Myndigheten för samhällsskydd och beredskap

ÖREBRO UNIVERSITET

STUDIE

Säkerhet vid molnlösningar

Faktaruta

Säkerhet vid molnlösningar

2017-2018

Örebro universitet

Ann-Sofie Hellberg, Sirajul Islam, Fredrik Karlsson

Syftet var att: 1) kartlägga användningen av molnlösningar hos offentliga aktörer, 2) identifiera samhällsrisker när offentliga aktörer använder molntjänst(er), 3) skapa en uppfattning av graden av centralisering kring molntjänster, 4) kartlägga utmaningar vid upphandling av molntjänster, samt 5) ta fram prioriterade krav och rekommendationer inom informationssäkerhet som MSB behöver ge ut.

MSB:s kontaktpersoner:
Carl Önne, 010-240 42 49

Foto: Marcus Årskog, MSB

Publ.nr MSB1196 – maj 2018
ISBN 978-91-7383-819-1

MSB har beställt och finansierat genomförandet av denna studierapport. Författarna är ensamma ansvariga för rapportens innehåll.

Förord

I takt med digitaliseringen behöver offentliga aktörer tillhandahålla nya samhällsviktiga funktioner och tjänster, och hitta nya sätt att göra detta på. När dessa aktörer väljer att använda sig av publika molntjänster uppstår ett behov av att förstå tjänsterna ur ett informationssäkerhetsperspektiv för att kunna ställa krav på de som tillhandahåller olika typer av molnlösningar.
Den här studien syftar till att kartlägga hur molnlösningar används av kommuner och myndigheter samt identifiera eventuella risker med detta. Studien syftar även till att bilda en uppfattning om hur många som levererar molntjänster till offentliga aktörer samt om de har upplevt några utmaningar i att upphandla molntjänster ur ett informationssäkerhetsperspektiv. Författarna formulerar rekommendationer av åtgärder som kan möta dessa utmaningar.
Studien har genomförts av Örebro universitet på beställning av Myndigheten för samhällsskydd och beredskap (MSB). Det är författarna själva som svarar för sakinnehållet i studien.
Vi hoppas att studien kan bidra till att öka förståelsen för vikten av att bedriva ett systematiskt informationssäkerhetsarbete i takt med samhällets digitalisering.

Margareta Palmqvist
Enhetschef, enheten för systematiskt informationssäkerhetsarbete

Innehållsförteckning

Sammanfattning

Användandet av publika molntjänster som driftsform för att erbjuda verksamheter IT-stöd ökar i vårt samhälle. När offentliga aktörer skiftar till molntjänster innebär det att samhällsviktiga funktioner och tjänster tillhandahålls på detta sätt. Detta skapar nya förutsättningar kring hur funktioner, tjänster och den information som hanteras skall garanteras och hanteras på ett säkert sätt. Studien syftar till att: 1) kartlägga användningen av molnlösningar hos offentliga aktörer, 2) identifiera de samhällsrisker som uppstår med att offentliga aktörer använder sig av molntjänst(er), 3) skapa en uppfattning av graden av centralisering kring tillhandhållandet av molntjänster, 4) kartlägga utmaningar som offentliga aktörer upplevt vid upphandling av molntjänster, samt 5) ta fram prioriterade krav och rekommendationer inom informationssäkerhet som MSB behöver ge ut.

Studien är baserad på en mixad forskningsmetod bestående av en litteraturstudie, en enkät till kommuner och myndigheter, samt semi-strukturerade intervjuer med urval av enkätrespondenterna. De empiriska resultaten visar att en övervägande del av de offentliga aktörerna använder upphandlade molntjänst i sin verksamhet. Den typ av molntjänst som är vanligast förekommande är mjukvara som tjänst. Studien har identifierat ett fåtal molntjänster där det finns tydlig centralisering. De utmaningar som organisationerna ger uttryck för rör i hög grad kunskapsfrågor relaterade till lagar och regelverk, kontraktsfrågor och upphandlingsfrågor. Samtidigt visar studien att det inte verkar finnas en systematik i hur kontrakt med molntjänstleverantörerna följs upp, det är en minoritet av organisationerna som genomför revisioner. Detta gör det svårt att veta exakt vilka av de ställda kraven som uppfylls och till vilken nivå.

Baserat på ovanstående resultat redovisas sju rekommendationer uppdelade på tre prioritetsgrupper.

1. Inledning

Vårt samhälle befinner sig i en stark omvandling från ett industrisamhälle till ett digitalt samhälle. Digitaliseringen innebär att informationsteknologi (IT) används av företag och offentliga aktörer för att göra saker på nya sätt och för att tillhandahålla helt nya tjänster och produkter. Det gör att i dagens samhälle är allt mer verksamhet beroende av välfungerande IT-infrastrukturer för att tillhandahålla dessa tjänster och produkter.

IT-infrastruktur har alltid varit en väldigt komplex fråga och det kan vara svårt att förutsäga konsekvenser av incidenter då det inte alltid är känt vilka beroenden som finns mellan olika system och leverantörer av tjänster. Idag ökas den komplexiteten ytterligare av att både IT-infrastruktur och tjänster i sig kan tillhandahållas via molntjänster, d.v.s. via en lösning ”som möjliggör nätverksåtkomst till en skalbar och elastisk pool av delade fysiska eller virtuella resurser som via självbetjäning levereras och administreras på begäran” (ISO, 2014). Publika molntjänster kan erbjuda många fördelar för köpande organisationer såsom flexibilitet, lägre behov av egen driftskompetens samt kostnadseffektivitet.

Trenden i samhället är att nyttjande av molntjänster är en driftsform som ständigt ökar (Gartner, 2017). I studien som Myndigheten för samhällsskydd och beredskap (MSB) lät genomföra kring konsekvenserna i samhället efter driftstörningen hos Tieto i november 2011 (MSB, 2012), framgick det bland annat att allt fler svenska organisationer väljer att utlokalisera sin IT-drift. Därför kunde en enstaka säkerhetsincident hos en leverantör orsaka relativt långa avbrott i flera viktiga samhällsfunktioner.

När offentliga aktörer skiftar till molntjänster innebär det att samhällsviktiga funktioner och tjänster tillhandahålls på detta sätt. Det finns därför ett behov av att skapa en bättre bild över denna miljö och de beroenden som finns där för att förstå hur förebyggande arbete kan ske.

2. Syfte

Studiens syfte är att:

- Kartlägga användningen av molnlösningar hos offentliga aktörer
- Identifiera de samhällsrisker som uppstår med att, som en offentlig aktör, använda sig av molntjänst(er)
- Få en uppfattning om graden av centralisering, det vill säga hur många företag som står för att tillhandahålla molntjänster till de offentliga aktörerna
- Hur, och om, målgruppen har upplevt utmaningar i att upphandla molntjänster genom att i upphandlingskraven ställa höga krav gällande informationssäkerhet
- Ta fram vilka prioriterade krav och rekommendationer inom informationssäkerhet som MSB, enligt de offentliga aktörerna, behöver ge ut för att underlätta för de offentliga aktörer som påbörjar en process att nyttja molntjänster, baserat på en analys av den kvantitativa och kvalitativa undersökningen.

3. Avgränsningar

Studien studerar informationssäkerhet i molntjänster utifrån kommunerna och myndigheternas perspektiv. Således har ingen empiri samlats in kring faktiska förhållanden hos molntjänstleverantörerna.

Vidare är datainsamlingen gjord vid en specifik tidpunkt. Således har inga data samlats in för att beakta det faktum att upphandling av molntjänster görs i förhållande till den kravbild som gällt vid det aktuella tillfället, och att kravbilder ändras över tid.

4. Forskningsmetod

Forskningsmetoden som använts i denna studie kan beskrivas som en mixad-metod (Venkatesh et al., 2013). Studien kombinerar kvantitativ och kvalitativ metod för att triangulera data, dvs att flera olika tillvägagångssätt används för att samla in data om samma fenomen. Genom detta arbetssätt har vi kunnat verifiera data, men också kunnat åstadkomma både en bredd och ett djup i kartläggningen. Studien bygger på tre delar där olika forskningsmetoder använts för att komplettera varandra: litteraturstudie, enkät och intervjuer.

4.1 Litteraturstudien

Syftet med litteraturstudien var att utgöra en utgångspunkt för design av enkät- och intervjufrågor. Litteraturstudien är genomförd genom att analysera öppna källor, där utgångspunkten har varit att genomföra sökningar i databasen SCOPUS samt via Google. Den första typen av sökningar hade som syfte att ta fram forskningsmässigt kvalitetsgranskade artiklar inom området. SCOPUS valdes som databas för att den har en mycket god täckning kring samhällsvetenskaplig och teknisk forskning inom informationssäkerhet samt användning av IT i offentlig sektor. Den andra sökningen hade som syfte att samla in dokument skrivna av praktiker, vilka normalt inte återfinns i forskningsdatabaser såsom SCOPUS. Sökningen i Google har genomförts med fokus på utmaningar som finns med användning av molntjänster inom offentliga aktörer i Sverige samt i Norden och EU.

4.2 Enkäten

Utveckling av enkäten har genomförts med tre utgångspunkter:

- Litteraturstudien har använts som bas för att utvecklade enkätfrågor skall ha sin grund i existerande kunskap
    - Exempelvis så konstruerades svarsalternativen till fråga 32 (”Baserat på er organisations samlade bedömning, vilka är de tre huvudsakliga informationssäkerhetsriskerna vid användande av molntjänster?”) baserat på hoten listade i ”The Treacherous 12 - Cloud Computing Top Threats in 2016”, vilka identifierats av Cloud Security Alliance (2016).
- Dokument utpekade av MSB för att beakta tidigare specifika arbeten. Dessa dokument var:
    - ”Molntjänster i staten” (Pensionsmyndigheten, 2016)
    - E-delegationens förstudie om sekretess vid outsourcing (E-delegationen, 2015)
    - ”Vägledning, molntjänster” (SKL, 2017)

  - ”Rättsliga frågor vid flytten till molnet – en checklista” (Cloud Sweden, 2011)

- MSBFS 2016:2

Grundläggande för att få bra kvalitet i en statistisk undersökning är att de data som samlas in håller hög kvalitet. Därför har enkäten utvecklats iterativt, där en kvalitetssäkring av enkäten genomförts med MSB samt Svenska Kommuner och Landsting (SKL). Kvalitetssäkringen med SKL genomfördes enligt förordningen om statliga myndigheters inhämtande av uppgifter från kommuner och näringsidkare, SFS 1982:668. Kvalitetsgranskningen omfattade frågor, svarsalternativ och flödesinstruktioner i enkäten samt tillhörande informationsbrev. Den slutliga enkäten återfinns i Bilaga 1.

Datainsamlingen har gjorts gentemot två typer av offentliga aktörer, som båda har centrala funktioner i samhällsviktig verksamhet. Den första gruppen utgjordes av offentliga myndigheter som är rapporteringsskyldig till MSB enligt MSBFS 2016:2 (undantagna: Regeringskansliet, Kommittéväsendet, Säkerhetspolisen, Försvarsmakten, Försvarets materielverk, Försvarets radioanstalt och Totalförsvarets forskningsinstitut). Den andra gruppen utgjordes av svenska kommuner. Svenska kommuner har inte rapporteringsskyldighet till MSB, vilket har gjort att frågor som rör MSBFS 2016:2 inte har ställts till kommunerna.

Datainsamlingen genomfördes via en webbenkät. Inbjudan till enkäten skickades ut via brev samt genom en skriftlig påminnelse (se Bilaga 2, 3, 4, och 5). Det finns inga tillförlitliga och enhetliga register över informationssäkerhetsansvariga för offentliga myndigheter och svenska kommuner att tillgå för utskicken. Därför adresserades inbjudningsbreven till ”Informationssäkerhetsansvarig” och adresser hämtades från SCB:s myndighetsregister för offentliga myndigheter samt från SKL för kommuner.

Totalt skickades enkäten ut till 521 respondenter, fördelat på 231 offentliga myndigheter och 290 kommuner. Den totala svarsfrekvensen visas i Tabell 1.1

Kategori	Utskickade	Svarande	Svarsandel (%)
Offentliga myndigheter	231	119	52 %
Kommuner	290	80	28 %
Totalt	521	199	38 %

Tabell 1.1: Antal utskick och svarsfrekvens

Då studien har haft ett kartläggande syfte har analysen genomförts med hjälp av deskriptiv statistik. Analysen har delats upp på de två respondentgrupperna: offentliga myndigheter och svenska kommuner.

4.3 Intervjuer

Intervjuer har genomförts med ett urval av de aktörer som besvarade enkät-undersökningen. Syftet med intervjuerna var att fokusera på varför- och hur-

frågor relaterat till informationssäkerhet och användning/icke användning av molntjänster, frågor som är svåra att komma åt med enkät.

Intervjuerna utformades som semistrukturerade intervjuer (Denzin & Lincoln, 2005). Det innebär att intervjuerna genomfördes med en lista av teman och frågor att diskutera. Hur djupt varje intervju gick inom ett specifikt tema varierade från intervju till intervju. Intervjuerna anpassades efter vilka svar som respondenten gav. Konkret innebar det att ordningen och den exakta ordalydelsen på frågorna varierade också beroende vad som blev ett naturligt flöde i intervjun, samt att vissa frågor utelämnades beroende på vad som framkommit tidigare under intervjun.

Intervjuguiden innehöll totalt sex olika teman: 1) allmänt om molntjänster/ erfarenheter, 2) arbete med informationssäkerhet innan upphandling, 3) arbete med informationssäkerhet under avtalsperiod, 4) kravuppfyllelse från författningar, 5) riskbaserade krav och 6) identifierade hinder och samhällskonsekvenser. Utvecklingen av dessa teman och tillhörande frågor genomfördes parallellt med enkäten för att säkerställa att intervjuerna skulle utgöra en fördjupning av enkäten. En kvalitetssäkring av intervjufrågorna genomfördes med MSB.

Fördelningen av respondenter visas i Tabell 1.2. Intervjuerna genomfördes som telefonintervjuer. Varje intervju tog ungefär 45 minuter att genomföra och samtliga intervjuer spelades in.

Kategori	**Antal intervjuer**
Offentliga myndigheter	8
Kommuner	8
Totalt	16

Tabell 1.2: Fördelning av intervjuer

Kommunerna valdes ut utifrån storlek för att få en god spridning mellan små, mellanstora och stora kommuner. Myndigheterna valdes ut utifrån storlek samt samhällsfunktion. Vid urvalet togs hänsyn till SCBs indelning av myndigheter i sex kategorier samt Statskontorets indelning av statliga förvaltningsmyndigheter.

En kvalitativ analys av intervjuerna genomfördes. Analysen började med att samtliga intervjuer lyssnades igenom. För varje av de sex teman som nämns ovan noterades viktiga passager i intervjuerna som berörde varför och hur organisationen agerat i en viss riktning. Likaså noterades varför en organisation ansåg att en utmaning var mer eller mindre viktigt, samt de fall där organisationerna gav uttryck för behov av stöd. En andra del i analysen var att knyta intervjuresultaten till enkätresultaten. Detta gjordes genom att intervjufrågorna vid designen är knutna till (har sitt ursprung från) en eller flera enkätfrågor. Därför presenteras intervjuresultaten tillsammans med enkätresultaten i kapitel 6 för att ge en rikare illustration till enkätresultaten.

5. Genomgång av existerande kunskap

Dagens samhälle har en ökande takt i vilken IT används för att skapa nya processer, omvandla gamla processer och för att koppla samman organisationer och deras utrustning. För den offentliga sektorn innebär detta nya möjligheter att ge medborgarna tillgång till publika tjänster. Samtidigt innebär det också nya möjligheter för den offentliga sektorn att i sin tur använda tjänster såsom plattformar och mjukvara tillhandahållna av leverantörer. Tillsammans ger det en mångfacetterad gränsöverskridande miljö som bygger på en komplex infrastruktur i form av molntjänster.

Analytikerföretaget Gartner (2017) har visat att mer än 20 % av offentlig verksamhets IT-budget numera investeras i molnet. De drar, utifrån detta, slutsatsen att 47 % av offentlig verksamhet aktivt använder molntjänster och förutspår att utgifterna för molntjänster kommer att öka med i genomsnitt 17 % per år fram till år 2021. En enkätundersökning utförd av IDG (2016) omfattande 925 beslutsfattare inom teknik både i den offentliga och privata sektorn, visade att användningen av molnteknik kontinuerligt växt från 51 % år 2011 till 70 % år 2016. Även om uppskattningarna kring molnanvändning varierar, så visar studierna på att en betydande del offentlig verksamhet är beroende av molntjänster i olika utsträckning.

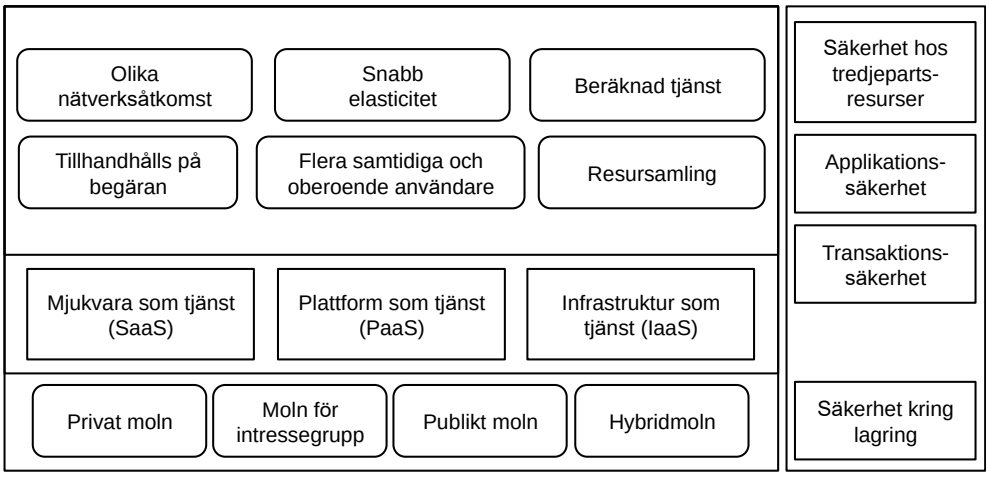
Det finns flera motiv för att använda molntjänster. Bland de vanligaste finns en större grad av administrativ flexibilitet och samarbete inom organisationen, kostnadsbesparingar och förbättrad kundservice dygnet runt. Müller et al. (2015) beskriver molntjänsternas fördelar i linje med de tre nivåer som presenteras i Pearlson och Saunders (2007) ”Business-IT Maturity Model”. De tre nivåerna stödjer affärseffektivitet (kostnadsreduktion och processeffektivitet), förbättrad verksamhetseffektivitet (med inriktning på kärnkompetenser, företagsintegration och samarbete inom företagsamhet) samt affärstransformering (samarbete mellan affärspartners, förbättrad flexibilitet och företagsutveckling genom innovation). CISCO (2011) presenterade liknande strategiska fördelar för offentlig sektor. Fördelarna som de lyfter är kostnadseffektivitet utan att underminera kritiska tjänster, vilket möjliggör t ex sammanslagning, arbetskraftsoptimering, effektiv användning av tillgångar, kostnadsbesparing, anpassade tjänster och spårning av kostnader samt multipla betalningsmodeller.

5.1 Molntjänster

Molntjänster kan definieras på flera olika sätt. I den här rapporten använder vi definitionen från ISO/IEC 17788:2014 (ISO, 2014), den internationella standard som dels tillhandahåller en översikt över vad molntjänster innebär, dels innehåller en rekommendation av termer och definitioner att använda i detta sammanhang. ISO/IEC 17788:2014 definierar molntjänst som ”en eller flera funktioner som ingår i molnbaserade datortjänster […] och anropas via ett

definierat gränssnitt" där en molnbaserad datortjänst är "ett koncept som möjliggör nätverksåtkomst till en skalbar och elastisk pool av delade fysiska eller virtuella resurser som via självbetjäning levereras och administreras på begäran. Resurserna i denna definition inkluderar bland annat servrar, operativsystem, nätverk, mjukvara, applikationer och lagringsutrustning".

Den här typen av resurs som ISO talar om kan skötas på flera olika sätt, där en indelningsgrund är vem som har ansvar för den. Subashni och Kavitha (2011) lyfter fram att en molntjänst kan sättas upp av den egna organisationen i form av ett privat moln (private cloud). En annan lösning är att en grupp med gemensamma intressen går samman och skapar en molntjänst (community cloud), eller att molntjänsten köps in från en leverantör i form av en publik molntjänst (public cloud). Slutligen kan hybridmoln (hybrid cloud) användas, där organisationen kombinerar sin interna infrastruktur, t ex datacentrum, med en extern molnbaserad miljö.



Figur 5.1: Komplexitet i molnmiljön (Översatt från Subashni & Kavitha, 2011)

Med grund i ovanstående definition kan sex centrala egenskaper identifieras hos molntjänster (ISO, 2014), vilka illustreras i Figur 5.1. Enligt Subashni och Kavitha (2011) kan en molntjänst erbjudas via olika nätverksåtkomst (Ubiquitous network). Egenskapen avgör hur användaren ges bred tillgång till fysiska och virtuella resurser, från var och när som helst genom t ex mobiltelefoner, surfplattor, bärbara datorer och arbetsstationer. Tjänsten som tillhandahålls kan också anpassas till olika grad (Measured service), vilket innebär en övervakad, kontrollerad, rapporterad och fakturerad användning av molntjänster. Vidare så innebär multitenans (Multi-tenancy) att flera användare samtidigt och oberoende av varandra kan använda samma exemplar av ett program. Multitenans avser således en mjukvaruarkitektur där en enda instans av programvara körs på en server men som tjänar flera kunder (en grupp användare som delar en gemensam åtkomst genom specifika privilegier till programvaruinstansen). En molntjänst kan även tillhandahållas på begäran (On-demand self-service), vilket innebär att användaren ges möjlighet att enkelt anpassa tjänstens volym efter de behov som finns för stunden. Detta innebär att en molntjänst har en snabb elasticitet och skalbarhet (Rapid elasticity and scalability), genom vilken en proportionell anpassning av tillgång till fysiska eller virtuella resurser till användarens behov kan åstadkommas. En

molntjänst bygger på en resurssamling (Resource pooling), där fysiska eller virtuella resurser aggregeras och abstraheras för att möjliggöra multitenans samtidigt som komplexiteten i processen döljs för kunderna.

Molntjänster kan kategoriseras på flera olika sätt. ISO/IEC 17788:2014 (ISO, 2014) anger sju kategorier av molntjänster, där vi fokuserar på de tre mest vanligt förekommande. Dessa är 1) infrastruktur som tjänst (Infrastructure as a Service, IaaS) – som tillhandahåller infrastrukturmöjligheter, 2) plattform som tjänst (Platform as a Service, PaaS) – som tillhandahåller plattformskapacitet, och 3) mjukvara som tjänst (Software as a Service, SaaS) – som tillhandahåller applikationsmöjligheter till molntjänstkunderna. Figur 5.1 visar en översikt över komplexiteten i molnmiljön, tillsammans med typer av säkerhetsproblem som Subashni och Kavitha (2011) lyft fram: säkerhet kring lagring (Data storage security), säkerhet kring dataöverföring (Data transmission security), säkerhet i applikationerna (Application security), och säkerhet relaterat till leverantörens resurser (Security related to third party resources). Att relatera säkerhet till molntjänstens egenskaper ger dock ett tekniskt fokus, vilket dessa fyra kategorier visar. Risker som är relaterade till molntjänster är dock inte enbart tekniska. Detta visas exempelvis i en empirisk studie om den nederländska offentliga sektorn. Janssen och Joha (2011) delar där in fördelar och risker med mjukvara som tjänst i fyra kategorier: strategiska och organisatoriska, politiska och lagstiftande, tekniska samt ekonomiska.

5.2 Användning av molntjänster – Risker och utmaningar

Fördelarna med användning av molntjänster kan potentiellt undergrävas om riskerna och utmaningarna med dessa lösningar inte är identifierade och hanterade. Nedan diskuteras att faktorer som kvalitet, integritet, säkerhet, leverantörsinlåsning och kontinuitet i affärsverksamheten har i allt större utsträckning blivit frågor som måste hanteras kring molntjänster i offentlig sektor. De anses i många fall vara viktigare än kostnadsbesparingar, särskilt frågor kring informationssäkerhet. Paquette et al. (2010) har i detta sammanhang lyft fram att en viktig utmaning som kommer till följd av molntjänster är svårigheten att hantera och kontrollera leverantörer som finns utanför den egna verksamheten, dvs när molntjänsterna är publika eller hybridlösningar. Enligt dessa författare finns ett behov av en grundlig förståelse för riskerna med molntjänster och att organisationerna skapar starka avtal.

Samtidigt ska detta ses i ljuset av det allmänna informationssäkerhetsarbetet inom offentlig sektor. Microsoft (2014) genomförde under november 2012 till februari 2014 en omfattande undersökning innefattande 12 000 respondenter från offentlig sektor världen över. Undersökningen visade att:

- 45 % använder inte standardiserad informationsklassificering
- 40 % använder fortfarande sekretessavtal på papper och använder dem inkonsekvent
- 36 % har ingen plan i händelse av informationssäkerhetsincidenter

- 34 % har inte budgeterade planer för återställning vid incidenter
- 33 % har inte enhetligt tillämpade informationssäkerhetspolicyer
- 20 % använder inte roller för att hantera åtkomst
- 24 % har adekvata policyer och metoder för säker dataförvaltning

Det har visserligen gått ett par år sedan undersökningen, men resultaten indikerar ändå att det med dessa förutsättningar kan finnas betydande utmaningar med att skapa starka avtal gentemot leverantörer. Flera av ovanstående egenskaper i informationssäkerhetsarbetet är centrala för att kunna ställa krav på leverantörerna.

Microsofts (2014) undersökning visar också att informationssäkerhet inom offentlig sektor har fler utmaningar än de tekniska som lyfts av Subashni och Kavitha (2011). Janssen och Joha (2011) har lyft fram flera utmaningar kring användning av publika molntjänster inom offentlig sektor: potentiell brist på juridisk expertis, ägarskap av data, integritet, åtkomstkontroll och säkerhet, inlåsning av leverantörer, kvalitetssäkring, anpassningsmöjligheter, hantering av prestanda och skalbarhet samt frågan om det ansvar som tjänsteleverantören har. En mer nylig undersökning utförd av IDG (2016) visade på liknande frågor, även om den undersökningen inte specifikt fokuserade på offentlig verksamhet. Undersökningen visade dock att säkerheten hos molntjänster kvarstår som ett hinder för implementering. De tre huvudbekymren vid flytt till molnet är känsligheten hos det data som skall vara åtkomligt för molnapplikationerna, graden av hur verksamhetskritiska applikationerna är för det dagliga arbetet, samt kostnaderna som är associerade med flytten. Undersökningen visade även att de viktigaste utmaningarna för att gå över till molntjänster berör platsen där data ska lagras, säkerheten hos själva molntjänsten (risker för obehörig åtkomst, riskerad dataintegritet och skydd) samt leverantörsinlåsning. Sammantaget visar dessa undersökningar på utmaningar som direkt eller indirekt berör informationssäkerhet. Det innebär för att framgångsrikt införa molntjänster i offentlig verksamhet behöver organisationerna kompetenser inom tekniska, organisatoriska, processmässiga och juridiska områden för att undvika informationssäkerhetsproblem och leverantörsinlåsning. Därför förutspår Gartner (2017) att offentlig verksamhet kommer implementera privata moln dubbelt så fort som publika moln fram till år 2021, trots att privata moln inte levererar samma fördelar som publika moln kan, exempelvis i form av kostnadsfördelar.

Att flytta information till molnsystem som hanteras av ett fåtal leverantörer kan potentiellt utgöra säkerhetsproblem när det kommer till att riskera integritet och konfidentialitet. De integrerade/aggregerade analysramverk som kan finnas i en molnarkitektur och som kan användas på flertalet källor, skulle i grunden kunna möjliggöra att molnleverantören får tillgång till betydligt mer information om sin användarbas än vad som frivilligt avslöjats av varje enskild användare (Filippi & McCarthy, 2012). När det kommer till centralisering är det annars vanligt att existerande forskning fokuserat informationssäkerhet utifrån en centraliserad och decentraliserad arkitektur (ex. Khalid, Yousaf,

Iftikhar, & Fatima, 2016; Pasupulati & Shropshire, 2016). Det gör att riskerna ofta får ett tekniskt fokus och mindre uppmärksamhet har getts till exempelvis samhällsmässiga eller affärsmässiga konsekvenser av att många organisationer använder samma tjänst eller leverantör.

I en annan studie har Paquette et al. (2010) undersökt materiella och immateriella risker med användning av molntjänster. Några av de områden som de diskuterar – konfidentialitet, tillgänglighet och riktighet – har tydlig koppling till informationssäkerhet. Deras undersökning identifierade ett antal essentiella delar som bör ingå i en riskhanteringsplan i offentlig verksamhet. Risker kopplade till konfidentialitet innebär att information riskeras på grund av obehörig åtkomst till privata data, osäkerhet kring de konventioner och lagar som gäller där servrarna är placerade, samt svaga servicenivåavtal (Service Level Agreement) mellan den offentliga verksamheten och leverantören. Att tjänster inte är tillgängliga för behöriga användare kan orsaka allvarliga och kostsamma konsekvenser. Dessa kan, enligt Paquette et al. (2010), bero på överbelastade system, fel i mjukvara, skadliga attacker, strömavbrott, och naturkatastrofer. Innan avtal tecknas behövs således kompetens för att kunna bedöma riskerna och effekterna av även kortare avbrott och vad som därmed är acceptabla nivåer av driftstopp. Inom området riktighet lyfter man fram att information som lagras i molntjänster inte ska förändras på oönskade sätt. Leverantören måste därför kunna visa upp hur data lagras för att inte bli korrupt eller förändrad. Paquette et al. (2010) lyfter specifikt fram att antaganden om detta inte kan göras från kundens sida, utan att det måste finnas uttryckt i servicenivåavtalet. Vidare lyfter de frågan om vems ansvaret är för att korrekta åtgärder vidtas i de fall där problem med riktigheten uppstår.

En annan sammanfattning av informationssäkerhetsutmaningar för molntjänster erbjuds av Zissis och Lekkas (2012). De har sammanfattat utmaningarna utifrån applikationsnivå, virtuell nivå samt fysisk nivå. Enligt dessa nivåer är några större säkerhetshot på applikationsnivå: avlyssning, modifiering av data, dataförlust, brott mot integritet, sessionskapning och exponering för nätverk. På virtuell nivå består säkerhetshoten av: programvarubuggar, förändrad mjukvara eller mjukvaruavbrott, distribuerat avbrott av tjänst samt störd kommunikation. På den fysiska nivån handlar det om: nätverksangrepp, hårdvarustöld, modifiering och avbrott, distribuerat avbrott av tjänst, missbruk av infrastruktur och naturkatastrofer.

5.3 Molntjänstincidenter

ENISA (2013) definierar molntjänstincident som “a breach of security or a loss of integrity that has an impact on the operation of network and information system core services, which public administrations and market operators provide. The ‘reportable incident’ is the one that has deemed significant impact”. Graden av betydande inverkan beror på hur kritiska de berörda molntjänsterna är, vilket i sin tur kan bedömas på två sätt. Det första sättet berör tjänster som tillhör den kritiska infrastrukturen som säkerställer den dagliga verksamheten. Det andra sättet berör tjänster som erbjuder funktioner för medborgarna som är kritiska.

Enligt Fiondella et al. (2013) kan incidenter kategoriseras på fem sätt. Dessa fem sätt är avbrott (tillgång till tjänster), sårbarhet (platsspecifika sårbarheter hos molntjänstleverantören), automatiska fel (genererade av automatiska uppdateringar av systemen som kan innebära avbrott av kärnfunktioner), dataförlust (oavsiktlig förlust av data) och hackning (intrång i ett system av hackare som syftar till att äventyra konfidentialitet och integritet). Bland dessa fem sätt är avbrott och sårbarhet de vanligaste förekommande och snabbast växande.

Cloud Security Alliance (2013) rapporterade, baserat på en undersökning av 172 unika incidenter över hela världen under åren 2008-2012, att 75 % av incidenterna hade en känd orsak medan resterande 25 % var incidenter som avslöjats utan särskilt mycket detaljer om dem. Studien rapporterade även att osäkra gränssnitt och API:er, dataförlust och dataläckage samt hårdvarufel tillsammans står för 64 % av alla molntjänstincidenter globalt. Av dessa bedömdes osäkra gränssnitt och API:er utgöra det största hotet. Deras slutsats är baserad på information som finns att tillgå online. Andra kända stora hot omfattar missbruk och kriminell användning av molntjänster, ondskefulla aktörer hos leverantören som har tillgång till resurser (malicious insiders), delade teknikproblem, konto- eller tjänstekapning, naturkatastrofer, stängning av molntjänst, molnrelaterad skadlig kod och otillräcklig infrastrukturdesign och planering.

Karaktären på molntjänstincidenter visar att det behövs olika typer av åtgärder, både från offentliga organisationers och tjänsteleverantörernas sida. Som lyfts fram ovan är det centralt med ett anpassat servicenivåavtal som regelbundet följs upp. Därigenom kan leverantörernas ansvar säkerställas, inklusive obligatorisk rapportering i samband med hot och incidenter och eventuella åtgärder. Utöver detta föreslås ofta följande åtgärder (Bhargava, 2016; Cloud Security Alliance, 2013; EU, 2013; Fiondella et al., 2013; MSB, 2015):

- Upprättande av en gemensam respons- och återställningsplan tillsammans med molntjänstleverantören.
- Övervakning och analys av utvecklingen och uppkomsten av olika typer av incidenter.
- Analys av data från olika källor som varit inblandade i någon incident, t ex avseende hur kännbar incidenten var, varaktigheten samt antalet drabbade kunder.
- Diagnosverktyg och säkerhetsåtgärder som övervakar infrastrukturen och molntjänsterna.
- Konsultation av EU-ENISAs vägledning om hur man upphandlar molntjänster på ett säkert sätt.
- Konsultation av ISO/IEC 27018: 2014 och ISO/IEC 29100: 2011 för att utvärdera leverantörernas överensstämmelse avseende dataskydd.
- Konsultation av EUs PICSE-riktlinjer (PICSE, 2014) för upphandling av molntjänster.

- Konsultation av MSBs guide till informationssäkerhet vid upphandling.

5.4 Molntjänster inom EU och Norden

Europeiska unionen (EU) har lyft fram vikten av molntjänster som en katalysator för en stark digital ekonomi, som är avgörande för Europas tillväxt och konkurrenskraft. Det beräknas att molntjänster kan bidra till EUs BNP med 940 miljarder euro, skapa 450 000 nya företag, mer än 3 miljoner arbetstillfällen samt reducera kostnaden med 20 % för majoriteten av de organisationer som anammar molntjänster (EU, 2013). EUs politik för molntjänster baseras på ”Unleashing the Potential of Cloud Computing in Europe Strategy”.

Informationssäkerhet har en central del i denna strategi. Det syns i att två av de centrala åtgärderna är: 1) att utveckla en säker och rättvis kontraktsmodell för att reglera frågor som rör datasäkerhet och integritet, 2) att formulera en standardkarta för interoperabilitet och dataöverförbarhet vid molntjänster samt att stödja arbetet med att utveckla ett certifieringssystem inom EU för tillförlitliga molnleverantörer.

ENISA (2014) klassificerar offentliga moln inom EU-länderna i fyra grupper. Indelningen är gjord baserad på nationella strategier för molntjänster eller på digitala agendor och hur långt man har kommit i detta arbete:

- Tidiga användare – vissa specifika beslut har fattats och ett antal initiativ är redan på plats. Här ingår bland annat Storbritannien, Spanien och Frankrike.
- Välinformerade – strategier finns för storskalig implementering men är inte fullt ut på plats. Här ingår t ex Sverige, Danmark, Norge, Finland, Nederländerna, Tyskland, Moldavien, Irland, Slovakien, Belgien och Grekland.
- Innovatörer – här saknas fortfarande strategier på nationell nivå men på gräsrotsnivå finns vissa initiativ. Här ingår t ex Italien, Österrike, Slovenien, Portugal och Turkiet.
- Tvekande – man är fortfarande i planeringsstadiet och det saknas en nationell molnstrategi, däremot kan det finnas en digital agenda. Här ingår Malta, Rumänien, Cypern och Polen.

Denna klassificering indikerar också att regeringar i de europeiska länderna har en viss skillnad i nivå i politiska prioriteringar, ekonomiska förhållanden, teknisk infrastruktur och framför allt styrning (Accenture, 2013). Några fokuserar på sänkta kostnader, andra på att bygga infrastruktur eller på att uppmuntra medborgarna att engagera sig i den offentliga verksamheten. De flesta länder är fortfarande i ett pilotsstadium avseende molntjänster där en stor helhetsbild framförallt saknas. Det saknas också ofta samordning mellan olika initiativ. Även om molnrelaterad säkerhet kontinuerligt förbättras finns det fortfarande stora orosmoment beträffande dataskyddslagar i EU och runt regelverk för datahantering (lagring och konfidentialitet) som sker av tredje part i ett annat land. Detta utgör ett hinder eftersom offentlig verksamhet inom

EU måste följa EUDPD (European Union Data Protection Directive) (Microsoft, 2014). Under 2016 ersattes EUDPD av GDPR och denna förändring har betraktats som en av de viktigaste förändringarna avseende datasekretessregleringen de senaste 20 åren. Lagen träder i kraft under 2018 och dess syfte är att harmonisera lagar om integritetsskydd inom Europa för att skydda och stärka dataintegriteten för alla EU-medborgare. Organisationer som inte uppfyller kraven kan utsättas för stora böter i händelse av kränkning av personuppgifter enligt denna förordning.

Enligt en studie från EU (2014) om upptagande av molntjänster i Europa står anställda inom finanssektorn för användningen av flest molntjänster medan offentlig verksamhet har den lägsta användningen av alla. Molntjänster inom offentlig verksamhet används främst för att möjliggöra kontorssamarbete, för att hantera lagring, CRM (Customer Relationship Management), säkerhetstjänster eller Enterprise Resource Planning (ERP).

Företag i Norden har en framåtskridande position när det gäller att använda molntjänster i Europa. Deras användning i Norden är nästan dubbelt så stor som EU-genomsnittet. Faktum är att de nordiska länderna är de främsta aktörerna enligt olika IT-relaterade index. Till exempel enligt FNs eGovernment Development Index, EUs Digital Agenda Scoreboard, World Economic Forums Network Readiness Index och EUs Digital Economy and Society Index (DESI). Norden lyckas bäst med att integrera ny teknik i sina strategier för konkurrenskraft (Dutta & Mia, 2011).

Enligt en studie utförd av Radar (2017) innefattande Finland, Norge och Sverige har det skett en stark marknadssegmenttillväxt i publika moln som tillsammans utgör 51 % av de totala molnutgifterna för organisationer i dessa länder. Med hänvisning till IT-beslutsfattarnas uppfattning visar studien att användningen av publika moln förväntas öka från 3 % av den totala IT-utgiften till 27 % fram till år 2020. Bortsett från att bara vara användare har även nordiska företag en "hög grad av beroende" av molntjänster för sin kritiska affärsverksamhet. Dock har mindre än hälften av dem (förutom Sverige) formellt definierat säkerhetspolicyer relaterade till användning av IT. Trots att företag i Norden leder resten av EU-länderna i implementation av molntjänster återstår fortfarande ekonomiska vinster som skulle komma från ett större nyttjande av den växande globala användningen. De största utmaningarna när det kommer till implementation av molntjänster i Norden är de juridiska frågorna kring säkerhet och personuppgifter. I det här fallet är lokalisering ett viktigt rättsligt krav som alla nordiska länder måste hantera. Enligt de lagliga kraven kan personuppgifter endast överföras till länder inom EU/EES, så länge som en korrekt säkerhetsnivå upprätthålls. Data kan också överföras till vissa länder utanför EU/EES om landet som de överförs till samtycker till att uppfylla EU-standarder enligt direktivet Safe Harbors principer. Företagen måste se till att molntjänstleverantörerna har den säkerhet och infrastruktur som krävs för att organisationerna skall kunna leva upp till den säkerhetsnivå och de nationella lagar som krävs, vilket kan göra implementationen av molntjänster väldigt komplex på grund av deras distribuerade natur (Nordiska ministerrådet, 2012).

För att hantera sådana hinder har det Nordiska rådet en aktiv roll. I Nordiska rådet inrättades 2011 en informell arbetsgrupp för det nordiska offentliga molnsamarbetet (Nordiska ministerrådet, 2012). Det nordiska samarbetet medför möjligheter att fokusera på frågorna tillsammans, eftersom de nordiska offentliga verksamheterna delar organisationslikheter och då regionerna har en solid grund (stark infrastruktur och stor mognad när det gäller e-förvaltning) vilket är positivt för att implementera molntjänster i regionen. De frågor som man skall samarbeta kring är bland annat kunskapsdelning, regler, standardisering, upphandlingsprocesser och verktyg, samt hur man skapar en attraktiv miljö för etablering av datacenter.

Nedan presenteras en summering av utvecklingen inom molntjänster i Norden (ENISA, 2014; JUHTA, 2015; MSB, 2015; Nordiska ministerrådet, 2012; WEF, 2016).

5.4.1 Danmark

- Danmark är ett av de ledande länderna i antal molntjänster inom offentlig sektor.
- Danmark har en gemensam digital strategi som bidrar till att öka användningen av digitala tjänster för att effektivt förnya den offentliga sektorn.
- Programmet ”Digitale veje til vækst” (Digitala vägar till tillväxt) från 2011 innehåller åtgärder för att övervinna hinder för användning av molntjänster, inklusive riktlinjer för bättre säkerhet och integritet för offentliga myndigheter och privata företag.
- cloud.dk erbjuder offentliga molntjänster helt i överensstämmelse med den danska datalagen.
- Dataskyddsmyndigheten har verifierat att molntjänsten Microsoft Office 365 överensstämmer med EUs och den danska lagstiftningen.
- Reglerna för skydd av personuppgifter har anpassats av en arbetsgrupp för snabb tillväxt av molnbaserade lösningar inom den offentliga sektorn (Danish Government, 2013).
- Digitaliseringsbyrån tog 2012 fram en riktlinje om lagstiftningskrav och den kontraktsmiljö som är relaterad till molntjänster (Digitalisér, 2012).

5.4.2 Finland

- Finlands parlament har antagit en rapport med titeln ”Produktiva och innovativa Finland - Digital agenda för år 2011-2020”. Denna rapport inkluderar molntjänstinitiativ.
- Enligt Eurostat (2017) leder Finland inom EU med den högsta andelen molntjänster hos företag. Enligt Network Rediness Index, ligger Finland på andra plats och har därmed den högsta placeringen inom EU. De faktorer som har lett till Finlands höga globala rankning är god

tillgång till den senaste tekniken, riskkapital och internetanslutning för företag (WEF, 2016).

- The Public Procurement General Terms and Conditions for IT Procurement (JHS 166 - Julkisen hallinnon IT-hankintojen yleiset sopimusehdot /JIT 2015) tillhandahåller detaljerade villkor för offentlig IT-upphandling, inklusive upphandling av mjukvarutjänster som produceras som en molntjänst som är avsedd för specifika organisationer eller användargrupper (JUHTA, 2015).
- Finland har genom Handi-programmet, ett nyckelprojekt för digitalisering av offentliga tjänster, automatiserat processen för att verifiera officiella uppgifter i samband med anbudsförfarandet för offentlig upphandling. Programmet medfinansieras av EU (VM, 2018).

5.4.3 Norge

- Norge har en nationell digital agenda baserad på den digitala agendan för Europa och den globala trenden.
- Norge har stark tillväxt i användningen av molntjänster. Företag som använder molntjänster ökade från 29 % 2014 till 38 % 2015.
- Den genomsnittliga mognadsgraden för molntjänster i Norge har ökat signifikant (47 % från 2015 till 2017) (Radar, 2017).
- En av de viktigaste åtgärderna i den nationella IKT-politiken för en användarcentrerad och effektiv offentlig förvaltning är regeringens åtagande att presentera en nationell strategi för användning av molntjänster.
- Norska dataskyddsmyndigheten har publicerat en riktlinje för användande av offentliga molntjänster. Detta var ett resultat av att kommunerna Narvik och Moss förbjöds använda molntjänster år 2012. Deras användning ansågs utgöra ett brott mot säkerhet och integritet för känsliga data. Norska dataskyddsmyndigheten anklagade nämligen kommunerna för att inte ha någon aning om var i världen deras data lagras och vem som kan få tillgång till dem. De tjänster som användes i kommunerna var Googles molntjänster.

5.4.4 Sverige

- Regeringskansliet publicerade 2011 den digitala agendan ”IT i människans tjänst – en digital agenda för Sverige”. Denna agenda inkluderar molntjänster som en av de strategiska frågorna för ekonomisk tillväxt.
- Sverige outsourcar molntjänster i brist på en nationell gemensam molntjänst.
- Det finns ett stort antal privata företag i Sverige, nationella och internationella, som tillhandahåller privata och publika molntjänster.
- Datainspektionen har riktlinjer för användande av molntjänster. Datainspektionen har även gjort tillsyn av molntjänstanvändning, t ex

nr 1475-2013 (Datainspektionen, 2014a) som handlar om hur personliga uppgifter hanteras i Microsoft Office 365. I en genomförd tillsyn nr 2633-2014 (Datainspektionen, 2014b) har de kritiserat bland annat användningen av Google Apps for Education i de fall avtal saknas för att säkerställa att personuppgiftslagen följs.

- SKL använder flera olika molntjänster, bland annat Microsoft Office 365 och Google Apps for Education. De har riktlinjer för hur användningen bör ske för att vara i enlighet med Datasinspektionens krav för att undvika tvivelaktig hantering av personuppgifter (SKL, 2017).
- Digitaliseringskommissionen upprättades 2012-2016 för att utveckla Sveriges framtida färdplan för ett digitalt samhälle.
- MSB har ansvar för att stödja och samordna samhällsinformationssäkerhet, inklusive molntjänster.
- CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter. Verksamheten bedrivs vid MSB.
- Cloud Security Alliance (CSA) tillhandahåller information inriktad på att främja svensk användning av bästa praxis för att tillhandahålla god säkerhet inom molntjänster.
- Cloud Sweden är ett oberoende kompetensnätverk kring frågor som rör molntjänster. Nätverket startade i mars 2010. De har bland annat tagit fram checklistan ”Rättsliga frågor vid flytten till molnet”.
- Baserat på resultaten från en undersökning om molntjänster som genomfördes bland 211 offentliga myndigheter i Sverige år 2015 föreslog Pensionsmyndigheten åtta åtgärdsplaner för öppen och effektiv hantering av molntjänster i Sverige.
- eSamverkansprogrammet (eSam) är en frivillig fortsättning efter E-delegationen och består av 21 medlemmar samt SKL. Syftet med programmet är att vara ett forum för fortsatt samverkan mellan myndigheter och SKL och programmet ska bygga vidare på de kunskaper och erfarenheter som byggts upp inom ramen för E-delegationen. En viktig uppgift för programmet är att ge ut vägledningar som skapar förutsättningar för att öka digital samverkan inom offentlig förvaltning. En vägledning är ”Outsourcing – en vägledning om sekretess och persondataskydd”. Denna vägledning bygger vidare på den förstudie som E-delegationen gjorde under våren 2015, ”Sekretess och outsourcing” (E-delegationen, 2015).

Enligt Europas digitala framstegsrapport (EDPR, 2017) fortsätter Sverige att tillhöra det "högpresterande landklustret" bland de 28 europeiska medlemsländerna, Sverige rankas som tredje land efter Danmark och Finland. Å andra sidan är de digitala offentliga tjänsterna i Sverige relativt svaga (åttonde plats i EU). I undersökningen som gjorts av Pensionsmyndigheten

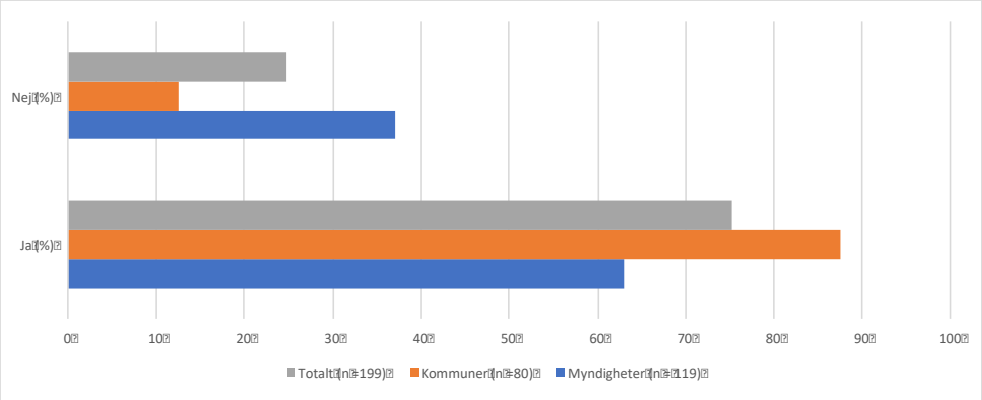
(2016) konstateras att 23 % av de offentliga myndigheterna använder molnrelaterade IT-plattformar och att över hälften av myndigheterna (53 %) har medellånga eller omfattande erfarenheter av SaaS. Riskhantering inom den offentliga sektorn är dock ett stort problem. MSB (2015) rapporterade i detta sammanhang att 65 % av de svenska myndigheterna inte har någon riskhantering och kontinuitetsplan. Med tanke på samhällets växande beroende av den digitala miljön kräver därför Försvarsberedningen en kontinuerlig utvärdering av IT-robustheten i samhället (MSB, 2015).

6. Empiriska resultat

Resultatet av enkätundersökningen och intervjuerna redovisas här i tio delområden. Det första avsnittet redovisar användandet av publika molntjänster (kommer fortsättningsvis refereras till som molntjänster). Därefter följer två avsnitt om vilka typer av tjänster och leverantörer som är vanligast. Syftet är delvis att analysera molntjänst- och leverantörskoncentration. Sedan följer ett avsnitt om var molntjänsterna finns geografiskt. Därnäst följer tre avsnitt som rör olika aspekter kring informationssäkerhetskrav och molntjänster, krav som ställs, hur krav följs upp och hur kravs bemöts av leverantörerna. I det efterföljande avsnittet redovisas vilka utmaningar som organisationerna ser i förhållande till molntjänster. Det sista avsnittet handlar om incidentrapportering enligt 9 § MSBFS 2016:2.

6.1 Användandet av molntjänster hos offentliga aktörer

I undersökningen ställdes en generell fråga om organisationerna har några upphandlade molntjänster. Figur 6.1 visar profilen som finns i svenska kommuner och myndigheter. När de två kategorierna slås samman har 75 % av de tillfrågade organisationerna, dvs både kommuner och myndigheter en upphandlad molntjänst. Kommunerna verkar ha upphandlat molntjänster i en högre grad (88 %) än myndigheter (63 %). Skillnaderna skall dock tolkas med viss försiktighet då skillnader i svarsfrekvensen kan påverka utfallet.



Figur 6.1: Andelen kommuner och myndigheter som har upphandlad molntjänst som stöd för delar och/eller hela verksamheten

Denna bild delas dock (enligt intervjuerna) av en av kommunerna: ”Det är jätteintressant tycker jag, och jag har faktiskt tagit upp det på konferenser att kommuner brukar ju vara sist i ledet men nu tuffar vi som ett glatt litet tåg rakt upp i molnet medan de statliga myndigheterna, som jag uppfattar det, inte gör det. Det är ju världens smartaste grej, att gå via skolan, det är ju snudd på att det är ett samhällsproblem kan jag tycka. Det är så uppenbart att man har hittat en väg in till kommunerna via licenserna och kommunerna håller inte emot. Det är en ekonomisk fråga och en resursfråga, att man har hittat att

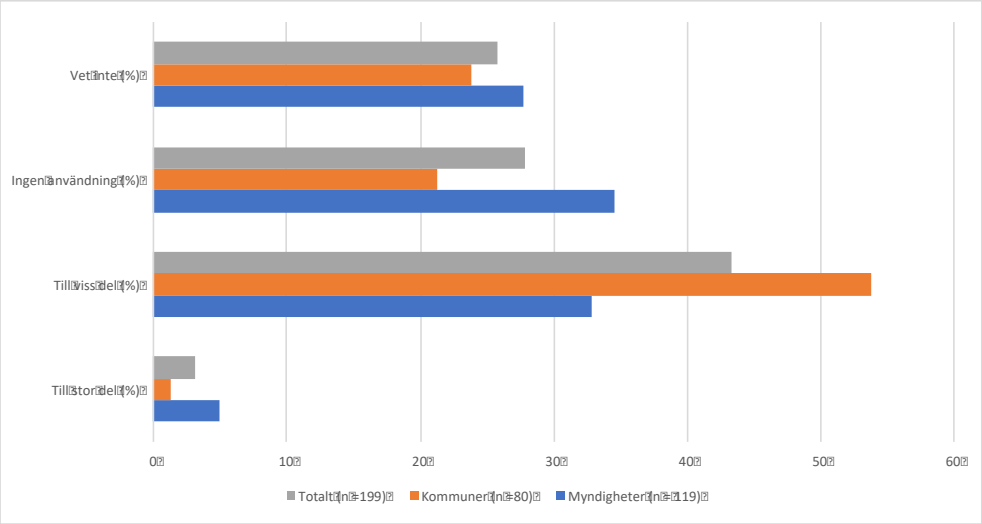
kommunerna inte hinner med verksamheten och då har man via skolan som är modiga hittat en väg".

De licenser som diskuteras har flera kommuner nämnt som problematiska då det egentligen inte finns något alternativ. Det är traditionella licenser som omvandlats till molnlicenser och det finns inte längre något "offline"-alternativ till dem. Därmed ser de det inte som att det varit ett aktivt val med molnet utan att de mer eller mindre är intvingade i det. Att de blir "intvingade" innebär dock inte att de måste ta steget fullt ut. Det finns även de som valt ett mer försiktigt angreppssätt: "Den enda molntjänsten som vi har och betalar licens för är [utelämnat namn på tjänst] men vi använder den inte ännu, den är inte driftsatt. […] Anledningen till att vi inte har driftsatt är att vi inte har kompetens, vi är inte säkra, eller jag är inte säker på avtalet exakt och jag måste titta på det innan och exakt var de har sina servrar. De kan ju ligga inom EU och då är det ju okej, men det får ju inte ligga utanför. Jag tror de har dem i Holland och jag tror de är på väg att bygga i Sverige och så har de på Irland, men det måste ju dokumenteras först innan vi går ut i detta, så att vi är säkra på vart det finns. Vi har betalat licenser för detta i några års tid men aldrig gått in i det."

Dessa två berättelser ger alltså två helt olika bilder av hur kommuner resonerar angående molntjänster. I fall där befintliga licenser omvandlats till molnlicenser är en konsekvens att det inte har skett någon egentlig upphandlingsprocess. Det betyder att det därmed inte ställts krav avseende informationssäkerhet och att eventuella råd vid upphandling av molntjänster inte kunnat följas. Vi ställde frågor vid intervjuerna om vilka krav som ställts vid upphandling och fick följande svar från en av kommunerna: "Tankarna kring detta och problematiseringen kring detta är så långt ifrån verkligheten att det blir alldeles absurt. Man kan bli fnissig. Verkligheten är ju att jättemånga kommuner redan är i molnet." Kommunen berättar om att upphandlingen ofta inte sker på detta sätt utan att verksamheter agerar utan IT-avdelningens inblandning och att det ofta inte handlar om en upphandling utan om att licenser omvandlas. Att kommunerna är före myndigheterna i molnet kan förklaras av sådana omständigheter. En annan förklaring är att till skillnad från myndigheterna så består kommunerna av olika verksamheter och flera av kommunerna uttrycker att deras IT-personal inte alltid involveras utan att verksamheterna ofta fattar beslut på egen hand. En kommun uttrycker det som att: "De [verksamheterna] har velat lösa sina problem men kanske inte insett att det skapar nya problem". Ytterligare en annan omständighet är att vissa licenser till och med har varit gratis.

Att åtminstone vissa av myndigheterna har en något försiktigare inställning fick stöd av följande citat: "vi har inte upphandlat molntjänster till kärnverksamheten […] Myndigheten har gjort ställningstagandet att inte lägga ut någon verksamhetskritisk information i molntjänster. Allt som rör verksamhetskritisk information hanteras i egen datorhall då man har gjort bedömningen att det skulle innebära för stor risk att lägga det i molntjänster". Myndigheten uttryckte att de är priviligierade som har denna möjlighet och inser att alla inte har det, dvs att alla inte kan ha egen datorhall. För

myndigheten är det dock viktigt då tillgängligheten till deras verksamhetskritiska information är av stor samhällsbetydelse.



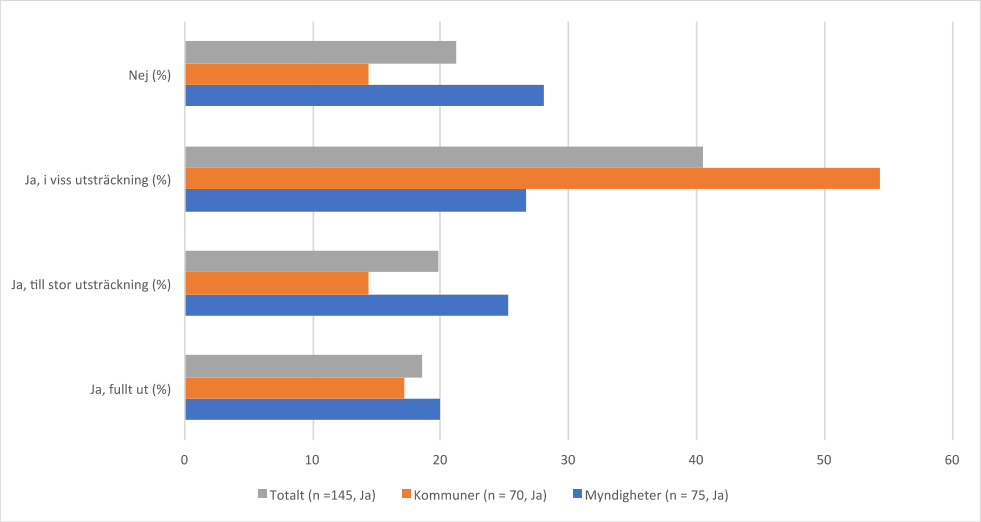
Figur 6.2: I vilken utsträckning använder anställda egna molntjänstkonton, dvs konton som inte är arbetsrelaterade

Användning av upphandlade molntjänster är en sanktionerad typ av användning. Sett till molntjänsters natur, att de är enkla att skaffa och att flera finns i gratisversioner, kan det förekomma användning på anställdas eget initiativ. Dessa molntjänster är privat knutna till den anställda men kan användas i tjänsten. Figur 6.2 visar organisationernas uppskattning i vilken utsträckning deras anställda använder egna molntjänstkonton hos t ex Dropbox i tjänsten, dvs konton som inte är arbetsrelaterade. Resultaten visar att 46 % av organisationerna uppskattar att deras anställda använder den här typen av molntjänstkonton, antingen till viss del eller till stor del. Användandet uppskattas som högre i kommunerna (55 %) än i myndigheterna (38 %). Kanske kan graderna av decentralisering i dessa olika typer av organisationer bidra till skillnaden. Det är också en betydande andel, 26 %, som inte vet i vilken utsträckning denna typ av molntjänstkonton används. Detta illustreras också av följande fritextsvar: ”vi har inte utfört någon intern revision kring användande av icke godkända molntjänster”.

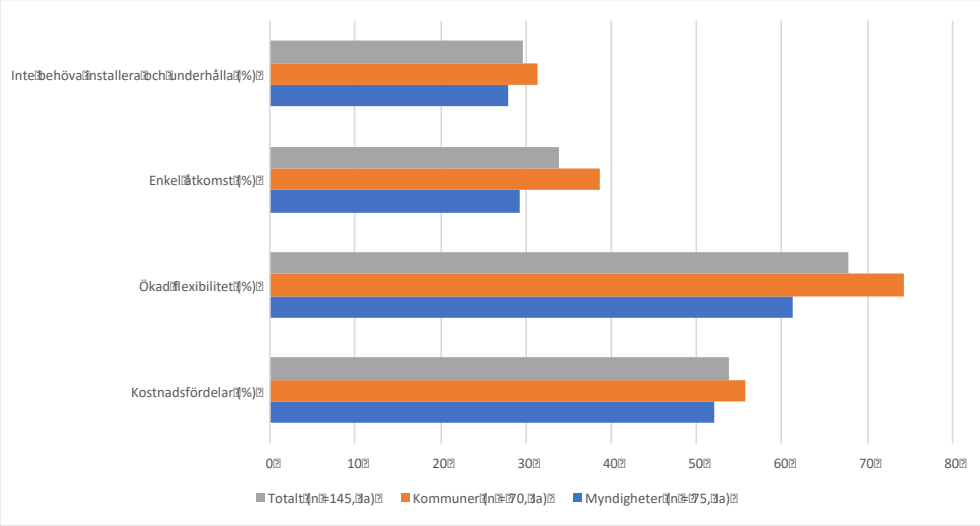
Anledningen till att medarbetarnas egna molntjänstkonton används kan naturligtvis vara flera. En anledning kan vara att anställda anser sig behöva viss funktionalitet för att lösa sina arbetsuppgifter. I enkäten fick organisationerna därför ange i vilken utsträckning de ansåg att de erbjuder upphandlade och godkända molntjänster, som alternativ till molntjänster införskaffade av användaren själv. Figur 6.3 visar att en majoritet (79 %) av organisationerna anser sig erbjuda sådana molntjänster i viss utsträckning, i stor utsträckning eller fullt ut. Det är dock endast cirka en femtedel som anser att de erbjuder molntjänster som fullt ut gör att anställda inte bör ha behov av att använda egeninförskaffade molntjänstkonton.

En av de större myndigheterna svarar dock att de inte tillåter anställda att använda sådana tjänster men att det ändå kan förekomma: ”Någon i verksamheten kan ha beställt en tjänst för ett lägre pris, en gratistjänst, ett lågt

pris utan att ha haft kontakt med oss som arbetar med de här frågorna men vi bedömer nog att den risken också är låg, vi tar det på allvar, vi pratar om det löpande". Som exempel tar respondenten upp att det skulle kunna ske inom ett projekt att man måste kunna dela stora filer och att man vill ha en gemensam yta i form av ett projektrum i någon extern funktion eller en Dropbox-lösning: "Då kommer de till oss på något sätt. Jag tror att de flesta är medvetna om att vi kan inte bara kan lägga ut grejer. Jag har ju varit involverad i saker som kostar nio kronor i månaden för att säkerställa att det blir rätt. Sedan vet man inte, man vet inte om det är någon lokal chef som tycker att det verkar jättefinurligt och planerar alla medarbetaraktiviteter i något olämpligt verktyg".



Figur 6.3: I vilken utsträckning erbjuder organisationerna godkända molntjänster, som alternativ till molntjänster införskaffade av användaren själv



Figur 6.4: Huvudsakliga anledningarna till att kommuner och myndigheter använder molntjänster

Figur 6.4 visar de fyra huvudsakliga anledningarna till att kommuner och myndigheter väljer att använda sig av upphandlade molntjänster. Oavsett om vi ser till snittet mellan dessa två typer av organisationer, eller till typerna var för sig är rangordningen densamma. Enligt enkätsvaren är huvudanledningarna, i

fallande ordning, ökad flexibilitet (68 %), kostnadsfördelar (54 %), enkel åtkomst (34 %) och att inte behöva installera och underhålla (28 %).

Flexibilitet kommer från att kunna hantera komplexa IT-frågor, minimera arbetsbelastning och kunna möta kapacitetsbehov ”on-demand”. Därigenom kan organisationerna förbättra servicen till verksamhetens kärnfunktioner, och fokusera på verksamhetskritiska uppgifter samtidigt som kostnaderna minimeras. Skalbarhet och att möta en ökande efterfrågan på IT-tjänster är också viktiga faktorer. Detta kan exemplifieras med ett av fritextsvaren från en myndighet: “IT-driften blir bekvämare att hantera bokföringsmässigt med löpande fakturor istället för höga investeringar vissa tider. Molntjänster är skalbara i förhållande till hur verksamheten ökar/minskar.”

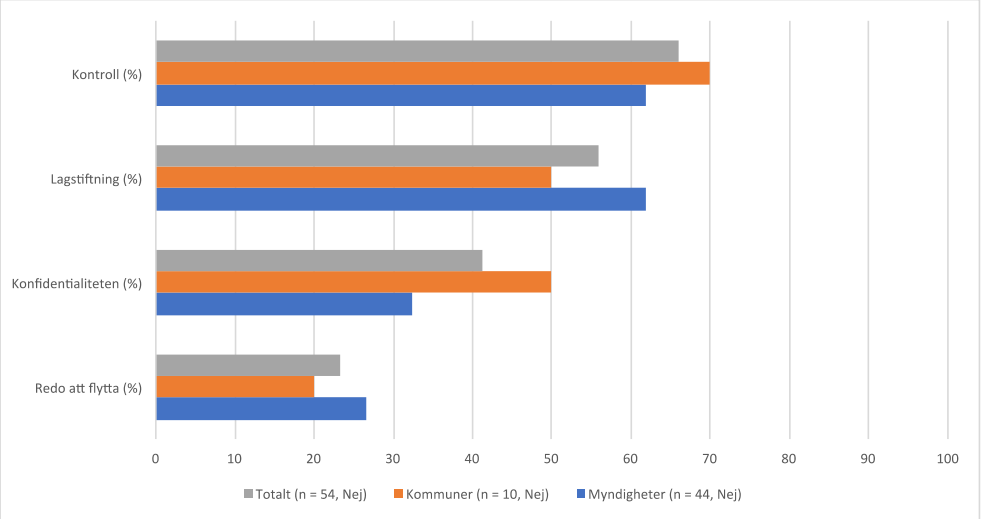
Samtidigt visar fritextsvaren på att i vissa fall har organisationerna inga andra alternativ än molnlösningar. En kommun uttryckte “[f]ör vissa funktioner/tjänster erbjuds det inga alternativ än molntjänster”. Det har stora likheter med det en av myndigheterna gav uttryck för, att det ”[f]inns vissa tjänster som är svåra/omöjliga att få på annat sätt än som molntjänst”. Detta exemplifierades även, som tidigare presenterats, i intervjuerna med kommunerna.

Det kan vara en bidragande orsak till att organisationerna inte lägger ett primärt fokus på om den efterfrågade funktionaliteten tillhandahålls via en molntjänst eller ej, vilket följande fritextsvar får illustrera: “Vi lägger ingen särskild vikt vid om det är en molntjänst eller inte under förutsättning att vi får den funktion som efterfrågas. Dock beaktar vi normalt våra informationssäkerhetskrav utifrån genomförda systemsäkerhetsanalyser och lägger inte ut information i molntjänster om vi har bedömt att det inte är lämpligt.” Samtidigt visar citatet på att organisationerna arbetar med att balansera behovet av funktionalitet som stödjer verksamheterna och informationssäkerhet. Dessutom kan upphandlade molntjänster bidra till informationssäkerheten, genom att medarbetarna använder dessa tjänster i stället för tjänster de funnit själva och som inte kvalitetssäkrats. Detta illustreras av följande svar från en av kommunerna: “även förbättrad informationssäkerhet då kommunen erbjuder tjänster som annars skulle utnyttjas av privata alternativ”.

När det gäller huvudsakliga orsakerna till varför organisationerna inte har upphandlat molntjänster så visas de i figur 6.5. Organisationerna fick ranka de tre viktigaste anledningarna utifrån elva olika kategorier (se fråga 1.1 i Bilaga 1). Här visar vi de fyra högst rankade orsakerna. I fallande ordning så är anledningarna följande, risk att förlora kontrollen över informationen (66 %), risk att inte kunna uppfylla gällande lagstiftning (56 %), risk att äventyra konfidentialiteten i informationen (41 %), och att organisationen inte är redo att flytta existerande system till molntjänster (23 %). Vid sidan av dessa kategorier skall också lyftas fram fritextsvar som visar på att det inte funnits något verksamhetsbehov att anskaffa molntjänster.

Enkäten visar att kommunerna (50 %) är mer upptagna med konfidentialitetsfrågan än myndigheterna (32 %). Samtidigt skall sägas att den frågan är tätt förknippad med lagstiftningen, där förhållandet mellan

kommunerna och myndigheter är det omvända. Att detta är en komplex fråga gör att en försiktighetsprincip tillämpas, något som illustreras av följande citat från en kommun: “Vi säger i våra riktlinjer att det [molntjänst] INTE är tillåtet. Och på de små områdena där det finns är det moduler vi blivit intvingade i av befintliga leverantörer”.



Figur 6.5: Vilka är de viktigaste anledningarna till att organisationer inte har en upphandlad molntjänst som stödsystem för verksamheten

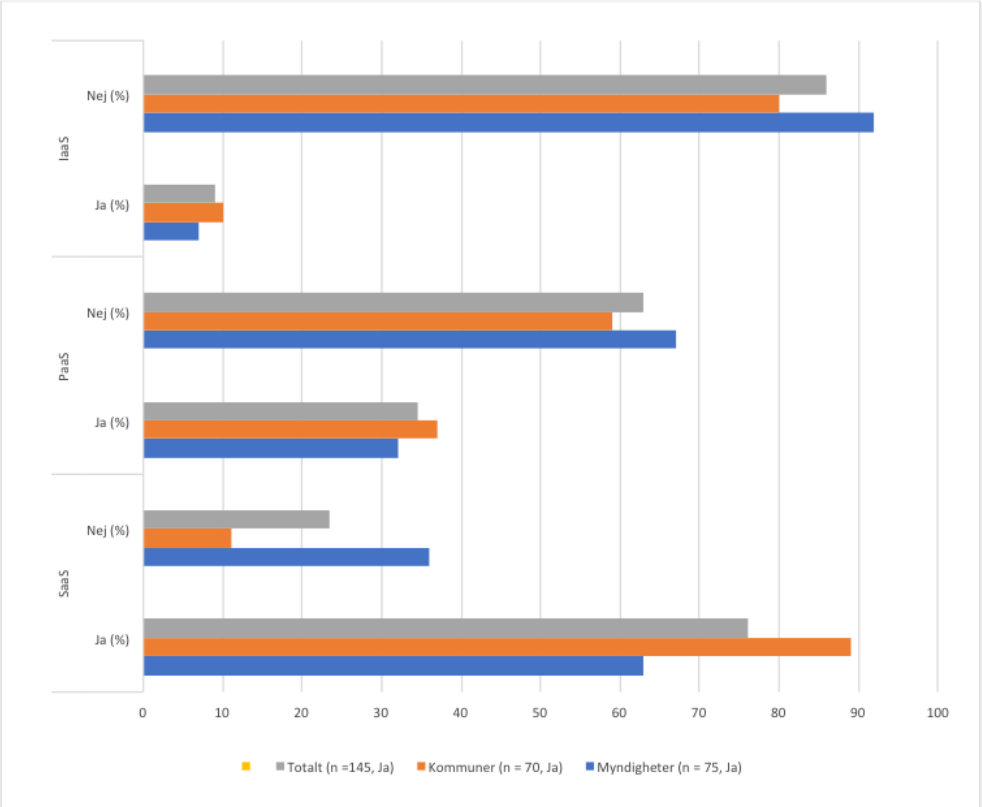
Enkäten visar även på att det finns en grupp organisationer, ofta mycket små myndigheter, som inte gör ett eget ställningstagande kring att upphandla molntjänster. Istället använder de sig av större myndigheters IT-lösningar. Baserat på det empiriska underlaget är det dock svårt att uttala sig om hur och i vilken utsträckning som de mindre myndigheternas specifika informationssäkerhetsbehov beaktas.

6.2 Typiska tjänster som svenska offentliga aktörer lagt ut på molntjänster

När det gäller typen av tjänster som kommuner och myndigheter använder så finns det naturligtvis många olika sätt att kategorisera dessa på. I undersökningen undersöktes upphandlingen baserat på uppdelningen SaaS, PaaS och IaaS (se avsnitt 5.1 för närmare beskrivning). Figur 6.6 visar att av de organisationer som upphandlat molntjänster så är SaaS vanligast (76 %), följt av PaaS (35 %) och IaaS (9 %). SaaS får anses mycket vanligt i kommunerna där 89 % använder den typen av molntjänst. Användningen i myndigheter är något lägre (63 %). Både PaaS och IaaS är något vanligare i myndigheter än i kommuner.

I enkäten fanns det möjlighet att ange vilka specifika molntjänster som användes relaterat till de tre kategorierna SaaS, PaaS och IaaS. Givet den profil på användningen som visas i figur 6.6 så är de flesta av de namngivna tjänsterna relaterade till SaaS. Tabell 6.1 visar en analys av vilka molntjänster inom SaaS som används. Kategorierna i kolumnen till vänster är skapade induktivt baserat på de faktiska molntjänsternas primära användningsområde. Tabellen visar att kommunerna har den mest spridda användningen i kategorin utbildningsadministration. En närliggande kategori där är också lärande

plattform/pedagogiskt stöd. När det gäller myndigheter är fördelningen mellan de olika kategorierna jämnare, där det är svårt att identifiera en central kategori.



Figur 6.6: Användning av SaaS, Paas, and IaaS

Tabell 6.2 visar en analys av centralisering av SaaS-molntjänster baserat på de fritextsvar som respondenterna angett i enkäten. I den vänstra kolumnen presenteras om en molntjänst delas av mer än en organisation, och hur många i sådant fall. Exempelvis kan samma tjänst delas av 3 organisationer (n=3). Höger kolumn visar hur många identifierade molntjänster som vi funnit inom respektive kategori. Resultaten visar att de molntjänster som delas, delas av ett fåtal organisationer. I de flesta fall är det molntjänster som delas av två organisationer. Det är i ett fåtal fall som en specifik tjänst delas av många organisationer. Här identifierades en tjänst som delas av 14 organisationer och en tjänst som delas av 61 organisationer. Således finns det få SaaS där det finns hög centralisering. Det bör dock noteras att analysen är baserad på svar från 51 kommuner och 37 myndigheter, dvs samtliga organisationer som använder molntjänster har inte namngivit molntjänsterna de använder. Således är det rimligt att tro att antalet organisationer som delar en tjänst är högre, än vad som redovisas i tabellen.

Typ av molntjänstkategori	Antalet olika tjänster som rapporterats inom respektive kategori	
	Kommuner	**Myndigheter**
Ärende- och dokumenthantering	1	4
Kommunikation och applikationssäkerhet	1	1
Kundsamarbete/relation	1	4
Datadelning och lagring	2	6
Datavisualisering	1	1
Utbildningsadministration	12	5
Ekonomihantering	Inga data	2
Hälsovård	5	1
Lärande plattform/pedagogiskt stöd	4	5
Bibliotekstjänst	1	3
Organisatoriskt samarbete och produktivitet	3	4
Personalhantering	2	2
Upphandlingsstöd och kontraktshantering	1	4
Projektstyrning	Inga data	1
Rekryteringsstöd	1	3
Undersökningsstöd	Inga data	4
Socialtjänstehantering	1	Inga data
Webbpublicering och analys	2	1
Verksamhetsstyrning, planering och uppföljning	1	2
Summa	*39*	*53*

Tabell 6.1: Analys av typer SaaS

Molntjänst som delas av n organisationer	Antal förekomster av molntjänster som delas av n organisationer
n = 1 (dvs delas inte)	59
n = 2	18
n = 3	5
n = 4	3
n = 5	1
n = 6	1
n = 7	0
n = 8	1
n >=9 till n <=13	0
n = 14	1
n >=15 till n <=60	0

n = 61	1

Tabell 6.2: Analys av centralisering av SaaS

När det kommer till användningen av PaaS så identifierades 12 unika plattformar. Av dessa finns sju stycken hos enbart kommunerna och fem enbart hos myndigheterna, och en används av båda typerna av organisationer. Här är det en plattform som tydligt förekommer hos flera av organisationerna, den delas av 27 organisationer. Således finns det en tydlig centralisering kring denna plattform. När det gäller användningen av IaaS så är den som framgår av figur 6.6 begränsad. Här identifierades fyra unika infrastrukturer. De empiriska resultaten visar inte att de delas av flera organisationer.

6.3 Vilka är leverantörer av molntjänster och vilken typ av tjänst den offentliga aktören nyttjar den specifika leverantören för

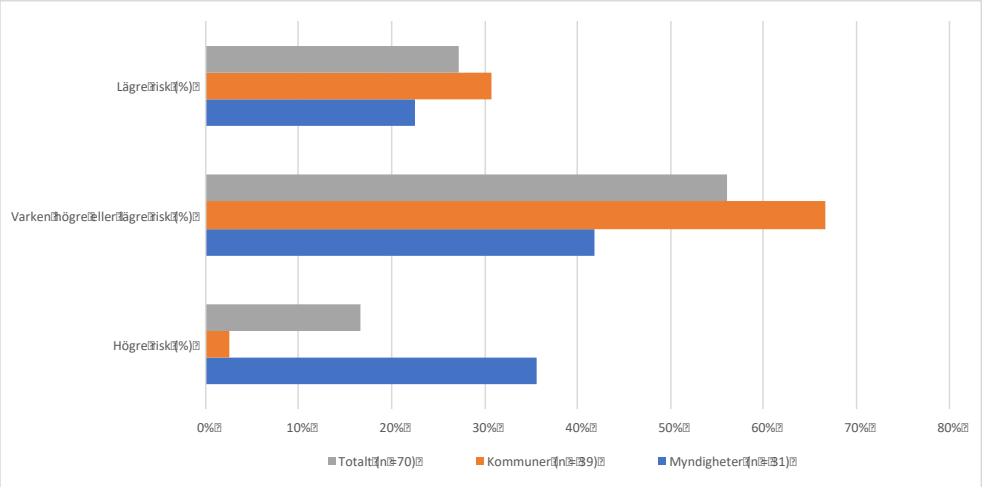
De empiriska resultaten presenterade i sektion 6.2 är delvis intressanta för att visa vilka som levererar molntjänster, dvs antalet identifierade SaaS, PaaS och IaaS är också en indikation på leverantörsspridningen. Baserat på data från en öppen fråga där organisationerna har haft möjlighet att ange namnen på leverantörer har dock leverantörsspridningen analyserats specifikt. Frågan besvarades av 29 kommuner och 39 myndigheter, och totalt identifierades 70 molntjänsteleverantörer.

Leverantör som delas av n organisationer	**Antal förekomster av leverantör som delas av n organisationer**
n = 1 (dvs delas inte)	48
n = 2	12
n = 3	1
n = 4	2
n = 5	2
n = 6	1
n = 7	0
n = 8	1
n = 9	1
n >=10 till n <=12	0
n = 13	1
n >=14 till n <=28	0
n = 28	1

Tabell 6.3: Analys av centralisering kring leverantörer

Tabell 6.3 visar en analys av centralisering kring leverantörer. Den vänstra kolumnen visar om en leverantör delas av mer än en organisation, och hur många i sådant fall. Exempelvis om en leverantör delas av 4 organisationer (n=4). Den högra kolumnen visar hur många leverantörssamarbeten som vi funnit inom respektive kategori. På samma sätt som kring delandet av SaaS så

visar resultaten att organisationerna i ett fåtal fall använder samma leverantör i stor utsträckning. Här identifierades en leverantör som delas av 13 organisationer och en leverantör som delas av 28 organisationer. Att det finns en skillnad mellan hur SaaS fördelas kontra leverantörer kan åtminstone bero på två saker, dels en lägre svarsfrekvens på frågan om leverantörer, och dels att samma tjänst i vissa fall tillhandahålls av flera leverantörer. Även här bör noteras att de faktiska siffrorna sannolikt är högre på grund av den låga svarsfrekvensen.



Figur 6.7: Organisationernas riskbedömning om det utgör en lägre eller högre risk ifall flera offentliga verksamheter anlitar samma molntjänstleverantör

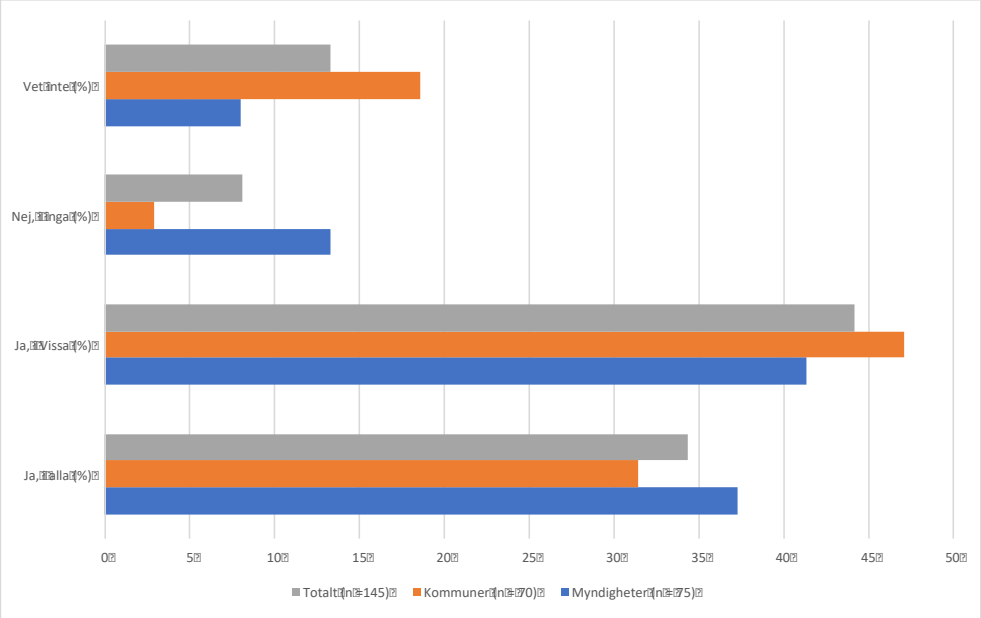
Figur 6.7 visar organisationernas syn på huruvida det utgör en risk att dela molntjänstleverantör. Våra empiriska data visar att mer än hälften av organisationerna (52 %) inte har gjort någon sådan riskbedömning. Av de organisationer som har genomfört en riskanalys kring frågan, ansåg 56 % att det varken innebär en högre eller lägre risk. När det gäller de organisationer som gör bedömningen att det utgör en högre eller lägre risk att anlita samma molntjänstleverantör så skiljer sig profilerna åt mellan kommunerna och myndigheterna. Kommunerna gör oftare bedömningen att anlita samma molntjänstleverantör minskar risken, och myndigheterna gör betydligt oftare bedömningen att det ökar risken.

6.4 De länder som informationen behandlas

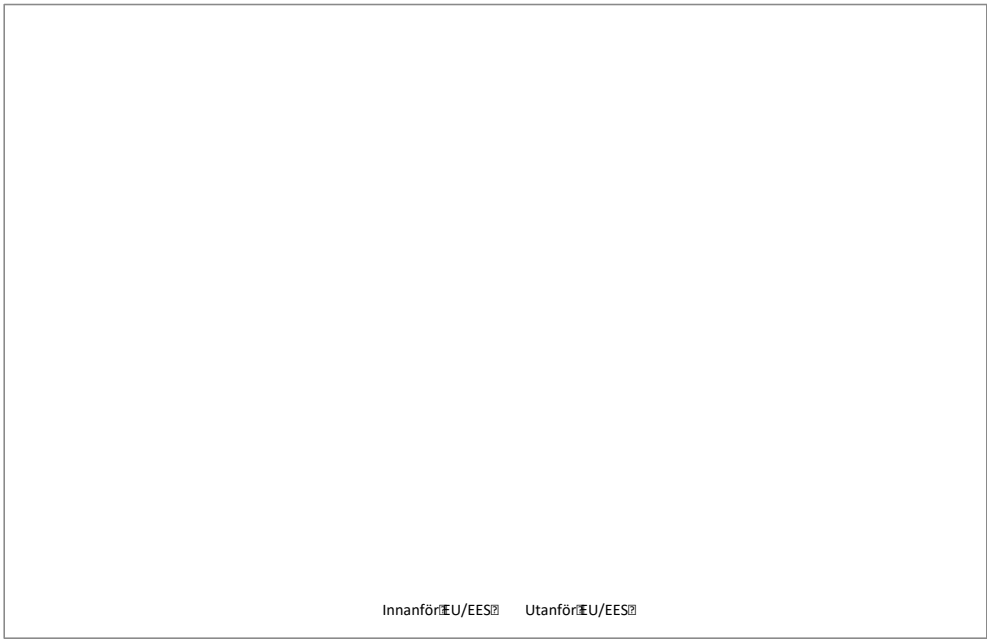
Molntjänster kan levereras från olika länder, vilket gör att det kan skilja i vilka lagar och regelverk som tillämpas. Figur 6.8 visar i vilken grad organisationerna har reglerat i existerande kontrakt i vilka länder som data processas.

Våra empiriska data visar att 34 % av organisationerna alltid har kontrakt som inkluderar namn på de länder där informationen processas. Sedan finns det en betydande andel organisationer (44 %) som har det i vissa fall. I 8 % av organisationerna så har man upphandlat molntjänster utan att det är reglerat var informationen processas. Slutligen finns det även en grupp (13 %) som inte vet i vilken grad denna fråga är reglerad. Här kan noteras att den andelen är

betydligt högre för kommuner än för myndigheter samtidigt som det är fler myndigheter som vet att de inte har reglerat frågan.



Figur 6.8: Andelen organisationer som har reglerat i kontrakten med molntjänstleverantören/leverantörerna i vilket land data processas

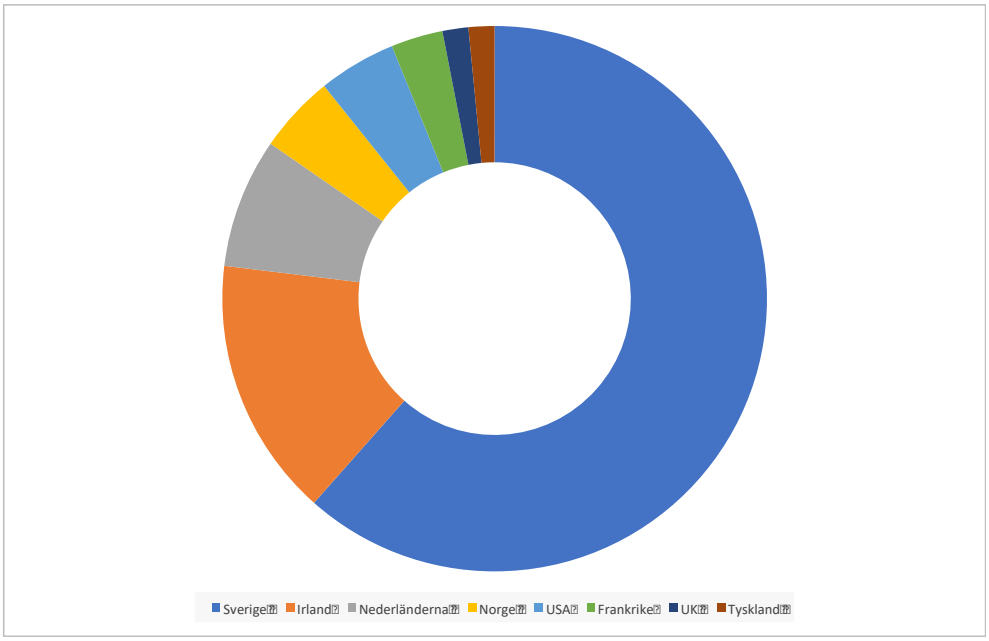


Figur 6.9: Fördelning mellan innanför EU/EES och utanför EU/EES där informationen i molntjänsterna processas

Baserat på en öppen enkätfråga har organisationerna fått ange i vilka länder som informationen processas. Figur 6.9 visar fördelningen av var informationen processas, fördelat på inom EU/EES och utanför EU/EES. Baserat på de empiriska data som angivits i den öppna frågan så finns den stora merparten av molntjänster som processar information (95 %) inom EU/EES området. En närmare precisering vad gäller länder visas i figur 6.10. Här visas att majoriteten (62 %) av alla molntjänster som processar information är geografiskt placerade i Sverige. Det land som sedan har den största andelen är

Irland (15 %), men det är en betydande skillnad i andel. Därefter följer sedan i storleksordning Nederländerna (8 %), Norge (5 %), USA (5 %), Frankrike (3 %), UK (2 %), och Tyskland (2 %).

Det är värt att notera att andelen molntjänster som processar information utanför Sverige är 28 % högre för myndigheter än för kommunerna. Det visas också av fritextsvaren, och får illustreras av följande uttalande från en av kommunerna: “Vi brukar känna oss lite lugnare när tjänster levereras i Sverige och i andra hand EU där vi måste tänka till lite mer. Ej utanför EU om vi medvetet kan säkerställa detta”.

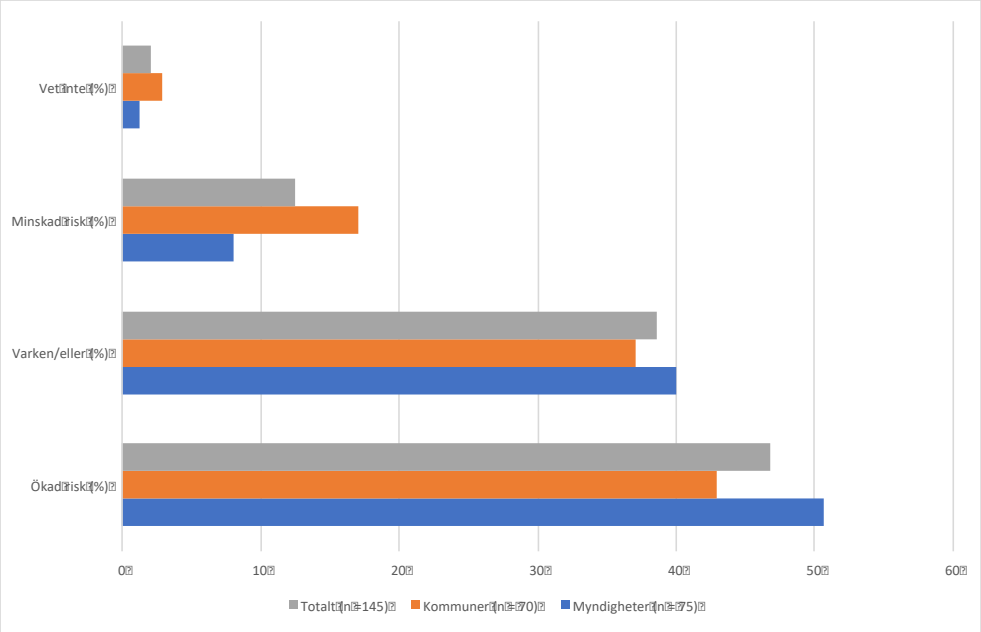


Figur 6.10: Fördelning av länder där informationen i molntjänsterna processas

Resonemanget som kommunerna för i intervjuerna är att majoriteten undviker att anlita leverantörer utomlands, bland annat på grund av informationssäkerhetsrisker men även för att följa nuvarande och kommande lagstiftning. De kan tänka sig inom EU men helst inom Sverige för att känna sig trygga. Ett uttalande från en kommun är dock att de inte har anlitat leverantörer utomlands men att de råkat ut för att leverantörer blivit uppköpta. De krav som de ställer är att datorhallarna ska vara i Sverige. En kommun menar dock att det är en bedömning från fall till fall beroende på vad det är för tjänst. Myndigheterna resonerar liknande, att det är Sverige eller EU som gäller men påpekar att det kan bli problem vid avtal med de ”stora amerikanska jättarna”. Även en myndighet uttrycker att bedömningen görs från fall till fall och tar upp ett exempel om en nuvarande tjänst som leverantören vill flytta från Sverige till ett annat land inom EU. Både myndigheterna och kommunerna har således gjort ställningstaganden om vilka länder de kan tänka sig att anlita leverantörer från. När det gäller uppgifter om ifall land angavs i kontraktet eller inte tog en myndighet upp att det varierar mellan leverantörerna om de vill dela med sig av den informationen eller inte. De angav också att deras största leverantör sett till mängden data inte gärna delar med sig av sådan information.

6.5 Informationssäkerhetsrisker som har identifierats

Figur 6.11 visar organisationernas bedömning av riskerna med molntjänster jämfört med egen IT-drift. Resultaten visar att en stor andel (47 %) anser att anlitande av externa molntjänster medför en ökad informationssäkerhetsrisk. I denna fråga är myndigheterna något mer skeptiska än kommunerna. Följande citat från en av myndigheterna illustrerar detta: “Viss information, som vi ändå bedömer som mer känslig än annat, kommer vi att hantera lokalt på egna servrar. Vi har också helt lokal backup på allt”. En nästan lika stor andel (39 %) av organisationerna anser dock att det inte innebär någon förändring i risk. Det finns även organisationer (13 %) som gör bedömningen att riskerna minskar, och kommunerna gör den bedömningen i högre grad än myndigheterna.



Figur 6.11: Organisationernas bedömning av om informationssäkerhetsrisken ökar med molntjänst jämfört med egen IT-drift

Den bild som framkom i intervjuerna visar att bland kommunerna så anser de att det kan innebära både en ökad och minskad risk, det beror på hur de går tillväga. För att det ska bli bra behövs mer kontroll och eftertanke. Om man inte gör det på ett bra sätt så ökar risken men om man gör det på ett bra sätt så kan den istället minska. En kommun säger: ”Det är ingen skillnad rent principiellt, det handlar om att veta vad man skriver avtal om. Det är inte säkert att säkerheten är högre internt, man kanske tror det men jag tror vi är dåliga på säkerhet internt och då skulle ju möjligtvis säkerheten vara högre för de [leverantörerna] är mer noga, men sedan finns det ju missar där med”. Åtkomst tas upp som den största utmaningen, att veta vart data lagras och vem som har åtkomst till det. En annan kommun påpekar dock att det främst är ett juridiskt problem snarare än att det handlar om säkerhet, vad man har rätt att göra utifrån offentlighetsprincipen och sekretesslagen. Organisationen anser dock att det på så vis även blir ett säkerhetsproblem, men att problemet är hur man behandlar uppgifterna. Organisationen har även uppfattningen att det inte går att stoppa utvecklingen så egentligen handlar det om hur man gör det så

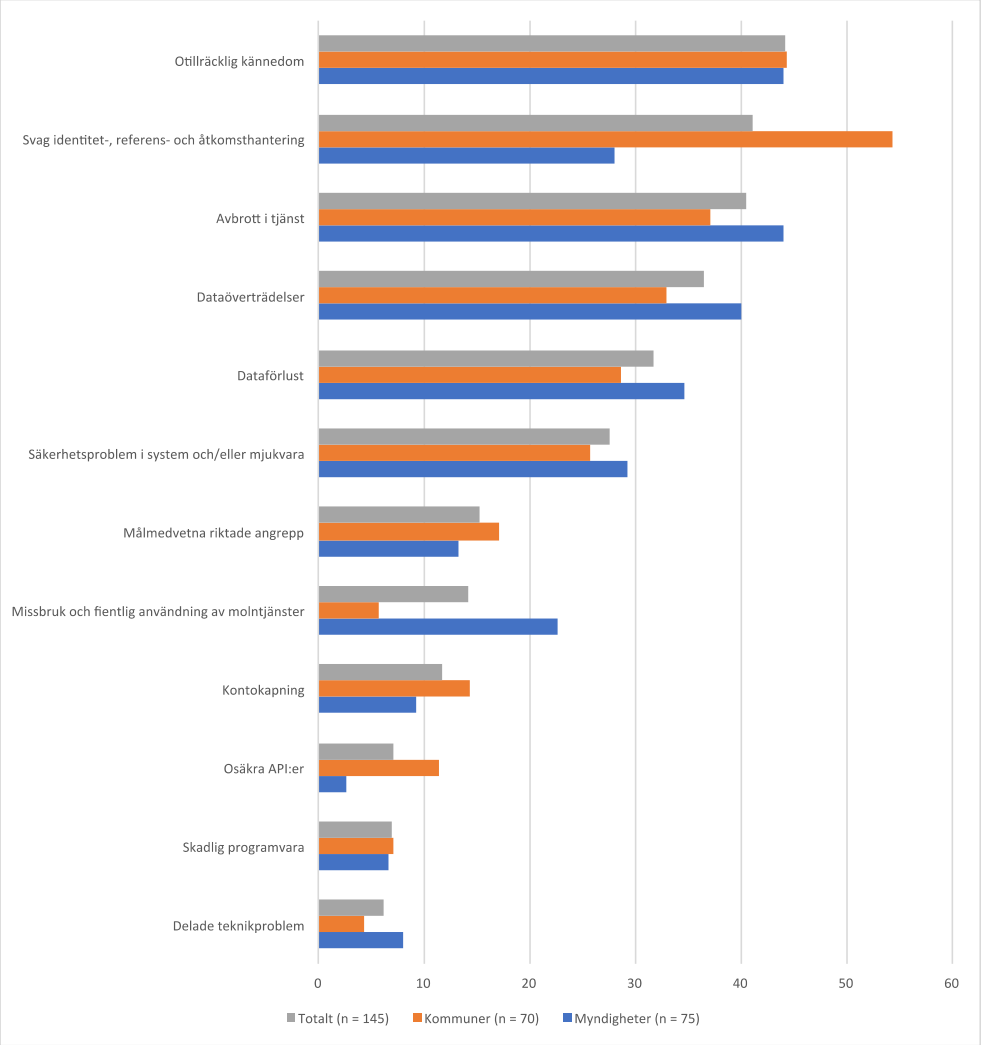
bra som möjligt: ”Det stora huvudbryet för mig nu är att det går ju inte att stoppa utvecklingen så vad behöver man göra för att hantera att det ska bli så bra som möjligt? Det känns som att man diskuterar att ja men det går ju inte, ja men hur gör vi? Folk tassar runt som katter kring het gröt men vi måste ta ett beslut att antingen får man inte eller också så måste vi göra de här sakerna”.

Enligt intervjuerna skiljer sig inte synen på om risken ökar eller minskar nämnvärt åt beroende på om det är en myndighet eller kommun som besvarar frågan. Däremot motsäger svaren delvis enkätsvaren både kommuner och myndigheter är överens om att det handlar mer om hur man gör, vilka krav som ställs. Ett citat från en myndighet illustrerar tydligt detta: ”Det är ju allmänt känt när man pratar om molntjänster att det finns stora risker. Men man måste ju veta vad man gör och det gäller alla sammanhang. Det som avgör om det blir säkert eller inte är ju hur man tar ansvar för sin information och det gäller oavsett om man har egen drift eller om den ligger i molnet. Det är ju fullt möjligt att ha egen drift som är usel och att ha drift i molnet med jättebra säkerhet t ex”. En annan myndighet uttrycker dock att det kan bli problem när man inte själv hanterar informationen, eftersom det inte är säkert att den hanteras korrekt. Myndigheten tar upp ett fall med en leverantör. Enligt avtalet fick inte leverantören använda informationen i systemen men det fanns ändå indikationer på att så skedde. Till exempel hanterade myndigheten ett specifikt ärende nästan uteslutande utanför den digitala sfären. Enda tillfället som myndigheten diskuterade ärendet digitalt var i ett e-postmeddelande, i övrigt hade all annan kommunikation i ärendet skett muntligen eller på papper. Det e-postmeddelande som förekom skickades från en lokal dator med hög säkerhet. Kort därpå fick personen som skickat meddelandet reklam relaterat till det ärende som diskuterats i meddelandet från två olika företag. Respondentens bedömning var att det var osannolikt att det skulle vara ett sammanträffande då detta inte hänt tidigare. Leverantören kontaktades men besvarade aldrig ärendet.

En myndighet som aktivt valt att inte ha sin kärnverksamhet i molnet menar dock mer säkert än de övriga att risken ökar: ”risken ökar och det är därför vi har valt att ha kärnverksamheten i egen drift, det är inte aktuellt att flytta ut den i molnet eftersom vi är en myndighet som styrs av allmänhetens förtroende”. Även de andra myndigheterna talar mycket om hantering av information i detta sammanhang. En myndighet menar att man tappar kontroll över hur informationen hanteras om den lagras i molnet och att det även kan vara svårt att veta hur man skall få tillbaka sin information. Detta relaterar till leverantörsinlåsning som även det togs upp av kommunerna.

Organisationerna fick möjlighet att ange deras samlade bedömning om vilka de tre huvudsakliga informationssäkerhetsriskerna är. För detta ändamål användes de tolv risker som identifierats i “The Treacherous Twelve Cloud Computing Top Threats in 2016” (Cloud Security Alliance, 2016). Resultatet av rankingen visas i figur 6.12. Om vi ser till den samlade bedömningen av båda typerna av organisationer så är de fem mest centrala riskerna 1) otillräcklig kännedom om hantering av molntjänster, 2) svag identitet-, referens- och åtkomsthantering, 3) avbrott i tjänst, 4) dataöverträdelser, och 5) dataförluster. Det finns dock skillnader mellan de två typerna av organisationer.

Kommunerna rankar svag identitet-, referens- och åtkomsthantering som den mest betydande risken, medan myndigheterna anser att otillräcklig kännedom om hantering av molntjänster och avbrott i tjänst är de mest betydande riskerna.



Figur 6.12: Organisationernas rankade informationssäkerhetsrisker avseende molntjänster

Ett flertal respondenter lyfte fram att de hade svårt att ranka riskerna i figur 6.12 på grund av deras nuvarande kunskapsnivå och erfarenhet om molntjänster. Detta illustreras av följande citat från en av kommunerna: “vi har för lite erfarenhet av molntjänster, svårt att svara på frågan”.

För att fånga upp risker som inte täcks in i “The Treacherous Twelve Cloud Computing Top Threats in 2016” (Cloud Security Alliance, 2016) så gavs även möjlighet att ange andra risker. De risker som angavs i fritext går att relatera till regulativa aspekter och hantering av känslig information, vilket följande citat får symbolisera: “Felaktig hantering av personuppgifter, speciellt utifrån nya dataskyddsförordningen. Brister i informationsklassningen vilket leder till känslig information i system som inte upptäcks i tid” och “[r]isk att sekretessreglerad information röjs, risk att skyddsvärd men inte sekretessreglerad information röjs, risk att handlingar som tekniskt

behandlas/tekniskt lagras av molntjänstleverantören lämnas ut när vi lägger upp dem och därmed blir allmänna och blir föremål för begäran om utlämnande vilket skapar osäkerhet och merarbete".

Risker kan också materialisera sig i faktiska incidenter. I studien undersöktes även förekomsten av incidenter relaterade till molntjänster. Av de organisationer som besvarade enkäten hade 84 % inte upplevt några incidenter. De som hade upplevt incidenter fick även klassificera incidenten enligt följande alternativ: avbrott i tjänsten, dataförlust, förvanskning av information och att obehöriga fått åtkomst till informationen. Kategorierna är således relaterade till begreppen konfidentialitet, riktighet, och tillgänglighet (ISO, 2017). Nästan 100 % svarade att incidenterna har rört avbrott i tjänsten. Det bör dock poängteras att studien inte undersökt orsakerna till dessa avbrott.

Enligt vad som framkom i intervjuerna hade en kommun av åtta råkat ut för incidenter. Det handlade om en tjänst relaterad till ett specifikt verksamhetsområde som hade ett driftstopp. Därmed förlorade kommunen åtkomst under fyra timmar. Samma kommun hade även ett fall där molnleverantören skulle flytta lösenord men istället kopierades lösenorden vilket fick konsekvensen att två personnummer blev åtkomliga för obehöriga. Dock skedde ingen obehörig inloggning. Även hos myndigheterna var det en av de intervjuade som råkat ut för incidenter. Myndigheten uttryckte att det sker "då och då, men ingen har varit så allvarlig att vi behövt rapportera till MSB […] Det är inga riktiga incidenter egentligen, det är mer intrimning, inga riktiga risker eller faror egentligen som jag har hört talas om".

I intervjuerna frågade vi även organisationerna om konsekvenser av ett avbrott i tjänsterna i förhållande till olika tidsintervall. Tabell 6.4 visar en samlad bild som gavs från respondenterna i förhållande till olika tidsperioder. Den vänstra kolumnen innehåller längden på avbrotten och de övriga två kolumnerna innehåller konsekvensbedömningarna uppdelade på kommuner och myndigheter. Föga förvånande så innebär längre driftsstopp större problem. Bilderna ser dock lite olika ut mellan de båda typerna av organisationer där längre avbrott bedöms vara allvarligare av kommunerna än av myndigheterna.

Organisationerna fick även besvara vilka samhällskonsekvenser ett avbrott skulle få, det vill säga konsekvenser som inte bara drabbar den egna verksamheter utan samhället och andra enskilda aktörer. Idag ligger få kritiska system i molnet och samhällskonsekvenserna bedöms därför som ganska små. I kommunernas fall är dock undantag vård och omsorg samt vatten och värme. I myndigheternas fall är det beroende av verksamhet. Två av myndigheterna uttrycker att det skulle få samhällskonsekvenser, samtidigt framhålls att det finns reservrutiner som kan tillämpas istället.

Längd på avbrott	Kommuner	Myndigheter
24 h	Överlag få konsekvenser, dock beroende på datum och verksamhetsområde. Inom vård och omsorg kan det få stora konsekvenser. Ett exempel på uttalande är: ”beror på vilken tjänst och vad det gäller, vi har kontinuitetsplanering men läkemedelstjänst kan vara allvarligt annars inte. Beror även på datum, vid utbetalning kan det vara jobbigt”.	Överlag få konsekvenser men allvarlighetsgraden varierar beroende på myndighetens verksamhet och vilka system som berörs. Två exempel på allvarligare konsekvenser är: ” beror på tjänst men om en viss strategisk tjänst ligger nere så ligger hela verksamheten nere” och ”personer kan inte nå oss på telefon vilket gör att folk blir upprörda, en stödfunktion kan lamslå mycket annat”.
48 h	Börjar bli kännbart. Beroende på verksamhet kan det bli kritiskt.	Börjar bli kritiskt.
1 vecka	Kritiskt för flera delar av verksamheten.	För vissa myndigheter är detta kritiskt/allvarligt.
1 månad	Kris	Kritiskt/allvarligt

Tabell 6.4: Analys av konsekvenser av avbrott i molntjänster vid olika tidsintervall för kommuner och myndigheter

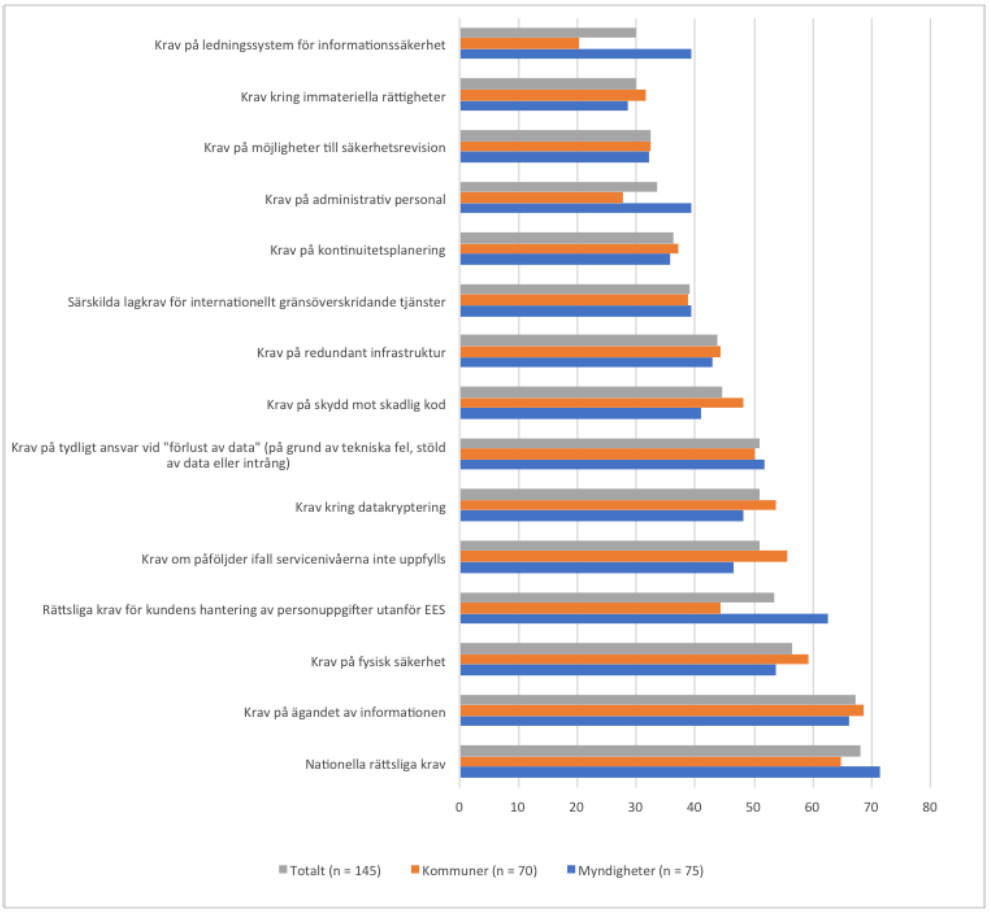
6.6 Vilka informationssäkerhetskrav som aktörerna har på molntjänst-leverantören

Enkäten inventerade vilka informationssäkerhetskrav som organisationerna granskar när molntjänstleverantörerna använder standardkontrakt. Inventeringen gjordes med hjälp av en flervalsfråga med femton fördefinierade alternativ som byggts upp baserat på krav som existerade litteratur lyft fram som viktiga. Dessutom gavs möjlighet att med fritext ange egna krav. Figur 6.13 visar andelen organisationer som har krav som är relaterade till de femton fördefinierade alternativen. Om vi ser till den samlade bedömningen av båda typerna av organisationer är de sju vanligaste informationssäkerhetskraven i fallande ordning: 1) nationella rättsliga krav, 2) krav på ägandet av informationen, 3) krav på fysisk säkerhet, 4) rättsliga krav för kundens hantering av personuppgifter utanför EES, 5) krav om påföljder ifall servicenivåerna inte uppfylls, 6) krav kring datakryptering, och 7) krav på tydligt ansvar vid "förlust av data". Det finns några skillnader mellan kommuner och myndigheter.

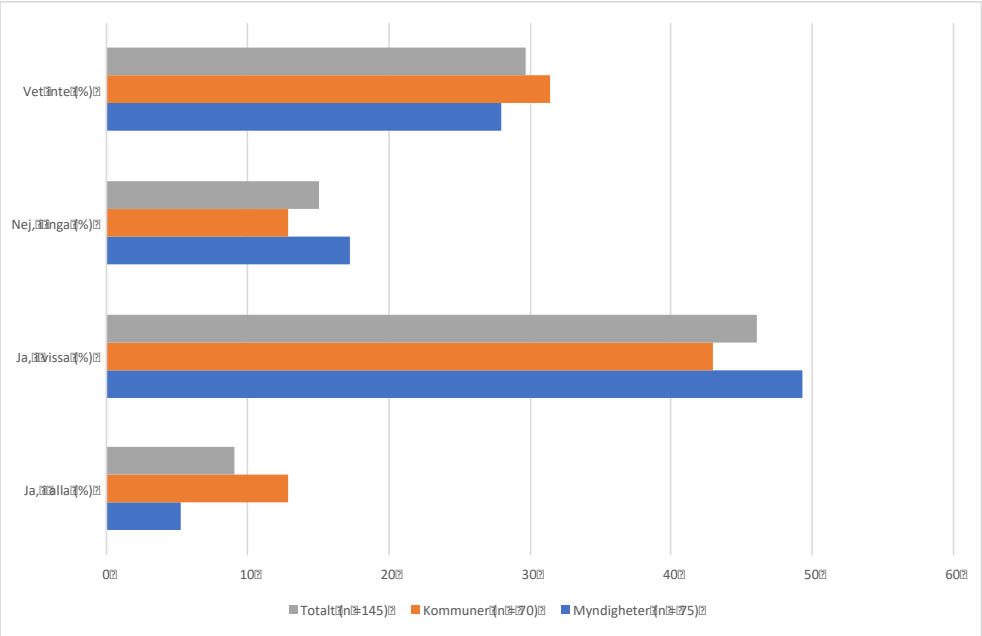
Två noterbara skillnader är att myndigheter i högre grad granskar krav på hantering av personuppgifter utanför EES och att det ska finnas ledningssystem för informationssäkerhet. När det gäller fritextsvaren tillkom

inga tydliga mönster kring ytterligare krav. Däremot förekom det preciseringar att ISO-27000 serien är viktig kring krav på ledningssystem. Följande citat från en kommun illustrerar detta: “Övergripande ska ISO-standarden för informationssäkerhet, ISO/IEC 27001 och 27002, följas”.

Detta citat reflekteras även i figur 6.14 som visar i vilken grad det är reglerat i kontrakten med molntjänstleverantörerna att informationssäkerhetsarbetet ska utföras utifrån internationella standarder (ex ISO-27001 och ISO-27002). Figuren visar att mer än hälften (55 %) har i samtliga fall eller i vissa fall inkluderat som krav att informationssäkerhetsarbetet skall baseras på internationella standarder. Det är dock noterbart att en betydande andel (30 %) inte vet om så är fallet.



Figur 6.13: Informationssäkerhetskrav som organisationerna granskar när molntjänstleverantören använder standardkontrakt



Figur 6.14: Andelen organisationer som reglerat i kontrakten med molntjänstleverantörerna att informationssäkerhetsarbete ska utföras utifrån internationella standarder för informationssäkerhet

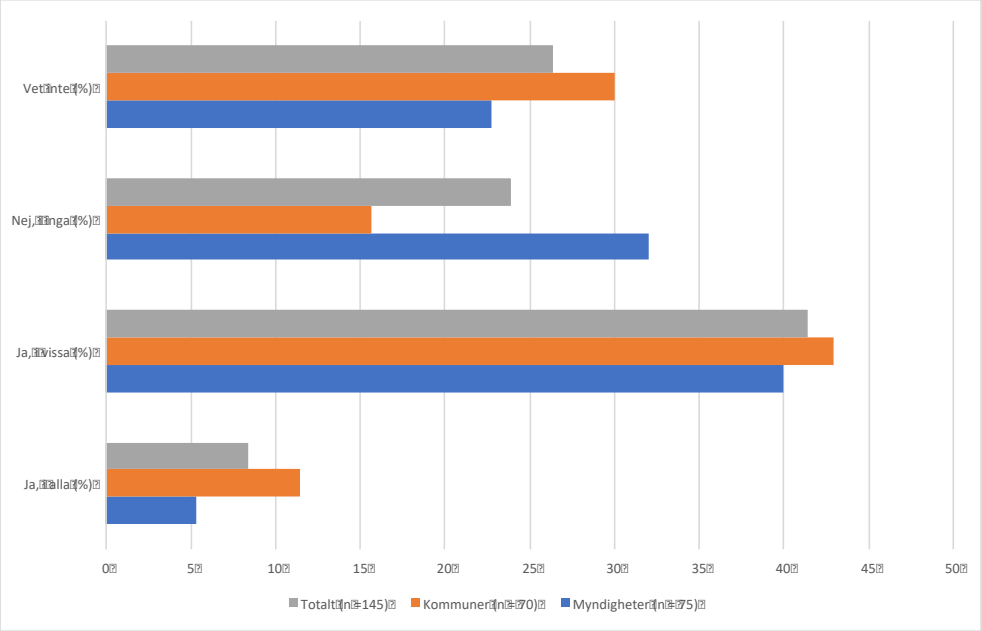
Intervjuerna avslöjade att det är stor skillnad på de krav som skulle ställas vid en upphandling idag och de som ställdes för några år sedan. Det gäller både kommuner och myndigheter och de talar om att händelser i omvärlden har lett till ett ökat fokus på informationssäkerhetsfrågor och att informations-klassningar och riskanalyser därmed fått högre prioritet. Dock har många organisationer molntjänster som upphandlades för några år sedan och de tjänsterna har därför upphandlats med dåvarande kravbild. En myndighet konstaterar: ”ja, det finns tidigare upphandlingar som är gjorda utan diskussion, men man har fått större medvetenhet nu, men generellt är man pigg på ny teknik”. En annan myndighet uttrycker i samma anda: ”säkerhetsenheten har endast en rådgivande roll. Vi rekommenderar alltid med bestämdhet att inte gå vidare om inte riskerna är hanterade. Sedan har det hänt tidigare att det blivit kompromisser avseende tid, pengar, inflytelserika aktörers vilja etc. Men efter ”Transportgate” har man alltid lyssnat på oss. Nu finns det i stället en försiktighet vid beslut”.

Vi ställde även frågan om organisationerna har upphandlat en tjänst trots att de vet att vissa risker inte kommer att hanteras. Svaret på den frågan blev att det skett historiskt men även att de skulle kunna tänka sig att det sker framöver om de kan hitta alternativa skyddsåtgärder eller om det gäller molntjänster med låg informationssäkerhetsklassning. En myndighet uttrycker: ”inget som det är kännedom har upphandlats men det blir en bedömningsfråga om hur hårdsatt krav det gäller och om det finns alternativa skyddsåtgärder som i så fall bedöms likvärdiga”. Liknande uttalanden finns bland kommunerna: ”Nja, vi har köpt vissa brister avseende backup men vet man bara om det kan man komplettera själv”.

Vilka krav organisationerna faktiskt ställer skiljer sig mycket åt beroende på tjänst. Som en myndighet uttrycker det: ”Det beror på vad som kommer fram

av klassningen av det som ska upphandlas. Vid förekomst av känsliga personuppgifter enligt PUL ställs det krav på två-faktors autentisering vid inloggning samt kryptering, PKI eller liknande". En annan myndighet konstaterar: "Vi ställer krav som fungerar utifrån personuppgiftslagstiftningen och kommande GDPR kommer ju att bli ännu noggrannare att vi gör rätt men informationen får inte förvanskas, jag kommer inte ihåg ordagrant, men information och uppgifter får inte förvanskas eller försvinna, eller hamna i orätta händer". Vidare talade samma myndighet om behovet av backup och riskminimering men att vilka krav som ställs är beroende av vilken tjänst det är som upphandlas: "informationsdata ska finnas på backup och det ska finnas riskminimering i form av hantering av informationsförluster och sedan har vi det här med säker inloggning, vissa saker ska vara krypterade och ibland har vi privata moln också och då kanske man kräver att det ska finnas dubbla internetuppkopplingar […] det måste vara väldigt skilda nät på det sättet också. Jag skulle påstå att det finns ett jättebatteri, men sedan kan man skala ner det om det är en väldigt enkel molntjänst".

Vidare undersökte studien specifikt om organisationerna angivit i kontrakten med molntjänstleverantörena vilken personal hos leverantörerna som har åtkomst till data som finns lagrad i molntjänsten. Figur 6.15 visar att hälften av organisationerna (50 %) ställer den typen av krav i vissa eller i samtliga fall. Ungefär en fjärdedel (24 %) ställer inga sådana krav, och ungefär lika många (26 %) vet inte om sådana krav ställs.



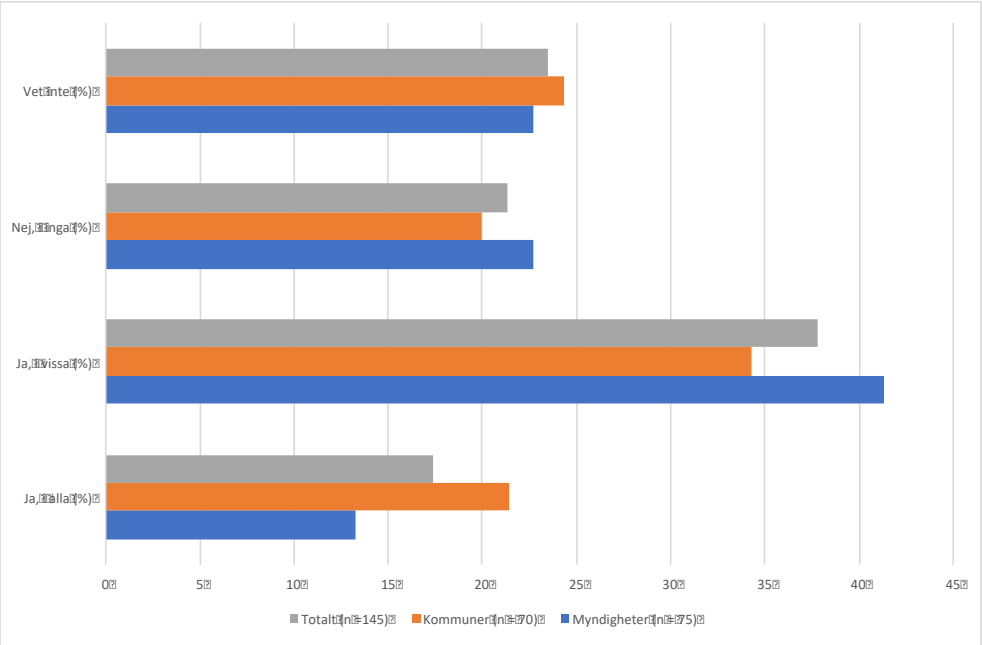
Figur 6.15: Andelen organisationer som i kontrakten med molntjänstleverantörerna har angivit vilken personal som har åtkomst till data som finns lagrat

Enligt intervjuerna ställer de flesta kommuner den typen av krav. Av de åtta tillfrågade kommunerna svarade fem ja på frågan och de som preciserade sitt svar berättade att det sker på rollnivå. Två av kommunerna gav dock lite vagare men ändå positiva svar: " Generellt avseende roller, men jag är lite osäker, vi har ingen bra skrivelse" och "ja, men jag vet inte exakt hur". Den senare av de

två var dock en kommun som ännu inte driftsatt systemet utan valt att avvakta. En av kommunerna uttryckte dock att de inte ställer den typen av krav och att det beror på att verksamheterna ofta agerat på egen hand. När det kom till myndigheterna svarade en myndighet nej: ”inte kollat upp, men nej tror jag. För oss handlar det om att sätta behörigheter i vårt interface, hur det är hos dem känner jag inte till.” Av de som svarade ja fick vi följande svar: 1) ”Ja, inte på individnivå, att de är namngivna, men vi ställer krav på utbildning och klassning”. 2) ”Ja vi beskriver behörighetstyp och om informationen ska blandas med andra eller inte. Vi har inte listor, personliga listor, det är olika för olika sorts information, hur känslig den är. Vi har en extern leverantör som har tillgång till vår känsliga information och då är det nästan personliga, namngivna personer, som kan komma åt informationen, men sedan finns det molntjänster där vi har information som inte är lika känslig när det gäller integritet och då säger vi bara att behörigheterna skall vara tilldelade till de som i sin arbetsroll skall ha tillgång till det, i allmänna ordalag”. 3) ”Ja, vi har ju ett avsnitt i våra krav där vi säger att data inte får åtkommas av andra än oss, men de som driftar kan ju göra saker i och för sig, själva molntjänstleverantören kommer ju alltid att komma åt, men några utomstående får inte komma åt. Vårt data ska vara skyddat”.

Att denna fråga är beroende av hur känslig information det gäller är tydligt: ”Det beror på vilken tjänst det är, för vissa leverantörer har vi säkerhetsskyddsavtal och då ska ju de som jobbar med våra grejer vara säkerhetsklassade men sedan har vi också, jag kan nämna en tjänst […] där det är publik information och då lägger vi oss inte i vem som jobbar med det”. Klassningen av informationen har en avgörande roll: ”det är ju vi som äger informationen och den ska ju inte ut i molnet om den är känslig. Vi har en säkerhetsorganisation som kontrollerar om data får komma ut i molnet, vi får inte lägga känslig information”. Myndigheten tar upp ett exempel om en app som diskuterades utifrån vilket förväntat innehåll användare skulle kunna lägga in: ”och då diskuterade vi vad kommer att läggas in i den här? Kommer […] att kartläggas? Är det okej? Så känslig information ska inte ut, är det känslig information då behövs säkerhetsskyddsavtal och det har vi för den större tjänsten där vi har privat moln”. Enligt myndigheten är alla som arbetar med känslig information hos leverantören säkerhetsklassade. Dock påpekar myndigheten att det är en förtroendefråga: ”sedan vet ju inte vi om de hyr in en […] som de ger åtkomst utan att meddela oss, det är ju den här förtroendefrågan. Teoretiskt sätt kan man nog orsaka skada, men på de saker som är känsligare har vi någon typ av övervakning så vi får rapporter och kan se vad som kommer in och vad som går ut”.

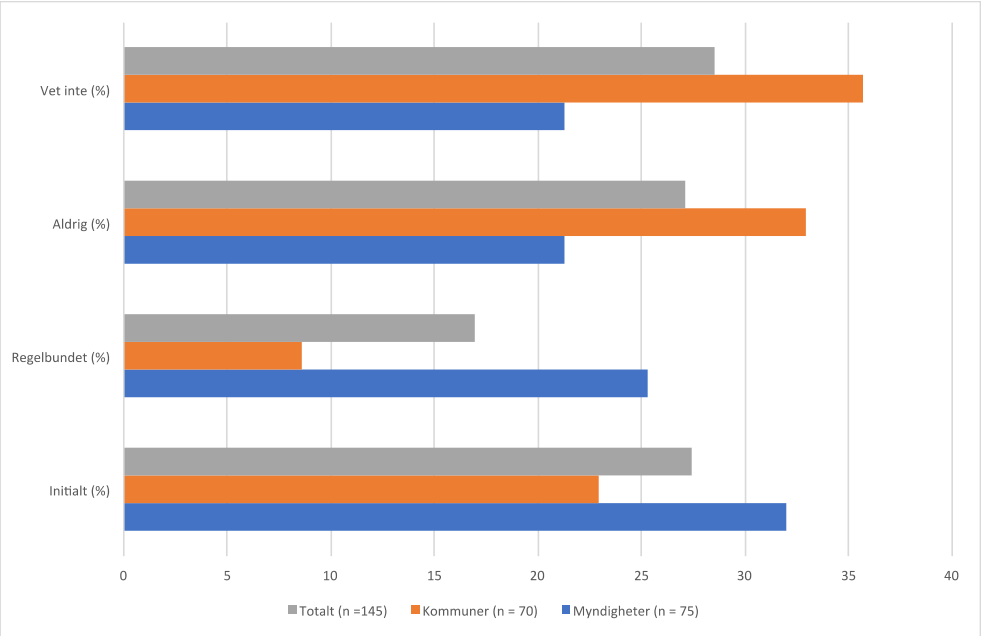
Vidare undersöktes om organisationerna i kontrakten med molntjänstleverantörena har angivit om informationen skall behandlas separerat från andra kunders information. Figur 6.16 visar att mer än hälften av organisationerna (55 %) ställer den typen av krav i vissa eller i samtliga fall. Andelen kommuner som i samtliga fall har detta krav i kontrakten är högre än för myndigheterna. Ungefär lite mindre än en fjärdedel av organisationerna (22 %) har inte med detta krav i kontrakten, och ungefär lika stor andel (23 %) vet inte om det finns med i kontrakten.



Figur 6.16: Andelen organisationer som i kontrakten med molntjänstleverantörerna har angivit skall behandlas separerat från andra kunders information

6.7 Hur informationssäkerhetskrav som formulerats i avtalsförhållandet följs upp initialt och löpande

Avsnitt 6.6 fokuserade på informationssäkerhetkrav när kontrakt tecknas med molntjänstleverantörerna. Det kan dock finnas skillnader mellan kontrakten och hur kraven implementeras av molntjänstleverantörerna och studien undersökte därför hur kraven följs upp. Figur 6.17 visar hur organisationerna angett att de arbetar med revisioner av molntjänstleverantörerna. Endast 17 % av organisationerna genomför revisioner regelbundet. Här finns även en betydande skillnad mellan myndigheter och kommuner där myndigheterna i högre grad utför revisioner regelbundet. Mer än en fjärdedel (27 %) genomför en initial revision, och även här är andelen myndigheter som genomför det högre än andelen kommuner. Det är dock betydande andelar där organisationerna aldrig genomför revisioner (27 %) eller inte vet om revisioner genomförs (29 %).

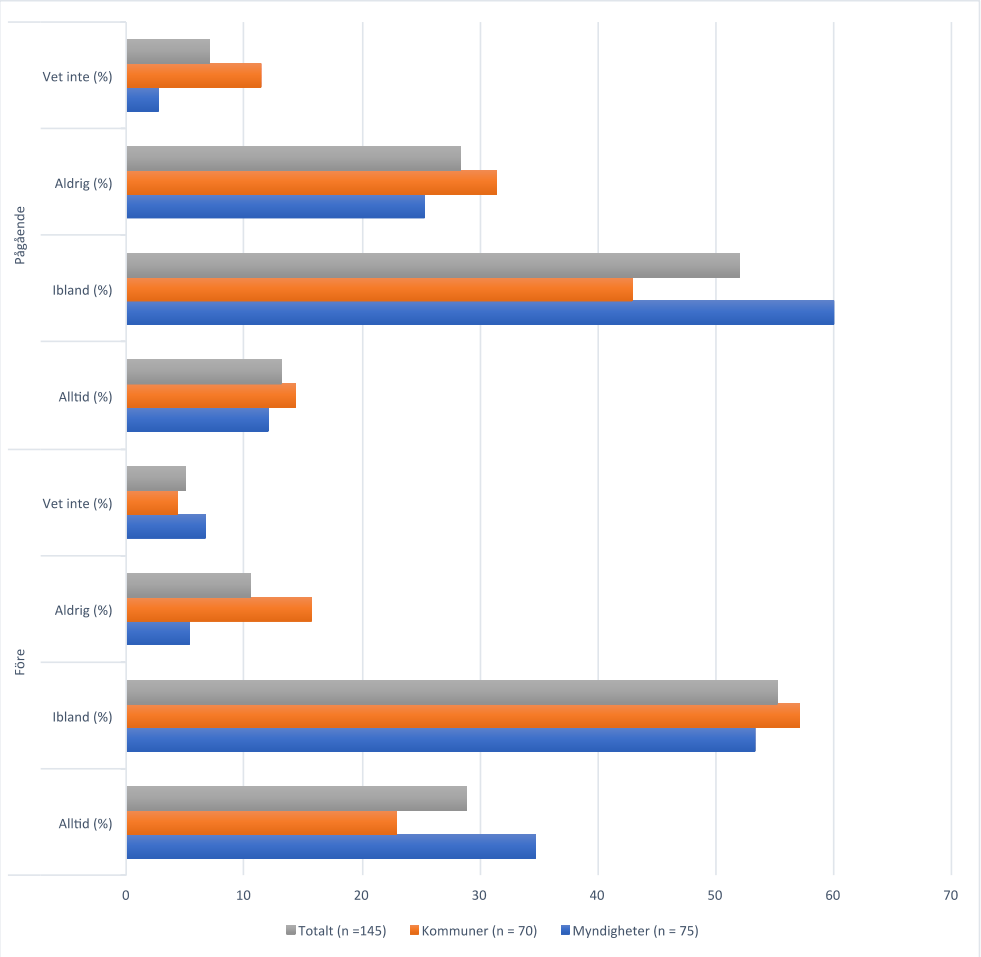


Figur 6.17: Hur organisationerna anger att de följer upp informationssäkerhetskraven i kontrakten med molntjänstleverantörerna

Enligt intervjuerna så verkar det vara ett pågående arbete för kommunerna att bygga upp systematik kring uppföljning av krav. Flera av kommunerna berättade att det är något som man arbetar på men som man historiskt har varit dålig på. Detta gäller dock inte bara molntjänster utan generellt. Av de som utför revisioner nämns t ex att det finns en leveranskontrollperiod där de säkerställer att funktioner och dokumentation finns. Det verkar bara vara i ett initialt skede som detta sker. Osäkerheten verkar stor, en kommun uttrycker att ”jag utgår från att man gör det men jag vågar inte svara på det”. Av revisioner som planeras att utföras i framtiden nämns bland annat stickprovskontroller som ett tänkbart tillvägagångssätt.

Myndigheterna förefaller göra detta i något större utsträckning än kommunerna. Dock är uppfattningen att revisioner är svårt: ”De gör vi på lite olika sätt, det vill jag nog påstå, sedan är det alltid svårt med uppföljningar, man får förlita sig på vad leverantören säger, vad man gör och hur man jobbar. Så jag tycker det är svårt med uppföljningar.” Uppföljningen sker ofta genom ett besök på plats och sedan ett uppföljande besök efter upphandling. Vid uppföljande besök har det sett bra ut: ”det är ofta inför att man skall teckna ett avtal, vi har tillämpat att man gör besök på plats och sedan har man efter avtalet gjort ett besök och tittat på det vi kravställt om det ser ut som vi har tänkt. Man kan väl säga att det inte är med systematik, det kan vi inte säga”. En annan myndighet uttrycker att de inte följer upp avseende informationssäkerhet men att det skulle kunna ske för andra krav: ”ja, men inte alla krav, vi har inga revisioner på informationssäkerhetsområdet men det är något som vi talar om. Vi följer upp om de får ny personal så ska de säkerhetsprövas och vi följer upp ekonomiska förhållanden, men just på informationssäkerhet så kommer vi att bli bättre”. Den uppföljning som nämns sker månads- eller kvartalsvis: ”det är IT-tjänsteledarna, de följer ofta upp månadsvis men inte alltid, det ser lite olika ut, beroende på vad det är för tjänster. Det skulle kunna vara månadsvis eller kvartalsvis och då är det för

leveranserna under den här månaden, tillgängligheten, incidenter.” Uppföljning vid behov sker även vid denna myndighet: ”vid behov eller vid inrapporterade incidenter”. Denna myndighet påpekar att regelbunden logguppföljning inte är motiverad då de inte har någon känslig information i molnet.



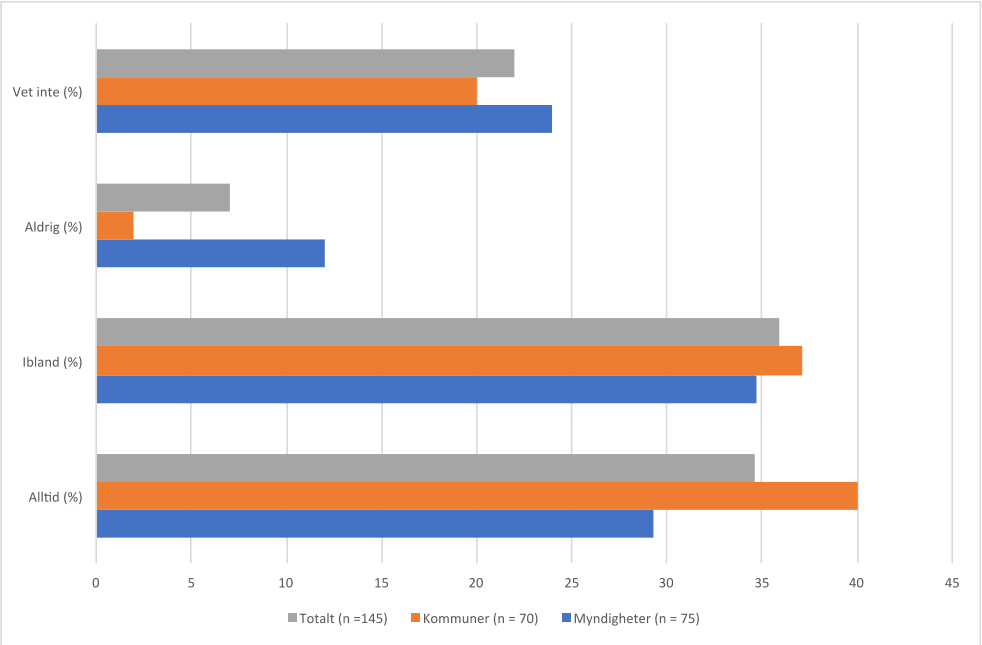
Figur 6.18: Andelen organisationer som utför systematiska riskanalyser före och/eller under pågående avtalsperiod.

Relaterat till hur revision genomförs har studien också undersökt hur organisationerna arbetar med systematiska riskanalyser relaterat till molntjänster. Figur 6.18 visar hur organisationerna arbetar före och/eller under pågående avtalsperiod (dvs regelbundet). De empiriska resultaten visar att 29 % av organisationer alltid genomför en systematisk riskanalys före det att ett molntjänstkontrakt ingås. En lägre andel, 13 %, genomför alltid systematiska riskanalyser under pågående kontraktsperiod. En majoritet genomför ibland riskanalyser före och under pågående avtalsperiod. Med andra ord finns det ingen systematik i att de skall genomföras. Andelen som aldrig genomför systematiska riskanalyser före att kontrakt ingås var 11 %. Det finns dock en skillnad mellan kommuner och myndigheter, där andelen kommuner som aldrig genomför systematiska riskanalyser före att kontrakt ingås är högre. När det gäller andelen organisationer som aldrig genomför systematiska riskanalyser under pågående avtalsperiod så är den andelen högre (28 %) jämfört med andelen som aldrig gör det före kontrakt skrivs (11 %). Detta är

naturligt då andelen som alltid genomför systematiska riskanalyser under pågående avtalsperiod är lägre.

Vid intervjuerna framkom att vissa kommuner gör en riskanalys före upphandling eftersom det ingår i risk- och sårbarhetsanalyser och att de utför det i vissa fall när det gäller kritiska system. Då har t ex KLASSA används som grund. En kommun uttrycker dock att de är osäkra på om det är en systematisk säkerhetsanalys. En annan kommun uttrycker lite mer vagt att ”de gör det på sitt sätt” eftersom de är en liten kommun. En annan åsikt är att riskanalyser utförs men inte systematiskt utan att det är beroende av upphandling och hur känslig informationen är. Det är även upp till förvaltningens vilja eftersom beställaren styr. Följande citat från en kommun belyser att det är en resurs- och ledningsfråga men som fått ökat fokus: ”informationssäkerhet är en ledningsfråga, en resursfråga, det har inte varit fokus på de frågorna, inte på ledningens bord. Men man börjar vakna nu, Transportstyrelsen var en väckarklocka och det händer saker i världen, det är förändring, det är en viktig ledningsfråga”. En annan kommun uttrycker att de mer har ”reagerat än agerat”, att det inte har varit ett aktivt val med molnet utan att det inte fanns andra alternativ. Intervjuerna bekräftar således resultatet av enkäten, att det förekommer men att det inte sker systematiskt. Det samma verkar gälla för myndigheterna. En myndighet uttrycker att det inte skett vid tidigare upphandlingar men att det idag finns grundläggande rutiner som dock inte har tillämpats då ingen ny upphandling utförts efter deras uppkomst. En annan myndighet uttrycker att det ingår i deras ledningssystem för informationssäkerhet. Att det utförts före är vanligare än under pågående process, en myndighet uttrycker att eftersom de inte har lagt ut något verksamhetskritiskt har de inte sett behov av att göra det löpande: ”det vill jag inte påstå [att de utför analyser löpande], inte de tjänsterna för det som vi har lagt ut är inte ur vårt perspektiv den typen av verksamhetskritiska tjänster, vi gör det på basverksamheten men den har vi som sagt inte lagt ut, så nej det gör vi inte på de tjänsterna på det sättet”. Att det löpande arbetet beror på typ av tjänst uttrycks även av följande myndighet: ”det kan hända men det är inte speciellt vanligt eftersom det oftast rör sig om tjänster som inte är så känsliga". Sammanfattningsvis visar intervjuerna att båda typerna av organisationer ofta genomför en analys före upphandling men sällan under pågående avtalsperiod.

I arbetet med att upphandla en molntjänst är det möjligt att ta hänsyn till molntjänstleverantörernas historik. Figur 6.19 visar hur stor andel av organisationerna som beaktar leverantörernas historik vid upphandling. Figuren visar att en tredjedel (35 %) alltid gör det, och kommunerna gör det i högre grad än myndigheterna. En ungefär lika stor andel (36 %) beaktar historiken ibland. Således har organisationernas analys av molntjänsteleverantörernas historik en betydande roll i hur de initialt arbetar med informationssäkerhetskrav. Samtidigt kan det noteras att nästan en fjärdedel (22 %) inte vet om en sådan analys görs.



Figur 6.19: Andelen av organisationerna som leverantörens historik i beaktning vid upphandling av molntjänst

När det gäller kunskap om molntjänstleverantörerna undersöktes också i vilken grad som organisationerna har några rutiner för att identifiera om leverantörerna har anlitat underleverantörer för att tillhandahålla de molntjänster som upphandlas. I dagsläget saknar 70 % av organisationerna en sådan rutin. Fritextsvaren visade att organisationer som har en rutin upplever det svårt att få fram den här typen av information. Följande citat från en myndighet illustrerar detta: “Där är det mycket svårgenomträngligt att få fram samma information. Det finns även tjänster via en leverantör som använder en annan leverantör för sina tjänster ex Leverantör X använder […] för sin leverans. I avtalet redovisar enbart leverantör X sina åtaganden och inte ett ord om vilka åtaganden som […] har”.

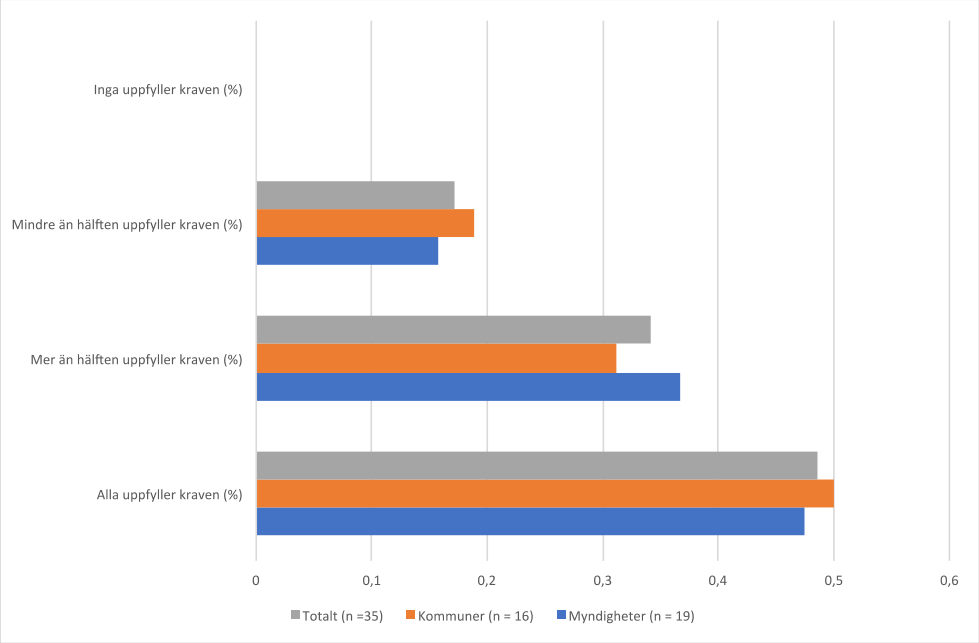
Det finns ingen samstämmig bild bland kommunerna om deras kännedom om underleverantörer. Enligt intervjuerna varierar det om de vet om ifall leverantörerna anlitat underleverantörer eller inte. Två kommuner angav att de inte har kännedom om detta. Den ena av de kommunerna trodde däremot inte att det sker medan den andra förutsatte att det gör det. Vidare menade en kommun att vissa leverantörer anlitar underleverantörer medan en annan kommun menade att de flesta gör det. Åsikterna går således isär. En kommun poängterade att det är problematiskt att kravställa underleverantörer i upphandlingsprocessen.

För myndigheternas del svarade de flesta att de känner till om underleverantörer anlitas och tre av myndigheterna krävde att få godkänna underleverantörer. Tre exempel på detta är: 1) ”I de fall det anlitas underleverantörer skall det framgå i avtalen men jag kan inte uttala mig om hur det ser ut i varje specifikt fall. Men organisationen kravställer att få godkänna underleverantörer”. 2) ”Detta är en av osäkerhetsfaktorerna som nämnts tidigare. Enligt avtal och baskrav för informationssäkerhet får en leverantör inte göra detta med mindre än att detta godkänns av oss samt att

dessa undertecknar motsvarande avtal angående hantering av personuppgifter”. 3) ”Ja, i vårt privata kontakt- och kommunikationscenter så är det en leverantör som vi har avtal med och så har de en underleverantör som står för kommunikationsplattformen och då har vi säkerhetsskyddsavtal med underleverantören och vi träffar dem också regelbundet”.

6.8 Hur molntjänstleverantörer bemöter de informationssäkerhetskrav som ställs vid upphandling

Figur 6.20 visar hur organisationerna anser att molntjänstleverantörerna uppfyller ställda informationssäkerhetskrav vid genomförda revisioner. För det första visar de empiriska resultaten att en mycket stor andel av organisationerna (75 %) inte kan besvara frågan för att inga revisioner har genomförts. Den här andelen är högre än andelen organisationer som säger sig inte genomföra revisioner initialt eller regelbundet (se avsnitt 6.7).



Figur 6.20: Andelen molntjänstleverantörer som vid organisationernas revision uppfyller informationssäkerhetskrav som finns enligt kontrakten

I de fall revisioner genomförs, visar enkäten att ungefär hälften (49 %) av molntjänstleverantörerna uppfyller samtliga informationssäkerhetskrav som finns i kontraktet. När det gäller leverantörer som inte uppfyller samtliga krav så är har organisationerna funnit att 34 % uppfyller mer än hälften av kraven och 17 % uppfyller mindre än hälften av kraven. Det finns inga betydande skillnader mellan resultaten från kommunernas och myndigheternas genomförda revisioner.

Även vid intervjuerna framkom att få revisioner utförs men av de som utfört revisioner konstaterade en kommun att man inte har hittat några ”skräckexempel utan endast buggar”. De två myndigheter som utfört revisioner konstaterade att: ”det sett bra ut vid de besök som utförts” samt att ”jag förutsätter att det har sett bra ut. Jag brukar få veta om det trasslar men teoretiskt sätt skulle det kunna vara någon som inte har pratat med mig”.

6.9 De utmaningar och hinder offentliga aktörer mött vid upphandling och användning av molntjänster

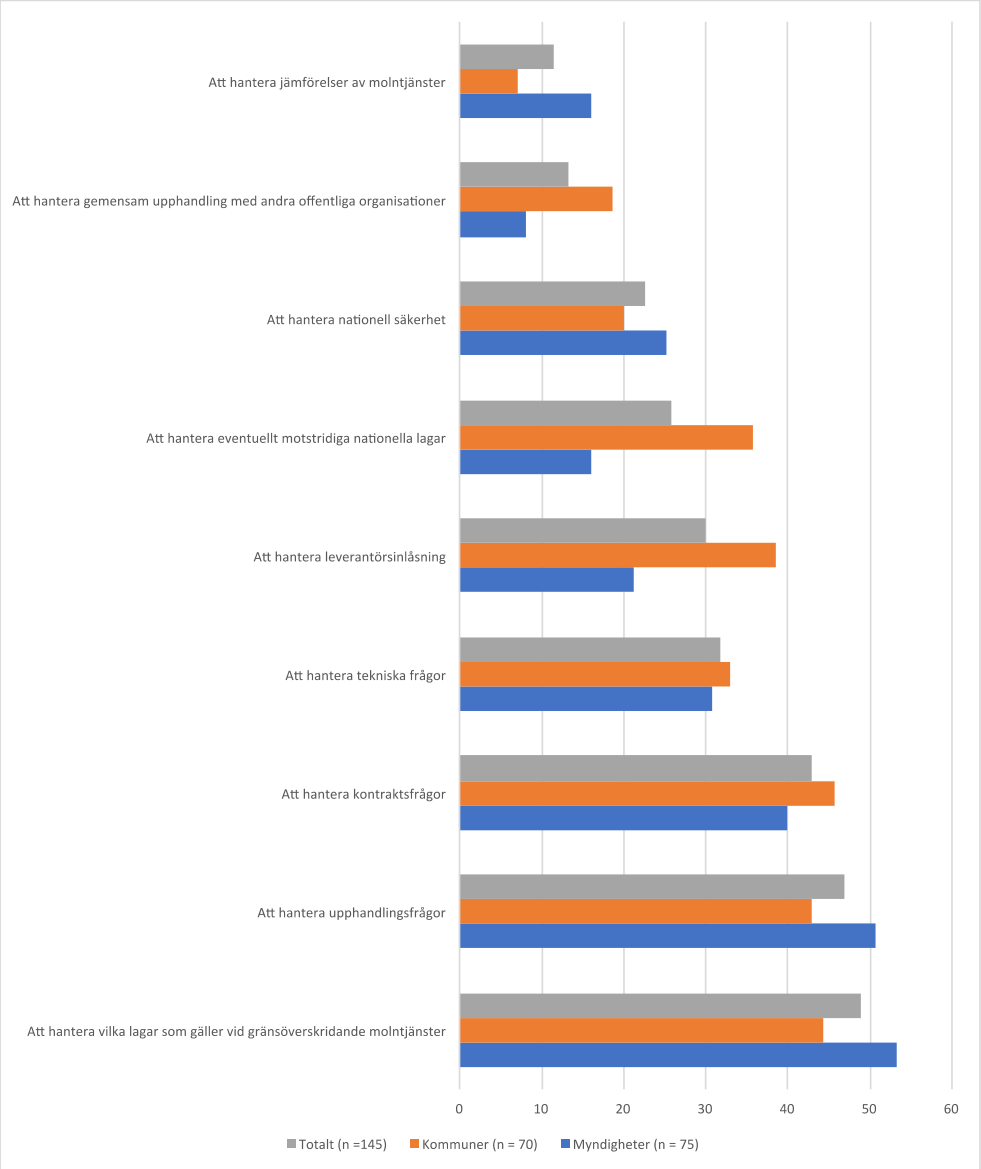
Enkäten undersökte vilka organisationerna ansåg vara de mest centrala utmaningarna och hindren de mött vid upphandling och av molntjänster. Det gjordes med nio fördefinierade alternativ som byggts upp baserat på krav som existerade litteratur lyft fram som viktiga. Organisationerna fick möjlighet att ange vilka de anser är de tre huvudsakliga utmaningarna. Resultatet av rankingen visas i figur 6.21. Om vi ser till den samlade bedömningen av båda typerna av organisationer så är de fem mest centrala utmaningarna 1) att hantera vilka lagar som gäller vid gränsöverskridande molntjänster, 2) att hantera upphandlingsfrågor, 3) att hantera kontraktsfrågor, 4) att hantera tekniska frågor, och 5) att hantera leverantörsinlåsning. Som figuren visar finns det även skillnader mellan vilka frågor som kommunerna och myndigheterna anser utmanande. Kommunerna anser i högre grad än myndigheterna att leverantörsinlåsning och motstridiga nationella lagar utgör utmaningar.

Vid intervjuerna fick organisationerna fritt uttrycka om de ansett att det varit svårt eller inte att upphandla molntjänster. Om de ansett att det varit svårt bad vi dem även att precisera vad som varit det. Överlag ansåg kommunerna att det är svårt att upphandla molntjänster och några anledningar som nämndes var till exempel att: ”veta vad som verkligen gäller, att tolka det juridiska läget”. En kommun nämner att de valt att avvakta lite för att de vill se ett utfall först, att någon annan blir granskad och vad som händer med resultaten. Även problem som att leverantörerna inte förstår verksamheten tas upp, att leverantörerna t ex fokuserar mer på funktionalitet än att förstå hur offentlig verksamhet fungerar. Men framförallt är det helheten som utgör ett problem, att få ihop det verksamhetskritiska med juridiken och det tekniska.

T ex lyfter kommunerna problemet med kännedom om vart data lagras som ett stort problem och att leva upp till krav som kommer att ställas i och med införandet av GDPR. Vidare tas även inlåsningsproblem upp och skillnaden mellan att hantera information själva internt och att någon annan gör det. En kommun nämner t ex att om de har en tjänst på en egen server så har de rutiner för backup men om man köper tjänsten är det svårare att veta i detalj vad som gäller avseende tillgänglighet och backup och hur man återställer om det behövs. En annan kommun nämner att det är krångligt att flytta data i egen regi men att det är ännu svårare med molntjänster.

Förutsättningarna för myndigheterna varierar beroende på om de är en stor eller liten myndighet och om de har mycket egen kompetens eller inte. Denna faktor påverkar om de upplever upphandlingsprocessen som svår eller ej. En myndighet uttrycker att de: ”är lyckligt lottade som har den expertis som krävs och att det därför inte är svårt att upphandla molntjänster”. En av de mindre myndigheterna uttrycker tvärtom att det är svårt och att det är svårt att veta om de bör satsa på molntjänster eller inte. Myndigheten menade att: ”tidigare var påtryckningarna hårda medan det idag snarare avråds från investering i molntjänster”. En annan myndighet uttrycker att det är alldeles för enkelt att upphandla: ”konsulter är väldigt duktiga på att sälja in molntjänster som

lösningen på allt. De går inte sällan till rätt personer i sakverksamheten som får en längtan efter enkla och smidiga lösningar". Ytterligare en annan förutsättning är att vissa myndigheter går samman gemensamt för att sköta upphandlingar och att det därmed ligger utanför den egna myndigheten.



Figur 6.21: Organisationernas rankade utmaningar vid upphandling av molntjänster

Många av kommunerna anser att juridiken utgör en utmaning. Bland annat efterlyser de prejudicerande domar och mer tydlighet angående vilka krav som bör ställas på leverantörerna och hur dessa krav skall följas upp. Framförallt lyfter man upp att det är tolkningen av lagtexterna som utgör ett problem: "beror ju på vilken tolkningshatt man har. Ska man läsa vad det står får ju ingen använda, nej det går ju inte. Eller det juridiska är väl tydligt men det är ju inte så folk agerar". Ett annat exempel är att det är svårt att veta vad som faller under sekretess. Ibland kan ärenden komma in via e-post som innehåller information som bör vara sekretessklassad även om e-post generellt inte är det. En kommun uttryckte dock att "det börjar klarna". Med det menade

kommunen att det är tydligare nu än vad det har varit historiskt. Kommunen ansåg dock att det fortfarande behöver bli ännu tydligare.

Myndigheterna tycker att juridiken är tydligare och mindre problematisk än kommunerna. Även de vill dock se utfall: ”ganska klart men det behövs rättsliga prövningar för att göra det riktigt klart, det behövs ett utslag från EU-domstolen”. Ett annat uttalande från en myndighet är att juridiken är tydlig med vad som är tillåtet men att den kan vara i konflikt med drivande krafter som vill ha större andel tjänster i molnet än idag: ”det är tydligt, problemet är att mycket går mot moln och verksamhetsansvariga och marknaden driver hårdare än vad IT kan godta”.

På en öppen fråga om vad organisationerna anser sig behöva hjälp med, vad de tycker är svårt svarade en kommun så här: ”Svårigheten att balansera lag, behov av digitalisering, ekonomi, att få ihop helheten. SKL har formulerat mål, så det finns ingen kommun som inte har diskuterat frågan, men det är extremt höga krav. Digitaliseringen går långsammare än den politiska viljan. Man får kompromissa”.

En annan kommun svarade: ”Det vore önskvärt om MSB och SKL tillsammans tar fram ett regelverk på hur vi ska göra, olika kommuner har olika bild och hänvisar till den myndighet som passar bäst, MSB eller SKL. Det behövs tydlighet som inte finns, inte att man kan tolka på olika sätt. Många kommuner samarbetar kring IT, t ex kan en annan kommun hantera driften hur blir det då med kravet på egna servrar? Stor otydlighet från MSB och SKL. Stämmer det här med egna servrar? Skulle man kunna tänka sig ett eget moln för alla småkommuner? Vi förväntas göra samma sak men med olika medel”.

Även att det är en brist på rekommendationer och att förutsättningarna varierar för kommuner beroende på storlek var en utmaning som togs upp: ”en lärdom som vi har dragit är att vara konservativa. Vi har inte kastat oss ut även om det varit väldigt trendigt. Vi har tagit det lugnt och under den tiden kanske uppfattats som bakåtsträvande men vi känner att det har varit rätt val, vi har ryggen fri. Så lärdomen är väl att inte förhasta sig. Därmed vill jag inte döma ut molntjänster men det behövs analys innan. Vi upplever att det är ganska skralt med rekommendationer, Cloud Sweden finns men det behövs mer och gärna från MSB. Vi jobbar på en IT-enhet på en liten kommun så vi har fullt upp med det dagliga, vi hinner inte med omvärldsbevakning, så vi vill gärna lita på att MSB tar den biten”.

Att det finns ett behov av mer toppstyrning uttrycktes också: ”det är bra att MSB går ut med rekommendationer och riktlinjer, man kan hänvisa mot MSB för att få bättre struktur och kontroll över sitt arbete. De stödjer oss småkommuner bra. Det är väldigt positivt eftersom egen IT-säkerhetskompetens saknas. Moln är ingen ny företeelse, det som är nytt är att behovet av moln är större och kontrollen över informationen mindre, vi behöver bli bättre. Det finns en konflikt mellan verksamheternas och IT:s funktion, min roll som IT-strateg är att få ut betydelsen av informationssäkerhet till förvaltningarna. MSB gör ett bra jobb men kanske skulle man inte ha skilda lagkrav för kommuner och myndigheter. Det vore bra med mer toppstyrning”.

En annan kommun var dock av åsikten att det är svårt att centralstyra kommuner, men även denna kommun höll med om att det finns en problematik kopplat till att verksamheterna har ett annat fokus än vad IT-avdelningarna har: ”att titta på hur det faktiskt är, vi kan inte värja oss. Det behövs tydlighet, statuera exempel, pröva juridiskt. Känns mer som datainspektionen än MSB egentligen. En kommun är Sverige, det är helt annorlunda på en kommun än på en statlig myndighet, det är svårt att centralstyra kommuner. Förvaltningschefer behöver informeras, inte IT egentligen utan det måste ut till verksamheterna. De vill lösa sina problem, men de behöver en samvetesröst att gör ni så här får ni istället andra problem. Det behöver ses på situationen som den faktiskt är, det är en lednings- och styrningsfråga”.

I samma anda (problemet med att verksamheterna ofta agerar på egen hand) tog en annan kommun upp behovet av hjälp från de som kommit längre i arbetet: ”jag har varit på MSBs träffar och tycker att de är bra, vi vill ha mer sådant. Risker finns, det behövs mer påtryckning utifrån. Verksamheterna har upphandlat själva, nu fångar vi upp men det är ett pågående arbete. Finns det sätt som är bättre än så som vi gör? Vi skulle vilja få ta del av erfarenheter från de som kommit längre”.

Ett annat önskemål från kommunerna var ett nytt BITS+, ett verktyg som man saknar: ”Ja, många småkommuner brottas med nya krav, det finns mycket stöd, metod, riktlinjer men man saknar gamla BITS+ som var välfungerande men skrotades. Där fick man bra stöd för riskanalys och åtgärder vilket var värdefullt men idag ska alla ta sig igenom djungeln. I en liten kommun är det svårt att ha folk som blir duktiga, man får sköta det med vänsterhanden. På KBM-tiden (före MSB) fanns BITS, nu finns LIS [Ledningssystem för Informationssäkerhet] och andra regelverk men de kräver mer av oss. Ett nytt BITS+ vore lysande! Att det tas ett nationellt grepp om det. Vi har en roll i en heltidstjänst eftersom vi är en liten kommun men allt är ju digitalt, ett kort stopp på 20 min får folk att rulla tummarna, ännu tydligare verktyg behövs, kanske ett BITS - basnivå i IS?”.

Även när myndigheterna besvarade denna fråga kom konflikter mellan viljor upp: ”olika delar som drar åt olika håll, teknik vs. risker och lagar. Vi måste involvera även de delarna, inte bara lyssna på försäljare”. Också myndigheterna nämnde ökad tydlighet som önskvärt: ”för att MSB ska bli ett stöd efterfrågas tydlighet avseende molntjänster för samhällskritisk information. I dag skickas det ut rekommendationer från olika håll. För närvarande finns inga krav utan varje myndighet får själva besluta och då hamnar man lätt i konsulternas händer om det inte finns en stark och erfaren säkerhetsfunktion”. En fråga som man undrade över var i vilka sammanhang man kan använda molntjänster och om det är rekommenderat att göra det eller inte, vilket understryker behovet av tydlighet och att det existerar en osäkerhet: ”stämmer det att man inte kan använda molntjänster om man har försvarssekretess på sin information? Om det blir av eller på, man inte kan kombinera, hur gör man då, delar vi upp informationen? Vi behöver mer stöd i sådana frågor. Direktiven har förändrats, tidigare uppmuntrades man använda molntjänster men efter Transportstyrelsen i somras har det svängt, molnet eller ej?”.

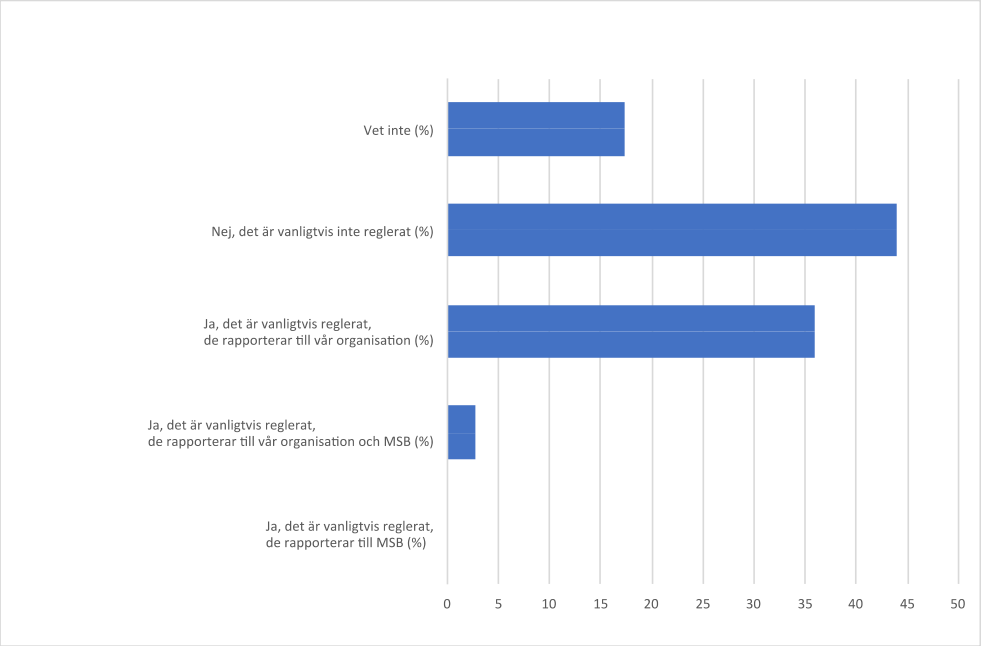
Problematiken att molntjänster kan vara väldigt lättillgängliga lyftes också: ”sunt förnuft ska styra innan någon annan får hantera ens information. Man behöver tänka på några saker, framförallt kanske att hantera det på samma sätt, det ska finnas riktlinjer, en enhetlig hantering men det är lättare sagt än gjort. Vissa molntjänster är väldigt lättillgängliga och kan börja användas utan att man behöver någon upphandling, det är svårt att kontrollera det”.

Även faktumet att upphandlingar är en långsam process lyftes: ”upphandlingar är en långsam process, ändring i rutiner tar ett tag innan de får effekt om de inte är akuta. Det tar ett tag för avtal och processer att fånga upp ny lagstiftning. Det viktigaste vid upphandling är informationssäkerhets-klassningen, öppen info då är riskerna små, riskerna beror på informationen”. Avslutningsvis lyftes frågan om alla länder i EU är att betrakta som första land? Eftersom det kan finnas stora skillnader mellan länderna och deras lagstiftning. Det exempel som togs upp var att t ex Rumänien har en avvikande lagstiftning.

6.10 Hur offentliga aktörerna har infört kravet om incidentrapportering för externa tjänsteleverantörer enligt 9 § MSBFS 2016:2

Myndigheter har krav på sig att implementera incidentrapportering enligt MSBFS 2016:2, och detta krav gäller även vid användning av molntjänster. Enligt 9 §, “[o]m en myndighet överlåter en del av sin informationshantering till en icke statlig aktör ska myndigheten i överlåtelseavtalet se till att motparten åtar sig att rapportera it-incidenter i berörda system till myndigheten på ett sätt som motsvarar kraven enligt denna författning. Myndigheten ska utan dröjsmål vidarebefordra en sådan rapport till Myndigheten för samhällsskydd och beredskap. Skyldigheten enligt första stycket gäller med avseende på avtal som träffas efter denna författnings ikraftträdande”.

Studien undersökte därför om myndigheterna reglerat i kontrakten med molntjänstleverantörerna hur incidentrapportering ska ske. Resultaten i Figur 6.22 visar en blandad bild. En mycket stor andel (44 %) anger att det vanligtvis inte är reglerat i kontrakten. En nästan lika stor andel anger att det är reglerat på något sätt i kontrakten, antingen att rapportering sker till organisationen (36 %), som i sin tur rapporterar till MSB, eller att rapportering sker till organisationen och till MSB (3 %). Nära en femtedel (17 %) av de svarande myndigheterna vet inte hur frågan har reglerats i kontrakten. Sammantaget visar resultatet på en bristande vetskap om kravet på incidentrapportering är implementerat gentemot molntjänstleverantörerna eller om det inte är implementerat.



Figur 6.22: Hur myndigheterna har reglerat i kontrakten med molntjänstleverantörerna att incidentrapportering enligt 9 § MSBFS 2016:2 skall ske

Resultatet av intervjuerna gav en annan bild av denna fråga. Här ställde vi dock inte frågan om hur incidentrapportering regleras i kontrakten utan hur myndigheterna infört MSBFS 2016:2 i relation till molntjänstleverantörerna. Flera myndigheter angav att det beror på allvarlighetsgraden av det inträffade om de är skyldiga att rapportera eller inte: ”ska bara röra en viss allvarlighetsgrad för att vara aktuellt, systemen som vi har i molnet innehåller ingen sådan info, men generellt är det organisationens ansvar, vi rapporterar till MSB”. Att rapporteringsansvaret låg hos den egna myndigheten delades som uppfattning av sex av de sju tillfrågade myndigheterna. Respondenten på den återstående myndigheten kunde inte uttala sig då denna uppgift utfördes av ett säkerhetsteam som arbetar med MSBs verktyg och då hen saknade insyn i denna process. Av de som tog upp avtalet i detta sammanhang, två av sju myndigheter, angav den ena att de föreskriver i avtal med leverantörer att alla incidenter ska inrapporteras till dem. Det är något som framgår av baskraven som ingår i alla avtal. Den andra myndigheten angav att rapporteringsskyldigheten trätt i kraft efter de avtal som de tecknat och att de därför sköter den rutinen själva utifrån egen bedömning.

Kommunerna har inte detta krav, de har inte skyldighet att rapportera till MSB. Vid intervjuerna frågade vi dem dock om de har något system för incidentrapportering i relation till molntjänstleverantörerna. För kommunerna är det ett pågående arbete där man har kommit olika långt. Några exempel på detta är: 1) ”ja, men behöver utvecklas, större och bättre, vi har haft i två år men vi har en plan för bredare användning i verksamheten”. 2) ”inte i drift idag men vi håller på och bygger upp det, det är en process med bland annat aktiviteter i maj, så det kommer att finnas”. 3) ”pågående men har inte hunnit! Under framtagande, vi ska ha ett möte den 23 maj, kontaktcenter och IT”. 4) ”rutiner för incidentrapportering uppdateras på grund av GDPR”. 5) ”vi har ett

system i enlighet med MSBs riktlinjer. Det systemet används vid incidenter som IT får kännedom om, men inte där verksamheterna själva hanterar incidenterna". När kommunerna utvecklade svaret på varför denna fråga blivit aktuell hänvisade många till den nya lagen, GDPR, som träder i kraft under 2018. Två kommuner saknar i dagsläget ett system eller rutiner för incidentrapportering.

7. Prioriterande krav, rekommendationer och slutsatser

Föreliggande studie visar att det är vanligt att kommuner och myndigheter har någon upphandlad publik molntjänst i sin verksamhet. I vår studie fann vi en högre grad av användande än Gartner (2017) gjort. Däremot går det inte att uttala sig om exakt hur många molntjänster de har. Studien visar även att vissa av molntjänsterna kommit till på grund av att leverantören bytt leveranssätt och nu tillhandhåller funktionaliteten via molntjänster istället för traditionella licenser. Således har inte alla organisationer aktivt upphandlat molntjänsterna. Vissa organisationer påpekar att detta kan begränsa möjligheterna att ställa specifika informationssäkerhetskrav, samtidigt som det visar att förändringar kan ske under avtalstiden.

Mjukvara som tjänst (Software as a Service, SaaS) är den typ av molntjänst som är vanligast förekommande. När det gäller centralisering av molntjänsterna så är det ett fåtal molntjänster som används av många. På samhällsnivå finns det en risk relaterat till dessa molntjänster om de skulle få problem. Samtidigt är dessa molntjänster som används av många organisationer, sett till typen, inte en grund för samhällskritisk infrastruktur eller samhällskritiska tjänster. Vidare visar analysen av leverantörcentralisering inte riktigt lika höga siffror, vilket delvis kan bero på att flera leverantörer ibland kan erbjuda samma molntjänst. Här är dock dataunderlaget något tunt, och de faktiska siffrorna får antas vara högre än vad som anges i studien. När det gäller geografisk placering av molntjänsterna är de allra flesta placerade inom EU/EES, och organisationerna verkar föredra molntjänster placerade i Sverige. Studien visar samtidigt att organisationerna har svårt att veta att om molntjänstleverantörerna är de faktiska leverantörerna eller om det finns underleverantörer. Dels beror det på att många organisationer saknar rutiner för att undersöka detta, dels för att det är svårt att få fram den typen av information. Myndigheterna har här en tydligare bild än kommunerna, likaså verkar de i högre grad ställa krav på att eventuella underleverantörer skall omnämnas i kontrakt. Varför myndigheterna lyckas bättre än kommunerna kan studien inte svara på. Sammantaget innebär detta dock att det finns en osäkerhet i den leverantörsbild som organisationerna angett i den här studien och som legat till grund för analysen.

Organisationerna ser ett flertal olika risker med användningen av molntjänster. Många av riskerna i existerande litteratur (Cloud Security Alliance, 2016; Paquette et al., 2010; Zissis & Lekkas, 2012) bekräftas även om de ges olika prioritet av organisationerna. Studien har dock inte jämfört om dessa risker, såsom identitet och åtkomsthantering, är högre för molntjänster relativt en egen drift. En risk som dock är specifik för molntjänster och som rankas högt av organisationerna är relaterad till att organisationerna inte har tillräcklig

kunskap om att hantera molntjänster. Nära förknippat med risker är också utmaningar som organisationerna anger. Studien visar att lagar och regelverk, kontraktsfrågor och upphandlingsfrågor är de största utmaningarna. Att lagar och regelverk utgör en central utmaning bekräftar således tidigare forskning inom området (Janssen & Joha, 2011). En nyansering av utmaningen för organisationerna är dock att de här ställs inför rekommendationer från flera olika organisationer, och att det inte finns en gemensam bild. Samtliga av dessa är kunskapsfrågor och går att relatera till risken om att inte ha tillräcklig kunskap. Detta påverkar möjligheterna att skapa starka kontrakt från beställarens sida, något som också Paquette et al. (2010) lyft som en utmaning.

Studien visar att det inte verkar finnas en systematik i hur kontrakt med molntjänstleverantörerna följs upp, det är en minoritet av organisationerna som genomför revisioner av informationssäkerheten. Detta gör det svårt att veta exakt vilka av de ställda informationssäkerhetskraven som uppfylls och till vilken nivå. Som Paquette et al. (2010) uttryckt så kan beställare inte utgå från att kraven uppfylls. Likaså tyder föreliggande studie på att det inte finns systematik i att genomföra riskanalyser innan och/eller under kontraktsperioden med en molntjänstleverantör. Generellt verkar det också finnas större utmaningar att åstadkomma systematiska aktiviteter relaterat till upphandling av molntjänster i kommunerna än i myndigheterna. Sett till kommunernas mer decentraliserade organisation är inte detta förvånande, men det förtar inte att avsaknaden av systematik i dessa aktiviteter medför risker. Detta ligger således i linje med Janssen och Joha (2011) som tidigare funnit att det finns organisatoriska risker kopplade till molntjänster.

Slutligen visar studien på att myndigheterna med varierande systematik hanterat frågan om incidentrapportering enligt 9 § MSBFS 2016:2 i kontrakten med molntjänstleverantörerna. Samtidigt bör påpekas att kontrakt i vissa fall tecknats innan denna föreskrift trädde i kraft.

Grundat i ovanstående slutsatser ges följande rekommendationer. Rekommendationerna är uppdelade i tre grupper baserat på prioritet. Inom respektive grupp är rekommendationerna inte prioriterade sinsemellan.

Rekommendationer med hög prioritet:

- *Observation:* Molntjänster är enkelt tillgängliga, vilket gör det svårare att styra upphandlingarna, speciellt i decentraliserade organisationer.

  Problembild: Det finns en risk att organisationerna saknar kunskap om vilka lagar som gäller, och hur kontraktsfrågor och upphandlingsfrågor ska hanteras.

  Rekommendation: Höja kunskapsnivån kring molntjänster och vad användningen av en molntjänst innebär. En ökad kunskap ökar medvetenheten om att upphandlingarna behöver inkludera olika kompetenser i organisationen, istället för att olika delar av en organisation agerar på egen hand. Här lyfts tolkning av lagar relaterat till användningen av molntjänster som ett specifikt efterfrågat stöd. Likaså önskas en ökad samstämmighet i de råd som ges, exempelvis från MSB, SKL och Datainspektionen.

- *Observation*: Kommuner och myndigheter saknar systematik i att genomföra riskanalyser när molntjänster upphandlas samt under kontraktstiden.

  Problembild: Det saknas medvetenhet om vilka risker som finns med molntjänster i de enskilda fallen.

  Rekommendation: Utveckla stöd för att kommuner och myndigheter skall kunna skapa a) systematik i att genomföra riskanalyser när molntjänster upphandlas och b) systematik i att genomföra riskanalyser under molntjänsternas avtalsperioder.

- *Observation*: Kommuner och myndigheter genomför få systematiska informationssäkerhetsrevisioner av upphandlade molntjänster.

  Problembild: Det finns lite kunskap i vilken grad och hur informationssäkerhetskrav som ställts i kontrakten faktiskt uppfylls.

  Rekommendation: Utveckla stöd till systematiska informationssäkerhetsrevisioner av upphandlade molntjänster, för att följa upp hur molntjänstleverantörerna uppfyller ställda informationssäkerhetskrav.

Rekommendationer med mellanprioritet:

- *Observation*: Kommuner och myndigheter har svårt att veta vem som faktiskt levererar hela eller delar av molntjänsterna. Studien indikerar att myndigheterna har en tydligare bild och ställer hårdare krav kring detta än kommunerna, vilket kan öppna möjligheter för kunskapsutbyte.

  Problembild: Det finns lite kunskap om i vilka fall som molntjänstleverantörer använder sig av underleverantörer och vilka dessa är. Det finns således en risk att kommuner och myndigheter inte vet vilka de faktiska leverantörerna är.

  Rekommendation: Utveckla stöd till kommuner och myndigheter kring bakgrundskoll av molntjänstleverantörer och specifikt kring kontroll och kravställande kring underleverantörer.

- *Observation*: Studien visar att molntjänster introduceras under kontraktsperioder trots att kommuner och myndigheter inte upphandlat molntjänst, dvs leverantörer byter leveranssätt.

  Problembild: Molntjänsten genomgår inte upphandling med tydligt ställda informationssäkerhetskrav.

  Rekommendation: Utveckla stöd till kommuner och myndigheter kring hur de skall arbeta med informationssäkerhetskrav när leverantörerna byter leveranssätt under en kontraktsperiod, dvs där installationer på organisationernas servrar omvandlas till molntjänster. Eventuellt är systematisk användning av riskanalyser, dvs punkt 2 under högt prioriterade rekommendationer ett steg i att hantera detta.

Rekommendationer med lägre prioritet:

- *Observation*: I dagsläget visar studien att det finns ett fåtal molntjänster som delas av ett betydande antal kommuner och myndigheter och att de tjänster som delas av flest ofta rör kontorsapplikationer. Andra studier förutspår dock att investeringarna, och således användandet, kommer att öka (ex. Gartner, 2017).

  Problembild: På sikt när användandet av molntjänster växer i omfattning kommer därmed riskerna med att flera kommuner och myndigheter delar molntjänst och/eller samma molntjänstleverantör att öka.

  Rekommendation: Att utarbeta/rekommendera säkerhetsåtgärder relaterat till centralisering av molntjänster.

- *Observation*: Det saknas idag en systematik i hur myndigheter hanterar 9 § MSBFS 2016:2 i kontrakten med molntjänstleverantörerna.

  Problembild: Det finns en risk att incidenter inte rapporteras i enlighet med 9 § MSBFS 2016:2.

  Rekommendation: Stödja myndigheterna i arbetet med att systematiskt hantera frågan om incidentrapportering enligt 9 § MSBFS 2016:2 i kontrakten med molntjänstleverantörerna. Rekommendationen ges dock låg prioritet då myndigheterna ändå visar god medvetenhet om frågan, där de påpekar att kontrakt ingåtts innan förordningen trädde i kraft.

Referenser

Accenture. (2013). A new era for European public services: Cloud computing changes the game: Accenture PLC.

Bhargava, R. (2016, Sep 2, 2016). Best practices for incident response in the age of cloud, NetworkWorld. Retrieved from http://www.networkworld.com/article/3116011/cloud-computing/best-practices-for-incident-response-in-the-age-of-cloud.html

CISCO. (2011). Cloud Computing Advantages in the Public Sector. CISCO White paper: CISCO.

Cloud Security Alliance. (2013). Cloud Computing Vulnerability Incidents: A Statistical Overview: Cloud Security Alliance.

Cloud Security Alliance. (2016). The Treacherous 12 Cloud Computing Top Threats in 2016: Cloud Secuirty Alliance.

Cloud Sweden. (2011). Rättsliga frågor vid flytten till molnet – en checklista: Cloud Sweden.

Danish Government. (2013). Denmark's Digital Growth 2013: Policy Statemnt to the Danish Parliament. Report nr 2012/2013: 39: Danish Ministry of Business and Growth, Danish Government.

Datainspektionen. (2014a). Tillsyn enligt personuppgiftslagen (1998:204) – Behandling av personuppgifter i molntjänsten Office 365 (Dnr 1475-2013). Stockholm: Datainspektionen.

Datainspektionen. (2014b). Tillsyn enligt personuppgiftslagen (1998:204) – uppföljning av beslut om behandling av personuppgifter i molntjänsten Google Apps For Education (Dnr 2633-2014). Stockholm: Datainspektionen.

Denzin, N K, & Lincoln, Y S. (2005). The Sage handbook of qualitative research. London: Sage.

Digitalisér. (2012). Cloud computing and the legal framework: Danish Agency for Digitisation.

Dutta, S, & Mia, I. (2011). The Global Information Technology Report: World Economic Forum and INSEAD.

E-delegationen. (2015). Sekretess vid outsourcing - en förstudie Fi 2009:01/2015/4: Finansdepartmentet.

EDPR. (2017). Europe's digital progress report (EDPR) 2017: Country profile Sweden: Digital Single Market, European Commission.

ENISA. (2013). Cloud Security Incident Reporting: Framework for reporting about major cloud security incidents. Heraklion, Greece.: European Union Agency for Network and Information Security (ENISA).

ENISA. (2014). Annex Good Practice Guide for securely deploying Governmental Clouds. Heraklion, Greece: European Union Agency for Network and Information Security (ENISA).

EU. (2013). Net-cloud Future: European Union (EU), European Commission's DG CONNECT.

EU. (2014). Uptake of Cloud in Europe: IDC Study on Quantitative estimates of the demand for Cloud Computing in Europe and the likely barriers to take-up: European Commission (EC), Communications Networks, Content & Technology.

Eurostat. (2017). Cloud computing - statistics on the use by enterprises. Luxemburg: Statistical office of the European Union (Eurostat).

Filippi, P D, & McCarthy, S. (2012). Cloud Computing: Centralization and Data Sovereignty. European Journal for Law and Technology, 3(2).

Fiondella, L, Gokhale, S S, & Mendiratta, V B. (2013). Cloud Incident Data: An Empirical Analysis. Paper presented at the IEEE International Conference on Cloud Engineering 2013.

Gartner. (2017). Understanding Cloud Adoption in Government. Retrieved December 5, 2017, from http://www.gartner.com/smarterwithgartner/understanding-cloud-adoption-in-government/

IDG. (2016). IDG Enterprise Cloud Computing Survey. USA: International Data Group (IDG).

ISO. (2014). ISO/IEC 17788:2014, Informationsteknik - Molnbaserade datortjänster - Översikt och terminologi: International Organization for Standardization (ISO).

ISO. (2017). ISO/IEC 27000:2017 Information technology - Security techniques - Information security management systems - Overview and vocabulary: International Organization for Standardization (ISO).

Janssen, M, & Joha, A. (2011). Challenges for Adopting Cloud-Based Software as a Service (SaaS) in the Public Sector. Paper presented at the ECIS 2011.

JUHTA. (2015). JHS 166 Terms and Conditions of Public IT Procurement, Advisory Committee on Information Management in Public Administration (JUHTA), Public Sector ICT: Ministry of Finance, Finland.

Khalid, M, Yousaf, M M, Iftikhar, Y, & Fatima, N. (2016). Establishing the state of the art knowledge domain of cloud computing. In H. Sulaiman, M. Othman, M. Othman, Y. Rahim & N. Pee (Eds.), 2nd International Conference on Communication and Computer Engineering, ICOCOE 2015 (pp. 1001-1014): Springer Verlag.

Microsoft. (2014). Security trends in public sector Key findings and recommendations: Microsoft Corperation.

MSB. (2012). Reflektioner kring samhällets skydd och beredskap vid allvarliga it-incidenter - En studie av konsekvenserna i samhället efter driftstörningen hos Tieto i november 2011 MSB 367-12. Stockholm: Myndigheten för samhällsskydd och beredskap.

MSB. (2015). Information Security – trends 2015: A Swedish perspective. Stockholm, Sverige: Myndigheten för samhällsskydd och beredskap.

Müller, S D, Holm, S R, & Søndergaard, J (2015). Benefits of Cloud Computing: Literature Review in a Maturity Model Perspective. Communications of the Association for Information Systems, 37(42), 851-878.

Nordiska ministerrådet. (2012). Nordic Public Sector Cloud Computing – a discussion paper. Copenhagen: Nordic Council of Ministers.

Paquette, S, Jaeger, P T, & Wilson, S C (2010). Identifying the security risks associated with governmental use of cloud computing. Government Information Quarterly, 27(3), 245-253.

Pasupulati, R P, & Shropshire, J. (2016). Analysis of centralized and decentralized cloud architectures. Paper presented at the IEEE SoutheastCon, 2016, Norfolk, United States.

Pearlson, K, & Saunders, C. (2007). Managing and using information systems. Hoboken, NJ: John Wiley & Sons

Pensionsmyndigheten. (2016). Molntjänster i staten - en ny generation av outsourcing: Pensionsmyndigheten.

Radar. (2017). The benefits of Cloud maturity: Cloud Maturity Index 2017: Tieto.

SKL. (2017). Vägledning, molntjänster. Retrieved December 5, 2017, from https://skl.se/skolakulturfritid/skolaforskola/digitaliseringskola/molntjanster/vagledningmolntjanster.9032.html

Subashni, S, & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.

Venkatesh, V., Brown, S. A. & Bala, H. (2013). Bridging the qualitative-quantitative divide: guidelines for conducting mixed methods research in information systems. MIS Quarterly, 37(1), 21-54.

VM. (2018). Finland automates verification of official data in public procurement process. The Ministry of Finance.

WEF. (2016). Global Information Technology Report 2016, Network Readiness index. Geneva, Switzerland: World Economic Forum

Zissis, D, & Lekkas, D. (2012). Addressing cloud computing security issues. Future Generation Computer Systems, 28(3), 583-592.

Bilaga 1: Enkätfrågor

Tabell B1.1 innehåller de enkätfrågor som studien är baserad på. Den exakta numreringen i webbenkätverktyget kan skilja sig från numreringen som används här. Vidare så anpassades presentationen av frågorna i webbenkäten baserat på hur respondenten svarat tidigare, dvs vissa följdfrågor ej var relevanta beroende på tidigare svar. Likaså var inte samtliga frågor relevanta för kommunerna. Här visas samtliga frågor tillsammans med de styrinstruktioner som användes genom enkäten. Styrinstruktionerna återfinns kursivt inom hakparenteser i tabellen.

1. Har er organisation någon upphandlad molntjänst som stöd för delar av och/eller hela verksamheten? • Ja • Nej
[Endast om nej på fråga 1] 1:1 Vilka är de tre viktigaste anledningarna till att er organisation inte har en upphandlad molntjänst som stödsystem för verksamheten? • Risk att förlora kontroll över informationen • Risk att äventyra konfidentialiteten i informationen • Risk att äventyra riktigheten i informationen • Risk att äventyra tillgängligheten i informationen • Risk att inte kunna uppfylla gällande lagstiftning • Risk för avbrott i tjänst • Flytten från egen drift till molntjänster är svår att genomföra • Organisationen saknar kunskap om vad molntjänster kan erbjuda • Organisationen är inte redo att flytta existerande system till molntjänster • Avsaknad av interna policys för bruk av molntjänster • Budgetbegränsningar • Övriga, ange_____
2. I vilken utsträckning använder era anställda privata molntjänstkonton hos t ex Dropbox i tjänsten, dvs konton som inte är arbetsrelaterade? • Till stor del • Till viss del • Ingen användning • Vet inte
[Enkäten avslutas här om nej på fråga 1] 3. Baserat på de riskbedömningar som er organisation gjort, utgör det en risk att anställda använder privata molntjänstkonton (dvs konton som inte är arbetsrelaterade) i tjänsten? • Ja • Nej • Någon sådan riskbedömning har inte gjorts
4. Erbjuder ni era anställda godkända molntjänster, som alternativ till molntjänster införskaffade av användaren själv? • Ja, fullt ut • Ja, till stor utsträckning • Ja, i viss utsträckning • Nej
[Endast möjligt att välja tre alternativ]

5. Vilka är de tre huvudsakliga anledningarna till att er organisation använder molntjänster?

- Kostnadsfördelar
- Ökad flexibilitet
- Möjliggör fokus på organisationens huvuduppgifter
- Möjliggör enkel åtkomst till specialiserade IT-resurser
- Ökad kvalitet hos IT-resurser
- För att andra liknande organisationer använder molntjänster
- Förbättrad informationssäkerhet
- Att inte behöva installera och underhålla mjukvara
- För att fullfölja ett uppdrag som erhållits utifrån, exempelvis från Sveriges regering. [Svarsalternativet inte relevant för kommuner, visas ej]
- Övriga, ange_____

6. Hur bedömer er organisation informationssäkerhetsrisken med molntjänster jämfört med egen it-drift?

- Ökad risk
- Varken ökad eller minskad risk
- Minskad risk
- Vet inte

7. Använder er organisation upphandlad mjukvara som tjänst (SaaS - Software as a Service), såsom Microsoft Office 365, Google G Suite, och DropBox?

- Ja
- Nej
- Vet inte

[Endast om ja på fråga 7, annars gå till fråga 8]

7:1 Om möjligt, ange namnen på de SaaS-tjänster er organisation använder och som stödjer det er organisation bedömt är verksamhetskritiska funktioner:

_____

8. Använder er organisation en upphandlad plattform som tjänst (Paas - Platform as a Service), såsom Windows Azure, Google App Engine och Appredna?

- Ja
- Nej
- Vet inte

[Endast om ja på fråga 8, annars gå till fråga 9]

8:1 Om möjligt, ange namnen på de PaaS-tjänster er organisation använder och som stödjer det er organisation bedömt är verksamhetskritiska funktioner:

_____

9. Använder er organisation en upphandlad infrastruktur som tjänst (Iaas - Infrastructure as a Service), såsom Amazon EC2, Google Compute Enginee och DigitalOcean?

- Ja
- Nej
- Vet inte

[Endast om ja på fråga 9, annars gå till fråga 10]

9:1 Om möjligt, ange namnen på de IaaS-tjänster er organisation använder och som stödjer det er organisation bedömt är verksamhetskritiska funktioner:

_____

10. Har er organisations informationssäkerhetsklassning använts som utgångspunkt för kravhantering vid upphandling av molnjänster?

- Ja
- Nej
- Vet inte

11. Utför er organisation en systematisk riskanalys före upphandling av molntjänst?

- Alltid
- Ibland
- Aldrig
- Vet inte

12. Utför er organisation systematiska riskanalyser av er/era molntjänster under pågående avtalsperiod?

- Alltid
- Ibland
- Aldrig
- Vet inte

13. Tar er organisation leverantörens historik i beaktning vid upphandling av molntjänst?

- Alltid
- Ibland
- Aldrig
- Vet inte

[Endast möjligt att välja tre alternativ]

14. Vilka är de tre huvudsakliga utmaningarna vid upphandling av molntjänster?

- Att hantera tekniska frågor
- Att hantera upphandlingsfrågor
- Att hantera kontraktsfrågor
- Att hantera jämförelser av molntjänster
- Att hantera eventuellt motstridiga nationella lagar
- Att hantera nationell säkerhet
- Att hantera vilka lagar som gäller vid gränsöverskridande molntjänster
- Att hantera gemensam upphandling med andra offentliga organisationer
- Att hantera leverantörsinlåsning
- Övriga, ange_____

15. Om möjligt, ange namnet på er organisations molntjänstleverantör/ leverantörer som levererar stöd till det som er organisation bedömt är verksamhetskritiska funktioner:

_____

16. Vilka informationssäkerhetskrav relaterat till molntjänster har er organisation ställt när molntjänst-leverantören/leverantörerna inte använder standardiserade kontrakt?

- Nationella rättsliga krav

- Särskilda lagkrav för internationellt gränsöverskridande tjänster
- Rättsliga krav för kundens hantering av personuppgifter utanför EES
- Krav kring datakryptering
- Krav på redundant infrastruktur
- Krav på tydligt ansvar vid "förlust av data" (på grund av tekniska fel, stöld av data eller intrång)
- Krav på kontinuitetsplanering
- Krav på skydd mot skadlig kod
- Krav kring immateriella rättigheter
- Krav på möjligheter till säkerhetsrevision
- Krav om påföljder ifall servicenivåerna inte uppfylls
- Krav på ägandet av informationen
- Krav på administrativ personal
- Krav på fysisk säkerhet
- Krav på ledningssystem för informationssäkerhet
- Övriga, ange_____

17. Vilka informationssäkerhetskrav relaterat till molntjänster granskar ni att molntjänstleverantören /leverantörerna inkluderat när det använder standardiserade kontrakt?

- Nationella rättsliga krav
- Särskilda lagkrav för internationellt gränsöverskridande tjänster
- Rättsliga krav för kundens hantering av personuppgifter utanför EES
- Krav kring datakryptering
- Krav på redundant infrastruktur
- Krav på tydligt ansvar vid "förlust av data" (på grund av tekniska fel, stöld av data eller intrång)
- Krav på kontinuitetsplanering
- Krav på skydd mot skadlig kod
- Krav kring immateriella rättigheter
- Krav på möjligheter till säkerhetsrevision
- Krav om påföljder ifall servicenivåerna inte uppfylls
- Krav på ägandet av informationen
- Krav på administrativ personal
- Krav på fysisk säkerhet
- Krav på ledningssystem för informationssäkerhet
- Övriga, ange_____

18. Innehåller kontraktet med leverantören/leverantörerna skrivelser om vilket ansvar leverantören har vid eventuella säkerhetsincidenter?

- Ja
- Nej
- Vet inte

19. Finns det reglerat i era kontrakt att leverantörens informationssäkerhetsarbete ska utföras utifrån internationella standarder för informationssäkerhet (ex ISO-27001 och ISO-27002)?

- Ja, i alla
- Ja, i vissa
- Nej, i inga
- Vet inte

[Endast om något av ja-alternativen på fråga 19, annars gå till fråga 20]

19.1 Följer ni upp att leverantören uppfyller kraven (genom att t ex begära in SoA och certifikat)?

- Ja
- Nej

[Frågan är inte relevant för kommuner, visas ej. Om kommun gå till fråga 21]

20. Är det i kontrakten med molntjänstleverantören reglerat hur incidentrapportering enligt 9 § MSBFS 2016:2 skall ske?

- Ja, det är vanligtvis reglerat, de rapporterar till vår organisation
- Ja, det är vanligtvis reglerat, de rapporterar till MSB
- Ja, det är vanligtvis reglerat, de rapporterar till vår organisation och MSB
- Nej, det är vanligtvis inte reglerat
- Vet inte

21. När utför er organisation revisioner av avtalet med er/era molntjänstleverantör /leverantörer?

- Initialt
- Regelbundet
- Aldrig
- Vet inte

22. Innehåller de kontrakt (standardiserade/icke standardiserade) som er organisation har med molntjänstleverantören/leverantörerna bestämmelser om att ert data skall behandlas separerat från andra kunders data?

- Ja, alla
- Ja, vissa
- Nej, inga
- Vet inte

23. Står det angivet i kontrakten (standardiserade/icke standardiserade) som er organisation har med molntjänstleverantören/ leverantörerna i vilket land ert data behandlas?

- Ja, i alla
- Ja, i vissa
- Nej, i inga
- Vet inte

[Endast om ja på fråga 23, annars gå till fråga 24]

23:1 Om möjligt, ange i så fall land:

_____

24. Om ert data behandlas utomlands, står det angivet i kontrakten (standardiserade/icke standardiserade) som er organisation har med molntjänstleverantören/leverantörerna vilka lagar som gäller vid eventuella informationssäkerhetsincidenter?

- Ja, i alla
- Ja, i vissa
- Nej, i inga
- Inte behandlat utomlands
- Vet inte

25. Står det angivet i kontrakten (standardiserade/icke standardiserade) som er organisation har med molntjänstleverantören/ leverantörerna vilken personal hos leverantören som har åtkomst till data som finns lagrat?

- Ja, alla
- Ja, vissa
- Nej, inga
- Vet inte

26. Har er organisation rutiner för att identifiera om molntjänstleverantören/ leverantörerna har anlitat några underleverantörer för att tillhandahålla de upphandlade molntjänsterna?

- Ja
- Nej

27. Baserat på det upphandlingsarbete som genomförts, i hur hög grad skräddarsyr molntjänst-leverantörerna sina lösningar baserat på er organisations krav på informationssäkerhet?

- I samtliga fall
- I mer än hälften av fallen
- I mindre än hälften av fallen
- I inga fall

28. Baserat på det upphandlingsarbete som genomförts, i hur hög grad uppfyller molntjänst-leverantörerna era informationssäkerhetskrav vid upphandling?

- Alla uppfyller kraven
- Mer än hälften uppfyller kraven
- Mindre än hälften uppfyller kraven
- Inga uppfyller kraven

29. Baserat på de revisioner som er organisation genomfört, i hur hög grad uppfyller molntjänst-leverantörerna era informationssäkerhetskrav?

- Alla uppfyller kraven
- Mer än hälften uppfyller kraven
- Mindre än hälften uppfyller kraven
- Inga uppfyller kraven
- Inga revisioner har genomförts

30. Baserat på de uppföljningar som er organisation genomfört, i hur hög grad har molntjänst-leverantörerna uppfyllt era informationssäkerhetskrav vid incidenter?

- Alla har uppfyllt kraven
- Mer än hälften uppfyllt kraven
- Mindre än hälften uppfyllt kraven
- Inga uppfyllt kraven
- Inga uppföljningar har genomförts
- Inga incidenter har inträffat

31. Baserat på de riskbedömningar som er organisation gjort, utgör det huvudsakligen en högre eller lägre risk ifall flera offentliga verksamheter anlitar samma molntjänstleverantör?

- Högre risk
- Varken högre eller lägre risk
- Lägre risk
- Någon sådan riskbedömning har inte gjorts

32. Baserat på er organisations samlade bedömning, vilka är de tre huvudsakliga informationssäkerhets-riskerna vid användande av molntjänster?

- Dataöverträdelser
- Svag identitet-, referens- och åtkomsthantering
- Osäkra API:er
- Säkerhetsproblem i system och/eller mjukvara
- Kontokapning
- Skadlig programvara
- Målmedvetna riktade angrepp

• Dataförlust • Otillräcklig kännedom • Missbruk och fientlig användning av molntjänster • Avbrott i tjänst • Delade teknikproblem • Övrig anledning, ange_____
33. Har er organisation upplevt några incidenter, ex avbrott, förlust av data, eller liknande vid använd-ning av en upphandlad molntjänst? • Ja • Nej
[Endast om ja på fråga 33, annars avsluta enkäten] 33:1. Ange ange vilka typer av incidenter er organisation råkat utför i relation till användningen av molntjänster • Avbrott i tjänsten • Dataförlust • Förvanskning av information • Obehöriga har fått tillgång till information • Övrigt

Tabell B1.1: Frågeunderlag för webbenkät

Bilaga 2: Inbjudan till kommun

Örebro 2017-XX-XX

Säkerhet vid molnlösningar

Örebro universitet vill bjuda in er att delta i en undersökning om offentliga aktörers exponering gentemot molntjänster. Undersökningen genomförs av Örebro universitet på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB), där myndigheten vill genomföra en studie av användningen av molntjänster ur ett nationellt perspektiv. Den här enkäten tillsammans med ett begränsat antal uppföljande intervjuer är en del av detta arbete.

I dagens samhälle är i princip all verksamhet, även sådan som är samhällsviktig, beroende av välfungerande it-infrastruktur och it-tjänster. MSB har konstaterat att nyttjande av molntjänster är en driftsform som ökat, samtidigt som myndigheten för närvarande saknar en helhetsbild av hur offentliga myndigheter och kommuner använder sig av molntjänster. Att skapa sig en bättre bild över denna miljö och dess beroenden är en viktig uppgift för MSB, både för att kunna lämna råd och stöd i fråga om förebyggande arbete men även för att vara så väl förberedd som möjligt och därmed kunna stödja samhället i arbetet med att hantera informationssäkerhetsincidenter.

Era svar är viktiga

Att delta i undersökningen är frivilligt, men er medverkan är mycket betydelsefull. Er organisation är utvald för att som kommun har ni ett av det svenska samhällets mest komplexa uppdrag. Det omfattar allt från den dagliga omsorgen av äldre till att säkerställa att känslig infrastruktur fungerar, vilket innebär att en stor del av den samhällsviktiga verksamheten räknas till kommunernas ansvar. I samtliga delar av uppdraget spelar säker informationshantering en central roll, och vi är intresserade av den övergripande bild er kommun har kring molntjänster. Samråd har genomförts med Sveriges Kommuner och Landsting enligt förordningen om statliga myndigheters inhämtande av uppgifter från kommuner och näringsidkare, SFS 1982:668.

Du gör så här

Besvara frågorna via [url till webbenkät]

Logga in med användarnamn och lösenord.

Användarnamn: XX

Lösenord: XX

Vi ber dig besvara frågorna senast XX december.

Stort tack på förhand för er medverkan!

Med vänlig hälsning

Fredrik Karlsson	Carl Önne
Projektansvarig/Professor	Handläggare, beställare av studien
Örebro universitet	Myndigheten för samhällsskydd och beredskap
	carl.onne@msb.se

Frågor om undersökningens innehåll

Örebro universitet, Fredrik Karlsson

Telefon: 019-30 39 94, e-post: fredrik.karlsson@oru.se

Örebro universitet, 701 82 Örebro

www.oru.se

Bilaga 3: Inbjudan myndighet

ÖREBRO UNIVERSITET
HANDELSHÖGSKOLAN

Örebro 2017-XX-XX

Säkerhet vid molnlösningar

Örebro universitet vill bjuda in er att delta i en undersökning om offentliga aktörers exponering gentemot molntjänster. Undersökningen genomförs av Örebro universitet på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB), där myndigheten vill genomföra en studie av användningen av molntjänster ur ett nationellt perspektiv. Den här enkäten tillsammans med ett begränsat antal uppföljande intervjuer är en del av detta arbete.

I dagens samhälle är i princip all verksamhet, även sådan som är samhällsviktig, beroende av välfungerande it-infrastruktur och it-tjänster. MSB har konstaterat att nyttjande av molntjänster är en driftsform som ökat, samtidigt som myndigheten för närvarande saknar en helhetsbild av hur offentliga myndigheter och kommuner använder sig av molntjänster. Att skapa sig en bättre bild över denna miljö och dess beroenden är en viktig uppgift för MSB, både för att kunna lämna råd och stöd i fråga om förebyggande arbete men även för att vara så väl förberedd som möjligt och därmed kunna stödja samhället i arbetet med att hantera informationssäkerhetsincidenter.

Era svar är viktiga

Att delta i undersökningen är frivilligt, men er medverkan är mycket betydelsefull. Er organisation är utvald för att som offentlig myndighet har ni en central funktion i samhällsviktig verksamhet, samt att ni som myndighet är rapporteringsskyldig till MSB enligt MSBFS 2016:2.

Du gör så här

Besvara frågorna via [url till webbenkät]

Logga in med användarnamn och lösenord.

Användarnamn: Verdana 11

Lösenord: Verdana 11

Vi ber dig besvara frågorna senast XX december.

Stort tack på förhand för er medverkan!

Med vänlig hälsning

Fredrik Karlsson	Carl Önne
Projektansvarig/Professor	Handläggare, beställare av studien
Örebro universitet	Myndigheten för samhällsskydd och beredskap
	carl.onne@msb.se

Frågor om undersökningens innehåll

Örebro universitet, Fredrik Karlsson

Telefon: 019-30 39 94, e-post: fredrik.karlsson@oru.se

Örebro universitet, 701 82 Örebro

www.oru.se

Bilaga 4: Påminnelsebrev till kommun

Örebro 2017-XX-XX

Säkerhet vid molnlösningar: påminnelse om enkät

För ett par veckor sedan bjöd Örebro universitet in er att delta i en undersökning om offentliga aktörers exponering gentemot molntjänster. Vi har inte erhållit något svar från er organisation och vill därför påminna om undersökningen. Om ni under de senaste dagarna besvarat enkäten, så ber vi er bortse från denna påminnelse.

Undersökningen genomförs av Örebro universitet på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB), där myndigheten vill genomföra en studie av användningen av molntjänster ur ett nationellt perspektiv. Enkäten tillsammans med ett begränsat antal uppföljande intervjuer är en del av detta arbete.

Era svar är viktiga

Att delta i undersökningen är frivilligt, men er medverkan är mycket betydelsefull. Er organisation är utvald för att som kommun har ni ett av det svenska samhällets mest komplexa uppdrag. Det omfattar allt från den dagliga omsorgen av äldre till att säkerställa att känslig infrastruktur fungerar, vilket innebär att en stor del av den samhällsviktiga verksamheten räknas till kommunernas ansvar. I samtliga delar av uppdraget spelar säker informationshantering en central roll, och vi är intresserade av den övergripande bild er kommun har kring molntjänster. Samråd har genomförts med Sveriges Kommuner och Landsting enligt förordningen om statliga myndigheters inhämtande av uppgifter från kommuner och näringsidkare, SFS 1982:668.

Du gör så här

Besvara frågorna via [url till webbenkät]

Logga in med användarnamn och lösenord.

Användarnamn: XX

Lösenord: XX

Vi ber dig besvara frågorna senast XX december.

Stort tack på förhand för er medverkan!

Med vänlig hälsning

Fredrik Karlsson	Carl Önne
Projektansvarig/Professor	Handläggare, beställare av studien
Örebro universitet	Myndigheten för samhällsskydd och beredskap
	carl.onne@msb.se

Frågor om undersökningens innehåll

Örebro universitet, Fredrik Karlsson

Telefon: 019-30 39 94, e-post: fredrik.karlsson@oru.se

Örebro universitet, 701 82 Örebro

www.oru.se

Bilaga 5: Påminnelsebrev till myndighet

Örebro 2017-XX-XX

Säkerhet vid molnlösningar: påminnelse om enkät

För ett par veckor sedan bjöd Örebro universitet in er att delta i en undersökning om offentliga aktörers exponering gentemot molntjänster. Vi har inte erhållit något svar från er organisation och vill därför påminna om undersökningen. Om ni under de senaste dagarna besvarat enkäten, så ber vi er bortse från denna påminnelse.

Undersökningen genomförs av Örebro universitet på uppdrag av Myndigheten för samhällsskydd och beredskap (MSB), där myndigheten vill genomföra en studie av användningen av molntjänster ur ett nationellt perspektiv. Enkäten tillsammans med ett begränsat antal uppföljande intervjuer är en del av detta arbete.

Era svar är viktiga

Att delta i undersökningen är frivilligt, men er medverkan är mycket betydelsefull. Er organisation är utvald för att som offentlig myndighet har ni en central funktion i samhällsviktig verksamhet, samt att ni som myndighet är rapporteringsskyldig till MSB enligt MSBFS 2016:2.

Du gör så här

Besvara frågorna via [url till webbenkät]

Logga in med användarnamn och lösenord.

Användarnamn: XX

Lösenord: XX

Vi ber dig besvara frågorna senast XX december.

Stort tack på förhand för er medverkan!

Med vänlig hälsning

Fredrik Karlsson	Carl Önne
Projektansvarig/Professor	Handläggare, beställare av studien
Örebro universitet	Myndigheten för samhällsskydd och beredskap
	carl.onne@msb.se

Frågor om undersökningens innehåll

Örebro universitet, Fredrik Karlsson

Telefon: 019-30 39 94, e-post: fredrik.karlsson@oru.se

Örebro universitet, 701 82 Örebro

www.oru.se

Myndigheten för samhällsskydd och beredskap
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1196 – maj 2018 ISBN 978-91-7383-819-1