FSPOS

Finansiella Sektorns Privat-Offentliga Samverkan

Riskhantering vid användning av molntjänstleverantörer

21-12-14

FSPOS Arbetsgrupp Analys

Innehållsförteckning

1. Inledning

Molntjänster används i utökad utsträckning i finanssektorn. För många innebär det avgörande fördelar genom att effektivisera och tillgängliggöra verksamhetsprocesser. Samtidigt finns det utmaningar som användare behöver förhålla sig till, såväl vid användning av molntjänster som vid outsourcing av verksamhet, inte minst hur krav på hantering av risk ska tillämpas och följas upp.

Allt fler leverantörer prioriterar en leveransmodell som bygger på molntjänstlösningar. Det gör att det på sikt kan förväntas bli svårare för verksamhetsutövare inom såväl den finansiella sektorn som andra branscher, att förse verksamheten med IT-funktionalitet som bygger på produktköp och produktinstallation på egen infrastruktur. I förlängningen innebär det att verksamheterna kan hämmas om det inte skapas möjligheter att kunna dra nytta av molntjänster.

Till viss del kan molntjänstesektorn betraktas som en omogen bransch, där exempelvis regelverk, standarder, kvalitetscertifieringar eller avtal inte är standardiserade. Ett flertal initiativ och aktiviteter pågår för att skapa förtroende mellan kunder och molntjänstleverantörer. Ett exempel är Cloud Security Alliance (CSA) som är en ideell organisation där molntjänstleverantörer kan göra självskattningar utifrån en kravlista eller bli granskade av CSA-revisorer. Hos EU-kommissionen pågår ett arbete med att ta fram standardklasuler för branschen som stöd till finansiella sektorn där särskilda krav på styrning och hantering av risker beskrivs.[1]

Syfte och metod

Detta dokument syftar till att beskriva ett riskbaserat förhållningssätt till användning av molntjänster och belyser viktiga steg i processen, med särskilt fokus på att upphandla, avtala samt utvärdera tjänsten. Dokumentet ger även exempel på verktyg som kan användas och regelverk som kan ge vägledning.

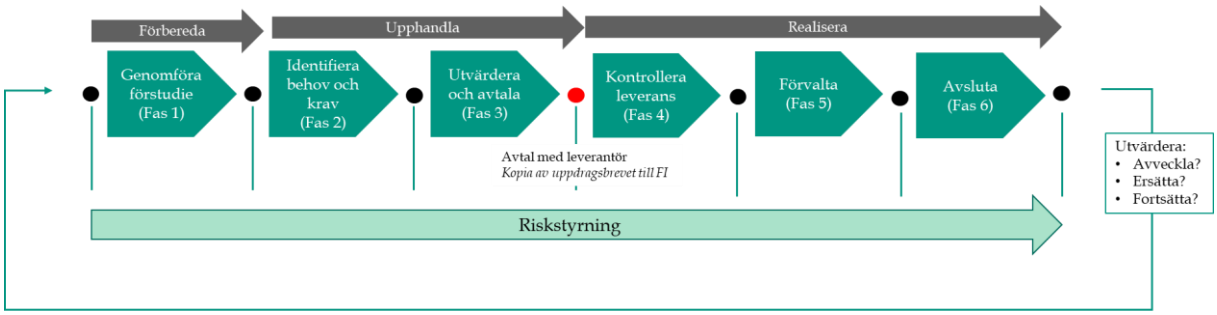
Rapporten är baserad på information från öppna källor, exempelvis standarder och rapporter, Finansinspektionens föreskrifter, *Digital operational resilience act* (Dora) samt de europeiska tillsynsmyndigheterna, European Bank Authority (EBA), European Insurance and Occupational Pensions Authority (Eiopa) och European Securities and Markets Authoritys (Esma) riktlinjer för användning av molntjänster.

Rapporten följer en struktur som utgår från MSB:s vägledning ”Upphandla informationssäkert”,[2] anpassat till den finansiella sektorns perspektiv och med särskilt fokus på att kravställa och följa uppmolntjänster avseende riskhantering.

---

[1] *Standard Contractual Clauses for Cloud Services*

[2] *MSB1177-november 2018*



Figur 1. Översikt över steg för att upphandla och använda en molntjänst.

2. Beskrivning molntjänst

Molntjänster är ett samlingsbegrepp för olika typer av IT-lösningar och det finns olika definitioner vad gäller begreppet molntjänst. I detta dokument används Swedish Standards Institutes (SIS) definition[3] kompletterat med det amerikanska standardiseringsorganet National Institute for Standards and Technologys (NIST) definitioner[4] av en molntjänst. SIS har antagit en svensk standard (ISO/IEC 17788:2014, IDT) som fastslår att 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. NIST definition är mycket lik och har, sedan den publicerades 2011, fått stor spridning.[5]

Huvudegenskaperna hos molnbaserade tjänster, enligt SIS och NIST, är:

- Brett tillgänglig nätverksåtkomst.
- Fleranvändande och resursdelning.
- Självbetjäning på begäran.
- Snabb elasticitet och skalbarhet.

Brett tillgänglig avser att tjänsten är åtkomlig via Internet eller motsvarande nätverk.

---

[3] *Se: SS-ISO/IEC 17788:2014 (definition av moln) och SS- ISO/IEC 27017:2015, Riktlinjer för säkerhetsåtgärder för molntjänster baserade på ISO 27002*

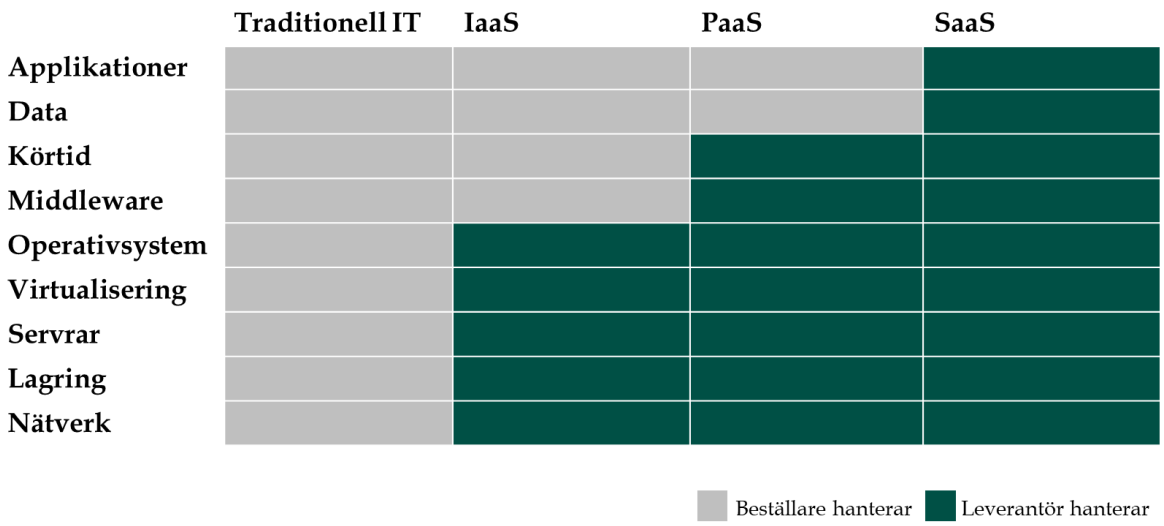
[4] *NIST Special Publication 800-145*

[5] *NIST definition: "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"*

Fleranvändande och resursdelning används för att beskriva dataresurser som tillhandahålls för flera användare som delar en gemensam åtkomst till tjänsten. Även om tjänsten tillhandahålls från samma elektroniska utrustning, genomförs informationsbehandlingen separat för varje användare
Självbetjäning innebär att användare själva kan ansluta sig för att skaffa nya tjänster eller avsluta tjänster utan manuellt stöd från leverantören.
Elasticitet används för att beskriva dataresurser som avsätts och utnyttjas beroende på efterfrågan för att tillgängliga resurser snabbt ska kunna utökas och minskas i takt med kapacitetsbehovet.
Skalbarhet avser dataresurser som leverantören av molntjänster fördelar på ett flexibelt sätt, oberoende av resursernas geografiska läge, för att hantera variationer i efterfrågan.

Tjänstemodeller

Det finns tre internationellt etablerade tjänstemodeller av molntjänster.[6] Bilden nedan visar skillnaden mellan dessa tjänstemodeller.



Figur 2 - Skillnaden på olika tjänstemodeller

1. *Infrastruktur som tjänst (Infrastructure as a Service, IaaS)* – kunden kan skapa och använda resurser hos en eller flera molntjänstleverantörer i form av fysisk hårdvara såsom servrar, nätverk, lagringsutrymme, lastbalansering, beräkning med mera. Kunden tillhandahåller själv de plattformar och applikationer som används i infrastrukturen. Kunden har inte kontroll över den underliggande infrastrukturen, men kontrollerar till exempel operativsystem, lagring och utvecklade och utrullade applikationer i infrastrukturen. Ibland kan kunden ha

[6] *Regeringskansliet, "Statens molnutredning, 2021*

begränsad kontroll över utvalda nätverkskomponenter, som till exempel brandväggar. Ett exempel är MS Azure.

2. *Plattform som tjänst (Platform as a Service, PaaS)* – leverantören tillhandahåller applikationsplattformar via internet eller annat nät, för användare att installera sina egna applikationer i. Ett exempel på en sådan tjänst är utvecklingsmiljöer som inkluderar en underliggande infrastruktur men adderar ett ramverk (programspråk och utvecklingsmiljöer) där det går att använda eller utveckla nya system. Kunden driftsätter egna eller anskaffade applikationer men kan använda språk, bibliotek, tjänster och andra verktyg som leverantören tillhandahåller i plattformen. Ett exempel på det senare är Amazon Web Services.

3. *Mjukvara som tjänst* (Software as a Service, SaaS) – leverantören tillhandahåller mjukvara som tjänst, det vill säga färdiga eller konfigurerbara applikationer över internet eller annat nät. Tjänstetypen kallas ibland *applikation som tjänst*. Denna tjänstetyp kan levereras på flera sätt och vara tillgänglig genom till exempel en webbläsare. Leverantören står för allt underhåll. Kunden kan inte påverka leverantörens infrastruktur och plattform (nätverk, servrar, operativsystem, lagring, språk och plattformsuppbyggnad) eller andra individuella förmågor, med eventuellt undantag för vissa användarspecifika inställningar kopplat till användaren eller dennes konto. Exempel på en sådan molntjänst är Google Docs eller Office 365 samt AI-stöd som till exempel Watson.

Leveransmodeller

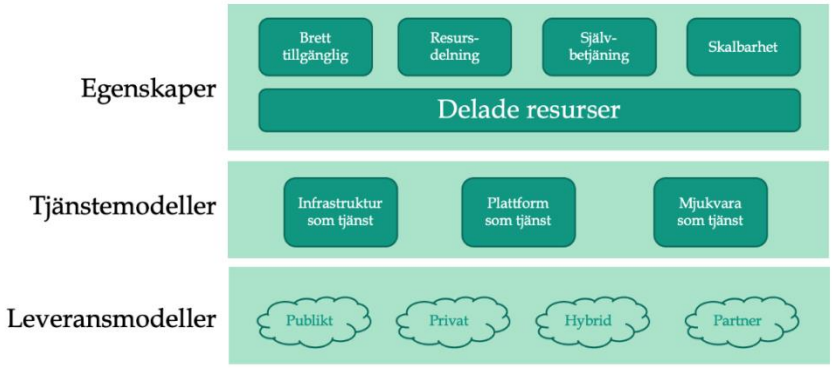
Utöver tjänstemodellerna finns fyra leveransmodeller för tillhandahållande av molntjänster.

Publikt moln – Molntjänsten ägs och hanteras av en molntjänstleverantör (tredje part) som säljer resurser till flera kunder på samma infrastruktur. Tjänster i publika moln är potentiellt tillgängliga för alla som så önskar. Även i ett publikt moln kan olika kunders information vara olika mycket separerad. Ju mer separerad, desto mindre potentiella skalfördelar. Samtidigt kan säkerhetsmässiga fördelar göra en separering inom det publika molnet rationell.

Partnermoln – erbjuds till en begränsad och väldefinierad grupp av intressenter och kunder. Molntjänsten levereras åt kunder med likartad kravbild. Den gemensamma kravbilden kan till exempel avse uppdrag, målsättning, säkerhetskrav och krav på efterlevnad. Partnermolnet ägs och hanteras av en eller flera av kunderna i samarbete, alternativt av, eller tillsammans med, en tredje part. Molnet kan tillhandahållas antingen i eller utanför kundens lokaler. Partnermoln används bland annat inom offentlig sektor där exempelvis flera kommuner eller regioner kan gå ihop och skapa en gemensam molntjänst men leveransmodellen förekommer även inom finanssektorn.

Privat moln – Molntjänsten levereras på en infrastruktur avsedd för endast en kund. Infrastrukturen kan hanteras av kunden själv eller av en annan aktör.

Hybridmoln – Avser en sammansättning av två eller flera molntyper som möjliggör kopplingar mellan olika tjänster och molntyper. Det kan till exempel innebära att behålla befintlig IT-infrastruktur och -drift och komplettera med en molnlösning från tredje part. Googles tjänst *Dedicated Interconnect* är ett exempel på en hybridmolntjänst.



Figur 1 - Molntjänsters egenskaper, tjänstemodeller samt leveransmodeller

Det finns många olika molntjänstleverantörer. Bland svenska organisationer diskuteras vanligen om det ska vara en svensk molntjänst, en molntjänst levererad från EU eller en tredjelandsleverantör. Det grundar sig bland annat i behovet – och kravet - av att förhålla sig till lagstiftning, vilken skiljer sig mellan olika länder. Molntjänster är ofta förknippat med att lämna ut personuppgifter; därför behöver det utredas om en leverantör från tredje land är lämplig och/eller laglig att anlita utifrån t.ex. *General Data Protection Regulation* (GDPR). I fråga om att välja en svensk molntjänst eller en molntjänst från något EU-land, är GDPR inte ett hinder i sig men det kan däremot skilja sig vilken lag som gäller vid en tvist. Detta dokument fördjupar sig inte mer i denna aspekt utan stannar vid att uppmärksamma diskussionen.

3. Kravbilden

I detta avsnitt beskrivs innehåll i regelverk och riktlinjer som den finansiella sektorn tillämpar avseende utkontraktering till molntjänster, särskilt vad gäller krav på riskhantering.

Finansinspektionens föreskrifter

I *Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut*[7], beskrivs dels att instituten ska ha interna regler för hantering av outsourcing, uppdragsavtal, dels att den upphandlande organisationen ska ”...handla med den skicklighet, omsorg och aktsamhet som krävs när det ingår, hanterar och säger upp uppdragsavtal som avser arbete eller funktioner som är av väsentlig betydelse för verksamheten”. Vidare ska den organisation som outsourcar en eller flera verksamheter, bland annat se till att leverantören är lämplig och att den följer tillämpliga regler. Detta ska regleras genom ett skriftligt avtal. För outsourcing av investeringstjänster utanför EES för privatkunder tillkommer särskilda regler.

I *Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker*[8] anges att ett företag ska identifiera operativa risker i sina produkter, tjänster, funktioner, processer och it-system, samt beskriva vilka it-system som stödjer processen i processdokumentationen. För att möjliggöra detta krävs att konsekvensanalys och riskbedömning görs på ett korrekt sätt inom ramen för kontinuitetsarbetet, med särskilt fokus på de it-system som stödjer processen. Ett företag ska även ha en process för att godkänna nya eller väsentligt förändrade produkter, tjänster, marknader, processer, it-system samt för större förändringar i företagets verksamhet och organisation. Det innebär att kontinuitetsplaner och återställningsplaner ska granskas vid större förändringar. Ett företag ska se till att dess huvudsakliga it-driftställe finns på ett tillräckligt stort geografiskt avstånd från den plats där företaget förvarar säkerhetskopior. För samtliga bestämmelser avseende hur ett företag ska hantera it-system hänvisar föreskriften till FFFS 2014:5 om informationssäkerhet, it-verksamhet och insättningssystem.

Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, it-verksamhet och insättningssystem (FFFS 2014:5)[9] omfattar bland annat krav på att företagen ska arbeta strukturerat och metodiskt med informationssäkerhet. De reglerar även styrning och processer för it-verksamheten samt ställer krav på säkerheten för insättningssystem.

I promemorian *Finansinspektionens syn på revisionsrätten för verksamhet som läggs ut på molntjänstleverantörer*[10] beskrivs även varför revisionsrätten är så viktig. Den upphandlande organisationen kan komma överens med en molntjänstleverantör om

---

[7] *Finansinspektionens föreskrifter och allmänna råd om styrning, riskhantering och kontroll i kreditinstitut (FFFS 2014:1)*

[8] *Finansinspektionens föreskrifter och allmänna råd om hantering av operativa risker (FFFS 2014:4)*

[9] *Finansinspektionens föreskrifter och allmänna råd om informationssäkerhet, IT-verksamhet och insättningssystem (FFFS 2014:5)*

[10] *Finansinspektionens syn på revisionsrätten för verksamhet som läggs ut på molntjänstleverantörer (FI Dnr 18-5393)*

begränsad revisionsrätt, men måste i detta fall göra en grundlig riskanalys och kunna motivera varför begränsningen inte påverkar organisationens kontrollmöjligheter.
Finansinspektionen utövar tillsyn på företaget och inte molntjänstleverantören, vilket innebär att myndigheten i första hand vänder sig till företaget för att få information. Om företaget inte kan ge den information som behövs, måste det finnas beskrivet i avtal med molntjänstleverantören att Finansinspektionen ska få fullständig information och även kunna göra kontroller på plats om det skulle behövas. Denna rättighet får inte begränsas i avtalet.

Finansinspektionen kan även ställa krav på företaget att anmäla utlagd verksamhet samt skicka in en kopia av uppdragsavtalet till Finansinspektionen . Syftet är att Finansinspektionen behöver förstå omfattningen på den utkontrakterade verksamheten samt vilka risker det kan innebära. Finansinspektionen åtar sig dock inte att granska avtalen i sin helhet beträffande företagets riskhantering och godkänner formellt inte heller avtal.

Vidare lyfter Finansinspektionen vikten av att använda standardavtal. Detta underlättar vid upprättande av ett avtal med en molntjänstleverantör för att undvika att avtalet begränsar möjligheter att leva upp till regelverkets krav.

Finansinspektionen har även information på sin hemsida, till exempel frågor och svar om utlagd verksamhet[11].

Finansinspektionen deltar i internationella samarbeten genom EU:s tillsynsmyndigheter (EBA, Eiopa och Esma) och följer EBA:s riktlinjer om utkontraktering samt Esma:s riktlinjer om utkontraktering till molntjänstleverantörer. I tillsynsarbetet motsvarar dessa riktlinjer Finansinspektionens allmänna råd.

EBA, Eiopa och Esma – riktlinjer

De europeiska tillsynsmyndigheterna, European Bank Authority (EBA), European Insurance and Occupational Pensions Authority (Eiopa) och European Securities and Markets Authority (Esma), har upprättat riktlinjer och förhållningssätt till användning av molntjänster. Riktlinjerna från respektive myndigheterna är i hög utsträckning lika. EBA:s riktlinjer är något mer allmänt hållna då de berör outsourcing generellt medan Eiopa och Esma särskilt fokuserar på outsourcing till molntjänstleverantörer.

[11] *Finansinspektionens frågor och svar om utlagd verksamhet*

EBA – Riktlinjer för utkontraktering

EBA:s *Riktlinjer för utkontraktering*[12] har gällt sedan den 30 september 2019. Utkontraktering gjord tidigare än så ska granskas och avtal eventuellt omförhandlas. Om detta inte är färdigställt ska verksamheten anmäla situationen till Finansinspektionen och beskriva vilken åtgärdsplan de har för att uppfylla riktlinjerna. EBA har också krav på revisionsrätt men deras rekommendationer lämnar utrymme för alternativa sätt att utföra kontroller. Det kan till exempel vara tillräckligt med oberoende revisionsrapporter eller certifieringar från molntjänstleverantören.

Eiopa - Riktlinjer om uppdragsavtal med molntjänstleverantörer

I Eiopa:s *Riktlinjer om uppdragsavtal med molntjänstleverantörer*[13] finns råd och krav att utgå ifrån vid användning av en molntjänst. Syftet med dessa är att ge försäkrings- och återförsäkringsföretag vägledning för företagsstyrning vid användande av molntjänster.

Dokumentet omfattar 16 riktlinjer. Riktlinje 8 fokuserar på riskbedömning av uppdragsavtal om molntjänster. Här anges bland annat att den upphandlande organisationen bör tillämpa en strategi som är proportionerlig för riskerna med den outsourcade tjänsten och särskilt bedöma påverkan på operativa risker och ryktesrisker. Om den outsourcade verksamheten avser kritiska eller viktiga operativa funktioner bör fördelar och förväntande kostnader för molntjänsten beaktas och samtidigt överväga risker med att outsourca till en molntjänst respektive att inte göra det.

Esma – Riktlinjer för utkontraktering till molntjänstleverantörer

I Esma:s *Riktlinjer för utkontraktering till molntjänstleverantörer*[14] finns råd och krav att utgå ifrån vid användning av en molntjänst beskrivna i nio riktlinjer[15]. Syftet med riktlinjerna är att företag ska identifiera, hantera och övervaka de risker och utmaningar som uppstår i samband med uppdragsavtal om molntjänster. Vidare innebär riktlinjerna att det etableras konsekventa och ändamålsenliga tillsynsmetoder inom det europeiska systemet för finansiell tillsyn.

Nedan följer en sammanställning av riktlinjerna i Eiopa och Esma:s respektive regelverk, samt vilka riktlinjer som behandlar liknande områden.

---

[12] *EBA, Riktlinjer för utkontraktering (EBA/GL/2019/02)*

[13] *Eiopa, Riktlinjer om uppdragsavtal med molntjänstleverantörer (EIOPA-BoS-20-002)*

[14] *Esma, Riktlinjer för utkontraktering till molntjänstleverantörer*

[15] *Riktlinjerna gäller från den 1 januari 2022. Inom två månader efter att riktlinjerna har offentliggjorts ska behöriga myndigheter meddela Esma om att de följer riktlinjerna eller inte. Företagen är inte skyldiga att rapportera att de följer riktlinjerna.*

Eiopa	Esma
Riktlinje 1: Molntjänster och uppdragsavtal	
Riktlinje 2: Allmänna principer för styrning av uppdragsavtal om molntjänster	Riktlinje 1: Styrning, tillsyn och dokumentation
Riktlinje 5: Dokumentationskrav	
Riktlinje 3: Uppdatering av den skriftliga policyn om uppdragsavtal	
Riktlinje 4: Skriftligt meddelande till tillsynsmyndigheten	Riktlinje 8: Skriftlig anmälan till behöriga myndigheter
Riktlinje 6: Analys innan uppdragsavtal ingår	Riktlinje 2: Analys före utkontraktering och företagsutvärdering
Riktlinje 7: Bedömning av kritiska och viktiga operativa funktioner och verksamheter	
Riktlinje 8: Riskbedömning av uppdragsavtal om molntjänster	
Riktlinje 9: Företagsbesiktning av molntjänstleverantören	
Riktlinje 10: Avtalsenliga krav	Riktlinje 3: Viktiga delar av avtalet
Riktlinje 11: Åtkomst och revisionsrättigheter	Riktlinje 6: Åtkomst- och revisionsrättigheter
Riktlinje 12: Uppgifts- och systemsäkerhet	Riktlinje 4: Informationssäkerhet
Riktlinje 13: Underentreprenad för kritiska eller viktiga operativa funktioner eller verksamheter	Riktlinje 7: Underentreprenad
Riktlinje 14: Övervakning och tillsyn av överenskommelser om uppdragsavtal om molntjänster	Riktlinje 9: Tillsyn över utkontrakteringslösningar till molntjänster
Riktlinje 15: Rätt till uppsägning och utträdesstrategier	Riktlinje 5: Utträdesstrategier
Riktlinje 16: Tillsyn av överenskommelser om uppdragsavtal om molntjänster av tillsynsmyndigheter	

Digital Operational Resilience Act (Dora)

I EU-kommissionens förslag till förordning om digital operativ motståndskraft i den finansiella sektorn (Dora-förordningen[16]) finns förslag på bestämmelser om styrning, riskhantering, rapportering och testning. Med förordningen skapas en enhetlig reglering på EU-nivå med krav på hantering av IT-risker och cybersäkerhet som omfattar i princip all finansiell verksamhet. Genom förordningen ställs krav på styrning, organisation och innehåll beträffande hantering av operativ risk inom verksamheten. Vidare ställs krav på hantering och rapportering av IT-incidenter. Verksamheter ska genomföra tester av sin förmåga att hantera störningar och cyberangrepp och dessa tester ska vara mer avancerade för systemviktiga aktörer. Ytterligare en del av förordningen behandlar krav på riskhantering då tredjepartsleverantörer används i verksamheten, vilket avser företag av en viss storlek som är kritiska för finansiell sektor (t.ex. de stora molntjänstleverantörerna). Dora förväntas träda i kraft inom ett par år.

Artikel 25, 26 och 27 är särskilt intressanta för upphandling av molntjänster. Där framgår att finansiella sektorn är beroende av ITK-tjänster för att möta den globala konkurrensen (art 25) utifrån både affärseffektivitet och kundernas krav. I artikel 26 beskrivs hinder och utmaningar för den finansiella sektorn för att upprätta avtal som uppfyller de villkor som finansiella sektorn har. Exempel på krav är tillsyn, tillträdesrättigheter och revisionsrättigheter. Vidare belyses utmaningen med kontroll över eventuella underleverantörer, där det kan bli svårt att bedöma den risk det medför om man inte kan få tillräckliga garantier från molntjänstleverantören avseende dessa. I artikel 27 beskrivs utmaningen att övervaka avtal samt behovet av att definiera minimigarantier en leverantör ska avtala om, vilket skulle underlätta tillsyn och revisoner.

ISO27000-serien

Av Eiopa:s, Esma:s och Finansinspektionens föreskrifter framgår ett övergripande krav på att företagen i finansiell sektor har ett ledningssystem för informationssäkerhet. ISO27001 är en internationell standard som beskriver vilka mål ett ledningssystem för informationssäkerhet ska ha. ISO27002 beskriver generella säkerhetsåtgärder för att uppnå dessa mål och ISO27017 beskriver specifika säkerhetsåtgärder för molntjänster. Vid upphandling av molntjänster kan dessa standarder användas för att tydliggöra generella krav på molntjänstleverantörer och dess tjänster.
Övriga ISO-standarder som kan vara relevanta att studera är:

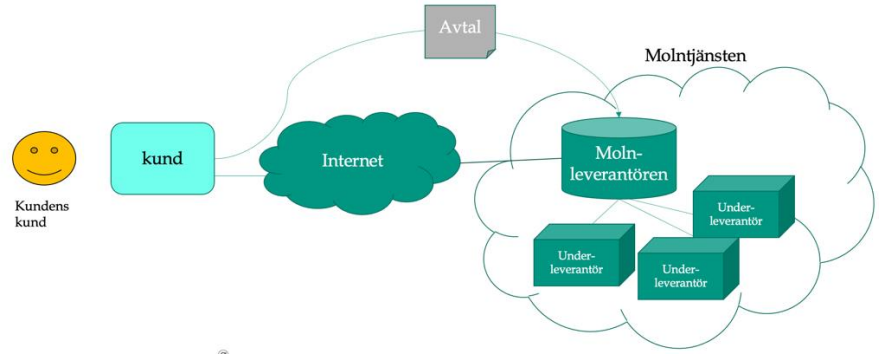
- ISO/IEC 27007: "Guidelines for information security management systems auditing"
- SIS-ISO/IEC TR 27008, "Vägledning för revisorer om informationssäkerhetsåtgärder" ger också vägledning för genomförandet av den oberoende granskningen.

---

[16] *Regeringskansliet Faktapromemoria 2020/21:FPM16 (förordning om digital operativ motståndskraft i den finansiella sektorn, Dora)*

Certifieringsramverk

Cybersecurity Act från EU-kommissionen, är en förordning för att säkerställa molnbaserade, digitala och uppkopplade produkter, processer, system och tjänster. Syftet med Cybersecurity Act är att bidra till en enhetlig säkerhetsnivå och standard i EU och innebär ett utökat mandat för Europeiska unionens cybersäkerhetsbyrå (ENISA). Cybersecurity Act har sedan den bildades 2017 haft i uppdrag att föreslå omfattning och nivå på ett gemensamt certifieringsramverk för molntjänstleverantörer. I likhet med övriga certifieringar under förordningen kommer molncertifieringen, åtminstone initialt, att vara frivillig både för företag inom och utanför EU. Certifieringen är aktuell för både leverantörer och kunder, och kan komma att bli en viktig del i kravställningar inom upphandling och inköp. Med hjälp av en cybersäkerhetscertifiering blir det lättare att köpa och sälja uppkopplade produkter och tjänster i hela Europa och målet med certifieringen är att den ska garantera regelefterlevnad och att *privacy by design* samt *privacy by default* tillämpas.



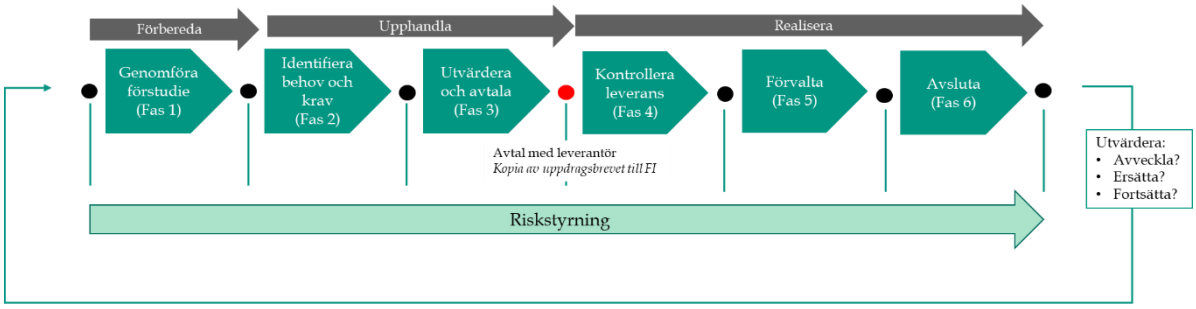
Figur 2 - Dora, art. 26, belyser att vikten av att säkerställa styrning och kontroll även för molntjänstleverantörernas underleverantörer. Riskprofilen höjs, och innebär ett komplext riskarbete.

4. Upphandla molntjänst

Upphandling av en molntjänst följer samma process som upphandling av andra IT-tjänster. Nedan illustreras de steg och faser som beskrivs i MSB:s vägledning ”Upphandla informationssäkert”[17]. Figuren har utvecklats mot finansiella sektorns perspektiv och har ett särskilt fokus på att upphandla molntjänster. Exempelvis inkluderar bilden att Finansinspektionen ska få en kopia på uppdragsbrevet när en organisation anlitar en molntjänstleverantör för en kritisk/viktig funktion.[18] I upphandlingsprocessen finns även moment för riskanalyser och bedömningar som behövs göras enligt de europeiska tillsynsmyndigheterna EBA, Eiopa och Esma.

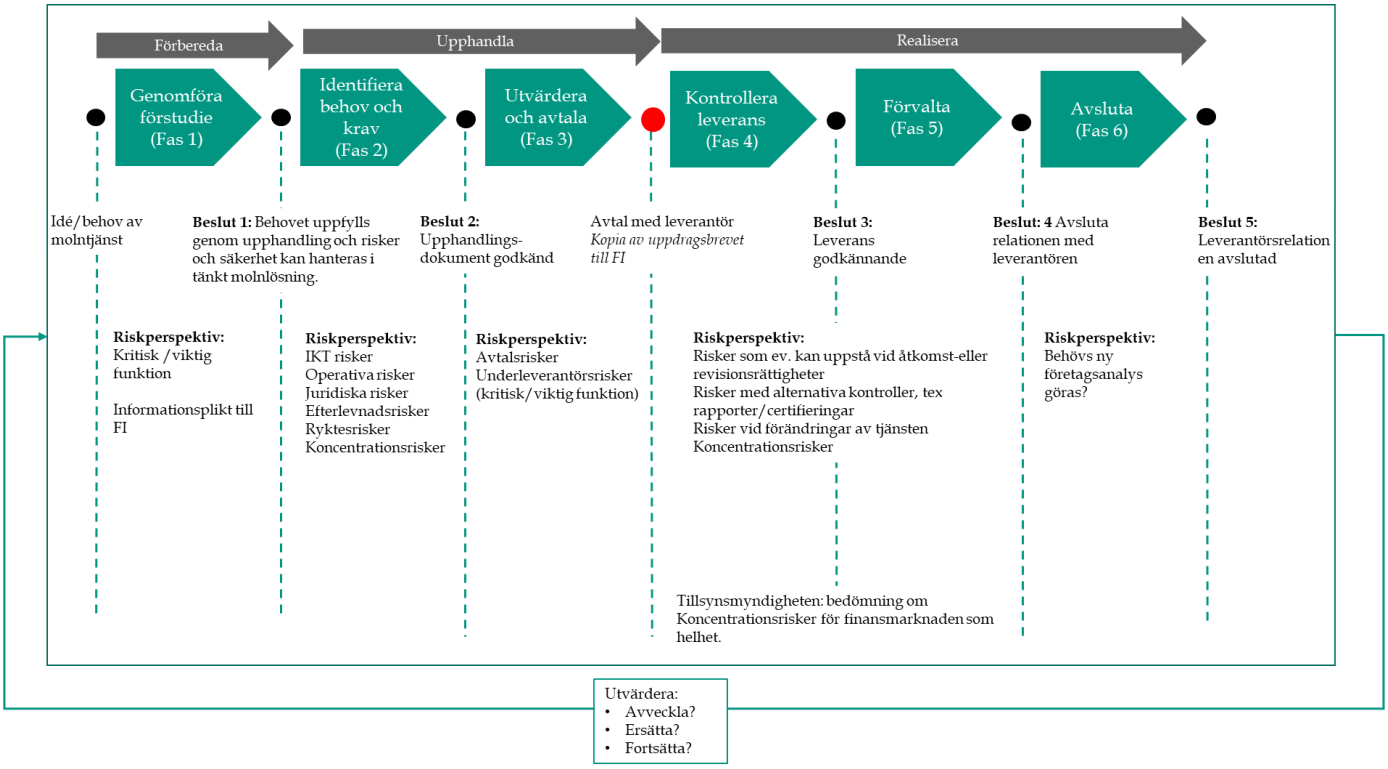
[17] MSB1177-november 2018

[18] Finansinspektionens syn på revisionsrätten för verksamhet som läggs ut på molntjänstleverantörer, FI Dnr 18-5393



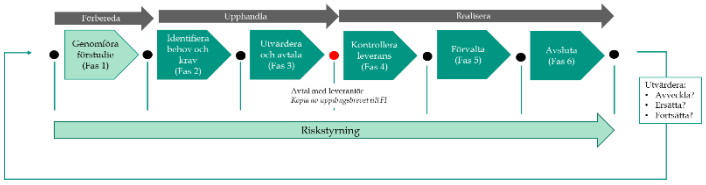
Figur 3 - Upphandlingsprocessens steg och faser.

Riskstyrning sker under tjänstens hela livscykel. Särskilt viktigt är det vid upphandling, i kravspecifikation och utformning av avtal (fas 2 och 3) samt vid realiserande av affären, att säkerställa att tjänsten och leverantören följer kraven (fas 4 och 5). Inför en upphandling ska organisationen gå igenom kraven och omvandla dessa till risker, d.v.s. vilka risker finns det om kraven inte uppfylls? På detta sätt upprättas en risklista vilken ligger till grund för framtagandet av åtgärdsplaner. Arbetet kan ses som en cirkulär process, där utvärdering är återkommande. I bilden nedan illustreras risker som behöver bedömas i respektive fas. Bilden synliggör att flertalet finns i fas 2-5, vilket pekar på vikten av att teckna bra avtal och följa upp dem.



Figur 4 – Översikt över upphandlingsprocessen och riskperspektiv i respektive fas.

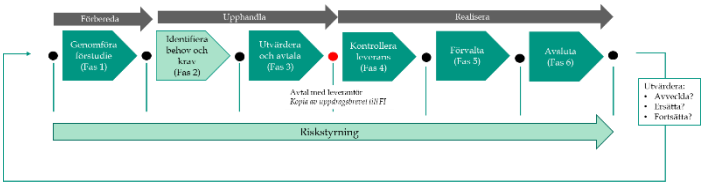
Fas 1: Genomföra förstudie (förbereda)



När verksamheten har identifierat ett idé eller behov av att anlita en molntjänstleverantör och vill realisera detta behövs vissa förberedelser. Förberedelsefasen kan exempelvis innebära att en verksamhetsanalys, informationsklassificering och laglighetsprövning görs. Utifrån dessa analyser kan beslut fattas om den tänkta molntjänsten uppfyller de initiala kraven, vilket i sin tur kan innebära att beslut om att avstå från en molntjänstlösning.

Detta PM fördjupar sig inte vidare i förberedelsefasen. I fortsättningen utgår dokumentet ifrån att molntjänsten ska hantera kritiska eller viktiga operativa funktioner för verksamheten. Om molntjänsten inte ska hantera kritiska eller viktiga funktioner ställs inte lika höga krav på analyser eller riskbedömningar.

Fas 2: Identifiera behov och krav



Upphandling av en molntjänstlösning för en kritisk eller viktig operativ funktion bör involvera flera specialister i organisationen. Verksamhetens behov driver ofta processen medan funktioner som exempelvis juridik, säkerhet och compliance är viktiga stödfunktioner som säkerställer att processen går rätt till och omfattar rätt bedömningar. Upphandlingen behöver också involvera experter inom IT, som exempelvis IT-ansvarig, informationssäkerhetsexpert, säkerhetsansvarig m.fl.

Figur 5 - Exempel på en upphandlingsorganisation

Inför upphandling av en molntjänst behöver behovet definieras och därefter behöver kraven tydliggöras. Medan ett behov av att använda en molntjänstleverantör kan identifieras redan i förstudien i fas 1, förvaltas behoven i fas 2 genom att formulera en kravspecifikation. Det är viktigt att tänka ur ett ”livcykelperspektiv” redan vid upphandlingen av en molntjänst, d.v.s. krav på en molntjänstleverantör, krav under tiden tjänsten levereras samt krav på hur tjänsten ska kunna förändras och avvecklas.

Risk- och säkerhetsbedömning
Det är viktigt att redan i detta steg genomföra risk- och säkerhetsanalyser för att utforma kravspecifikationen utifrån organisationens regelverk, förutsättningar och riskaptit. Riskanalyserna ska göras innan avtalet tecknas med molntjänstleverantören.

Vid all användning av digitala tjänster behöver en analys med risk- och konsekvensbedömning genomföras. Detsamma gäller vid upphandling och användande av en molntjänst. Det är viktigt att vara en aktiv kravställare och beställare och att vara medveten om vilka risker det innebär att lägga ut information till en extern part. Bland annat i MSBs vägledning beskrivs tillvägagångssätt för att genomföra verksamhetsanalyser eller klassning av information.

Specifika risker i denna fas finns beskrivna till exempel i Esma:s riktlinje 2, Eiopa:s riktlinje 8 samt Finansinspektionens FFFS 2014:4.

Krav på en molntjänstleverantör
En beställare av molntjänster behöver ställa motsvarande krav på en molntjänstleverantör, som på leverantörer av andra IT-tjänster.

Inför en upphandling behöver följande utredningar genomföras beträffande leverantören:

- Juridisk utredning, exempelvis en dataskyddsutredning för att säkerställa efterlevnad av GDPR.
- Molntjänstleverantörens lämplighet, avseende kompetenser, infrastruktur, ekonomisk situation, företags- och tillsynsstatus, bevis/certifieringar som exempelvis ISO27001, ISAE/SOC m.fl. Detta ger en bra bild av leverantören och dess arbete med exempelvis informationssäkerhet och interna revisionsrapporter, samt vilka referenser de har och fördelaktligen om dessa återfinns i den finansiella sektorn.
- I vilket land/vilka länder molntjänstleverantören är registrerad och därmed vilka lagar och regleringar som styr dess arbete.
- Namn på eventuella underleverantörer och i vilket/vilka länder dessa är registrerade.
- Om molntjänstleverantörens infrastruktur är lokaliserad i samma land eller i andra länder jämfört med eventuella underleverantörer samt var data/information fysiskt kommer att lagras.

- Vad som händer med data/information som har lagrats i molnet när kontraktet upphör eller om relationen måste avslutas på annat sätt.
- Obegränsad revisionsrätt, om tjänsten är kritisk.

En annan viktig aspekt är att avtala om regelbunden översyn av molntjänsten och leverantören för att säkerställa fortsatt kravuppfyllnad från leverantör och eventuella underleverantörer.

Utöver kraven på leverantören behöver även krav på själva tjänsten definieras. Exempelvis behöver det beskrivas vad som ska uppnås genom tjänsten, d.v.s. vad den ska bidra med samt tjänstens tillgänglighet och eventuella Service Level Agreements (SLA). Det är viktigt att vara tydlig med sina krav och vad som gäller för just den egna organisationen. Till exempel kan krav på lagring av data skilja sig åt mellan leverantörens kunder.

Informationssäkerhet
Informationsklassning bör göras i alla steg i upphandlingen men särskilt i detta steg för att därefter kunna formulera krav på leverantören. Medan man i den inledande fasen klassar tjänsten/funktionen som kritisk eller ej kritisk, klassificeras i detta steg den information som hanteras i tjänsten. God praxis är att klassa informationens konfidentialitet, riktighet och tillgänglighet.

Tänk på att information som berörs av säkerhetsskyddslagen och är säkerhetsskyddsklassificerad, inte ska hanteras i en molntjänst. Det är därför viktigt att ha värderat och klassificerat sin information inför driftsättningen av en molntjänst.

Organisationer som berörs av NIS-direktivet bör även beakta detta.

Det finns verktyg för att ta fram kravspecifikationer för informationssäkerhet. Sveriges kommuner och regioner (SKR) har tagit fram ett verktyg, KLASSA, som kan vara till hjälp för att ställa krav på en leverantör och dess tjänster.[19] KLASSA utgår från ISO27001 och kan automatiskt skapa en kravspecifikation utifrån den upphandlande organisationens svar i ett formulär. Kravspecifikationen kan därefter bifogas tillsammans med upphandlingsunderlaget alternativt som en avtalsbilaga.

Ett annat verktyg är Cloud security alliance (CSA), som också kan ta fram kravspecifikationer på molntjänster.[20] CSA har kravdokument, CCM v4, som innehåller 197 kontrollmål. Molntjänstleverantörerna kan själva göra egenkontroller mot detta, och publicera sitt resultat där.

---

[19] https://klassa-info.skl.se

[20] https://cloudsecurityalliance.org/star/registry/

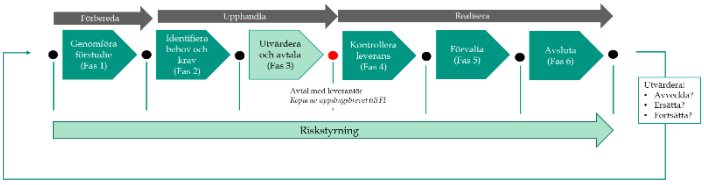
IT-säkerhet
IT-säkerhet handlar om att vidta tekniska åtgärder för att säkerställa och skydda information vid lagring, behandling/bearbetning och kommunikation/överföring. Vilka åtgärder som behöver genomföras beror många gånger på informationens klassificering.

Nedan beskrivs exempel på vilka it-säkerhetsområden som organisationen bör gå igenom i samband med att information ska läggas ut i en molntjänst, men även på annat sätt till en tredje part.

Område	Beskrivning
Applikations- och interfacesäkerhet	Avser bland annat att säkerställa att applikationer och API:er är designade och utvecklade i enlighet med branschstandard, exempelvis OWASP[21] för webbapplikationer. Det är också rutiner för in-och utdata, dokumenterade rutiner för ändringshantering, produktionssättning och testning.
Datasäkerhet och informationslivscykelhantering	Avser bland annat att produktionsdata inte ska användas utanför produktionsmiljöer samt att det finns dokumenterade processer och rutiner för att säkra att man destruerar och fullständigt ta bort data från lagringsmedier.
Datacentersäkerhet	Avser bland annat fysiskt skydd hos datacentret, att supportpersonal och användare ska ha restriktiv och bevakad fysisk åtkomst till information och funktioner och att tillåtelse måste erhållas skriftligen innan data, hårdvara och /eller mjukvara flyttas till en offsite-plats.
Kryptering och nyckelhantering	Avser bland annat säker hantering av nycklar exempelvis lagring, protokoll och algoritmer som används vid kryptering.
Identitets-och accesshantering (IAM)	Avser bland annat hantering av konton och behörigheter, åtkomstpolicies.
Infrastruktur och virtualiseringssäkerhet	Avser bland annat hantering av audit-och säkerhetsloggar, resurskapacitet, konfiguration av nätverk och virtuella instanser, härdning, separation av miljöer.
Interoperabilitet och portabilitet	Avser bland annat användning av öppna och publicerade API:er, användning av säkra och standardiserade nätverksprotokoll för import och export av data.
Säkerhetsincidenthantering	Avser bland annat rutiner vid en incident eller hur forensiskt arbete genomförs.
Kontinuitetshantering	Avser att berörda tjänster kan levereras utan störningar och avbrott och att konsekvenserna minimeras i händelse av att en incident skulle inträffa.

[21] *OWASP (The Open Web Application Security Project®)*

Fas 3: Utvärdera och avtala



I denna fas utvärderas inkomna offerter eller den tänkta lösningen och dess leverantör. Om en tydlig kravspecifikation har upprättats, och leverantörerna kan svara på dessa, kan ett beslut om vilken molntjänst och vilken leverantör som bäst uppfyller kraven fattas.
Ibland kan den upphandlande organisationen själv undersöka kravuppfyllnad hos en leverantör, genom inhämtning av information från öppna källor. Detta kan bli aktuellt om det är en väldigt stor leverantör, t.ex. Microsoft. *För kritisk/viktig information/funktioner måste anpassade avtal skrivas.*

I denna fas behöver man genomföra riskanalyser avseende avtalsrisker samt bedöma om det finns underleverantörsrisker och om underleverantören kommer hantera en kritisk/viktig funktion. Om underleverantören kommer att hantera en kritisk/viktig funktione är det dock viktigt att reglera bland annat vilka villkor som gäller för dessa samt om det finns eventuell verksamhet som inte får hanteras av underleverantören. Vidare villkor finns definierade av EBA, riktlinje 78.

Avtal med molntjänstleverantörer
EU-kommissionen genomför ett arbete för att ta fram standardklasuler för avtal med molntjänstleverantörer, vilka kan förväntas bli klara inom kort.[22]
Ett råd vid upprättande av avtal med en molntjänstleverantör, är att försöka använda standardvillkor. Om möjligt kan särskilda villkorstillägg för finansiell sektor efterfrågas, vilket kan visa om leverantören har gjort anpassningar och förstår beställarens verksamhetsförutsättningar.

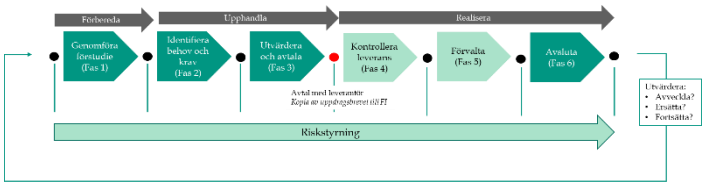
Inför avtalsskrivning om användning av molntjänst ska följande beaktas[23]:

- Tillgänglighet - kravställning om att informationen som finns i molntjänsten är tillgänglig när den behövs.
- Revisionsrätt - att det finns tillräckliga kontrollmöjligheter. Se mer om revisionsrätt i kommande avsnitt.
- Redan vid anskaffning av en tjänst hos extern part ska det säkerställas att det även finns förutsättningar att antingen kunna ta hem tjänsten igen eller kunna genomföra leverantörsbyte av tjänsten. I Esma:s riktlinje 5 finns krav på vad som behövs göras och hos Eiopa finns motsvarande i riktlinje 15. Avtalet med leverantören ska reglera hemtagning och avveckling av tjänsten och därmed hur

[22] *Standard Contractual Clauses for Cloud Services*
[23] *EBA:s riktlinjer innehåller också krav på att avtal om outsourcing för institut omfattar en tydlig hänvisning till den nationella resolutionsmyndighetens (Riksgäldens) befogenheter (riktlinje 75.o).*

informationen hanteras när tjänsten stängs eller när ett leverantörsbyte sker. Det är bra om exitstrategin kan testas så långt det är möjligt för att på detta sätt minimera risken att det blir problem längre fram.

Beroende på vilken typ av organisation beställaren är och vilken typ av utlagd verksamhet det är fråga om, ställs krav på att organisationen ska anmäla utläggningen samt skicka in en kopia på uppdragsbrevet till Finansinspektionen.



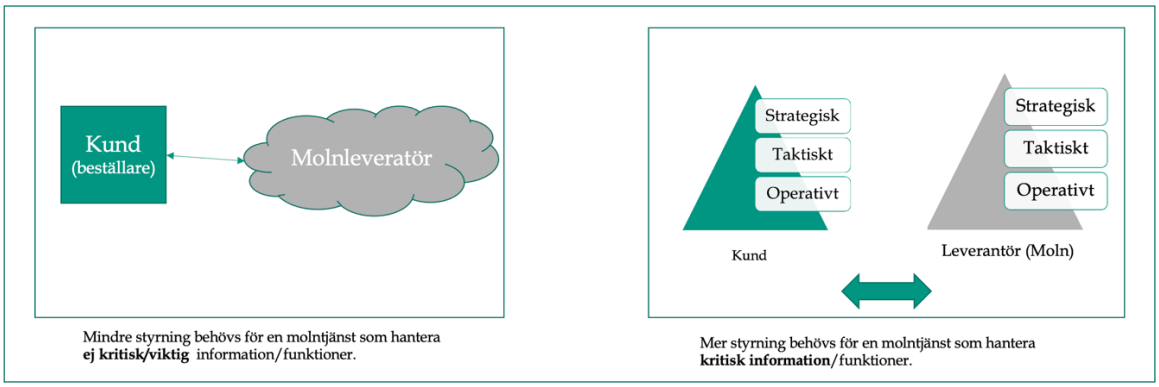
Fas 4 och fas 5: kontrollera leverans och förvalta

Detta avsnitt beskriver hur en beställare av molntjänster kan kontrollera att leverantören uppfyller de krav som ställts i avtalet. Som tidigare beskrivits är avtalet och avtalsvillkoren viktigast för att samverkan och arbetet med en molntjänstleverantör ska fungera bra. Allt som ska kunna kontrolleras och information som ska kunna efterfrågas av leverantören (t.ex. statistik eller möjlighet till att göra penetrationstester) är krav och villkor som måste finnas med redan i upphandling och därefter i avtal.

I avtalet bör det även framgå hur uppföljningen ska gå till. Alla krav som ställs i en upphandling och i ett avtal kan och bör kontrolleras för att kontinuerligt kontrollera leveransen av molntjänsten.

En vanlig modell för samverkan är att upprätta olika forum med en leverantör (strategiska, taktiska, operativa). Exempel på ämnen som löpande bör hanteras i leverantörsforum är uppföljning av fakturering, SLA:er, supportärenden, revisioner och byte av underleverantörer. Stora leverantörer har normalt bara tre månaders framförhållning för att meddela ändringar i tjänsten.

Med stora globala molntjänstleverantörer finns ofta begränsad möjlighet att få en önskvärd leverantörsstyrning. I dessa lägen blir beställaren informerad genom att automatiska rapporter skickas utifrån t.ex. servicenivåer eller kapcaitetsutnyttjande. Med en mindre molntjänstleverantör etablerad inom t.ex. Sverige, går det däremot ofta att bygga en nära relation där leverantörstyrningen liknar en traditionell IT-outsorcing. Det är viktigt att definiera en process som behöver tas fram är hur säkerhetsincidenthanteringen och rapportering av incidenter ska hanteras, vilket föreslås inkluderas i den kommande Dora-förordningen.



Figur 6 - En modell för leverantörsstyrning behövs även för en molntjänst. Vilken modell som behövs beror på vilken information en leverantör hanterar och hur kritisk informationen är.

Revision

För en kritisk tjänst ska det i avtalet finnas revisionsrätt, vilken inte får avtalas bort. Syftet med revisionen bygger på den riskanalys som beställaren gjort, se Eiopa riktlinje 16 och Esma riktlinje 6.

I Finansinspektionens promemoria om revisionsrätten,[24] framgår att de företag som vill använda sig av molntjänster måste säkerställa att företaget, dess revisorer och Finansinspektionen får tillgång till relevant information och lämpliga lokaler. För de fall ett avtal med begränsningar i revisionrätten ingås behöver en grundlig riskanalys göras. Vidare behöver beslutet kunna motiveras till Finansinspektionen. EBA:s riktlinjer säger dessutom att denna rätt inte får begränsas i en avtalstext.

En organisation kan välja att utföra revisioner i egen regi, genom en utsedd tredje part, sin egen internrevision eller externrevision eller möjligtvis tillsammans med andra. Vilket som passar bäst bestämmer organisationen i fråga själv, baserat på riskanalysen och med hänsyn till händelser som påverkar risker som hör samman med den utlagda verksamheten (molntjänsten).

Som tidigare nämnts får revisionsrätten inte avtalas bort. I de specifika fall där det uppstår en risk för molntjänstleverantörens andra kunder vid en begärd revision, ska molntjänstleverantören erbjuda andra möjligheter till beställaren för att få liknande försäkring. Exempel på andra möjligheter är att en gemensam revision sker genom molntjänstleverantörens försorg, genom att anlita en extern part som gör revisionen och att molntjänstleverantörernas kunder sedan får ta del av denna revision.

[24] *Finansinspektionens syn på revisionsrätten för verksamhet som läggs ut på molntjänstleverantörer, FI Dnr 18-5393*

När en revision ska genomföras är det viktigt att kvalitetssäkra den individ som utför revisionen. Idag finns det inga lagstadgade eller formella krav men det finns olika internationella certifieringar.

- CIA (Certified Internal Auditor)
- CISA (Certified information systems Auditor)
- CISM (Certified information Security Manager)
- CGEIT (Certified in the Governance of Enterprises IT)
- CRISC (Certified in Risk and Information Systems Control)
- CCSP (Certified Cloud Security Professional)
- CISSP (Certified Information Systems Security Professional)
- CCSK (Certificate of Cloud Security Knowledge)
- CCAK (Certificate of Cloud Auditing Knowledge)

Säkerhetsrevisioner kan utföras av revisionsbyråer, internrevisorer eller andra interna resurser, konsultbolag eller tillsammans med andra kunder. Det är även möjligt att molntjänstleverantören beställer en revision av en oberoende part och sedan delar dokumentationen med kunderna.

ISO27001 (avser informationssäkerhetsmål) och ISO27002 (riktlinjer för informationssäkerhetsåtgärder för att uppnå målen i ISO27001) kan användas i som utgångspunkt i revisioner. Efterlevnad av standarderna ställer som krav att leverantören har **kontroll på sina processer** och att det finns ett ledningssystem för informationssäkerhet (LIS). En molntjänstleverantör som är certifierad enligt dessa standarder genomför årligen återkommande revisioner för att upprätthålla certifieringen. Notera att det räcker inte med att en molntjänstleverantör visar upp ett certifikat. Certifikatet behöver granskas för att säkerställa att det uppvisade certifikatet gäller för den del som beställarens leverans utgår ifrån. Ett certifikat som exempelvis anger att en ISO27001-granskning är genomförd för molntjänstleverantörens datacenter på Irland, innebär inte per automatik att datacentret i Amsterdam är också certifierat (se Eiopa riktlinje 13).

Det finns två typer av certifieringar för leverantören: typ 1 avser om design av kontrollerna är bra, och typ 2 om kontrollerna är effektiva. För att revisorer ska kunna ta fram en rapport om typ 2, krävs återkommande revisioner för att säkerställa att kontrollerna verkligen är effektiva.

Ytterligare en standard för revision är (International Standard on Assurance Engagements (ISAE) nummer 3402 (Assurance reports on controls at a service organization)[25], utfärdad av International Auditing and Assurance Standard Board (IAASB). Detta är en europeisk standard. En annan standard värd att nämna i

[25] *ISAE, Assurance reports on controls at a service organization, 3402*

sammanhanget är amerikanska System and organization controls (SOC) som liknar ISAE och avser tredjepartsleverantörsgranskning.

Cloud Security Alliance (CSA)[26] är en ideell organisation som leds av en bred koalition av branschutövare, företag och andra viktiga intressenter. Organisationen är dedikerad till att definiera bästa praxis för att säkerställa en säkrare molnmiljö och för att hjälpa potentiella molnkunder att fatta välgrundade beslut när de flyttar sin IT-verksamhet till molnet. År 2013 lanserades Security, Trust & Assurance Registry (STAR) av CSA och British Standards Institution. Detta är ett gratis, offentligt tillgängligt register där molntjänstleverantörer kan publicera sina CSA-relaterade utvärderingar baserat på följande komponenter:

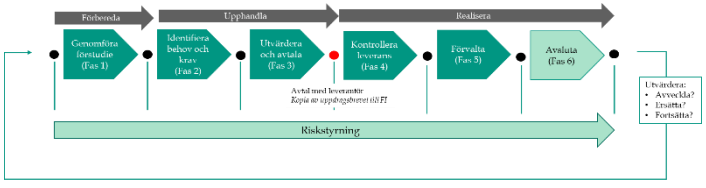
- Cloud Controls Matrix (CCM): ett kontrollramverk som består av 133 kontrollmål som täcker grundläggande säkerhetsprinciper på 16 domäner för att hjälpa molnkunder att bedöma den övergripande säkerhetsrisken för en CSP.
- Consensus Assessments Initiative Questionnaire (CAIQ): en uppsättning med över 300 frågor baserade på CCM som en kund eller molnrevisor kan vilja be CSP om för att bedöma om de följer CSA:s *best practise*.

För att säkerställa att molntjänsten levereras enligt avtal behöver regelbundna revisioner genomföras.

Frågor för beställare att beakta:

- Vilken insyn krävs? Kan vi verifiera eller släpper vi för mycket av kontrollen?
- I vilket syfte görs revisonen?
- Hur ofta får beställaren göra revision hos leverantören? Räcker en gång per år? Vad händer om det behövs fler, till exempel vid en incident?
- Hur fördelas kostnaden för revisionsarbete?
- Får/behöver/kan vi revidera på plats i leverantörens datacenter?

Fas 6: Avsluta



En molntjänst kan behöva avvecklas av olika anledningar. Det kan vara att tjänsten inte längre behövs, att tjänsten inte uppfyller de kvalitetskrav som ställts, att leverantören kommer anlita underleverantörer som inte bedöms uppfylla beställarens krav eller av andra anledningar. I avtalet ska det finnas beskrivningar över hur en molntjänst ska avvecklas (exitstrategi) och vilket stöd

[26] https://cloudsecurityalliance.org/star/registry/

leverantören ska erbjuda för att överföra informationen till annan leverantör eller att återgå till företaget. I avtalet ska det också finnas beskrivet vilka kriterier som kan initiera en avveckling, se Esma riktlinje 5.

5. Avslutning

För att effektivt kunna hantera de risker som användningen av molntjänster innebär krävs en omsorgsfull upphandlingsprocess. I ett tidigt skede behöver kravbilden konkretiseras avseende hur risker ska styras , mätas och följas upp. I detta dokument har vi gått igenom upphandlingsprocessen och beskrivit de regelverk som är särskilt viktiga för finansiella aktörer att förhålla sig till då molntjänster används, i synnerhet om detta omfattar verksamhet som identifieras som viktig eller kritisk enligt respektive rörelselagstiftning. På senare år har det kommit nya regler för utkontraktering till tredjeparter och vid användning av molntjänster. Området utvecklas snabbt, både när det gäller verktyg och metoder för riskhantering såväl som vid utformning av regelverken. Det kan konstateras att med EU-förordningen Digital Operationel Resilience Act , som förväntas träda i kraft inom några år, så kommer riskhantering inom detta område att fortsätta att utvecklas och ha ett stort fokus för alla aktörer som bedriver finansiell verksamhet.

6. Begrepp och definitioner

Begrepp och definitioner som används i detta dokument, där så är tillämpligt, är hämtade från SIS eller NIST.

Begrepp	Definition
Tredje land	Avser länder utanför EU.
Tredje partsrisker	Tredje partsrisker är de risker som ett företag exponeras mot eller kan exponeras mot som ett resultat av ett avtal med en annan part. (FI)
EBA	Europeiska bankmyndigheten (EBA), en tillsynsmyndighet
Eiopa	Europeiska försäkrings- och tjänstepensionsmyndigheten, en tillsynsmyndighet
Esma	Europeiska värdepappers-och marknadsmyndighet, en tillsynsmyndighet
GDPR	General Data Protection Regulation. Europeisk lag avseende hur hantering av personuppgifter
IaaS	Infrastructure-as-a-Service (infrastruktur som tjänst)
Molntjänst	Ett koncept som möjliggör nätverksåtkomst till en storleksmässigt flexibel pool av delade fysiska eller virtuella resurser som via självbetjäning administreras och levereras.
NIST	National Institute of Standard and Technology
PaaS	Platform-as-a-Service (plattform som tjänst)
SaaS	*Software-as-a-Service* (mjukvara/program som tjänst)
SIS	Svenska Institutet för Standarder
SLA	Service level agreement (tillgänglighet på en tjänst)
Säkerhetsstandarder	SOC 1, SSAE 16/ISAE 3402, SOC 2, SOC 3, ISO 27001; ”Cloud Code of Conduct”