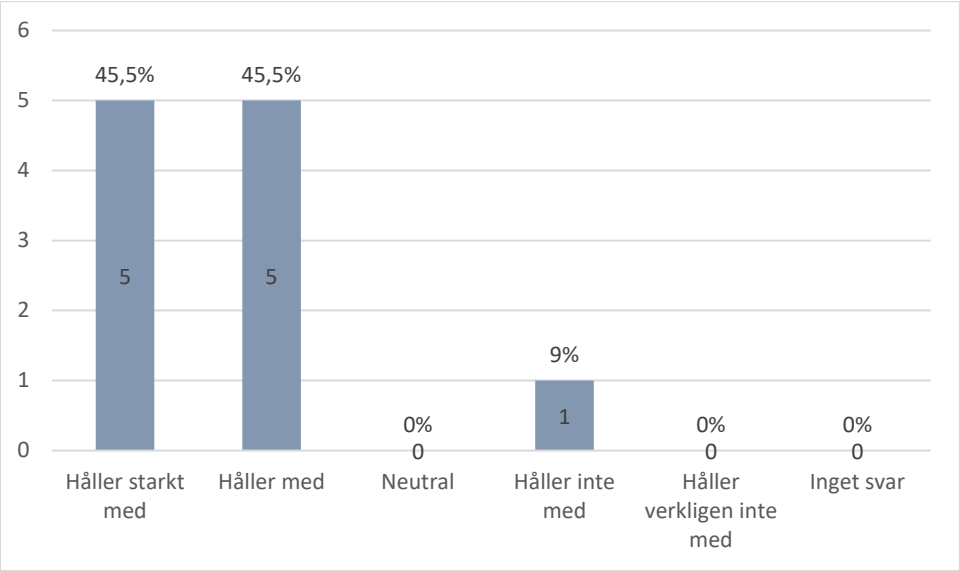
Resultaten från de kommuner som ej använder sig av en molnbaserad lösning för säkerhetskopiering samt återställning av data håller starkt med om att deras nuvarande lösning är stabil. En stor del av respondenterna, 88 %, ansåg detta med håller starkt med och håller med som svar medan 5 % ställde sig neutrala till påståendet och 14 % uppgav att de inte håller med i varierande utsträckning. Anledningen till att dessa 14 % valde att svara som de gjorde kan bero på att kommunen har för avsikt att gå över till en molnbaserad lösning, vilket denna studie påvisar att flera kommuner är öppna för att testa och utvärdera.

Vad för lösning använder sig er kommun av?

De kommuner som tillhandahåller egen lösning för säkerhetskopiering använder sig även av sekundära säkerhetskopieringsprocesser som till exempel snapshot, replikering, säkerhetskopiering till disklagring med en extra kopia på en sekundär plats och egen regelbunden backup. En kommun återgav att de använde sig av en helhetslösning med Fujitsu Siemens hårdvara och deduplicering vilket styrs av Netbackup, allt kopplat till ett SAN via fiberchannel samt via nätverk för enheter utanför SAN:et. En kommun kommenterade ”Vi har 99% virtualiserade servrar och tar snapshots till disk som sen flyttas till band för långtidsförvaring på annan ort.” Lösningar som nämndes är Veeam, Microsoft DPM, Netapp, Altaro, IBMTivoli Storage Manager, IBM Spectrum, IBM TSM, Vmvare, DELL EMC Networker, EMC Avamar, Backup Exec, Veritas Backup Exec, Rapid Recovery samt Asigra arcserve.

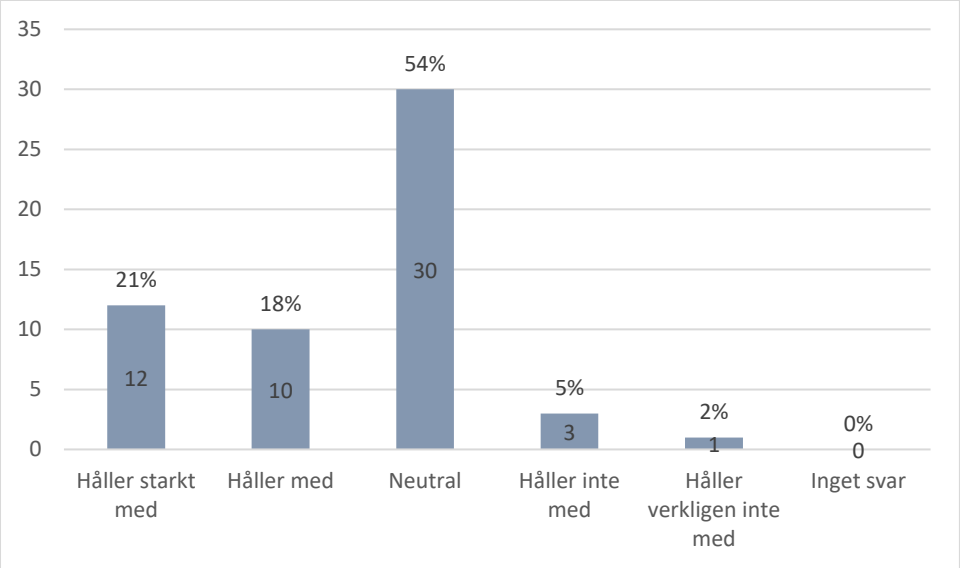
Vad för data är det er kommun sparar på era säkerhetskopior?

De kommuner som ej använder sig av en molnbaserad lösning för säkerhetskopiering besvarade denna fråga med att de sparar alla data som hanteras av kommunen. När de specificerade nämndes data från databaser, kommunens verksamhetsdata, verksamhetssystem, servermiljöer, digital information, filer, applikationer, systemkonfigurationer samt data från informationssystem. Det nämndes även att data sparas som är klassificerade på flera olika vis utifrån spårbarhet, riktighet, tillgänglighet och konfidentialitet. Dock nämnde kommuner att viss information som är av betydelse för rikets säkerhet är undantagen på säkerhetskopiorna.



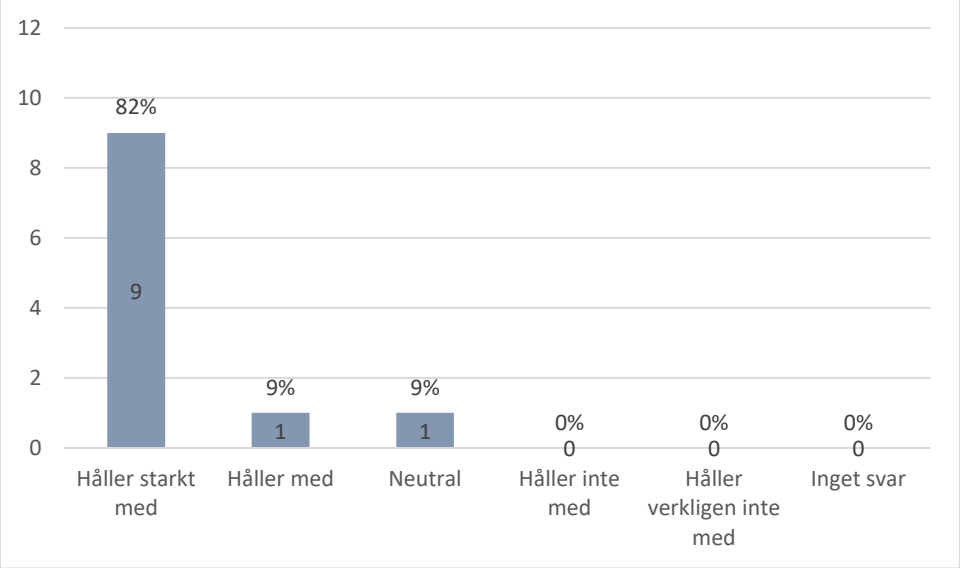
Figur 9. Molnbaserade lösningar för säkerhetskopiering har bedömts vara mer kostnadseffektivt för vår kommun jämfört med andra lösningar.

När frågan ställdes om kostnadsaspekten gällande molnbaserade lösningar och ifall denna har varit mer kostnadseffektiv för kommunen än lösningen de använde innan svarade 45,5 % att de starkt höll med och 45,5 % att de höll med. Resultaten visar att 91 % av kommunerna efter implementeringen av molnbaserade lösningar har kunnat uppnå kostnadsbesparingar. Enligt Ali m. fl. (2017) visar det att 62 % av respondenterna anser kostnad som starkt viktigt och 26 % som viktigt i studiens fråga om kostnadsbesparingar, de svarande beskrev även i frisvarsfrågor att det saknades statistik som kunde påvisa att molnbaserade lösningar verkligen är kostnadseffektivt. Denna studies resultat påvisar att molnbaserade lösningar har visat sig vara kostnadseffektivt, vilket efterlystes i studien av Ali m.fl. (2017).



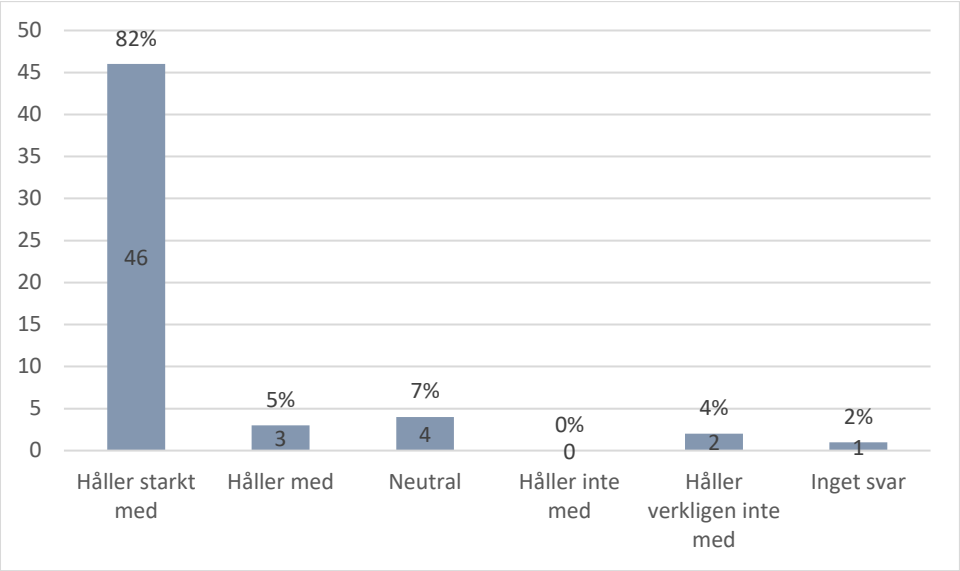
Figur 10. Vår nuvarande lösning för säkerhetskopiering har bedömts vara mer kostnadseffektiv för vår kommun jämfört med molnbaserade lösningar för säkerhetskopiering.

Lite mer än hälften av de svarande ställde sig neutrala till denna fråga, nämligen 54 %. Detta kan bero på att de flesta kommuner inte har testat att implementera en molnbaserad lösning eller inte har gjort några efterforskningar kring de kostnader en molnbaserad lösning skulle innebära. 21 % höll starkt med och 18 % höll med om att deras nuvarande lösning är mer kostnadseffektiv. Kommunerna svarade att kalkyler gällande kostnad har gåtts igenom och olika implementationer har vägts gentemot hur väl fungerande deras nuvarande lösning är och vad kostnadsfrågan för en molnbaserad lösning skulle bli. Flera kommuner nämnde i tidigare frågor att efter att de gått igenom hur en molnbaserad lösning skulle fungera gentemot den lösning de tillhandahåller i dag kom de fram till att en molnbaserad lösning skulle vara för kostsam.



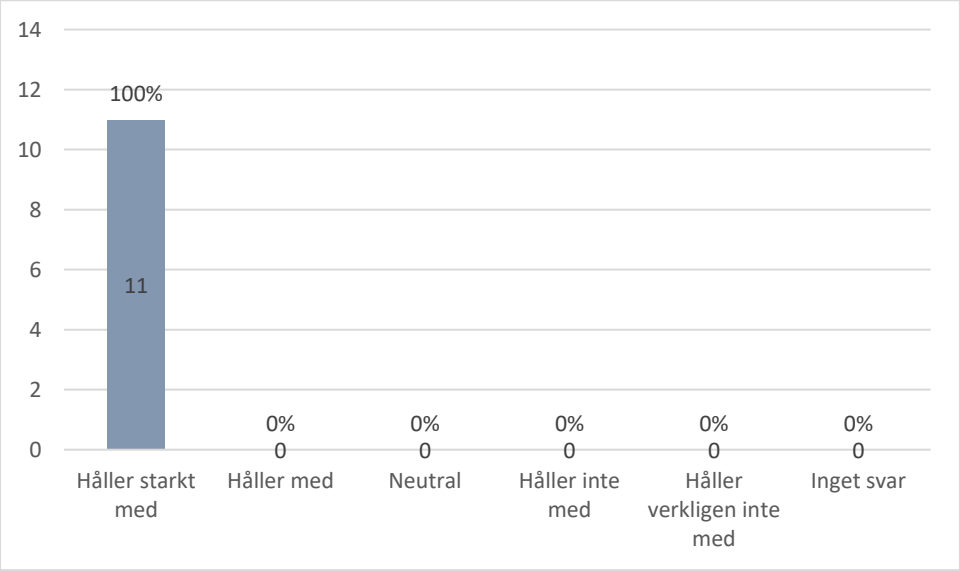
Figur 11. Att molnleverantörer följer lagar och regler avseende de data som lagras hos dem är en viktig aspekt gällande användning av molnbaserade lösningar för säkerhetskopiering.

Något som denna studie avsåg att utforska var säkerhetsfrågor och aspekten om personuppgifter. Resultatet återger att 82 % av respondenterna ansåg att lagar och regler är en viktig fråga då de indikerade att de starkt håller med om detta samt 1 respondent motsvarande 9 % svarade att de håller med. Endast en respondent ställde sig neutral till frågan. Vad som bekräftas i tidigare studier av Ali m. fl. (2017) är att 58 % i den studien när respondenterna blev tillfrågade ansåg säkerhet vara starkt viktigt och 34% ansåg det vara viktigt. Detta innebär att totalt 92 % av den studiens svarande ansåg säkerhet vara en stor faktor. I denna studie ansåg 91 % samma sak. Att säkerhet är en av de viktigaste aspekterna för kommuner att handskas med och att informationen som ska lagras hos en molntjänst har ett stort skyddsvärde är något flera kommuner påpekade.



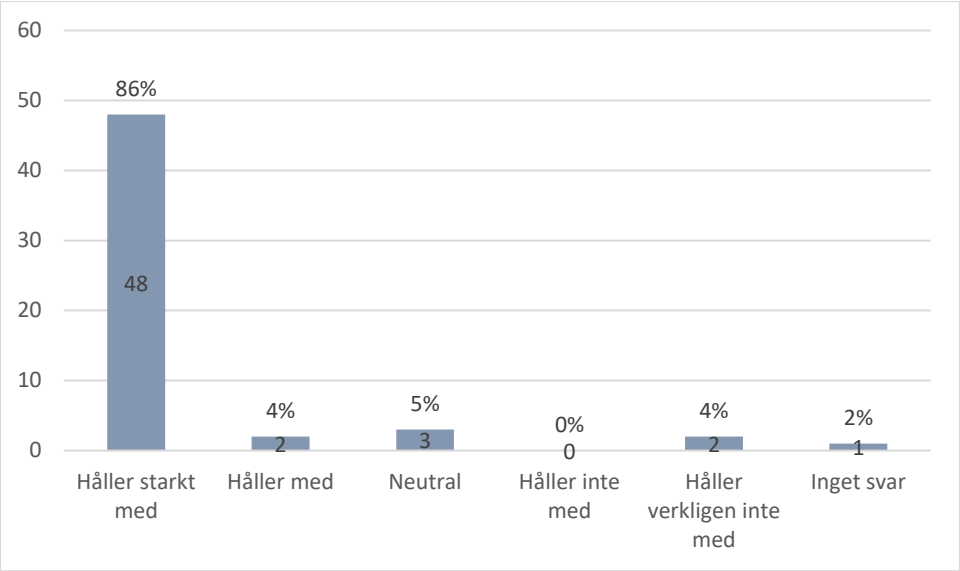
Figur 12. Att lagar och regler följs avseende de data som lagras är en viktig aspekt gällande säkerhetskopiering.

I enlighet med resultaten från föregående fråga återfinns i resultaten att oavsett lagringslösning värderar kommuner säkerhet såsom lagar och regler högt när det gäller deras informationshantering. Vad som är intressant att påpeka är studien gjord av MSB och SKL år 2015 där en undersökning av informationssäkerheten utfördes och 230 svenska kommuner medverkade och svarade på enkätfrågor om systematiskt informationssäkerhetsarbete. Enligt studien har många kommuner en utpekad funktion för informationssäkerhetsarbete, men denna funktion tillägnas ej tillräckligt mycket tid. Detta innebär att även om denna studie förespråkar att lagar och regler är viktigt sett ifrån kommunens sida visar resultat från tidigare studier att kommuner har svårt att omsätta detta i verkligheten.



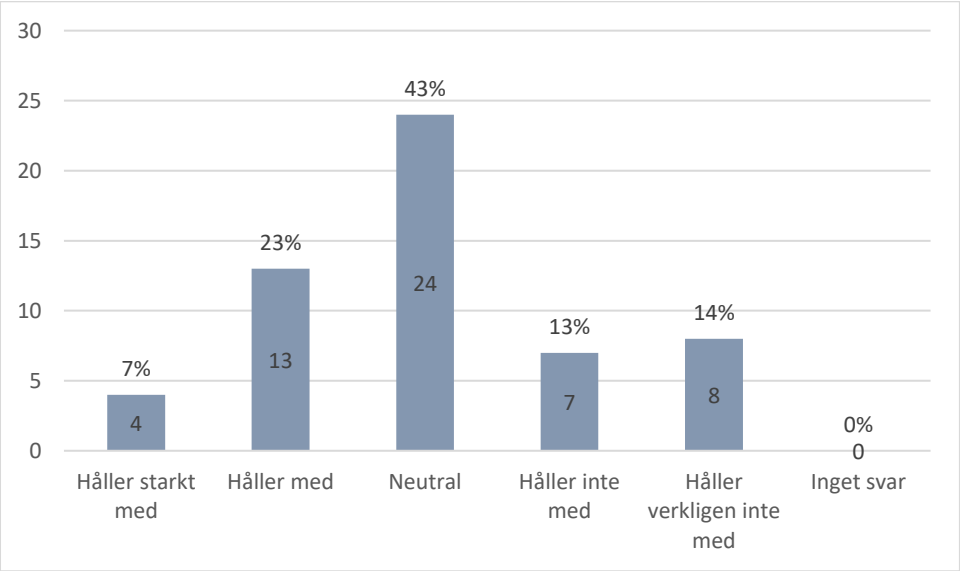
Figur 13. Det är viktigt att användningen av molnbaserade lösningar motsvarar vår kommuns krav på dataintegritet.

På frågan om hur viktigt kommunerna anser att dataintegritet är för dem när de använder sig av molnbaserade lösningar uppgav samtliga att de starkt höll med om att dataintegritet är viktigt. Med de stora mängder integritetskänslig information som kommuner hanterar däribland personuppgifter räknas in, som har ett högt skyddsvärde, blir analysen av detta att med ett resultat där samtliga är för håller starkt med rättfärdigat. Dataintegritet är alltså en betydande faktor vid användningen av molnbaserade lösningar.



Figur 14. Det är viktigt att vår lösning för säkerhetskopiering motsvarar vår kommuns krav på dataintegritet.

Likt svaren där de kommuner som använder sig av molnbaserade lösningar tillfrågades om dataintegritet är svaren på frågan kring dataintegritet överhängande lika för de kommuner som använder sig av en egen lösning för säkerhetskopiering. 86 % uppgav att de starkt höll med om påståendet, vilket än en gång bevisar att informationssäkerhetsarbete är något kommuner prioriterar. Vidare höll 4 % med och 5 % ställde sig neutrala till påståendet. Det avvikande är att 2 kommuner motsvarande 4 % valde alternativet håller verkligen inte med. Detta kan eventuellt bero att de kommuner som valde detta alternativ värderar dataintegritet men inte har hand om någon integritetskänslig information på sina egna säkerhetskopior och att deras integritetskänsliga information lagras och hanteras åt dem hos en annan kommun.

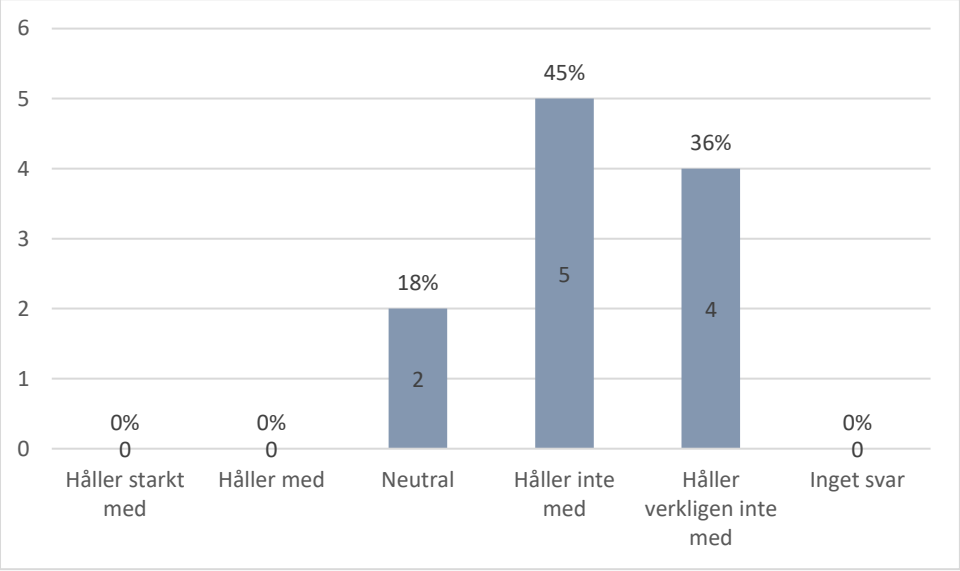


Figur 15. Vår kommun har valt bort molnbaserade lösningar för säkerhetskopiering på grund av integritetsproblem.

De kommuner som ej använder sig av molnbaserade lösningar för säkerhetskopiering fick frågan om de fattade beslutet att inte använda sig av detta utifrån integritetsproblem. Eftersom kommuner listar integritet som ett viktigt område är resultaten från denna fråga intressanta att belysa. Svaren är något spridda; 27 % svarade att de inte höll med och verkligen inte höll med om påståendet. De menade alltså att integritetsproblem inte skulle vara den avgörande faktorn för att inte ha implementerat molnbaserade lösningar för säkerhetskopiering. För att relatera tillbaka till frågan som ställdes tidigare i enkäten om varför kommuner ej använder molnbaserade lösningar för säkerhetskopiering handlar det i stället om att de har en väl fungerande lösning samt att kostnadsskäl varit en av de primära anledningarna till att molnbaserade lösningar valts bort. Den största gruppen från svaren ställde sig neutrala till frågan, det vill säga 43 %. Här kan det konstateras att integritet kan ha varit en av anledningarna till att molnbaserade lösningar ej implementerats men att detta inte skulle vara den avgörande faktorn. Vidare uppgav 30 % att de höll starkt med och höll med om påståendet. Detta kan återkopplas till frågan om varför kommuner ej använder molnbaserade lösningar med att det nämndes att juridiska överväganden, säkerhet och integritet haft en stor inverkan när kommunen övervägt en lösning för säkerhetskopiering. Detta är något analysen av resultaten från denna fråga bekräftar.

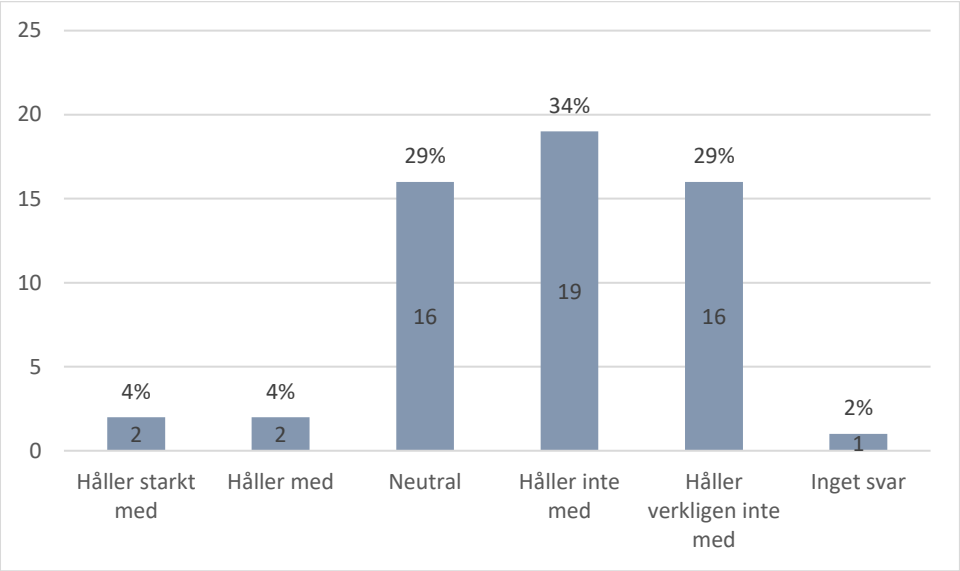
Vad var anledningarna till att det valdes bort?

Andra faktorer som kommunerna nämnde förutom de som tidigare belysts är att det finns policyer som begränsar användningen av molnbaserade lösningar och att molnlagring var i ett för tidigt skede när upphandling senast skedde. Även andra faktorer där kommuner ansåg att det ej funnits nog tydliga instruktioner på hur återställning går till. Vad som även omnämndes är att en molnbaserad lösning skulle ta för lång tid på grund av nätverkskapacitet. En kommun kommenterade ”Kompetens för att återläsa finns lokalt, vi önskar ha kontrollen själva, backup är en av de tre viktigaste uppgifterna att ha full kontroll över, kommuner hanterar integritetskänsliga data och det är en av orsakerna till att full kontroll önskas.” Det är även värt att nämna kommentaren från en annan kommun: ”Vi har tidigare haft en molnbaserad lösning som vi lämnat på grund av kostnadsskäl.” Kommunen har alltså valt att testa en molnbaserad lösning men sedan lämnat den och återgått till en alternativ lösning på grund av kostnadsskäl.



Figur 16. Vi har haft problem med att hantera personuppgifter enligt lagar och regler gällande molnbaserade lösningar för säkerhetskopiering.

De kommuner som använder sig av molnbaserade lösningar för säkerhetskopiering blev tillfrågade om de haft problem vad gäller deras hantering av personuppgifter enligt lagar och regler. Vad resultatet visar är att kommunerna övervägande inte håller med om påståendet. Detta kan analyseras med att reflektera över tidigare ställda frågor om integritet. Tidigare ställda frågor tyder på att personuppgifter behandlas på ett bra sätt av kommunerna och detta återspeglas i resultaten av denna frågan där kommunerna uppger att det inte har uppstått några problem större problem.



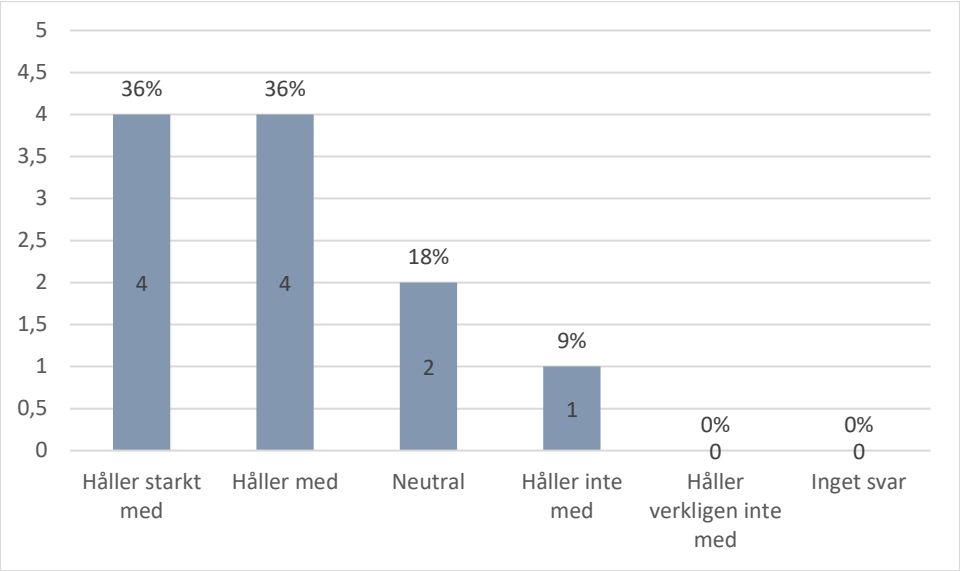
Figur 17. Vi har haft problem med att hantera personuppgifter enligt lagar och regler gällande säkerhetskopiering.

Vad föregående fråga förespråkar i resultaten så återspeglas det även samma resultat för denna fråga vilket är att kommuner inte har haft några problem att hantera personuppgifter även för de kommuner som använder sig av en egen säkerhetskopieringslösning. Dock uppgav fyra kommuner att de starkt höll med och höll med om påståendet. Dessa fyra kommuner kan vara de kommuner som nämnde att de skulle kunna tänka sig att gå över till en molnbaserad lösning. Ett av skälen för dessa fyra kommuner skulle kunna vara bristande resultat i hanteringen av personuppgifter och att de då skulle vilja implementera en annan lösning för att få bukt med problemen.

Vad är det för problem ni stött på gällande hanteringen av personuppgifter eller säkerhetsfrågor om det varit några?

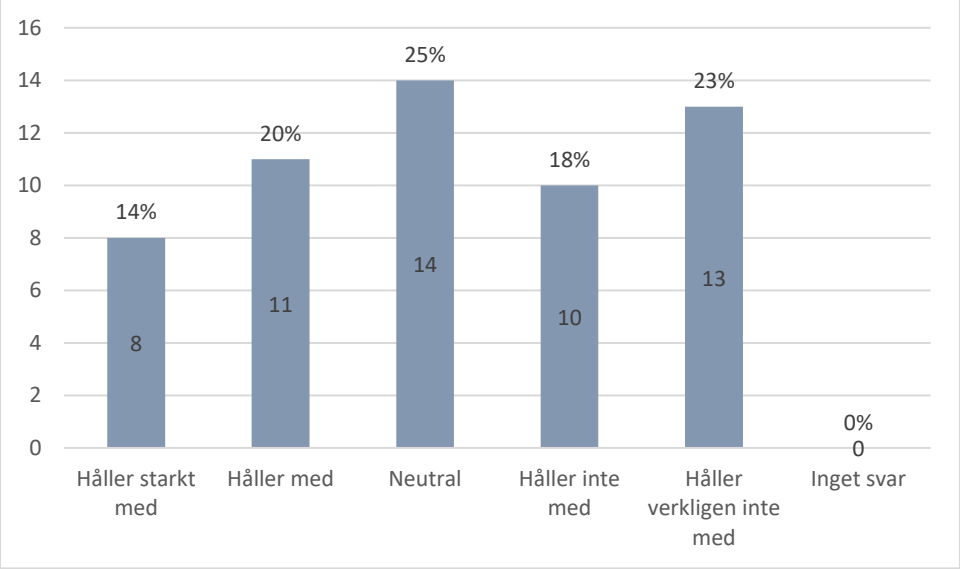
De kommuner som använder molnbaserade lösningar svarade att de inte upplevt några problem och menade att så länge kommunen lägger stor vikt vid undersökande av regler och avtalsvillkor med en grupp kunniga kompetenser inklusive jurister kan problem undvikas. En kommun kommenterade: ”Vi har inte stött på några problem eftersom vår data är krypterad och det är endast vi som har nyckeln.” En annan kommun nämnde dock att frågor om röjning av information har varit aktuellt och att lagring i molntjänst i sig innebär en röjning av information.

Gällande de kommuner som ej använder sig av molnbaserade lösningar kommenterade en av kommunerna ”Hanteringen av personuppgifter rör sig om dataskapandet, inte datalagrandet. Så länge hanteringsanvisningar och numera behandlingsregister och hanteringsplaner följs så lagras bara det som ska kunna lagras.” Kommuner nämnde gallring och lokala register som problem som uppstått. Gällande gallring nämndes GDPR där ifall en personuppgift gallras i verksamhetssystemet finns uppgiften fortfarande kvar i säkerhetskopian. I stort återgavs att kommuner inte haft incidenter vad gäller detta. Analysen av detta är därmed att genomförs och tillämpas regelverk utefter GDPR ska säkerhetsfrågor och personuppgifter inte medföra några allvarliga incidenter.



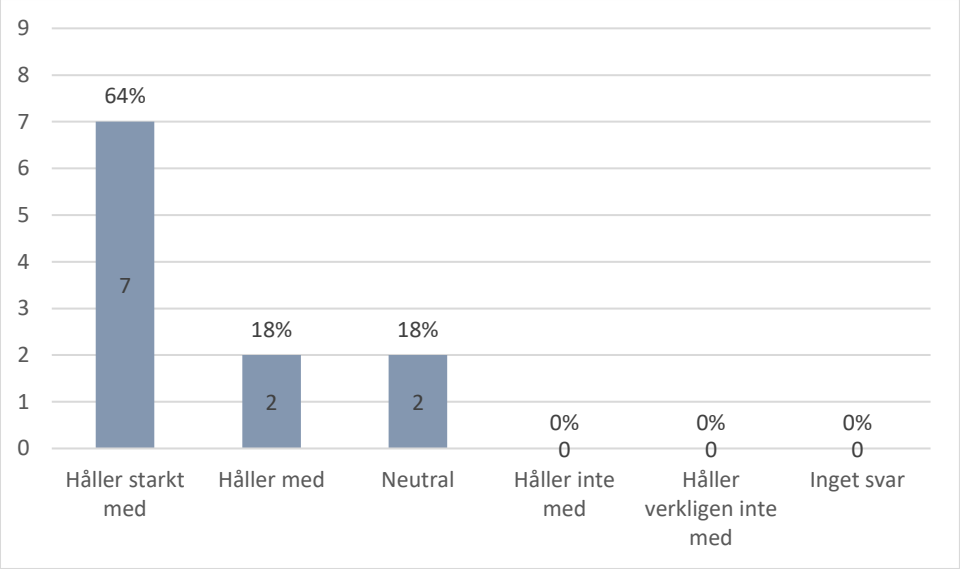
Figur 18. Vår kommuns tillgång till ett effektivt nätverk påverkade vårt beslut att börja använda molnbaserade lösningar för säkerhetskopiering.

I tidigare studier av Ali m. fl. (2017) behandlade en av frågorna som ställdes effektivt nätverk och dess påverkan i användandet av molnbaserade lösningar. Frågan gällande effektivt nätverk var den fråga som studien uppnådde högst svarsfrekvens för i det svarsalternativ som uppgav att respondenterna starkt höll med om hur viktigt de ansåg komponenten vara gällande molnbaserade lösningar. Gällande om effektivt nätverk hade en inverkan på användandet av molnbaserade lösningar svarade 80 % att detta var starkt viktigt. För att kunna använda sig av en molnbaserad lösning är produktivitet, mottaglighet och lätthet viktiga faktorer. Dessa faktorer är vad en väl fungerande nätverksinfrastruktur måste utgöra och något som en organisation måste ha en fullgod lösning för innan en eventuell implementation av en molnbaserad lösning sker. Vad denna studie bekräftar med tidigare studie är att de kommuner som implementerat en molnbaserad lösning har behövt ha ett stabilt nätverk som ett förkrav för implementering av en molnbaserad lösning.



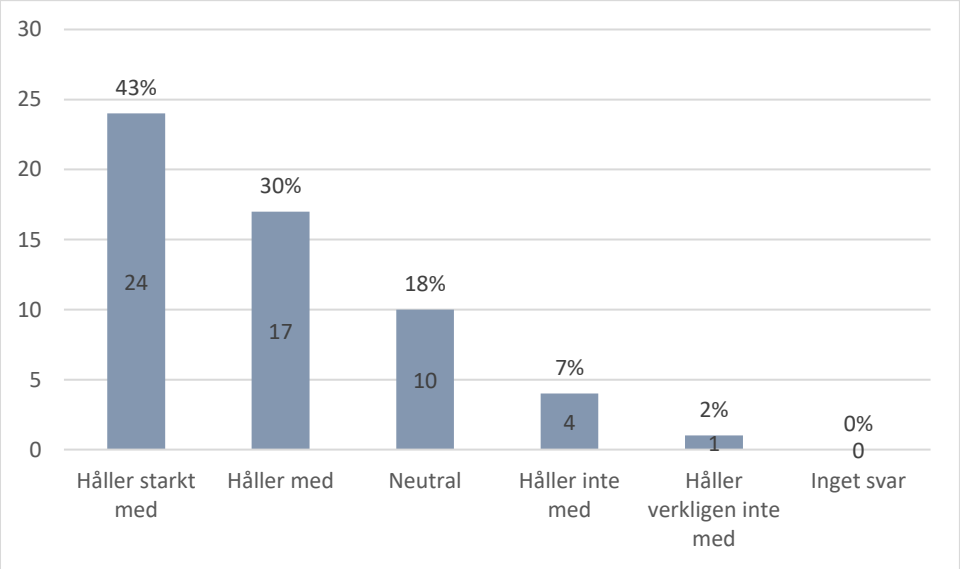
Figur 19. Vår kommuns tillgång till ett effektivt nätverk har påverkat vårt beslut att inte använda molnbaserade lösningar för säkerhetskopiering.

De kommuner som beslutat att inte använda molnbaserade lösningar för säkerhetskopiering blev tillfrågade om deras tillgång till ett effektivt nätverk har påverkat detta. Svaren är jämnt fördelade över svarsalternativen. Några extrema värden går inte att utläsa, men resultaten visar att nätverkskapacitet hade en betydande faktor för flera av kommunerna i deras beslut att använda molnbaserade lösningar eller ej. Detta är även något som omnämndes i frisvarsfrågor, där det uppgavs att oavsett andra faktorer hade kommunen inte kunnat implementera en molnbaserad lösning för säkerhetskopiering just eftersom de inte har tillräckligt med nätverkskapacitet.



Figur 20. Vår kommun kommer att fortsätta använda molnbaserade lösningar för säkerhetskopiering.

Kommuner som använder molnbaserad lösning för säkerhetskopiering fick besvara hur mycket de instämde med påståendet att de kommer fortsätta användningen. I resultaten återfinns att 64 % starkt höll med, 18 % höll med och 18 % ställde sig neutrala till påståendet. Eftersom kommuner som implementerat en molnbaserad lösning har sett mest positiva effekter av användningen kan detta förklara varför de avser att fortsätta med sin användning.



Figur 21. Vår kommun kommer att fortsätta använda nuvarande lösning för säkerhetskopiering.

Vad gäller de kommuner som inte använder sig av en molnbaserad lösning indikerar resultaten att de kommer att fortsätta använda sin nuvarande lösning. Anledningarna till detta har ett flertal faktorer som presenterats i resultatet och analysen i tidigare frågor.

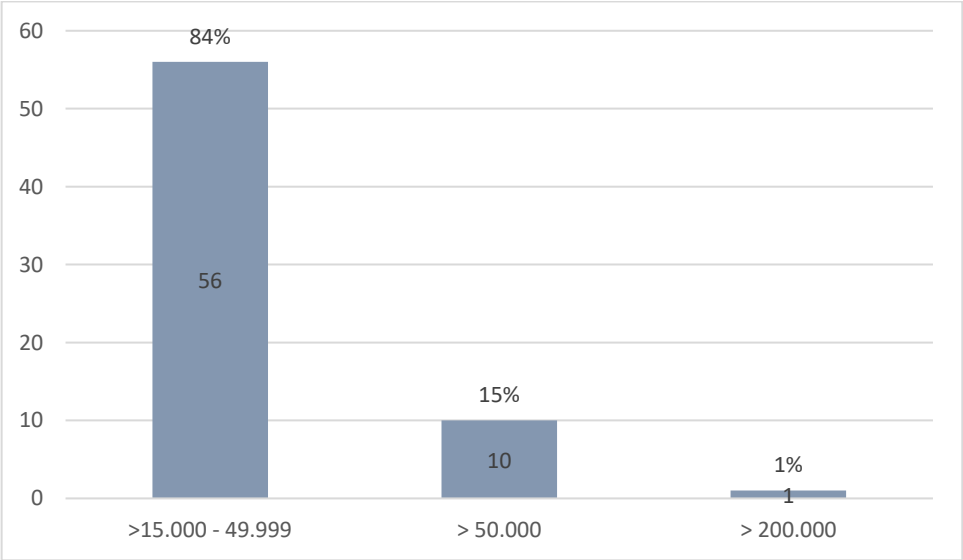
Varför?

De kommuner som svarade att de kommer att fortsätta använda sin nuvarande lösning för säkerhetskopiering motiverade det med att nuvarande lösning har en avskrivningstid, oklara riktlinjer från SKL om GDPR och att ställningstagande om annan lösning görs först efter riskanalys och ekonomisk kalkyl. Vad som belystes är att kommunens verksamheter och IT måste bli mer medvetna om hur informationsstrukturen ser ut detta genom att informationsklassificera och att arbeta mer med informationshantering överlag ses som ett eget begrepp för att kunna ställa krav på rätt nivå vid upphandling av molnbaserade lösningar.

De kommuner som använder molnbaserade lösningar för säkerhetskopiering hade inga kommentarer på varför de avsåg att fortsätta använda sig av det förutom att de ansåg sig nöjda med lösningen utifrån vad som nämnts i resultaten från föregående frågor.

5.4 Faktorer till användning sett till befolkningsmängd

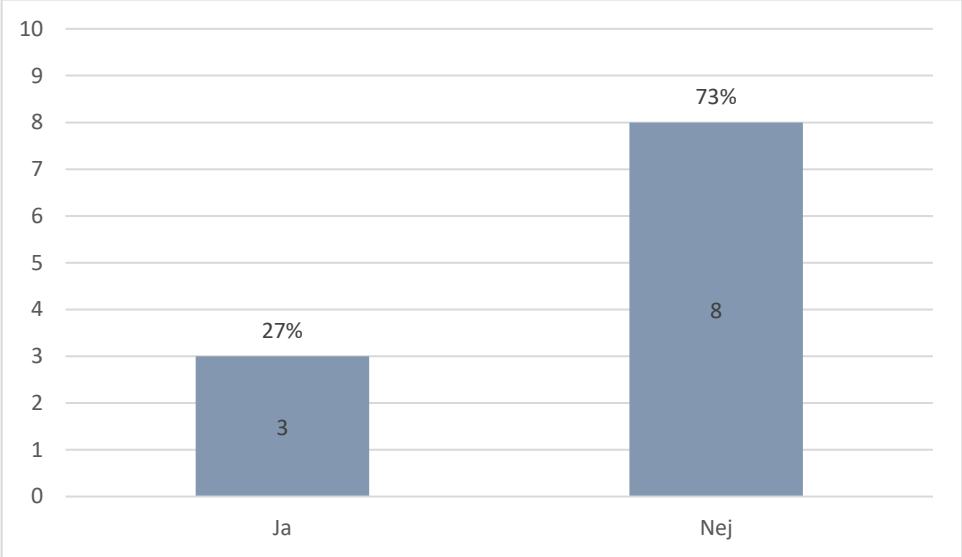
Vid analys av de 67 svarande kommunerna togs befolkningsmängden i beaktande, detta för att utefter hur stor befolkningsmängd en kommun har kunna nå ett flertal slutsatser. Eftersom den första frågan i enkätstudien rörde vilken kommun respondenten i fråga representerade fanns möjligheten att presentera resultat på befolkningsmängd i de kommuner som valde att besvara enkäten. Dock nämns inte kommunerna vid namn i resultatet med tanke på de etiska krav som har ställts upp för studien. På Statistiska centralbyråns (SCB) webbplats återfinns dokument som för varje år folkbokför folkmängden i Sveriges kommuner. Det senaste tillgängliga dokumentet är från den 1 januari 2018. Enligt SCB (2018) kan följande figur presenteras över hur befolkningsmängden ser ut enligt de svarande kommunerna i enkätstudien. Gränserna för befolkningsmängd och hur de presenteras i grafen baserades på vad SKL (2017) skriver i sin kommungruppsindelning. SKL:s kommungruppsindelning används för att underlätta i analyser och statistiska sammanhang genom att dela in kommuner i tre olika grupper beroende på befolkningsmängd.



Figur 22. Befolkningsmängd hos svarande kommuner.

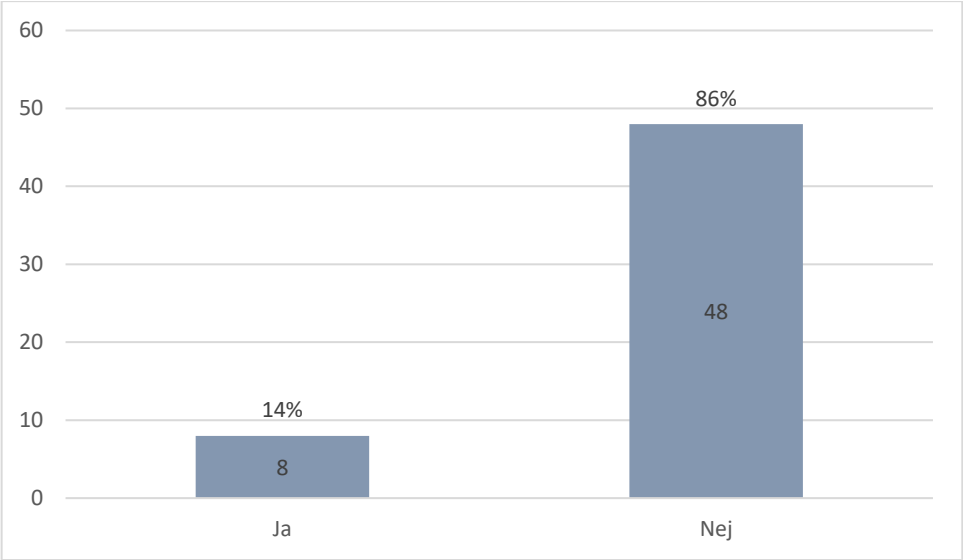
Som graferna presenterar är majoriteten, 84 %, av de svarande i enkäten kommuner som har en befolkningsmängd mellan 49 999–15 000 invånare eller mindre. Det är 15 % som har en befolkningsmängd på över 50 000 invånare och endast en kommun har en befolkningsmängd större än 200 000 invånare. Analysmässigt går det att utläsa att det är mindre kommuner som utgör den största svarsfrekvensen i denna studie, vilket betyder att studiens resultat till störst del är applicerbara för mindre kommuner.

För att analysera om befolkningsmängd gällande större kommuner skulle ha en korrelation med möjligheter för att implementera en molnbaserad lösning för säkerhetskopiering presenteras följande graf. För större kommuner inkluderades de kommuner som har över 50 000 invånare eller över 200 000 invånare.



Figur 23. Användningen av molnbaserade lösningar för säkerhetskopiering hos kommuner med större befolkningsmängd.

Från grafen går det att utläsa att motsvarande 27 % av de större kommunerna har implementerat en molnbaserad lösning för säkerhetskopiering medan 73 % av de större kommunerna ej gjort detta. Befolkningsmängd hos en kommun är något som är direkt överförbart på hur många anställda en kommun har. Detta är något som påverkar vilka resurser som kan tillgodoses för en kommun. Analysen från detta är att även om större kommuner oftast har en större budget är inte fallet så att kommunen har valt att implementera en molnbaserad lösning för säkerhetskopiering även om resurser skulle tillåta detta.



Figur 24. Användningen av molnbaserade lösningar för säkerhetskopiering hos kommuner med mindre befolkningsmängd.

Stapeldiagrammet som presenteras i figur 24 visar användningen av molnbaserade lösningar för säkerhetskopiering hos kommuner med mindre befolkningsmängd, det vill säga som har mellan 49 999–15 000 och mindre. Utifrån dessa resultat går det att se att 86 % inte har implementerat en molnbaserad lösning och att resterande 14 % har gjort detta. Det är som tidigare nämnts många faktorer som spelar roll när en kommun ska fatta beslutet att av använda sig av en molnbaserad lösning eller ej. Handlar det om en mindre kommun har kommunen oftast desto mer faktorer att förhålla sig till. En mindre kommun har oftast inte samma resurser som en stor kommun; då är det övervägande mer negativa faktorer som i slutändan påverkar beslutet att inte implementera denna lösning.

För att göra en analys av ifall befolkningsmängden hos kommunerna som deltog i enkäten har någon påverkan på ifall en kommun använder sig av en molnbaserad lösning för säkerhetskopiering eller ej användes Fishers exakta test. Med Fishers exakta test används en nollhypotes. Fishers exakta test avgör hur stor sannolikheten är att observera just de data som observerats, om det antas att nollhypotesen stämmer. Nollhypotesen i detta fall är enligt följande: ”Befolkningsmängden har ingen påverkan på proportionen av kommuner som använder molnbaserade lösningar.” Fishers exakta test gör det möjligt att observera två grupper med två kategorier var. En signifikansnivå behöver appliceras; 0,05, vilket användes i denna uträkning.

Fishers exakta test och formeln för testet ser ut enligt följande:

$$p = \frac{\binom{A+C}{A}\binom{B+D}{B}}{\binom{N}{A+B}} = \frac{(A+B)!\,(C+D)!\,(A+C)!\,(B+D)!}{A!\,B!\,C!\,D!\,N!}$$

Genom att använda siffrorna och resultaten från figur 23 och figur 24 förs de in i Fishers formel. För att förenkla uträkningen användes Microsoft Excel för själva uträkningen med de värden som återfinns från tabellerna. Vi väljer att avfärda nollhypotesen om sannolikheten att observera just våra data är mindre än 5 %, det vill säga vi sätter signifikansnivån p = 0,05 i Fishers exakta test. Eftersom sannolikheten att observera våra data beräknades till 37,1 % påvisar detta därmed att nollhypotesen inte kan avfärdas. Enligt de data som samlades in går det inte att med hög säkerhet påvisa ett samband

mellan befolkningsmängd och proportionen av kommuner som använder molnbaserade lösningar. Det går alltså att klarlägga att resultaten inte är signifikanta (University of Sheffield, 2012).

5.5 Skillnader och likheter kommuner emellan

Från resultaten går det att utläsa att det är mestadels skillnader i resultat vad gäller de kommuner som använder sig av molnbaserade lösningar för säkerhetskopiering och för de som inte gör detta. Även om det i slutändan är en säkerhetskopiering som ska utföras är det sättet att säkerhetskopiera på och den underliggande infrastrukturen för hur detta går till som är komponenterna som skiljer sig åt. Kommuner som använder en molnbaserad lösning beskrev en mängd effektiviseringsområden, något som de som har en på plats-lösning inte har kunnat uppnå. Resultaten visar dock att det finns en del likheter oavsett lösning för hur en kommun agerar i deras arbete med säkerhetskopiering. Angående frekvensen om hur ofta säkerhetskopior görs är detta något som överensstämmer. De data som sparas på säkerhetskopiorna är oavsett lösning alla kommunens data. Oavsett vilken lösning en kommun har valt att använda sig av ansågs lösningen vara stabil, detta tyder på oavsett lösning har kommuner lyckats i sitt arbete att som kommun tillgodose en bra och fungerande lösning för säkerhetskopiering och återställning. Vad gäller lagar och regler framgår av resultaten att det skiljer sig åt hur dessa appliceras beroende på vilken lösning kommunen har, men alla kommuner jobbar utefter samma vision att informationen som lagras ska ha högsta möjliga skydd. Detta för att skydda den integritetskänsliga information som återfinns på säkerhetskopiorna. Detta har lett till att alla kommuner oavsett lösning inte har haft incidenter som involverat personuppgifter. En annan likhet är att kommunerna var eniga; de kommer att fortsätta använda den befintliga lösning som de har. Anledningar till varför belyses under resultaten och analysen från frågorna i detta resultat och i analyskapitlet.

6 Slutsats

I detta kapitel presenteras de slutsatser som studien har kommit fram till. Kapitlet kommer först presentera slutsatser som har framkommit från resultat och analys av de kommuner som använder sig av molnbaserade lösningar för säkerhetskopiering. Sedan kommer resultat och analys presenteras för de kommuner som ej använder sig av detta. Slutsatser kommer även att sammanlänkas för de två kategorierna emellan och slutsatser för studien i stort och svaret på forskningsfrågan kommer att presenteras. Syftet med studien var att besvara följande frågeställning:

Hur ser användningen av molnbaserade lösningar för lagring av säkerhetskopior ut hos kommuner i Sverige?

Följande underfrågor kompletterade även forskningsfrågan:

Vilka fördelar samt nackdelar finns för kommuner med molnbaserade lösningar för säkerhetskopiering?

Hur ser hanteringen ut av personuppgifter gällande molnbaserade lösningar för säkerhetskopiering i kommuner?

Vilka effekter har kommuner som använder molnbaserade lösningar som implementation för säkerhetskopiering kunnat se?

En av slutsatserna som studien påvisar är att användningen av molnbaserade lösningar för säkerhetskopiering hos svenska kommuner är relativt låg. Även om molnbaserade lösningar har funnits som ett koncept en längre tid anses det vara ett outforskat område. Att använda säkerhetskopiering genom en molnbaserad lösning anses alltså inte vara särskilt vanligt förekommande hos kommuner i dag. Genom att molnbaserade lösningar erbjuder så pass många olika användningsområden för en kommun har säkerhetskopiering eventuellt inte varit den komponenten av molnbaserade lösningar som kommunen valt att lägga stort fokus på. Även om studien och dess resultat påvisar att kommuner tar informationssäkerhet på allra största allvar har kommuner inte valt att förlägga resurser på just arbetet med säkerhetskopiering. Det som är positivt är att de kommuner som faktiskt valt att implementera en molnbaserad lösning för säkerhetskopiering har använt denna lösning en längre tid. Slutsatser angående detta är att säkerhetskopiering inom molnbaserade lösningar anses som en stabil funktion för en kommun och som nämnt anser de att denna lösning har fungerat bättre än den de tidigare använt sig av. Att privata outsourcingleverantörer dominerar kan ses till att kommuner oftast vill arbeta mot att ha så pass lite arbetskraft på plats hos kommunen som möjligt och att genom en annan aktör sköter arbetsuppgifter resulterar det i att kommuner kan fokusera på andra arbetsuppgifter än de som hade behövts om de haft en på plats-lösning. I kombination med att studiens resultat tyder på att kommuner har ett stort förtroende för molntjänsteleverantörer kan slutsatsen dras att de existerande molnleverantörerna som finns på marknaden i dag har arbetat fram välfungerande koncept som kommuner kan känna sig trygga med att använda.

Slutsatserna kring vilka effektivitetsområden som har kunnat uppnås genom en implementation av en molnbaserad lösning för säkerhetskopiering är många. Genom minskad datalagring, arbetskostnader, lagringskostnader och mjukvarukostnader samt hantering av infrastruktur talar detta för att kommuner har kunnat tillgodose sig en lösning som ger en heltäckande lösning. Effektivitetsområden som annars skulle kräva enorma mängder tid och resurser att administrera själv som kommun. Andra viktiga slutsatser från studien av de som använder molnbaserade lösningar för säkerhetskopiering är att säkerhet är betydligt bättre med en molnbaserad lösning än innan. Eftersom säkerhet är en av en kommuners viktigaste frågor vad gäller deras arbete är det positivt att molnbaserade lösningar för säkerhetskopiering har kunnat lyfta detta område. Nämnvärt är även att jämfört med att ha en på plats-lösning där kommunen hela tiden behöver oroa sig för en potentiell dataförlust har kommunen nu ett betydligt bättre sätt för återställning av de säkerhetskopior som lagras hos en molnleverantör då behovet elimineras av att ha en fysisk plats att lagra sina säkerhetskopior på. En stor fråga som måste nämnas här är att kommunerna anser sig ha uppnått kostnadseffektivitet med en sådan här

implementation. Kommuner, stora som små, kämpar alltid med att hålla kostnaderna nere och finns det smarta lösningar som drastiskt kan sänka en kommuns utgifter bör detta vara något som ska utvärderas och implementeras så fort som möjligt. Slutsatserna från lagar och regler och hur de har kunnat tillämpas med en molnbaserad lösning samt frågor om integritet är övervägande positiva. Att säkerhetskopiering med den data som lagras på säkerhetskopiorna har tillräcklig säkerhet är av högsta prioritet. Hade säkerhet visat sig medföra problem hade kommuner inte kunnat se molnbaserade lösningar som ett alternativ. För att summera ser framtiden ljus ut för de kommuner som använder molnbaserade lösningar för säkerhetskopiering och förhoppningsvis kommer fler kommuner se fördelarna med att använda detta koncept och förhoppningsvis kommer det då att sprida sig inom Sveriges kommuner.

Slutsatserna gällande de kommuner som ej använder sig av en molnbaserad lösning för säkerhetskopiering är att de för närvarande har en fungerande befintlig lösning som de anser vara god nog. Som tidigare nämnts finns det många effektivitetsområden som gör att en molnbaserad lösning skulle vara applicerbar. Det som omöjliggör för vissa kommuner att uppta denna lösning är just kostnadsskäl och att de känner att juridiska skäl, säkerhet och integritet inte är helt klarlagt eller förståeligt. Det som omnämns från denna studie är att en genomgång av en tillräcklig juridisk bedömning och att kommuner förhåller sig till lagar och regler gällande kommuners användning av molnbaserade lösningar för säkerhetskopiering är viktiga aspekter. Kan en kommun tillämpa detta så kan problemen som skulle kunna uppstå minimeras. Därav skulle kommuner med denna vetskap behöva omvärdera sina funderingar kring en eventuell implementation av en molnbaserad lösning. De som inte använder sig av en molnbaserad lösning för säkerhetskopiering har till stor del valt bort detta på grund av säkerhetsfrågor. De som har implementerat en lösning för säkerhetskopiering med en molnbaserad lösning har dock inte upplevt några problem med säkerheten. Detta tyder på att när en implementation av en molnbaserad lösning har använts har säkerhetsfrågor i realiteten inte uppstått. Då problem med att hantera personuppgifter inte förekommit hos de kommuner som tillhandahåller en egen lösning för säkerhetskopiering kan slutsatserna dras att många kommuner känner sig bekväma med nuvarande arbetssätt och lösning. Detta kan vara en bidragande faktor till varför alternativa lösningar inte blivit tilltänkta. Därav kan det vara svårt att få kommuner att testa att istället implementera en annan lösning just för att de känner att nuvarande lösning är funktionell. I och med att molnbaserade lösningar blir mer vida spritt med de effektivitetsområden som finns att tillgå kan det dock finnas stor chans att fler kommuner kommer att implementera en molnbaserad lösning för säkerhetskopiering.

Slutsatsen av studien är att molnbaserade lösningar för säkerhetskopiering hos kommuner i Sverige fortfarande befinner sig i ett utvecklingsstadie. Svaret på forskningsfrågan är att i dagsläget är användningen av molnbaserade lösningar för säkerhetskopiering relativt låg. Skulle möjligheten finnas att kunna sprida användningen av molnbaserade lösningar och de funktioner som finns att tillgå kan ett flertal områden effektiviseras för säkerhetskopiering inom kommuner. Utfallet av detta kommer inte enbart att återspeglas hos kommuner utan det kommer säkerligen hjälpa i utbildning, sjukvård och infrastruktur som är nödvändiga för att upprätthålla en kommun och ett fungerande samhälle. Det finns flera användningsområden för molnbaserade lösningar för säkerhetskopiering och genom att ersätta förlegade samhällsfunktioner där information hanteras på fel sätt kan samhället i stort nyttja effektiviteten av molnbaserade lösningar för säkerhetskopiering.

6.1 Framtida arbete

Molnbaserade lösningar är något som har utvecklats alltmer under den senaste tiden. Denna studien fokuserade på att undersöka säkerhetskopiering och hur molnbaserade lösningar används just för detta i kommuner i Sverige. Studien skulle kunna göras gentemot andra stora samhälleliga organ för att se hur detta fungerar inom andra verksamheter. Även en studie som studerar företag och deras användning skulle vara av intresse då de antagligen har andra förutsättningar än en kommun. En enkätstudie skulle kunna användas som tillvägagångssätt, alternativt skulle en intervjustudie kunna tillämpas för att utforska ämnet mer ingående.

7 Diskussion

Detta kapitel kommer att diskutera studien utifrån metodval, urval, vetenskapliga aspekter, samhälleliga aspekter, etiska aspekter samt diskutera aspekter berörande GDPR och kommuner.

7.1 Metodval

För att besvara forskningsfrågorna användes en kvantitativ enkät utformad med likertskala-frågor och även öppna frågor som tillät fritextsvar. Enkäten var uppdelad i de svarande som använde molnbaserade lösningar för säkerhetskopiering och de svarande som inte använde detta. Ifall den svarande kommunen använde detta ställdes specifika frågor och de kommuner som inte nyttjade denna lösning fick en annan uppsättning av frågor. Med hjälp av likertskala-frågor kunde de svarande kommunerna ange på en skala hur mycket de höll med om påståendet vilket inte enbart ger möjlighet till fler svarsalternativ utan även tid för den svarande att tänka efter hur mycket påståendet stämmer in på verkligheten och vad som efterfrågas för den specifika frågan.

Metoden att använda en enkät fungerade till stor utsträckning bra då eftersom respondenterna nästan uteslutande valde att välja ett svarsalternativ på likertskala-frågorna och det var knappt några som valde att svara med alternativet ”inget svar”. Detta tyder på en väl utformad enkät som var förståelig med enkla koncisa frågor som behandlade ämnet som var tänkt att utforskas. Även frisvarsfrågorna blev till stor del besvarade med utförliga svar och få kommentarer indikerade att frågan var otydlig eller omöjlig att besvara. En del kommuner valde dock att inte besvara vissa frågor med tanke på deras informationssäkerhetsarbete.

7.2 Urval

Totalt tillfrågades alla Sveriges kommuner att delta i denna studie, alltså 290. Det totala insamlade underlaget blev 67 respondenter. Med hjälp av Cochrans formel beräknades en godtycklig svarsfrekvens för att svarsfrekvensen från studien skulle vara tillräcklig för att kunna presentera populationen. Genom uträkningar framkom att 55 svar var det antal som behövdes för att kunna anse studien som representativ, vilket det totala svarande antalet med 67 kommuner uppnår. Därav kan studien i sin helhet anses som användbar.

7.3 Vetenskapliga aspekter

Vid sökningen efter relaterad forskning inom området fokuserade de identifierade forskningsartiklarna på aspekter och faktorer gällande användningen av molnbaserade lösningar inom olika verksamheter och organisationer. Några studier som fokuserade just på säkerhetskopieringsaspekten gällande molnbaserade lösningar kunde inte identifieras. Dock så går det att se kopplingar studier emellan från de som nämnts från tidigare forskning, vilka är:

Studien från Ali m. fl. (2015) presenterar att molnbaserade lösningar skapade bättre funktioner för organisationerna såsom färre risker och bättre kontroll över data. Kostnadsreduceringar vid implementation av molnbaserade lösningar var en stor faktor samt att organisationer kunde minska på fysisk hårdvara. Studien tar även upp aspekten om katastrofåterställning och backup där en ordentlig backup kan vara en snabb väg för att återställa data i oväntade situationer. Studien av Ali m. fl. (2015) är en av studierna som användes för att kunna utföra denna studie och flera av slutsatserna överensstämmer med resultaten från denna studie vad gäller ovan nämnda faktorer.

I studien av Ali m. fl. (2017) presenteras flera områden inom molnbaserade lösningar som anses viktiga som även framhävdes i denna studie. De områden som anses viktiga och utpekas inom båda studierna är förtroende för molnleverantörer, kostnadseffektivitet, lagar och regler och behandling av data, säkerhet och effektivt nätverk. Alla dessa faktorer uppnådde i båda studierna höga procentenheter i svaren på studiernas frågor och dessa faktorer återfinns i resultaten med att respondenterna anser dessa som viktiga. Ali m. fl. (2017) belyser att det finns flera olika aspekter av molnbaserade lösningar som behöver utforskas och att säkerhet är en fråga som är ytterst kritisk ifall en organisation ska fatta beslutet att använda sig av molnbaserade lösningar. Denna studie utforskade

aspekten av säkerhetskopiering och resultaten tyder på att de som inte använder sig av en molnbaserad lösning för säkerhetskopiering till stor del har valt bort detta på grund av säkerhetsfrågor. Dock framgår av resultaten att de som använder sig av molnbaserade lösningar för säkerhetskopiering inte har upplevt några problem med säkerhetsfrågor. Detta indikerar att när molnbaserade lösningar implementerats för säkerhetskopiering har problem med säkerhet inte uppkommit.

7.4 Samhälleliga aspekter

Som ovanstående stycke tar upp är säkerhet en av de fundamentala frågorna vad gäller molnbaserade lösningar och hur detta ska hanteras. Eftersom kommuner hanterar mycket integritetskänslig information är det viktigt att den hanteras korrekt. De kommuner som tillhandahåller sin egen lösning är nöjda med denna lösning och har inte haft några större problem med säkerhet, detsamma gäller för de som använder en molnbaserad lösning för säkerhetskopiering där de inte heller haft några särskilda incidenter. Dock framgår av resultaten att de kommunerna som tillhandahåller sin egen lösning är väldigt kritiska till att implementera en annan lösning då de anser det vara förenat med för många risker. Då kommuner genom studien visat sig vara väldigt kritiska till att implementera en annan lösning än den de har lär de vara än mer kritiska nu i och med GDPR:s ikraftträdande. Lagar och regler har stramats åt än mer. Nu när GDPR gäller och kommuner kan tänka sig att implementera en molnbaserad lösning för säkerhetskopiering måste de på nytt genomgå en process med att utvärdera en anskaffning av en molnbaserad lösning utifrån GDPR-perspektivet. Även de kommuner som använder sig av en molnbaserad lösning kommer nu att få gå igenom och säkerställa att alla punkter i GDPR uppfylls i och med hur deras nuvarande lösning ser ut. GDPR är en lag som kommer att påverka de som på något sätt har hand om informationshantering och har kommuner inte tillräckliga riktlinjer på hur lagen ska följas kan det medföra stora konsekvenser. Eftersom GDPR är en lag som ska göra det enklare att veta hur personuppgifter ska hanteras anser författaren att det i slutändan kommer gynna kommuner då de på ett enklare sätt kommer att kunna skapa sig en uppfattning av om de ska implementera en molnbaserad lösning för säkerhetskopiering eller ej.

7.5 Etiska aspekter

De etiska aspekterna för denna studie är att respondenterna fick tillräckligt med information om vad deras medverkande i studien skulle innebära och vad studien ämnade att utforska. Genom att använda ett enkätverktyg som ej samlade in någon information från deltagarna kunde konfidentialitetskravet för studien uppnås. Det som kan påpekas och som erhölls som feedback från respondenterna var att länken som skickades ut för enkäten hade kunnat hanteras på ett bättre sätt. Till exempel hade enkäten som var en direkt länk från enkätverktyget kunnat göras om till en länk som ansågs säkrare att klicka på. Två kommuner valde av denna anledning att inte medverka i enkäten eftersom att trycka på en osäker länk inte uppfyllde hur de arbetade med informationssäkerhet.

7.6 GDPR och kommuner

Vad studien kommit fram till är att kommuner värderar sitt informationssäkerhetsarbete högt och att när data ska lagras vid säkerhetskopiering måste lagar och regler förhållas till strikt. Att kommuner förhåller sig till lagar och regler är något som alltid har varit viktigt oavsett om det precis har tillämpats en ny lag som ytterligare ska skydda individer och deras personuppgifter. Det finns dock en anledning till att GDPR har utvecklats och det är för att ytterligare stärka individers integritet. Även om GDPR stramar åt personuppgiftshanteringen gör den detta på ett positivt sätt då det nu är än mer tydligt hur de olika parterna inom en kommun som har hand om personuppgiftshantering ska gå tillväga när de hanterar sin information. Om GDPR hade varit implementerat redan innan enkäten hade skickats ut hade studien kunnat se annorlunda ut resultatmässigt. Även om GDPR är en väldigt tydlig lag hade exempelvis svaren på frågan om kommunen haft några problem med att hantera personuppgifter enligt lagar och regler kunnat variera. Kommuner hade kanske då med GDPR som ny lag haft incidenter där de inte fullt ut beaktat GDPR eller gjort något som brutit mot lagstiftningen. Då hade det eventuellt kunnat påvisats att kommuner i frågan om de haft problem med att hantera

personuppgifter då hållit med om detta påstående. Då hade även kanske frisvarsfrågorna kunnat variera där kommuner möjligtvis då hade kommenterat hur inträdandet av GDPR och hanteringen av personuppgifter har fungerat. Då kommuner i svaren på enkätfrågorna nämnde att lagar och regler har försvårat för dem i en eventuell implementation av molnbaserade lösningar för säkerhetskopiering hade det varit intressant att veta ifall GDPR hade påverkat kommuners beslut ännu mer i detta avseende. Möjligtvis hade GDPR gjort det ännu svårare att tillgodose sig en molnbaserade lösning. Resultaten hade potentiellt kunnat visa på att GDPR påverkat användarantalet av molnbaserade lösningar för säkerhetskopiering till att visa på att ytterligare färre kommuner hade använt sig av detta. Alternativt hade det kunnat vara tvärtom.

Referenser

Ali, M., Soar, J. & Yong, J. (2017). Challenges and Issues that are Perceived to Influence Cloud Computing Adoption in Local Government Councils. *IEEE 21st International Conference on Computer Supported Cooperative Work in Design*. DOI: 10.1109/CSCWD.2017.8066732

Ali, O. & Soar, J. (2014). Challenges and Issues Within Cloud Computing Technology. *Cloud computing 2014: The Fifth International Conference on Cloud Computing, GRIDs and Virtualization*. DOI: 10.13140/2.1.3210.3369

Ali, M., Soar, J., Yong, J., McClymont, H. & Angus, D. (2015). Collaborative cloud computing adoption in Australian regional municipal government: An exploratory study. *Computer Supported Cooperative Work in Design (CSCWD), 2015 IEEE 19th International*. Tillgänglig på Internet DOI: http://dx.doi.org/10.1109/CSCWD.2015.7231017

Berndtsson, M., Hansson, J., Olsson, B. & Lundell, B. (2002). *Thesis Projects. A Guide for Students in Computer Science and Information Systems*. Springer. ISBN: 978-1-84800-008-7

Carr, N. (2013). Cloud-computing. *Encyclopædia Britannica*. Tillgänglig på Internet: https://www.britannica.com/technology/cloud-computing [Hämtad 2018-02-08]

Computerhope. (2017). Backup. Tillgänglig på Internet: https://www.computerhope.com/jargon/b/backup.htm [Hämtad 2018-04-05]

Datainspektionen. (2018). Dataskyddsförordningen. Tillgänglig på Internet: https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/dataskyddsforordningen---fulltext/ [Hämtad 2018-05-29]

Gercek, B. Symantec. (2003). Säkerhetskopiera data: ett avgörande steg. Tillgänglig på Internet: http://www.symantec.com/region/se/resources/backingup.html [Hämtad 2018-02-09]

Israel, G. University of Florida. (2018). Determining Sample Size. Tillgänglig på Internet: https://www.tarleton.edu/academicassessment/documents/Samplesize.pdf [Hämtad 2018-06-03]

Sullivan, Gail M. & Artino, A R. (2013). Journal of Graduate Medical Education. Analyzing and Interpreting Data From Likert-Type Scales. Tillgänglig på Internet DOI: 10.4300/JGME-5-4-18

Myndigheten för samhällsskydd och beredskap. (2015). Informationssäkerheten i Sveriges kommuner. Tillgänglig på Internet: https://www.msb.se/RibData/Filer/pdf/28222.pdf [Hämtad 2018-02-13]

Pensionsmyndigheten. (2016). *Molntjänster i staten – En ny generation av outsourcing*. Tillgänglig på Internet: https://www.pensionsmyndigheten.se/nyheter-och-press/pressrum/pensionsmyndigheten-svenska-myndigheter-bor-gora-sig-molnberedda [Hämtad 2018-04-10]

Pensionsmyndigheten. (2016). *Juridisk analys*. Tillgänglig på Internet: https://secure.pensionsmyndigheten.se/download/18.5024285a1526bd01ab3e678/1506071294176/Bilaga%201%20Juridisk%20analys_Molntj%C3%A4nster%20i%20staten_Final%201.1.pdf [Hämtad 2018-05-29]

Sakurai, M. & Kokuryo, J. (2016). Data Backup Dilemma: Case Studies from the Great East Japan Earthquake. *Proceedings of the 17th International Digital Government Research Conference on Digital Government Research Pages 281-286*. Tillgänglig på Internet DOI: http://dx.doi.org/10.1145/2912160.2912207

Samrådsgruppen. (2016). *Molntjänster – ny rapport*. Tillgänglig på Internet: http://www.samradsgruppen.se/web/index.php/8-nyheter/151-molntjanster-ny-rapport [Hämtad 2018-05-28]

Schmitz, C. (2018). Limesurvey – Professional online surveys with LimeSurvey. Tillgänglig på Internet: https://www.limesurvey.org [Hämtad 2018-03-23]

Sinanc, D. & Sagiroglu, S. (2013). A Review on Cloud Security. *Proceedings of the 6th International Conference on Security of Information and Networks*. Tillgänglig på Internet DOI: http://dx.doi.org/10.1145/2523514.2527013

Statistiska centralbyrån. (2016). Frågor och svar om frågekonstruktion i enkät- och intervjuundersökningar. Tillgänglig på Internet: https://www.scb.se/contentassets/c6dd18d66ab240e89d674ce728e4145f/ov9999_2016a01_br_x08br1601.pdf [Hämtad 2018-03-22]

Statistiska centralbyrån. (2018). Befolkningsstatistik. Helårsstatistik – Kommun, län och riket. Tillgänglig på Internet: https://www.scb.se/hitta-statistik/statistik-efter-amne/befolkning/befolkningens-sammansattning/befolkningsstatistik/pong/tabell-och-diagram/helarsstatistik--kommun-lan-och-riket/folkmangden-i-sveriges-kommuner-enligt-indelning/ [Hämtad 2018-05-28]

Sveriges kommuner och landsting. (2017). Kommungruppsindelning 2017. Tillgänglig på Internet: https://skl.se/tjanster/kommunerlandsting/faktakommunerochlandsting/kommungruppsindelning.2051.html [Hämtad 2018-05-28]

Sveriges kommuner och landsting. (2017). Kommuner och landsting. Tillgänglig på Internet: https://skl.se/tjanster/kommunerlandsting.431.html [Hämtad 2018-06-02]

University of Sheffield. (2012) The analysis of categorical data: Fishers exact test. Tillgänglig på Internet: https://www.sheffield.ac.uk/polopoly_fs/1.43998!/file/tutorial-9-fishers.pdf [Hämtad 2018-06-04]

Velte, A., Velte, T. & Elsenpeter, R. (2009). *Cloud computing, a practical approach*. McGraw-Hill, Inc. Tillgänglig på Internet: http://secs.ac.in/wp-content/CSE_PORTAL/cloud1.pdf [Hämtad 2018-04-09]

Vetenskapsrådet. (2002). Forskningsetiska principer inom humanistisk-samhällsvetenskaplig forskning. Tillgänglig på Internet: http://www.codex.vr.se/texts/HSFR.pdf [Hämtad 2018-03-12]

Wohlin, C., Runesson, P., Höst, M., Ohlsson, C. M., Regnell, B. & Wesslén, A. (2012) *Experimentation in Software Engineering*. Springer-Verlag Berlin Heidelberg. DOI: 10.1007/978-3-642-29044-2

Wyld, D C. (2010). The cloudy future of government IT: Cloud computing and the public sector around the world. *International Journal of Web & Semantic Technology (IJWesT), Vol 1, Num 1, January 2010*. Tillgänglig på Internet: http://www.airccse.org/journal/ijwest/papers/0101w1.pdf

Appendix A - Enkätfrågor

Vilken kommun representerar du?

Använder er kommun molnbaserade lösningar för säkerhetskopiering?

(Frågan ställs för att ta reda på om den tillfrågade kommunen använder sig av molnbaserade lösningar eller ej gällande säkerhetskopiering. Beroende på detta kommer olika slags frågor ställas i enkäten. De som svarar ja får en uppsättning frågor, de som svarar nej får en annan uppsättning av frågor.)

Frågor indikerade med (J) avser de frågor som ställs till de som använder molnbaserade lösningar för säkerhetskopiering, frågor indikerade med (N) avser de frågor som ställs till de som ej använder detta.

Varför använder sig er kommun ej av molnbaserade lösningar för säkerhetskopiering? (N)

Vår kommun har planer på att införskaffa molnbaserade lösningar för säkerhetskopiering i framtiden. (N)

Hur länge har er kommun använt sig av molnbaserade lösningar för säkerhetskopiering? (J)

(Enligt Ali m. fl. (2015) påverkas användandet av teknologier beroende på organisationens teknologiska beredskap och infrastruktur samt vilka mänskliga IT-resurser som finns. Frågan ställs för att ta reda på hur länge kommunen i fråga har använt sig av molnbaserade lösningar.)

Hur ofta görs säkerhetskopior hos er kommun som sedan lagras hos en molnleverantör? (J)

Hur ofta görs säkerhetskopior hos er kommun? (N)

Användningen av molnbaserade lösningar för säkerhetskopiering har fungerat bättre än föregående lösningar. (J)

(Enligt Ali m. fl. (2017) är det intressant att veta var sin data befinner sig vad gäller lagringsplats samt vilken auktoriserad personal som har tillgång till dessa data inkluderat hur policyer gällande lagringen och informationen.)

Vad för slags molnbaserad lösning för säkerhetskopiering använder sig er kommun av? (J)

Vilken eller vilka lösningar för säkerhetskopiering använde er kommun sig av innan? (J)

Lagringen av säkerhetskopior med hjälp av molnbaserade lösningar har effektiviserat verksamheten för vår kommun. (J)

Vilka sorts effekter hos er verksamhet har er kommun kunnat se till följd av implementationen av molnbaserade lösningar för säkerhetskopiering? (J)

Vad för data är det er kommun sparar på era säkerhetskopior? (J)

Molnbaserade lösningar för säkerhetskopiering är en stabil lösning vad gäller säkerhetskopiering samt återställning av data. (J)

Vi känner förtroende till att lagra vår kommuns säkerhetskopior hos en molnleverantör. (J)

Vår kommuns lösning för säkerhetskopiering är en stabil lösning vad gäller säkerhetskopiering samt återställning av data. (N)

Vad för lösning använder sig er kommun av? (N)

Vad för data är det er kommun sparar på era säkerhetskopior? (N)

Molnbaserade lösningar för säkerhetskopiering har bedömts vara mer kostnadseffektivt för vår kommun jämfört med andra lösningar. (J)

(Enligt Ali m. fl. (2017) finns det inte tillräckligt med statistik som kan tala för att molnbaserade lösningar verkligen är kostnadseffektiva. Frågan ställs för att se ifall kommuner har kunnat göra besparingar med denna implementation.)

Vår nuvarande lösning för säkerhetskopiering har bedömts vara mer kostnadseffektiv för vår kommun jämfört med molnbaserade lösningar för säkerhetskopiering. (N)

Att molnleverantörer följer lagar och regler avseende de data som lagras hos dem är en viktig aspekt gällande användning av molnbaserade lösningar för säkerhetskopiering. (J)

(Enligt Ali m.fl. (2017) är säkerhet en stor och viktig aspekt gällande molnbaserade lösningar då förlorade data skulle skapa stora konsekvenser. Säkerhet är även en viktig aspekt med tanke på vilken information som kommuner lagrar.)

Att lagar och regler följs avseende de data som lagras är en viktig aspekt gällande säkerhetskopiering. (N)

Det är viktigt att användningen av molnbaserade lösningar motsvarar vår kommuns krav på dataintegritet. (J)

(Enligt Ali m. fl. (2017) finns det flera faktorer som kan påverka integriteten av data som lagras hos en molntjänstleverantör och det är viktigt att effektiva åtgärder vidtas för att behålla integriteten.)

Det är viktigt att vår lösning för säkerhetskopiering motsvarar vår kommuns krav på dataintegritet. (N)

Vår kommun har valt bort molnbaserade lösningar för säkerhetskopiering på grund av integritetsproblem. (N)

Vad var anledningarna till att det valdes bort? (N)

Vi har haft problem med att hantera personuppgifter enligt lagar och regler gällande molnbaserade lösningar för säkerhetskopiering. (J)

Vi har haft problem med att hantera personuppgifter enligt lagar och regler gällande säkerhetskopiering. (N)

Vad för problem har ni stött på gällande hanteringen av personuppgifter eller säkerhetsfrågor om det har varit några? (J/N)

Vår kommuns tillgång till ett effektivt nätverk påverkade vårt beslut att börja använda molnbaserade lösningar för säkerhetskopiering. (J)

(Enligt Ali m. fl. (2017) rankas ett effektivt nätverk högt för användningen av molnbaserade lösningar.)

Vår kommuns tillgång till ett effektivt nätverk har påverkat vårt beslut att inte använda molnbaserade lösningar för säkerhetskopiering. (N)

Vår kommun kommer att fortsätta använda molnbaserade lösningar för säkerhetskopiering. (J)

Vår kommun kommer att fortsätta använda nuvarande lösning för säkerhetskopiering. (N)

Varför? (J/N)