TRAFICOM

Transport- och kommunikationsverket
Cybersäkerhetscentret

Säkerhetskriterier för molntjänster (PiTuKri)

Traficom publikationer 21/2021
PiTuKri – version 1.1 – mars 2020

Innehåll

Transport- och kommunikationsverket Traficom
Cybersäkerhetscentret
ISBN 978-952-311-757-0
21/2021
ISSN 2669-8757

Inledning

Syftet med säkerhetskriterierna för molntjänster (förkortas ibland PiTuKri, en förkortning av finskans Pilvipalveluiden turvallisuuden arviointikriteeristö) är att förbättra säkerheten för sekretessbelagd myndighetsinformation som behandlas i molntjänster. Kriterierna är ett bedömningsverktyg som hjälper avgöra hur säker en molntjänst är. Kriterierna har framtagits utgående från Finlands nationella behov. De pågående lagreformerna har beaktats, vilket innebär att kriterierna är kompatibla med den nya lagstiftningen som trätt i kraft i början av 2020 [1] [2]. Arbetet med kriterierna har till största del byggt på BSI-kriterierna för molnsäkerhet [3], skyddsmatrisen framtagen av CSA – en organisation för som arbetar för att stärka molnsäkerhet [4], standarderna ISO27001 [5] och ISO27017 [6] samt kriterieuppsättningen Katakri [7]. Kriterierna är också avsedda att fungera som stöd och en konkret referensram då finansministeriets riktlinjer för den offentliga förvaltningens molntjänster [8] införs.

Kriterierna omfattar både myndigheters nationella sekretessbelagda information och sekretessbelagd information som tilldelats säkerhetsklass IV. Kriterierna tangerar [9] också de allmänna principerna för skydd av säkerhetsklassificerad information på den internationella RESTRICTED-nivån. Säkerhetskraven har dimensionerats med målet att de mest typiska riskerna för sekretessbelagd information ska hållas på tolerabel nivå. Säkerhetsarrangemangen för högre säkerhetsklasser omfattas endast i fråga om en allmän lämplighetsbedömning för molntjänster. Kriterierna kan användas bl.a. av myndigheter för att skydda offentlig information och av näringslivet.

I uppdateringsversion 1.1 för kriterierna preciseras de begrepp och användningsfall som beskrivs i den första versionen [10], kompletteras tillämpningsmöjligheterna samt introduceras andra ändringar som önskats i responsen till exempel beträffande kravindelningen. Cybersäkerhetscentret fortsätter att utveckla kriterierna. Cybersäkerhetscentret samlar in respons och önskemål om fortsatt utveckling [11], vilka kommer att beaktas i de uppdaterade versionerna av kriterierna. För att underlätta tillämpningen av kriterierna kommer det även att publiceras stödverktyg och dokument med kompletterande information.

[1] Lagen om informationshantering inom den offentliga förvaltningen (906 / 2019). URL: https://www.finlex.fi/sv/laki/alkup/2019/20190906.

[2] Statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019). URL: https://www.finlex.fi/sv/laki/alkup/2019/20191101.

[3] Bundesamt für Sicherheit in der Informationstechnik. 2017. Cloud Computing Compliance Controls Catalogue (C5) - Criteria to assess the information security of cloud services. URL: https://www.bsi.bund.de/EN/C5.

[4] Cloud Security Alliance. 2018. The Cloud Security Alliance Cloud Controls Matrix (CCM). URL: https://cloudsecurityalliance.org/working-groups/cloud-controls-matrix.

[5] ISO/IEC 27001:2013 — Information technology — Security techniques — Information security management systems — Requirements.

[6] ISO/IEC 27017:2015 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.

[7] Försvarsministeriet. 2015. Katakri 2015 – Tietoturvallisuuden auditointityökalu viranomaisille. URL: http://www.defmin.fi/Katakri.

[8] Finansministeriet. 2019. Riktlinjer för den offentliga förvaltningens molntjänster. URL: http://urn.fi/URN:ISBN:978-952-251-982-5

[9] Internationell säkerhetsklassificerad information omfattas av krav på skydd som varierar beroende på uppgiftens originator och ägare och kan ställvis skilja sig avsevärt från nationella motsvarigheter. Mer information: ncsa (at) traficom (punkt) fi.

[10] Cybersäkerhetscentret. 2019. Säkerhetskriterier för molntjänster – v1.0. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri.pdf.

[11] Återkoppling och förslag till utveckling: ncsa (at) traficom (punkt) fi.

Användning

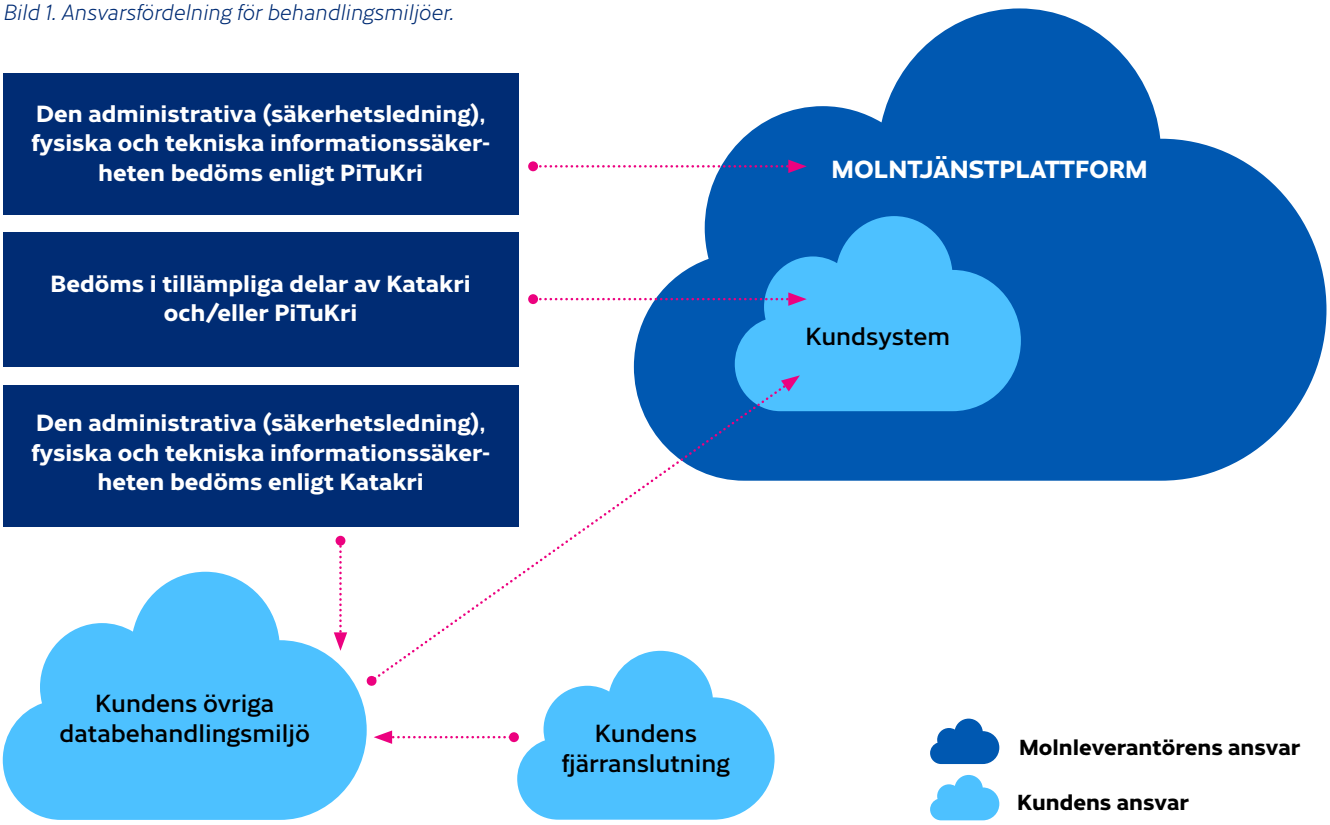
Användningsfall

Kriterierna är avsedda att användas vid bedömning av hur säkra olika molntjänster är. Även molntjänstleverantörer kan använda dem som ett stöd i sitt säkerhetsarbete. Kriterierna tar hänsyn till olika slags molntjänster och användningsfall. För att kriterierna ska fylla sitt syfte är det viktigt att man tillämpar dem enligt användningsfallet i fråga.

I de flesta användningsfall är det antingen molnleverantören eller kunden som har ansvar för bedömningen av skyddet av den information som behandlas i molntjänsterna [12]. Till kundens ansvar hör vanligen både kundsystemet och andra informationsbehandlingsmiljöer som hänför sig till kunden. Ansvarsfördelningen för behandlingsmiljöerna visas i bild 1. För bedömning av de delar som kunden har ansvar för kan också till exempel referensramen Katakri 2015 användas.

I de flesta användningsfallen är det motiverat att tillämpa de beskrivna kraven endast på det som molntjänstaktören ansvarar för, i vissa andra fall gäller de både molntjänstaktörens och kundens respektive ansvar och i vissa fall kan de endast tillämpas på det som kunden ansvarar för. Beträffande vissa typer av skydd kan det vara motiverat att utnyttja funktionerna både i kundsystemet, som kunden ansvarar för, och i molnplattformen, som molnleverantören ansvarar för. Den som utför säkerhetsbedömningen, den som tillhandahåller molntjänsten och kunden måste alla vara tillräckligt insatta i ämnet för att kriterierna ska fylla sin funktion. Exempel på hur kriterierna fördelas enligt ansvarsområde finns i bilaga 1.

Bild 1. Ansvarsfördelning för behandlingsmiljöer.



[12] Det är typiskt att eventuella externa aktörers skydd i anslutning till molnleverantörens eller kundens ansvarsområden omfattas av bedömningen av ansvarsområdet i fråga. Till exempel i en situation där programvaruutvecklingen i ett kundsystem, som kunden har ansvar för, har lagts ut på en tredje part ligger ansvaret för den tredje partens säkerhet hos kunden.

Bedömningsmetoder

Det finns olika metoder man kan använda för att bedöma molntjänsters säkerhet. För vissa typer av data kan skyddet till exempel gott och väl bedömas baserat på den självkontroll som molnleverantören använder samt på eventuella andra certifieringar och avtalsförpliktelser. För vissa typer av data bör man dessutom kräva att skyddet kontrolleras av en utomstående och oberoende aktör. Hur tillförlitliga resultaten av kontrollen är beror i hög grad på hur tillförlitliga kontrollmetoderna är. Det är till exempel inte samma sak att man enbart läser igenom dokumentationen som att skyddet dessutom kontrolleras genom tekniska test. Det är ofta möjligt att få kompletterande data för kontrollen, till exempel från löpande auditering. För vissa data bör helst den nationella informationssäkerhetsmyndighetens bedömningstjänst användas [13]. Mer information om utmaningarna med bedömning av molntjänster samt några förslag på lösningar finns bl.a. i publikationerna inom projektet EU-SEC [14].

Med vissa förbehåll kan även andra ramverk och certifieringar användas för att påvisa överensstämmelse med säkerhetskriterierna (PiTuKri). Då är det särskilt viktigt att komma ihåg att olika ramverk och certifieringar mäter olika saker. I vissa ramverk kan till exempel administrationssystemet för informationssäkerhet certifieras på grundval av organisationens riskhanteringsbeslut, enligt vilka de tekniska skyddsåtgärdernas tillräcklighet bedöms. Denna princip avviker bland annat från den ofta förekommande modellen för skydd av säkerhetsklassificerad information, där originatorn och/eller ägaren definierar minimikraven för skyddet och dessa följer med informationen under hela dess livscykel, i alla behandlingsmiljöer och -sammanhang. En annan rekommendation då man bedömer olika certifieringar är att dessa kan vara begränsade till att omfatta endast en del av processerna eller -miljöerna där sekretessbelagd information behandlas, att olika ramverk och krav har olika tillförlitlighetsmål för skyddet och att det även förekommer variationer i hur tillförlitligt det går att kontrollera att kraven uppfylls. Certifieringar som gjorts mot andra referensramar kan utnyttjas i bedömningarna, men som sådana utgör de inte underlag för att till exempel Cybersäkerhetscentret ska kunna bevilja godkännande [15].

[13] Cybersäkerhetscentret. 2019. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf

[14] The European Security Certification Framework (EU-SEC). 2019. URL: https://www.sec-cert.eu/.

[15] Processen för godkännande inom Cybersäkerhetscentrets NCSA-funktion beskrivs mer detaljerat i bilaga 3.

Riskanalys

Varje myndighet har ansvaret för att informationsbehandlingen på myndigheten är tillräckligt säker. Myndigheter har i sista hand själva ansvaret för att en tillräckligt omfattande och tillförlitlig bedömning ordnas för varje användningsfall och för att gjorda observationer behandlas ur ett riskperspektiv. I användningsfall där tjänsten tillhandahålls flera myndigheter inom statsförvaltningen via en centraliserad serviceproducent rekommenderas att bedömningarna och utvärderingsobservationerna utnyttjas så att överlappande bedömningar undviks. I sådana användningsfall ska man särskilt beakta att restriskerna ska godkännas av alla myndigheter som använder tjänsten.

För att säkerhetskriterierna (PiTuKri) ska fylla sin funktion krävs att kraven tolkas mot bakgrund av respektive användningsfall. Kraven kan eventuellt ersättas med andra skyddsåtgärder av motsvarande säkerhetsgrad. Kraven och genomförandeexemplen definierar inte vad som utgör ett tillräckligt skydd för alla miljöer eller specialfall.

Det är till exempel möjligt att inrätta tjänster på en molnplattform som det till avsevärda delar ligger på kundens ansvar att skydda. Tillgången till tjänster är dessutom beroende av flera olika faktorer, och det räcker med att en av dem fallerar för att hela tjänsten ska bli otillgänglig. Till exempel kan tillgänglighetsproblem i plattformslagret göra att applikationslagret inte kan tillhandahålla tjänster. På motsvarande sätt kan problem i applikationslagret göra servicen otillgänglig även om plattformslagret har genomförts så att det stöder en hög tillgänglighet. Tillgång till tjänsten kan också förhindras på grund av problem i kundens terminal eller i dataanslutningen mellan terminalen och molntjänsten. Alla de krav som beskrivs i kriterierna är å andra sidan inte direkt tillämpliga på alla användningsfall utan måste bedömas fall för fall. Vissa skyddsåtgärder kan behövas i molnplattformen, andra endast i kundsystemet. För vissa skyddsåtgärder är det motiverat att kombinera molnplattformens och kundsystemets funktioner.

Kriterierna kan också användas för att bedöma om myndigheternas sekretessbelagda information är förenlig med kraven. I bilaga 2 finns exempel på hur kriterierna kan tillämpas på bedömning av skyddet av sekretessbelagd respektive säkerhetsklassificerad sekretessbelagd information.

I användningsfall där målet är att inhämta den behöriga myndighetens godkännande15 för en molnplattform eller ett kundsystem förankrat i plattformen måste skyddet vara tillräckligt med hänsyn till både målorganisationens och den behöriga myndighetens riskobservationer. I synnerhet i situationer där något ersättande tillvägagångssätt används istället för skydd enligt kriterierna måste målorganisationen kunna bevisa att den skyddande effekten är tillräcklig.

Struktur

Kriterierna för säkerhetsbedömning av molntjänster omfattar 11 delområden. Delområde 1, ramvillkoren, är av särskild betydelse. Ramvillkoren avgör möjligheten för vidare bedömning och är viktiga för riskhanteringsarbetet hos de myndigheter som ansvarar för säkerheten för sekretessbelagd information. För viss sekretessbelagd information är det motiverat att till exempel en offentlig, internationell molntjänst genomgår ytterligare bedömning. För viss information kan möjligheterna till vidare riskbaserad bedömning gälla endast nationella privata molntjänster. I den fortsatta bedömningen ska man beakta att förhandsvillkoren endast omfattar en del av de allmänna riskerna. Att förhandsvillkoren uppfylls garanterar alltså inte att informationen är tillräckligt säker, utan man ska dessutom beakta skyddet i de övriga delområdena.

Delområdena består av kravkort. Varje kravkort innehåller temat för kravet, det konkreta kravet, tillämpningsobjekten, målet för skyddet och information avsedd som stöd för genomförande och tolkning. Kraven har beskrivits så att de så långt som möjligt tillåter olika genomförandealternativ. En del av kraven gäller sekretessbelagd information., en del endast säkerhetsklassificerad sekretessbelagd information. Det beskrivs i samband med respektive krav vilken typ av information kravet gäller.

Datatyper

Olika datatyper har olika risker. Till exempel kan man generellt anse att säkerhetsklassificerad myndighetsinformation ska skyddas med den nationella säkerheten (det allmänna bästa) i åtanke. Man kan dessutom anta att säkerhetsklassificerad information intresserar andra aktörer än till exempel personuppgifter, som inte omfattas av någon säkerhetsklass. Datatyperna är indelade i olika kategorier enligt skyddsklass så som visas i tabell 1.

Tabell 1. Datatyper.

Dadatyp	Beskrivning
Offentlig	Offentlig information. Skyddsbehov typiskt ur integritets- och tillgänglighetssynvinkel.
Sekretessbelagd	Nationell sekretessbelagd myndighetsinformation, som inte har tilldelats någon säkerhetsklass. Sekretessbelagd myndighetsinformation innehåller i de flesta fall personuppgifter och omfattas då även av speciallagstiftning om skydd av personuppgifter, jfr. datatypen "Personuppgift".
Personuppgift	Speciallagstiftning om skydd av personuppgifter (inkl. dataskyddslagen [16], lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten [17], samt information som omfattas av EU:s allmänna dataskyddsförordning [18].
Information som ska skyddas med tanke på beredskapen	Det finns ett behov att ha informationen tillgänglig även i exceptionella förhållanden (beredskap). Med exceptionella förhållanden avses här en situation där nätverksförbindelserna i samhället har begränsats geografiskt så att de endast fungerar inom Finlands gränser.
SK IV	Nationell sekretessbelagd myndighetsinformation som hör till säkerhetsklass IV. Skyddsbehovet bedöms i allmänhet ur ett nationellt säkerhetsperspektiv (det allmänna bästa). I skyddet ska även lagstiftningsrelaterade risker beaktas [19].
Internationell RESTRICTED (KV-R)	RESTRICTED och annat internationellt informationsmaterial som omfattas av särskild säkerhetsklassificering på motsvarande nivå. Till exempel omfattar bilaterala och multilaterala avtal med främmande stater och internationella organisationer [20] information på RESTRICTED-nivå. Skyddsbehovet bedöms i allmänhet ur en eller flera staters säkerhetsperspektiv (det allmänna bästa). I skyddet ska lagstiftningsrelaterade risker samt de särskilda krav som originatorn och/eller ägaren ställer på informationen i fråga beaktas [21].
En stor mängd sekretessbelagd information och/eller personuppgifter (SK IV- eller SK III-datamassa)	Situationer där masseffekten bedöms [22] ge upphov till en informationsmängd av säkerhetsklass IV eller III. Till exempel kan en del av affärshemligheterna hos företag som deltar i upprätthållandet av kritisk infrastruktur i Finland vara sekretessbelagda som enskilda uppgifter [23], men i form av en datamassa som täcker försörjningsberedskapskritiska helheter bestående av flera företag också säkerhetsklassificerad [24] sekretessbelagd information av klass III.
Stor mängd SK IV-information (SK IV-datamassa)	Situationer där masseffekten bedöms ge upphov till en informationsmängd av säkerhetsklass III. Till exempel ett gemenskapsmoln riktat till statsförvaltningen som samlar en betydande mängd information av säkerhetsklass IV från flera myndigheter också så att en informationsmängd av säkerhetsklass III kan bildas genom att förena informationen.

Indelningen i tabell 1 omfattar inte alla användningsfall på myndigheter. Olika myndigheter har till exempel olika behov i fråga om beredskap, och den visade indelningen tar endast delvis hänsyn till detta. I bedömningen bör man också beakta att en stor mängd sekretessbelagd information inte alltid leder till masseffekt och till att grunderna för säkerhetsklassificering [25] uppfylls. För att kriterierna för bedömning av molntjänsters säkerhet ska fylla sin funktion måste man identifiera vilka datatyper som behandlas och analysera riskerna kopplade till respektive användningsfall [26]. Förhållandet mellan datatyperna illustreras i bild 2.

[16] Dataskyddslag (1050/2018) URL: https://www.finlex.fi/sv/laki/alkup/2018/20181050.

[17] Lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018). URL: https://www.finlex.fi/sv/laki/alkup/2018/20181054.

[18] Europaparlamentets och rådets förordning (EU) 2016/679. 2016. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[19] Med lagstiftningsrelaterade risker avses att lagstiftningen i olika länder ger möjlighet att ålägga molnleverantörer att samarbeta med landets myndigheter och till exempel ge dem direkt eller indirekt tillgång till sekretessbelagda kunddata i molnet. De lagstiftningsrelaterade riskerna kan omfatta både den sekretessbelagda informationens fysiska förvaringsplats och bl.a. det att information överlåts från ett annat land via fjärråtkomst. I många länder har den lagstiftningsrelaterade möjligheten att få och undersöka information begränsats till att gälla endast polis och underrättelsemyndigheter.

[20] Mer information om internationella avtal finns på utrikesministeriets webbplats: https://um.fi/kahdenvaliset-ja-monivaliset-sopimukset.

[21] Typiskt specialkrav är skyldigheten att godkänna alla behandlingsmiljöer för säkerhetsklassificerad information hos den nationella myndigheten för godkännande av säkerhetsarrangemang (SAA, Security Accreditation Authority, i Finland Transport- och kommunikationsverkets NCSA-funktion).

[22] Bedömningen förutsätter att det nuvarande och det antagna informationsinnehållet i massan utreds, och en bedömning av om informationsmängden enligt 24 § 1 mom. 2, 5 eller 7–11 punkten i offentlighetslagen (1999/621) ska klassificeras till exempel enligt säkerhetsklass III.

[23] Sekretessgrunden är vanligen 24 § 1 mom. 20 punkten i offentlighetslagen (1999/621).

[24] Grunden för sekretess och säkerhetsklassificering kan i vissa fall vara till exempel 24 § 1 mom. 7, 8, 10 punkten i offentlighetslagen (1999/621).

[25] Enligt lagen om informationshantering inom den offentliga förvaltningen (906/2019) ska en anteckning om säkerhetsklass göras, om handlingen eller den information som ingår i den är sekretessbelagd med stöd av 24 § 1 mom. 2, 5 eller 7-11 punkten i lagen om offentlighet i myndigheternas verksamhet (1999/621) och obehörigt avslöjande eller obehörig användning av den information som ingår i handlingen kan orsaka skada för försvaret, beredskapen inför undantagsförhållanden, de internationella relationerna, bekämpningen av brott, den allmänna säkerheten eller stats- eller nationalekonomin, eller på något annat motsvarande sätt för Finlands säkerhet.

[26] Cybersäkerhetscentret stöder myndigheternas riskhanteringsarbete bland annat via NCSA-funktionens utvärderings- och godkännandetjänster samt rådgivningstjänsten för informationssäkerhet. Mer information: https://www.kyberturvallisuuskeskus.fi/sv/vara-tjanster/bedomning-godkannande-och-radgivning

Bild 2. Datatyper.

Särdrag hos molntjänster

Beskrivningarna i detta avsnitt bygger på de begrepp som används av NIST [27] och av Finansministeriet i riktlinjerna för den offentliga förvaltningens molntjänster. Begreppen har preciserats ur säkerhetssynvinkel och behandlas i en kontext av riskanalys av molntjänster.

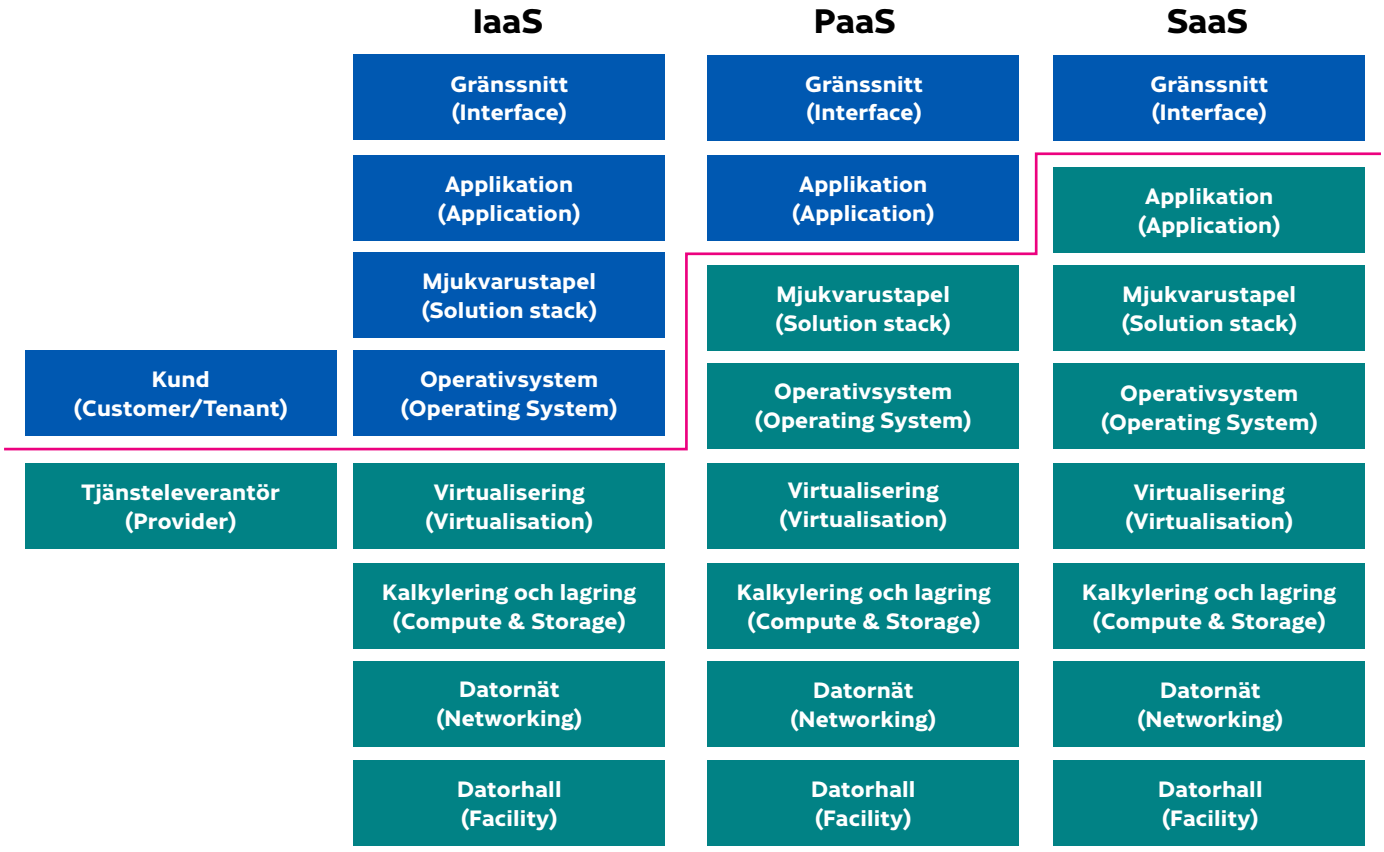
Med molntjänster avses databehandlingskapacitet eller -tjänster som är tillgängliga via webben, som produceras enligt en modell med gemensamma, skalbara och flexibla resurser och som är automatiserade till att delvis fungera via självbetjäning.

Leveransformer för molntjänster

De vanligaste leveransformerna för molntjänster är infrastruktur som tjänst (Infrastructure as a Service, IaaS), plattform som tjänst (Platform as a Service, PaaS) och mjukvara som tjänst (Software as a Service, SaaS). IaaS innebär att man köper all den infrastruktur man behöver av leverantören för att producera tjänster. PaaS innebär att man får en färdig serviceplattform som man kan producera tjänster från. SaaS innebär att leverantören producerar tjänsterna från början till slut.

I alla modeller är ansvaret för säkerheten fördelat på både leverantör och kund. Hur det är fördelat beror på leveransformen och på detaljerna i den konkreta tjänsteleveransen. Till exempel kan ansvarsfördelningen i PaaS till vissa delar skilja sig avsevärt mellan olika molnleverantörer. En typisk ansvarsfördelning visas i bild 3. Exempel på hur kriterierna fördelas per ansvar finns också i bilaga 1.

Bild 3. Typisk ansvarsfördelning.



[27] National Institute of Standards and Technology (NIST). 2011. Special Publication 800-145: The NIST Definition of Cloud Computing. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Distributionsmetoder för molntjänster

De vanligaste distributionsmetoderna för molntjänster är privat moln (private cloud), hybridmoln (hybrid cloud) och offentligt moln (public cloud). Andra distributionsmetoder, till exempel gemensamma moln med många olika aktörer (community/government cloud) kan oftast bedömas med de vanligaste distributionsmetoderna som utgångspunkt.

Privat moln avser en tjänst som produceras enbart för den organisation som använder tjänsten. Tjänsten kan tillhandahållas från leverantörens och/eller användarorganisationens datorhallar. Styrkan med ett privat moln är typiskt en tillförlitlig åtskillnad mellan molntjänstinfrastrukturen och den fysiska och logiska nivån hos den information som behandlas i den [28] från andra databehandlingsmiljöer, användarorganisationer och externa aktörer. Privata moln möjliggör typiskt tjänster med högre säkerhetskrav än andra distributionsmetoder.

Offentligt moln avser en tjänst som är allmänt tillgänglig och kan köpas av vem som helst. Tjänsten tillhandahålls så gott som alltid från leverantörens datorhallar. Offentliga moln har fler säkerhetshål, även kallat större angreppsyta eller sårbar yta, som är ett hot för molntjänstinfrastrukturen och informationen i den, än privata moln, på grund av att andra användare och externa aktörer har tillgång till dem.

Hybridmoln är en kombination av privat moln och offentligt moln. Ett hybridmoln kan till exempel fungera så att ett privat moln som körs i organisationens egen datorhall kompletteras med tjänster som köps från ett offentligt moln. Säkerhetsnivån är typiskt beroende av vilken information som kan överföras till det offentliga molnet och hur säkerheten har ordnats i gränsytan mellan det privata och det offentliga molnet.

[28] Man kan i allmänhet begränsa sårbarhetsberedskapen hos den infrastruktur för molntjänster som används för att tillhandahålla privata molntjänster (inkl. administrations- och övervakningslösningar) så att till exempel restriskerna i anslutning till programvarusårbarheter och felkonfigurationer är betydligt mindre än i molntjänstinfrastrukturen, som också används för att tillhandahålla offentliga molntjänster. Den interna åtskillnaden i molntjänstinfrastrukturen behandlas mer detaljerat på kravkortet JT-03.

Vem som levererar tjänsten

Molnleverantören har typiskt tillgång till all icke-krypterad information som behandlas i tjänsten. Olika molnleverantörer innebär olika risker. Molnleverantörer kan indelas i följande kategorier:

- Organisationen själv
- Nationell myndighet/nationell aktör
- Nationell privat aktör
- Internationell myndighet/internationell offentlig aktör (till exempel en grupp myndigheter i olika EU-länder)
- Icke-nationell privat aktör (EU eller EEG)
- Icke-nationell privat aktör (övriga länder)

Det viktiga ur säkerhetssynvinkel är hur man kan försäkra sig om att leverantören är kompetent och pålitlig. Om leverantören är inhemsk kan man till exempel utföra en nationell säkerhetsutredning av företag [29] för att utreda om leverantören är pålitlig. När flera organisationer [30] är med om att producera tjänsten måste en riskanalys utföras och tas i beaktande för varje medverkande organisation för sig.

Exempelvis dessa kan betraktas som nationella tjänsteleverantörer:

a) Ett företag som har beviljats ett nationellt företagssäkerhetsintyg (L 726/2014) enligt följande:

   - Företagets juridiska personer är finska medborgare som på ett tillförlitligt sätt kan administrera och ansvara för skyddet av säkerhetsklassificerad information både när det gäller administrativt, fysiskt och datatekniskt skydd.

   - Företagets verksamhet bedöms inte vara utsatt för risker som väsentligt påverkar tillförlitligheten, till exempel genom företagets ägarstruktur. (L 726/2014 37 §)

   - Andra än finska medborgare har inte tillgång till säkerhetsklassificerad information eller systemkomponenter som väsentligt påverkar skyddet av den. Till exempel har ett utländskt moder-/dotterbolag inte tillgång till säkerhetsklassificerad information eller systemkomponenter som väsentligt påverkar skyddet av informationen. Gränsfall, till exempel en situation där ett utländskt moder-/dotterbolag endast har tillgång till en begränsad övervakningsvy för vissa systemkomponenter, bedöms från fall till fall.

   - Säkerhetsklassificerad information finns under sin livscykel fysiskt inom Finlands geografiska gränser. Ett undantag är en situation där information i godkänd krypterad form överförs till exempel över internet.

b) En finsk myndighet. (Med tillämpning av motsvarande villkor.)

[29] Mer information om säkerhetsutredningen av företag: https://www.supo.fi/sakerhetsutredningarna/sakerhetsutredning_av_foretag

[30] Till exempel fall där A är leverantör för en molnplattform, B är kund och har inrättat ett kundsystem på plattformen och C är ett företag som administrerar och utvecklar applikationsfunktionen för kundsystemet.

Förvaringsplats för data och tjänster

Den information som behandlas eller förvaras i molntjänster samt underhållet och annan administration av molntjänsten kan vara belägna på olika håll geografiskt sett. Riskerna kopplade till det fysiska läget kan variera, till exempel beroende på vilken lagstiftning som gäller. Ur säkerhetssynvinkel kan fysiska platser kategoriseras enligt följande:

- Finland
- Platser som är möjliga enligt lagstiftningen om dataskydd, ofta till exempel EU eller EEG
- Övriga länder

Riskerna kopplade till den fysiska platsen kan också påverkas av avtal mellan länderna eller organisationerna. Tjänsten kan dessutom omfattas av andra säkerhetsrelaterade krav, till exempel i fråga om datasekretess eller beredskap, som kan sätta geografiska gränser för vilken molntjänst man kan välja. Då man bedömer riskerna i anslutning till placeringen, rekommenderas att man också beaktar att allmänna former av krypteringstekniskt skydd [31] för molntjänster inte ger något betydande tilläggsskydd mot lagstiftningsrelaterade risker. Det rekommenderas att man i bedömningen av möjligheterna, riskerna och kraven avseende placeringen också beaktar EU:s förordning om fri rörlighet för data (2018/1807 [32]), som dock inte tillämpas [33] på lokaliseringskrav som har sin grund till exempel i nationell säkerhet och beredskap.

[31] System baserade på egna nycklar dvs. BYOK (Bring Your Own Keys) eller på att utrustningen i molnleverantörens fysiska datorhall förses med särskilda säkerhetsmoduler (HSM, Hardware Security Module) är exempel på lösningar som begränsar molnleverantörens åtkomst till den information som behandlas i tjänsten, men de hindrar den inte i typiska fall. Jfr kravkort SA-03.

[32] Europaparlamentets och rådets förordning (EU) 2018/1807. 2018. URL: https://eur-lex.europa.eu/eli/reg/2018/1807/oj.

[33] Kommunikationsministeriets utredning om hinder för den fria rörligheten för annan information än personuppgifter i Finland (på finska). 2019. URL: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161774/LVM_11_19_Muiden%20kuin%20henkil%C3%B6tietojen%20vapaan%20liikkuvuuden%20esteist%C3%A4.pdf.

Delområde 1: Ramvillkor

EE-01	**Systembeskrivning**
Krav	1) Det finns en systembeskrivning för molntjänsten. Det ska gå att bedöma om molntjänsten är lämplig för kunden i användningsfallet i fråga baserat på systembeskrivningen. Systembeskrivningen ska innehålla åtminstone följande information: a) Molntjänstens service- och genomföringsmodeller samt därtill hörande servicenivåavtal (Service Level Agreements, SLAs). b) Vilka principer, rutiner och säkerhetsprocedurer, inbegripet övervakningsprocedurer, som styr molntjänstens livscykel (utveckling, användning, avveckling). c) En beskrivning av infrastrukturen, nätet och systemkomponenterna som används vid utveckling, underhåll/administration och användning av molntjänsten. d) Principer och rutiner för ändringshantering, med tonvikt på behandlingsprocesserna för ändringar med säkerhetsrelevans. e) Behandlingsprocesserna för avsevärda incidenter dvs. händelser som avviker från normal drift, till exempel omfattande systemfel. f) Roller och ansvarsfördelning mellan kunden och molnleverantören när det gäller leverans och användning av molntjänsten. Av beskrivningen ska tydligt framgå vilka åtgärder för att göra molntjänsten säker kunden ansvar för. Molnleverantörens ansvar ska omfatta skyldighet till samarbete i synnerhet när avvikelser utreds. g) Funktioner som överförts till eller lagts ut på entreprenad hos underleverantörer.
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Utifrån beskrivningen görs en allmän bedömning av tjänstens lämplighet och av riskerna med den i förhållande till kundens användningsfall.
Ytterligare information	Infrastruktur, nät och systemkomponenter ska beskrivas tillräckligt ingående så att man baserat på beskrivningen kan göra en allmän lämplighetsbedömning av tjänsten och en riskanalys med hänsyn till kundens användningsfall. Jfr KT-01 (Systembeskrivning till stöd för kontinuitet och driftssäkerhet). Infrastruktur kan med vissa förbehåll beskrivas med hjälp av den programkod som används för infrastrukturen i fråga. Exempel på leveransformer är infrastruktur som tjänst (Infrastructure as a Service, IaaS), plattform som tjänst (Platform as a Service, PaaS) och mjukvara som tjänst (Software as a Service, SaaS). Exempel på distributionsmetoder är privat moln (private cloud), hybridmoln (hybrid cloud) och offentligt moln (public cloud). Vissa molnleverantörer erbjuder kunder möjligheten att införa nya funktionaliteter redan i det skede då de förhandsvisas eller testas. Om man vill införa sådana funktionaliteter och använda dem för att behandla sekretessbelagd information bör man i riskanalysen bl.a. beakta vilka ansvar som gäller vid idriftsättningen. Nya funktionaliteter kan ha vissa olösta säkerhetsbrister och i avtalen läggs ansvaret för eventuella skador som sådana brister kan förorsaka på kunden.

EE-02	Lagstiftningsrelaterade risker
Krav	1) Det ska finnas en beskrivning av de lagstiftningsrelaterade riskerna och åliggandena. Det ska gå att bedöma om molntjänsten allmänt taget är lämplig för kundens användningsfall baserat på leverantörens beskrivningar. Beskrivningarna ska omfatta hela driftslivscykeln för tjänsten och livscykeln för den information som behandlas i tjänsten. Beskrivningarna ska innehålla åtminstone följande information: a) Den fysiska placeringen av den information som behandlas i tjänsten under informationens hela livscykel, inklusive eventuella underleverantörs-/utlokaliseringskedjor. b) Tjänstens olika funktioner (till exempel underhålls-/administrationslösningar, säkerheter) och komponenternas fysiska placering under informationens hela livscykel. c) Vilka andra som eventuellt medverkar i leveransen, till exempel underleverantörs-/utlokaliseringskedjor. d) Lagstiftning och forum i frågor som gäller drift av tjänsten och information som behandlas i den. e) Aktörer som på grund av tillämplig lagstiftning kan ha tillgång till informationen som behandlas i tjänsten. 2) Lagstiftningsrelaterade risker gör inte molntjänsten mindre lämplig för användningsfallet i fråga. 3) Kundens information finns under hela livscykeln endast på de fysiska platser som beskrivs i avtalet. Undantaget är en situation där kunden i förväg skriftligen har samtyckt till att information överförs eller behandlas på andra fysiska platser. 4) Molnleverantörens avtalsvillkor gör inte molntjänsten mindre lämplig för användningsfallet i fråga.
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Utifrån beskrivningen görs en allmän bedömning av tjänstens lämplighet och av riskerna med den i förhållande till kundens användningsfall.
Ytterligare information	Med lagstiftningsbaserade risker avses det att lagstiftningen i olika länder ger möjlighet att ålägga molnleverantörer att samarbeta med landets myndigheter och till exempel ge dem direkt eller indirekt tillgång till sekretessbelagda kunddata som finns i molnet. De lagstiftningsrelaterade riskerna kan omfatta både den sekretessbelagda informationens fysiska förvaringsplats och bl.a. det att information överlåts från ett annat land via fjärråtkomst. I många länder har den lagstiftningsbaserade möjligheten att få och undersöka information begränsats till att gälla endast polis och underrättelsemyndigheter. 1a) och 3) I fall där tjänsten är upplagd så att informationens fysiska plats kan variera ska alla potentiella fysiska platser där informationen kan befinna sig under sin livscykel beskrivas. 4) Det kan vara utmanande för en myndighet att till exempel uppfylla skyldigheten i 13 § i lagen om informationshantering (906/2019) att säkerställa informationssäkerheten i informationsmaterial och informationssystem under hela deras livscykel, om det är möjligt att ensidigt ändra avtalsvillkoren. Dataskyddsregleringen kan å andra sidan förhindra behandlingen av personuppgifter om molnleverantören inte kan erbjuda ett avtal i enlighet med dataskyddsbestämmelserna, som inte kan ändras ensidigt, dvs. utan kundens samtycke. Jfr TJ-07 (Överensstämmelse med krav och dataskydd). Vid bedömningen ska kraven i 28 artikeln 4 punkten i EU:s allmänna dataskyddsförordning samt i 17 § 2 mom. i dataskyddsagen avseende brottmål beaktas när så kallade underhanterare anlitas. Leverantören (den personuppgiftsansvariga) ska ingå ett skriftligt avtal med den instans som behandlar personuppgifter. Avtal och användarvillkor för molntjänster kan också omfatta olika sätt att definiera fysiska placeringsländer för tjänsten (eller en del av den). Överföring av personuppgifter utanför EU/EES ska alltid göras i enlighet med villkoren i EU:s allmänna dataskyddsförordning (V kap.) eller i dataskyddslagen avseende brottmål (7 kap.). Vid bedömningen rekommenderas de allmänna principerna för fortsatt bedömning i tabell 2.

Tabell 2. Möjligheter för fortsatt bedömning.

Datatyp	Typ av molntjänst	Fysisk plats	Tjänst-eleverantör	Mer information
Offentlig	Inga begräns-ningar	Inga begräns-ningar	Inga begräns-ningar	Då man bedömer vilket skydd som är lämpligt ska tonvikt läggas på tillräcklig integritet och tillgänglighet.
Sekretessbe-lagd	Inga begräns-ningar	Inga begräns-ningar	Inga begräns-ningar	Om inga personuppgifter ingår. Om personuppgifter ingår, jämför med raden "Personuppgift" nedan. Man bör också beakta att 13 § i lagen om informationshantering (906/2019) förutsätter identifiering av risker och dimen-sionering av skydd i enlighet med riskbedömningen. Re-sultaten av myndighetens riskbedömning kan förutsätta mer omfattande skydd eller begränsningar än vad PiTuKri omfattar.
Personupp-gift	Inga begräns-ningar	Områden som möj-liggörs av regleringen av dataskyd-det, ofta t.ex. Finland och/ eller EU/EES	Inga begräns-ningar, om inte be-gränsningar förutsätts utifrån riskbe-dömningen av person-uppgifterna i fråga	Servicehelheten ska uppfylla speciallagstiftningen om skydd av personuppgifter. Behandlingen av personuppgif-ter förutsätter en riskbedömning som görs utgående från uppgifternas karaktär, vilket kan leda till begränsningar även i fråga om den fysiska placeringen och administra-tionen av uppgifterna och valet av leverantör.
Information som ska skyddas med tanke på be-redskapen	Inga begräns-ningar	Finland	Nationell myndighet/ offentlig ak-tör/företag	Det finns ett behov att ha informationen tillgänglig även i exceptionella förhållanden (beredskap). Det ska vara möjligt att administrera informationen i en situation där nätverksförbindelserna i samhället har begränsats geografiskt så att de endast fungerar inom Finlands grän-ser. Tjänsteleverantörens tillförlitlighet kan utredas (till exempel som en del av en nationell säkerhetsbedömning av företag).
SK IV	Inga begräns-ningar	Finland	Nationell myndighet/ offentlig ak-tör/företag	Myndigheter i andra länder får inte ha direkt eller indirekt tillgång till informationen. Villkoret om fysisk förvarings-plats omfattar även administration, säkerhetskopiering och annat underhåll. Tjänsteleverantörens tillförlitlighet kan utredas (till exempel som en del av en nationell säkerhetsbedömning av företag).
En stor mängd sekre-tessbelagd information och/eller personupp-gifter (SK IV -datamassa)	Inga begräns-ningar	Finland	Nationell myndighet/ offentlig ak-tör/företag	Myndigheter i andra länder får inte ha direkt eller indirekt tillgång till informationen. Villkoret om fysisk förvarings-plats omfattar även administration, säkerhetskopiering och annat underhåll. Tjänsteleverantörens tillförlitlighet kan utredas (till exempel som en del av en nationell säkerhetsbedömning av företag).
Internationell RESTRICTED (KV-R)	Privat/sam-manslutning	Finland	Nationell myndighet/ offentlig ak-tör/företag	Myndigheter i andra länder får inte ha direkt eller indirekt tillgång till informationen. Villkoret om fysisk förvarings-plats omfattar även administration, säkerhetskopiering och annat underhåll. Tjänsteleverantörens tillförlitlighet kan utredas (till exempel som en del av en nationell säkerhetsbedömning av företag). Vid skyddet ska man beakta de särskilda krav som originatorn och/eller ägaren ställer på informationen i fråga. Jfr Katakri 2015.

Datatyp	Typ av molntjänst	Fysisk plats	Tjänst-eleverantör	Mer information
Stor mängd sekretess-belagd information och/eller SK IV-informa-tion och/eller personupp-gifter (SK III -datamassa)	Privat/sam-manslutning [34]	Finland	Nationell myndighet/ offentlig ak-tör/företag	Myndigheter i andra länder får inte ha direkt eller indirekt tillgång till informationen. Villkoret om fysisk förvarings-plats omfattar även administration, säkerhetskopiering och annat underhåll. Tjänsteleverantörens tillförlitlighet kan utredas (till exempel som en del av en nationell säkerhetsbedömning av företag). I fråga om masseffek-ter bör det finnas metoder med vilka åtkomsten kan begränsas till endast någon enskild eller snävare del av informationsinnehållet enligt vad som behövs, och me-toder med vilka obehöriga försök att komma åt en mer omfattande del av informationsinnehållet upptäcks. När PiTuKri används som bedömningsverktyg ska masseffek-ten tolkas så att det utöver kraven på SK IV även krävs ett säkerhetsområde för det fysiska skyddet av informations-mängden (FT-01), särskild tillförlitlighet för åtskiljande (JT-03) samt för applikationsskiktets säkerhet (MH-02/ punkt 1), effektiviserad spårbarhet och upptäcktskapaci-tet (JT-01/OH-05/punkterna 1f–g och 4e) samt tillförlitligt åtskiljande av uppgifterna (Ht-05/punkt 5). Jfr Katakri 2015 (I 01/Ytterligare information/Masseffekt).
SK III och SK II	Privat/sam-manslutning	Finland	Nationell myndighet/ offentlig ak-tör/företag	Myndigheter i andra länder får inte ha direkt eller indirekt tillgång till informationen. Villkoret om fysisk förvarings-plats omfattar även administration, säkerhetskopiering och annat underhåll. Tjänsteleverantörens tillförlitlighet kan utredas (till exempel som en del av en nationell säkerhetsbedömning av företag). Observera kraven på ytterligare skydd för säkerhetsklass III och/eller II [35], jfr Katakri 2015.

[34] Gemenskapsmoln (community/government cloud) med vissa begränsningar, till exempel tjänster som är avsedda endast för statsförvaltningen eller andra myndighetsgrupper.

[35] Modellen för praktiskt genomförande är i allmänhet användning av molnteknologi inom fysiskt skyddade säkerhetsområden så att den ifrågavarande hante-ringsmiljön för säkerhetsklass III/II i sin helhet är fysiskt och logiskt åtskild från andra miljöer.

Delområde 2: Säkerhetsledning

TJ-01	Säkerhetsprinciper
Krav	1) Organisationen har en serie säkerhetsprinciper antagna av högsta ledningsnivån som beskri-ver hur säkerhetsarbetet i organisationen är integrerat med verksamheten. 2) Säkerhetsprinciperna är heltäckande och ändamålsenliga med tanke på både organisationen och de objekt som ska skyddas. 3) Säkerhetsprinciperna styr säkerhetsarbetet. Ledningen informeras om hur säkerhetsprinciper-na följs och detta säkerställs även genom regelbunden övervakning.
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Med säkerhetsprincip avses det att ledningen förbinder sig vid säkerhetsarbetet i organisationen och att säkerhetsarbetet är till stöd för verksamheten.
Ytterligare information	Säkerhetsprinciperna ska förmedlas till personalen och lämpliga intressentgrupper. Principerna kan beskrivas på många olika sätt, till exempel i ett enskilt dokument eller som en del av organi-sationens anvisningar. Överensstämmelse med kravet kan påvisas genom giltig ISO27001-certifiering, under förut-sättning att certifieringen (inkl. genomförandeplanen) omfattar processerna för utveckling och tillhandahållande av molntjänsten.

TJ-02	Säkerhetsansvar
Krav	1) Säkerhetsuppgifterna och -ansvaren i fråga om molntjänsten har definierats och dokumenterats. 2) Det finns beskrivningar av ansvaren för kund och leverantör beträffande leverans och användning av molntjänsten. Jfr EE-01. 3) Det finns en utsedd person med ansvar för informationssäkerheten i molntjänsten.
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Syftet med definierade säkerhetsuppgifter och -ansvar är att säkerställa att det finns ansvariga personer för de viktigaste delområdena och att de är medvetna om sitt ansvar och sina behörigheter.
Ytterligare information	Att säkerhetsansvaren definieras är en väsentlig förutsättning för att ansvarspersonerna ska kunna utföra de säkerhetsuppgifter som de har ansvar för. Om inget annat anges är det ledningen som har samtliga säkerhetsansvar. Syftet med en molntjänstpolicy eller motsvarande beskrivning är att definiera klart och tydligt vilka säkerhetsfrågor som ligger på kundens ansvar och vilka som ligger på leverantörens ansvar.

TJ-03	Hantering av säkerhetsrisker
Krav	1) Organisationen ska ha en riskhanteringsprocess. Riskhanteringen ska utgöra en regelbunden, kontinuerlig och dokumenterad process. Riskhanteringsbesluten och instanserna som ansvarar för dem dokumenteras. 2) Det ska finnas en systematisk och begriplig metod för riskanalys. 3) Riskhanteringen ska omfatta åtminstone säkerhetsledning, utrymmessäkerhet och informationssäkerhet. 4) Identifierade risker ska beaktas i berörda intressentgrupper. Molnleverantören ska säkerställa att åliggandena som gäller kunddata tillgodoses också i situationer där informationen behandlas på uppdrag av organisationen. Jfr TJ-08. 5) Riskhanteringsprocessen och resultaten av den används för att ställa upp säkerhetsmål för organisationen, bedöma konsekvenserna av säkerhetsincidenter, planera säkerhetsåtgärder, hantera ändringar och i tillämpliga delar i upphandlingsförfarandena. 6) Säkerhetsåtgärderna har dimensionerats med beaktande av bl.a. klassificeringsgrund, mängd, form och förvaringsplats för den berörda informationen, i proportion till det bedömda hotet av fientlig eller brottslig verksamhet. 7) Organisationen dokumenterar de väsentligaste delarna av övervaknings- och säkerhetsåtgärderna.
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Målet för riskhanteringen är att identifiera och hantera faktorer som potentiellt kan äventyra verksamheten och att hålla riskerna på sådan nivå att verksamheten och målen inte löper fara.
Ytterligare information	**Integrering av lagstiftningskrav eller myndighetskrav i säkerhetsplaneringen.** Organisationen ska identifiera vilka lagstiftningsbaserade krav och myndighetskrav verksamheten omfattas av. Överensstämmelse med dessa krav, till exempel för att få ett myndighetsgodkännande, kan kräva att organisationen inför skyddsåtgärder som är striktare än de interna säkerhetskraven. Jfr TJ-07 (Överensstämmelse med krav och dataskydd). **Planering av riskhanteringen mot bakgrund av sekretessbelagd information** Riskhanteringsåtgärderna ska sättas in i den miljö där den sekretessbelagda informationen ska behandlas. Riskhanteringsåtgärderna kan vara administrativa (till exempel utbildning och anvisningar för personalen) eller tekniska (till exempel tekniskt skydd i miljön i fråga). **Flernivåförsvar i riskhanteringen** Riskhantering planeras för att minska riskerna i verksamheten. En bra princip att iaktta i planeringen är flernivåförsvar (defence in depth). Det betyder att om en viss säkerhetsåtgärd fallerar finns det andra att falla tillbaka på. I fråga om enstaka risker kan ett tillräckligt skydd bestå av enstaka, tillförlitliga skyddsåtgärder eller en kombination av flera åtgärder. **Metoder för riskhantering och riskanalys** Det finns flera olika metoder för riskhantering och riskanalys, som alla har sina styrkor och svagheter. Många av de systematiska metoderna bygger på identifiering av hot och sårbarheter, analys av sannolikheter och effektfullhet, bestämmande av sådana riskdämpande åtgärder som behövs, analys av kvarblivande risker och övervakning av korrigerande åtgärder.

TJ-04	Hantering av säkerhetsstörningar
Krav	1) Organisationen har rutiner för att hantera säkerhetsstörningar på behörigt sätt. 2) Organisationen har tydliga processer för att anmäla säkerhetsstörningar. Organisationen har klart definierade personer/instanser till vilka säkerhetsstörningar, konstaterade eller misstänkta, ska anmälas. 3) Säkerhetsstörningars antal och typer följs upp. Korrigerande planer ska sättas in för att undvika att konstaterade störningar upprepas. 4) Säkerhetsstörningar i samband med behandling av kunddata, konstaterade eller misstänkta, meddelas till kunden i fråga.
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	I fråga om hantering av säkerhetsstörningar är syftet att säkerställa att organisationen kan fungera effektivt i oönskade situationer så att skadan minimeras och normaliteten återställs. Genom att incidenter ska anmälas till kunden underlättas kundens riskanalysarbete och bl.a. minimeringen av skador hos kunden.
Ytterligare information	Överensstämmelse med kravet kan kontrolleras och påvisas till exempel enligt följande modell: Hanteringen av säkerhetsstörningar är 1) planerad, 2) baserad på direktiv och utbildning, 3) dokumenterad på tillräcklig nivå med hänsyn till användningsmiljön, 4) inövad, och framför allt 5) baserad på klart överenskommet förfarande och ansvar för information och kommunikation. Det rekommenderas att i synnerhet störningar, dataintrång eller försök till sådana som hänför sig till säkerhetsklassificerad information anmäls till Cybersäkerhetscentret. Om brottslig verksamhet identifieras bör man även kontakta polisen. Dessutom bör man beakta den korta tidsfrist som föreskrivs i artikel 33 i EU:s allmänna dataskyddsförordning samt skyldigheten för tjänsteleverantörer att anmäla uppgifter enligt 33 § i dataskyddslagen avseende brottmål.

TJ-05	Kontinuitetshantering
Krav	1) Processerna och rutinerna för kontinuitetshantering är planerade, genomförda, testade och beskrivna på ett sätt som innebär att organisationen kan fullfölja sina åligganden enligt serviceavtalen och lagstiftningen och de övriga affärsmässiga kraven för molntjänsten. Särskilda krav att beakta är a) att återhämtningen och säkerställandet av kontinuiteten med hänsyn till verksamhetens krav har beaktats i planeringen, b) att kontinuitetsplanerna ska innehålla förebyggande och korrigerande åtgärder för att minimera den effekt som avsevärda störningar eller exceptionella händelser har på behandlingen och förvaringen av information, c) att observerade incidenter integreras i riskanalyserna och att planerna för återställning och kontinuitetssäkring uppdateras enligt observationerna och resultaten, och d) att planerna för kontinuitetssäkring beaktar behovet att skydda informationen i nödsituationer, så att obehörig åtkomst eller obehörigt röjande av informationen eller förlust av integritet eller tillgänglighet förhindras.
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Målet för kontinuitetshanteringen är att säkerställa kontinuiteten i servicen så att kraven om tillgänglighet, integritet och konfidentialitet kan tillgodoses.
Ytterligare information	Överensstämmelse med kravet kan kontrolleras och påvisas till exempel enligt följande modell: Konsekvensanalysen för affärsverksamheten och planerna för kontinuitetssäkring och beredskap verifieras, uppdateras och testas med jämna mellanrum (åtminstone en gång om året) eller alltid när väsentliga ändringar har skett i organisationen eller användningsmiljön. Testerna omfattar även kunder och viktiga tredje parter (som till exempel viktiga leverantörer) som påverkas av dessa saker. Testerna dokumenteras och resultaten beaktas i kommande säkringsåtgärder för kontinuiteten. Datorhallstjänster (såsom vattenförsörjning, el, temperatur- och fuktreglering, datatrafik och internetuppkoppling) säkras. De övervakas, underhålls och testas med jämna mellanrum för att säkerställa att de fungerar oavbrutet och effektivt. Tjänsterna är försedda med automatiska mekanismer för feltolerans och till exempel dubblering. Underhållsarbeten utförs enligt de tidsintervall och mål som leverantören rekommenderar, och endast av behörig personal. Serviceprotokollen och eventuella anteckningar däri om misstänkta eller konstaterade brister förvaras i överenskommen tid. Jfr FT-05 (Beredskap och kontinuitetshantering) och KT-03 (Säkerhets- och returprocesser). Vid bedömning av det som kunden har ansvar för rekommenderas att man beaktar att tillgången till ett kundsystem i en molnplattform ofta är direkt beroende av hur molnplattformen fungerar.

TJ-06	Klassificering och identifiering av uppgifter och annat som ska skyddas
Krav	1) Det finns en enhetlig metod för klassificering och identifiering av alla de objekt som är viktiga för leveransen av molntjänsten och behandlingen av kunddata och som ska skyddas (information, maskinvara, programvara, verksamhetslokaler). 2) Skyddsobjekt som på grund av sitt informationsinnehåll är sekretessbelagda (informationsmaterial, maskinvara och system) har klassificerats i enlighet med vad som föreskrivs i lag. 3) Maskinvaran och programvaran som används för att tillhandahålla molntjänsten och behandla kunddata har identifierats. 4) Maskinvaran och programvaran har klassificerats enligt hur kritiska de är. 5) En ägare/ansvarsperson har utnämnts för varje maskinvara och programvara. 6) Bok förs över maskinvaran och programvaran så att ändringar i ett godkänt upplägg kan identifieras genom att upplägget jämförs med bokföringen. (Jfr MH-01: Ändringshantering.)
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Syftet med klassificeringen är att välja och dimensionera säkerhetsåtgärderna baserat på vilka skyddsbehoven är för varje objekt. Syftet med identifieringen är att göra det möjligt att sätta in de säkerhetsåtgärder som är aktuella baserat på klassificeringen.
Ytterligare information	Klassificeringen kan anges på olika sätt beroende på dokument, behandlingsmiljö och användare. Om databehandlingsmiljöerna klassificeras enligt typen av dokument kan man tydligare välja och motivera vilka säkerhetsåtgärder som är aktuella för varje databehandlingsmiljö. När det gäller krav 5 kan överensstämmelse också påvisas så att molnleverantören klassificerar all den dokumentation som kunden producerar i tjänsten enligt sitt interna klassificeringssystem, så att klassificerade skyddsobjekt (informationsmaterial, maskinvara och system) skyddas under hela livscykeln i överensstämmelse med kraven för sekretessbelagd och/eller säkerhetsklassificerad sekretessbelagd information. Automatiserade bokföringsrutiner för maskin- och programvara rekommenderas. Alternativt kan månatliga kontroller utföras manuellt för att säkerställa att bokföringen är à jour. Bokföringen ska ha en ändringshistorik (historik över gjorda ändringar) som kan kontrolleras i efterhand. Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att a) kunden har identifierat de skyddade objekten som ska placeras i molntjänsten (kundens informationsmaterial, system och eventuellt även maskinvara) och klassificerat dem utifrån de lagstadgade kraven, b) kunden har säkerställt att det inte finns några hinder för att placera de skyddade objekten i molntjänsten i fråga (jfr EE-02), c) kunden har försäkrat sig om att molnleverantören är medveten om klassificeringen av objekten och att d) det finns en aktuell bokföring över den helhet som ingår i kundens ansvar så att ändringar i ett godkänt upplägg kan identifieras genom att jämföra upplägget med bokföringen. (Jfr MH-01: Ändringshantering.)

TJ-07	Överensstämmelse med krav och dataskydd
Krav	1) Lagarna och författningarna som tillämpas på molntjänsten samt förfarandena för att följa dessa har identifierats och dokumenterats samt regelbundet uppdaterats. 2) Oberoende tredje parter ska minst en gång om året i tillämpliga delar bedöma verksamheten, processerna och informationssystemen som har anknytning till molntjänsten i enlighet med den beskrivning som fastställs i en separat utvärderingsplan. Syftet med bedömningen är att identifiera eventuella fall där lagar eller författningar inte följs. Utvärderingsplanen fäster avseende vid tjänstens säkerhet på så sätt att alla centrala helheter som är relevanta för säkerheten bedöms med högst tre års mellanrum. Konstaterade incidenter ska dokumenteras, prioriteras och åtgärdas enligt hur kritiska de är. 3) Molntjänsten ska åtminstone en gång om året genomgå en intern inspektion för att utreda hur tjänsten som helhet iakttar sina säkerhetsregler och tillgodoser sina avtals- och lagstiftningsbaserade ansvar. 4) Högsta ledningen har ansvar för att konstaterade incidenter prioriteras och för att ersättande skydd eller korrigerande åtgärder sätts in tillräckligt snabbt.
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Att lagbaserade krav och avtalsförpliktelser tillgodoses.
Ytterligare information	Molnleverantören ska till exempel se till att säkerheten beaktas vid behandling av personuppgifter i enlighet med bestämmelserna i fallet i fråga, se t.ex. dataskyddslagen (1050/2018), lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018, dataskyddslagen avseende brottmål) samt 32 artikeln i den allmänna dataskyddsförordningen (GDPR, (EU) 2016/679). Det kan bli nödvändigt att klassificera personuppgifter och behandla dem därefter om det finns olika slags personuppgifter med olika skyddsbehov (juridiska krav, värde, känslighet) och/eller om de behandlas med olika grad av skydd i molnleverantörens olika processer eller system. Jfr kravkort EE-02. Dataombudsmannen fungerar som tillsynsmyndighet för behandlingen av personuppgifter i Finland. Personuppgiftsincidenter ska anmälas till dataombudsmannen och vid behov även till användarna enligt vad som föreskrivs i 33 och 34 artikeln i GDPR. Även övrig lagstiftning bör iakttas då personuppgiftsincidenter anmäls. Telebolag åläggs till exempel att anmäla personuppgiftsincidenter till Transport- och kommunikationsverket och vid behov även till användarna enligt förordning (EU) 611/2013. Jfr TJ-04 (Hantering av säkerhetsstörningar). När kundens ansvar bedöms rekommenderas särskilt att man beaktar att kunden inte kan utlokalisera det kravenliga genomförandet av sitt ansvar, inberäknat säkerställandet av att utlokaliseringspartnern (här särskilt molnleverantören) tillgodoser kraven som ställs på den behandlade informationen.

TJ-08	Säkerheten för tjänsteleverantörer och andra leverantörer
Krav	1) Åligganden som gäller kunddata fullgörs också i situationer där informationen behandlas på uppdrag av organisationen. I synnerhet följande ska säkerställas: a) Innan leverantörens personal får åtkomst till skyddade objekt har den genomgått samma skyddsåtgärder som molnleverantörens personal (avtal, tystnadsplikt, säkerhetsutredningar, utbildning), b) leverantörerna har fått skriftliga direktiv och ålagts i avtal att iaktta skyddsåtgärder på åtminstone motsvarande nivå som organisationen, c) det finns tillförlitliga rutiner för att säkerställa och övervaka att avtalsskyldigheterna iakttas, d) leverantörer som direkt eller indirekt är med om att behandla säkerhetsklassificerad information har ett giltigt myndighetsgodkännande eller godkännande enligt ett motsvarande förfarande. Förfarandet omfattar i tillämplig utsträckning helheter för såväl administrativ (säkerhetsledning) som fysisk och teknisk informationssäkerhet.
Tillämplighet	Att garantera den övergripande säkerheten för den producerade tjänsten när det gäller externa tjänsteleverantörer och/eller andra leverantörer.
Datatyper	1a–1c: Sekretessbelagd, personuppgifter 1d: SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Skyddsobjekten ska säkras också i de situationer där molnleverantörens egna tjänsteleverantörer och/eller andra leverantörer har direkt eller indirekt åtkomst till dem. Jfr MH-02 (Systemutveckling).
Ytterligare information	Säkerheten i entreprenad- och leverantörskedjorna har ofta en direkt inverkan på skyddet för information som behandlas i molntjänsten. Om molnleverantörens tjänster säkerhetsmässigt är beroende av entreprenader eller leverantörskedjor i någon utsträckning måste säkerheten för dessa beaktas i den övergripande planeringen och upprätthållandet av molntjänstens säkerhet. Kraven i 28 artikeln 4 punkten i EU:s allmänna dataskyddsförordning samt i 17 § 2 mom. i dataskyddslagen avseende brottmål ska också beaktas i behandlingen av personuppgifter när så kallade underhandläggare anlitas. Tjänsteleverantören (den personuppgiftsansvariga) ska ingå ett skriftligt avtal med den instans som behandlar personuppgifter. Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och tjänsteleverantörer som har anknytning till kundens ansvarsområde.

Delområde 3: Personalsäkerhet

HT-01	Anställningarnas livscykel
Krav	1) Organisationen följer ett förfarande som beaktar säkerheten i de olika faserna av varje anställningsförhållande. Rekrytering, ändring av arbetsuppgifterna och avslutning av anställningsförhållanden är särskilt viktiga skeden att beakta.
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Att minimera de personalrelaterade riskerna under anställningsförhållandets livscykel.
Ytterligare information	En procedur som beaktar de relevanta säkerhetsaspekterna förutsätter typiskt direktiv som berörda personalgrupper får utbildning i och tillgång till. Direktiven kan förslagsvis grupperas enligt anställningsförhållandets livscykel. De kan exempelvis grupperas i rekryteringsdirektiv, inskolningsdirektiv, direktiv för situationer av förändring, direktiv för när anställningsförhållandet avslutas och direktiv för specifika situationer såsom ändringar i användar- och åtkomsträttigheter. Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

HT-02	Pålitlighetsbedömning av personalen
Krav	1) I den mån det är tillåtet enligt lokal lagstiftning görs bakgrundskontroller för interna eller externa anställda som har åtkomst till kunduppgifter i molntjänsten eller till gemensam IT-infrastruktur. Kontrollerna görs innan anställningsförhållandet börjar. Kontrollen ska omfatta minst följande, i den mån det är tillåtet enligt lag: a) Verifiering av identitet. b) Verifiering av tidigare anställningar. c) Verifiering av utbildningsbakgrund. 2) Säkerhetsutredningar på tillbörlig nivå görs för att utreda och övervaka att personer kopplade till behandlingen av säkerhetsklassificerat material är pålitliga.
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	1: Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa) 2: SK IV & KV-R, SK III (centrala säkerhetsansvariga, tekniska administratörer eller motsvarande personer med tillgång till stora mängder SK IV-information eller möjlighet att påverka skyddet av sådan information.)
Mål för skyddet	Att minimera riskerna kopplade till personalens pålitlighet.
Ytterligare information	2: Om det förekommer direkt eller indirekt åtkomst till skyddade kunddata. Till exempel administratörer av virtualiseringsplattformar (hypervisors) har i praktiken ofta tillgång till kunddata som behandlas i de virtuella maskinerna. Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

HT-03	Avtal om sekretess och tystnadsplikt
Krav	1) Molnleverantören har ett avtalsförfarande för sekretess eller tystnadsplikt. Sekretessavtalen ska undertecknas innan avtalsförhållandet börjar eller innan användarrättigheterna som ger tillgång till kunddata i molntjänsten ges.
Tillämplighet	Molntjänstens interna anställda, personal hos externa tjänsteleverantörer och andra externa leverantörer.
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Att minimera riskerna kopplade till personalens pålitlighet, framför allt genom ökad medvetenhet.
Ytterligare information	Sekretessavtalet (eller motsvarande) ska innehålla åtminstone följande: • En beskrivning av informationen som ska behandlas som sekretessbelagd • Villkoren för sekretessavtalet • Vilka åtgärder som ska vidtas när avtalet upphör att gälla (till exempel att datamedier ska förstöras eller returneras) • Vem som äger uppgifterna • Vilka regler och författningar som gäller användning och överlåtande av sekretessbelagd information till andra parter, om det behövs • Påföljder vid överträdelse av avtalsvillkoren Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

HT-04	Säkerhetsmedvetenhet
Krav	1) Det finns en beskrivning av de centrala säkerhetsprinciperna och arbetsrutinerna. 2) Säkra rutiner ska vara bekanta för personalen så att det råder visshet om att personalens säkerhetsmedvetenhet är tillräcklig. 3) Regelbundna kontroller, åtminstone årligen, av att beskrivningarna och direktiven med anknytning till säkerhet är aktuella och har omsatts i praktiken. 4) Direktiven med anknytning till säkerhet omfattar alla processer och behandlingsmiljöer där personuppgifterna och sekretessbelagd information behandlas, över hela livscykeln för informationen. 5) Efterlevnaden av säkerhetsdirektiven övervakas och behovet av översyn av direktiven bedöms regelbundet.
Tillämplighet	Molntjänstens interna anställda, personal hos externa tjänsteleverantörer och andra externa leverantörer.
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Syftet med de säkerhetsrelaterade principerna (jfr. TJ 01) och beskrivningarna/direktiven och med att omsätta dem i praktiken är att det finns planerade, säkra rutiner och att personalen också i praktiken kan följa dem, både i normala och i särskilda situationer. Jfr KT-01 (Systembeskrivning till stöd för kontinuitet och driftssäkerhet).
Ytterligare information	Att säkerhetsansvaren definieras är en väsentlig förutsättning för att ansvarspersonerna ska kunna utföra de säkerhetsuppgifter som de har ansvar för. Om inget annat anges ligger säkerhetsansvaren hos ledningen. Jfr TJ-02 (Säkerhetsansvar). Överensstämmelse med kravet kan kontrolleras och påvisas till exempel enligt följande: 1) Personalen får direktiv och utbildning om hur sekretessbelagd information ska behandlas. 2) Det ordnas regelbunden utbildning i behandling av sekretessbelagd information och det dokumenteras vem som har deltagit. 3) Efterlevnaden av säkerhetsdirektiven övervakas och behovet av översyn av direktiven bedöms regelbundet. 4) Personalen erbjuds säkerhetsutbildningar och utvecklingsprogram för bättre säkerhetsmedvetenhet, som är skräddarsydda enligt målgrupp. De är obligatoriska för all intern och extern personal hos molnleverantören. Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

HT-05	Behov av information och åtskillnad mellan funktioner
Krav	1) En förteckning förs över arbetsuppgifter som omfattar behandling av sekretessbelagd information. Till denna kategori räknas även utvecklings- och administratörsuppgifter i vilka man direkt eller indirekt kan få åtkomst till sekretessbelagd information eller på annat sätt har möjlighet att väsentligt påverka skyddet för sådan information. 2) Åtkomst till sekretessbelagd information kan bara ges efter att behovet av information som personen har på grund av arbetsuppgifter har klarlagts. 3) En förteckning över rättigheter att behandla säkerhetsklassificerad information förs per klass. 4) Funktionerna och ansvarsområdena har i mån av möjlighet skilts åt för att minimera risken för obehörig ändring eller missbruk av skyddad information. Om det uppstår riskabla funktionskombinationer ska det finnas en övervakningsmekanism för dem. 5) För datamassa i säkerhetsklass III dessutom: Kritiska funktioner och ansvarsområden har i mån av möjlighet fördelats på olika personer för att minimera risken för obehörig ändring eller missbruk av skyddad information. Särskild uppmärksamhet ska fästas vid att en enskild person inte kan avlägsna spår av sina handlingar eller i betydande grad förhindra att avvikande åtgärder upptäcks.
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	1–2: Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa) 3–4: SK IV & KV-R, SK III (datamassa) 5: TL III (datamassa)
Mål för skyddet	Syftet är att minimera riskerna för sekretessbelagd information genom att sekretessbelagd data endast kan komma i behöriga personers händer enligt deras behov av information (need to know).
Ytterligare information	Det blir lättare att definiera behovet av information om organisationen har beskrivit principerna enligt vilka personer i organisationen har åtkomst till sekretessbelagd information, och om man har beskrivit processen eller gett direktiv för hur åtkomst baserad på arbetsuppgifter ska ges och administreras i situationer av förändring. Viktigt att beakta då behandlingsrättigheter, arbetsuppgifter och roller definieras är att det inte får uppstå riskabla kombinationer av arbetsfunktioner eller roller. I de flesta system är det möjligt att göra en tillräcklig åtskillnad mellan administratörsroller (och personer) för systemet och rollerna (och personerna) som deltar i tillsynen över loggar. En ofta använd tillsynsmekanism är också att kritiska underhållsåtgärder och motsvarande åtgärder kräver godkännande av två eller flera personer (”two man rule”). Detta krav bör bedömas med beaktande av bl.a. ansvarsfördelningen mellan molnleverantör och kund. I typiska fall kan molnleverantören inte påverka till exempel det hur man kontrollerar behovet av information för utvecklare eller administratörer som sköter den del av systemet som kunden har ansvar för. Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

Delområde 4: Fysisk säkerhet

FT-01	Skydd och riskhantering baserade på flernivåförsvar
Krav	1) De fysiska säkerhetsåtgärderna iakttar principen om flernivåförsvar. 2) De utrymmen som ska skyddas i byggnaden har klassificerats som säkerhetsområden (administrativt område, skyddsområde) och de har tydligt definierade och synliga gränser. 3) Informationsmängder med sekretessbelagd information av säkerhetsklass IV eller lägre, och system som används för informationsbehandling ska placeras inom säkerhetsområdet. 4) Informationsmängder som har bildat en datamassa i säkerhetsklass III och de informationssystem som används för åtkomstbegränsningar och -övervakning av informationen ska placeras inom säkerhetsområdet. 5) De administrativa områdena har tydligt definierade synliga gränser och endast personer som organisationen befullmäktigat har tillträde till dessa utan följeslagare. 6) Säkerhetsområdena har tydligt definierade och skyddade gränser. Vid dem övervakas all passage in och ut med hjälp av passerkort eller genom att personligen identifiera dem som passerar. Endast personer som har konstaterats pålitliga och som har ett särskilt tillstånd har tillträde till området utan följeslagare. 7) Säkerhetsåtgärderna har dimensionerats med tillräcklig omfattning så att de motsvarar riskerna enligt riskanalysen.
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Målet för skyddet är att förhindra obehörig åtkomst till molnleverantörens datorhall och till sekretessbelagd information, samt att förhindra och minimera konsekvenserna av stöld, olyckor, förluster, ekonomiska förluster och störningar.
Ytterligare information	Flernivåförsvar avser att det finns en samling säkerhetsåtgärder som kompletterar varandra. Om möjligt ska utrymmena bilda zoner inne i varandra så att utrymmena med högre skyddsbehov ligger innerst. Säkerhetsåtgärderna ska planeras som en helhet där man tar i beaktande skyddsnivån för den sekretessbelagda informationen, mängden information, omgivningen runt byggnaderna och byggnadernas fysiska egenskaper. Molnleverantören ska ha en riskhanteringsprocess som tillämpas i organisationen (jfr TJ 03). Molnleverantören ska analysera riskerna för utrymmen eller byggnader som innehåller information, informationssystem eller annan nätinfrastruktur av känslig eller kritisk natur (åtminstone en gång om året). Riskerna ska ha namngivna ägare, personer med ansvar för riskanalysen och personer med ansvar för de hanteringsåtgärder som bestäms. Riskanalyserna ska dokumenteras. Överensstämmelse med kravet kan kontrolleras och påvisas enligt följande: Byggnaden planeras så att ytterväggarna och det yttre höljet bildar den första försvarsnivån. Tillträdet till byggnaden övervakas och hanteras till exempel med passerkontroll och lås. Information med ett högre skyddsbehov behandlas i de inre delarna av byggnaden för att försvåra och fördröja möjligheten till intrång. De konstruktionsmässiga lösningarna kompletteras med säkerhetstekniska lösningar. Fönster, dörrar och andra öppningar beaktas i planeringen.

FT-02	Konstruktioner och säkerhetssystem
Krav	1) Lokaler eller byggnader som innehåller information, datasystem eller annan nätinfrastruktur av känslig eller kritisk natur skyddas utvändigt på ett fysiskt hållbart sätt, med moderna och tillräckliga säkerhetsåtgärder.
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Målet för skyddet är att förhindra obehörig åtkomst till molnleverantörens datorhall och till sekretessbelagd information, samt att förhindra och minimera konsekvenserna av stöld, olyckor, förluster, ekonomiska förluster och störningar.
Ytterligare information	De staket som avgränsar området samt vägg-, tak-, golv-, fönster- och dörrkonstruktionerna och genomföringarna för husteknik i det yttre höljet omfattas inte av några särskilda krav. Konstruktioner som fyller sin funktion är lämpliga. Säkerhetstekniken ska underbygga den allmänna säkerheten för utrymmet och byggnaden. Exempel på möjliga säkerhetsåtgärder är ett tillräckligt avstånd till utomstående aktörer, staket, bevakning eller tekniska bevakningssystem (bl.a. passerkontroll, inbrottslarm, kameraövervakning). Systemen ska servas regelbundet i enlighet med tillverkarens rekommendationer och så att deras funktionsduglighet säkerställs. Säkerhetssystem och -utrustning ska testas (minst en gång i månaden) och hållas i användbart skick. Testerna ska dokumenteras. Överensstämmelse med kravet (SK IV) kan kontrolleras och påvisas enligt följande (eller motsvarande) kriterier: • Byggnadens väggkonstruktion: armerad betong (50 mm), mineralull för värmeisolering (80 mm), armerad betong (60 mm). Väggkonstruktionen i datorhallen där uppgifter förvaras: brandskiva (12 mm), gipsskiva + ull + gipsskiva (70 mm). • Hela byggnaden är skyddad med passerkontroll- och inbrottslarmsystem. Vägarna till datorhallen är försedda med kameraövervakning. Systemen administreras och övervakas av en utomstående bevakningsfirma med vilken organisationen har ett säkerhetsavtal. Den person som ansvarar för organisationens säkerhet ansvaret för service, underhåll, tester och dokumentering av ovan nämnda system. Systemen testas en gång i månaden. Överensstämmelse med kravet (SK III masseffekt) kan kontrolleras och påvisas enligt följande (eller motsvarande) kriterier: **Väggar, golv och tak i maskinrummet eller byggnaden:** • Konstruktionerna ska ha sådan hållfasthet och vara byggda så att det inte är möjligt att tränga in i utrymmet utan att söndra konstruktionerna med verktyg. • Konstruktionerna eller delar av dem får inte vara löstagbara från utsidan utan att de går sönder. En inbrottsskyddsvägg av klass 3 uppfyller kraven ovan. Mellanväggskonstruktionen ska sträcka sig från golv till tak. • Lätta konstruktioner måste förstärkas. • Väggkonstruktionerna kan till exempel vara: - 1 x 12 mm gipsskiva + 1,5 mm stålplåt + 12 mm faner + stomme + 12 mm faner + 1,5 mm stålplåt + 1 x 12 mm gipsskiva. - Armerad betong; ≥ 80 mm. - Bränt tegel; ≥ 85 mm + 2 x 1,5 mm stålplåt på insidan eller 1,5 mm stålplåt på utsidan och 1,5 mm stålplåt på insidan. - Block; ≥ 70 mm + 2 x 1,5 mm stålplåt på insidan eller 1,5 mm stålplåt på utsidan och 1,5 mm stålplåt på insidan. Ovanpå stålplåtarna gipsskiva. • Golvkonstruktionerna kan till exempel vara: - Hålplatta, över 320 mm. - Betong ≥ 80 mm. - Övriga golvkonstruktioner; förstärkning av stålplåt ≥ 3 mm. • Takkonstruktionerna kan till exempel vara: - Hålplatta. - Betong ≥ 80 mm. - Övriga takkonstruktioner; förstärkning av stålplåt ≥ 3 mm. Glaskonstruktioner, såsom glasväggar och glasskjutdörrar, ska ha inbrottssäkert glas enligt standarden SFS-EN 356 P6B eller skyddas med ett tillräckligt starkt rullgaller eller stålgaller.

FT-02	Konstruktioner och säkerhetssystem
Ytterligare information	**Fönster och öppningar** Fönsterrutorna ska fästas och fönstren stängas så att de inte kan lösgöras eller öppnas från utsidan utan att de går sönder. Fönster och takfönster ska ha inbrottssäkert glas enligt standarden SFS-EN 356 P6B eller så ska de skyddas med ett fast/låst rullgaller, stålgaller eller stålnät eller med en skyddsplåt för öppningar. Andra öppningar, såsom rökavlopp och luftintag, ska skyddas med fasta eller låsta stålgaller. Kravet gäller inte fönster eller öppningar på minst 4 m höjd från markytan eller från annat ståplan. Om något annat än inbrottssäkert glas används i fönster och glasskjutdörrar ska storleken på öppningskonstruktionen väljas enligt storleken på de apparater som ska skyddas så att det inte är möjligt att transportera föremål genom konstruktionen utan att söndra den. **Dörrar, gångjärn och karmar:** Dörrens konstruktion ska ha motsvarande hållfasthet som väggkonstruktionen. Dörrkonstruktionen ska vara följande: • Karmen ska kilas in i konstruktionerna vid lås och gångjärn. • Inbrottsskyddstappar ska fästas vid gångjärnen. • Gångintervallet på låssidan får inte vara större än 5 mm. • Driftslåset i en ofalsad dörr ska skyddas med springjärn. • Dörrglaset ska fästas så att det inte kan lösgöras från utsidan utan att det går sönder. Dörrglasen ska vara P6B inbrottssäkert glas eller så ska de skyddas med rullgaller, stålgaller eller stålnät. En dörr som har testats enligt standarden SFS-EN 1627 för klass 3 uppfyller kraven ovan. **Låsning:** • Med ett fast manöverlås som monteras med motdiskar på dörren och som enligt standarden SFS 7020 är klassificerat antingen i klass 1 eller 2. • Med ett fast säkerhetslås som monteras med motdiskar på dörren och som enligt standarden SFS 7020 är klassificerat i klass 3 eller 4. **Säkerhetssystem:** Utrymmet för säkerhetssystemutrustningen ska placeras på ett område som motsvarar säkerhetsområdet. Tillträdesrättigheterna till utrustningsutrymmet beviljas enligt det arbetsbaserade behovet. Säkerhetssystemen ska omfattas av regelbunden service, uppdatering och testning för att säkerställa att systemen är funktionsdugliga och informationssäkra. Säkerhetssystemens fjärranslutningar och installationen av fältutrustning ska överensstämma med datasäkerheten enligt riskbedömningen så att åtkomst till säkerhetssystemen är möjlig endast från auktoriserade terminaler/nätverk och så att trafikförbindelsen och säkerhetssystemets gränssnitt är skyddade på så sätt att utomstående inte har tillgång till förmedlad information. Höjd strukturell inbrottssäkerhet förutsätts dock inte om utrymmena ständigt är bemannade av säkerhetspersonal. Dessutom ska säkerhetspersonalen ha tillräcklig övervakningskapacitet för att polisen eller säkerhetspersonalen ska få en indikation på intrånget i så god tid att inkräktaren inte hinner få tillgång till den skyddade informationen. Övervakningen kan ske genom inspektionsrundor och övervakning i realtid av säkerhetssystemen eller kombinationer av dessa. **Brottsanmälningssystem och överföring av larm:** Dörrar, öppningar och fönster i det skyddade utrymmet ska övervakas med hjälp av ett system för brottsanmälningar. Systemets centraldator och detektorer ska vara godkända åtminstone enligt klass 3 i Finansbranschen (FA). Anmälan ska överföras som en övervakad eller dubbel förbindelse. Med hjälp av en larmöverföringsanordning ska åtminstone följande uppgifter överföras till bevakningsföretaget eller något annat säkerhetskontrollrum: inbrott, påslaget/avslaget, sabotage, fel. Systemet ska opereras med hjälp av en personlig kod (minst fyra tecken). Som radiodrivna detektorer godkänns endast personliga nödknappar. Utrymmena ska övervakas när ingen vistas i dem. **Passerkontrollsystem:** På gränsen till säkerhetsområdet ska elektronisk passagekontroll användas vid in- och utgång. Tvåfaktorsautentisering (t.ex. inträdeskod och elektronisk identifikation) används vid ingång. För passerkontrollkoderna ska modern och krypterad lästeknik användas eller så ska organisationen hantera identifieringen i enlighet med sina säkerhetsanvisningar (SK III + SK IV). **Kameraövervakningssystem:** Säkerhetsområden, rutter och omgivande områden övervakas med inspelande kameraövervakning. Kameraövervakningen och förvaringen av inspelningarna ska följa organisationens riskbedömning.

FT-03	Förhindrande av obehörigt tillträde
Krav	1) För att förhindra att obehöriga får tillträde till utrymmen eller byggnader som innehåller information, datasystem eller annan nätinfrastruktur av känslig eller kritisk natur skyddas och övervakas de med ett elektroniskt system för passerkontroll och/eller mekaniska/elmekaniska nycklar. 2) Tillträdesrätterna har ordnats så att obehörig åtkomst till sekretessbelagd information har förhindrats. Åtkomst till utrymmen där sekretessbelagd information förvaras ges endast åt personer som på grund av sina arbetsuppgifter har behov av informationen.
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Endast personal som fått tillstånd för det har åtkomst till sekretessbelagd information som behandlas i molntjänsten, maskinvaran med vilken de behandlas och säkerhetssystemen för dessa.
Ytterligare information	Överensstämmelse med kravet kan kontrolleras och påvisas enligt följande: a) ID-kort med foto eller motsvarande synlig identifiering används i organisationen och hålls framme när man rör sig i dess utrymmen. b) Organisationen har en ansvarsperson som för bok över beviljade tillträdesrätter och mekaniska nycklar i ett dokument eller en logg. Det finns en skriftlig beskrivning av rutinen för utfärdande av tillträdesrätter och mekaniska nycklar samt av rutinen i samband med borttappade nycklar och avskrivning. Tillträdesrätter och nycklar kontrolleras regelbundet och vid behov (åtminstone med sex månaders mellanrum eller när ett anställningsförhållande inleds eller upphör, eller när en person byter arbetsuppgift). c) Personen med ansvar för nycklarna har låsschemat och ett nyckelkort. d) Systemet för passerkontroll har tvåfaktorsautentisering (till exempel identifikation + PIN-kod). Tillträdesrätter och mekaniska nycklar specificeras per användare. Om organisationen har koder i gemensam användning finns en ersättande metod för tillförlitlig identifiering av personer. e) Mekaniska nycklar är kopieringsskyddade. De mekaniska nycklarna till datorhallen hör till en annan serie än byggnadens övriga nycklar. Reservnycklar eller reservnyckelbrickor (avsedda t.ex. för nödsituationer) förvaras förseglade och i ett låst utrymme. Nycklar eller nyckelbrickor ges ut mot kvittering som kan verifieras i efterhand. f) Nycklarna ska förvaras säkert och får inte märkas så att de kan kopplas till objektet. I nyckelförvar som sänkts in i ytterväggen kan endast separata nycklar till serviceutrymmen eller ruttnycklar till fastigheten förvaras.

FT-04	Serviceproducenter och besökare
Krav	1) Besökare identifieras, förses med besökarkort och registreras. Organisationen har en dokumenterad besökarpolicy. Vid besök gäller alltid värdprincipen. 2) Städ- och underhållspersonal och annan servicepersonal identifieras, förses med besökarkort och registreras. Regelbundna serviceproducenter förses med ID-kort med foto. 3) Serviceproducenter som rör sig självständigt på området eller har tillgång till skyddade objekt har genomgått en säkerhetsutredning. Personer för vilka en säkerhetsutredning inte är möjlig eller ännu inte har gjorts rör sig med följeslagare. Jfr HT-02. 4) Det finns beskrivna och dokumenterade rutiner för servicearbeten, uppdateringar och underhåll.
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Endast personer som bedöms vara pålitliga och som fått tillstånd för det har åtkomst till sekretessbelagda uppgifter i molntjänsten, maskinvaran med vilken de behandlas och säkerhetssystemen för dessa.
Ytterligare information	Åtminstone följande är viktigt att beakta i rutiner och direktiv: a) Det ska tryggas att information bibehåller sin integritet under hela livscykeln, b) sekretessbelagd information ska avlägsnas tryggt före reparation eller service utförd av utomstående, c) underhålls-, installations- och städåtgärder i anslutning till inbrottslarm, passerkontrollsystem och andra övervakningssystem avseende förvaringsplatsen för sekretessbelagd information eller området som avgränsar platsen utförs endast av personer med särskilt tillstånd och säkerhetsutredning för området eller under övervakning av personal inom organisationen, d) organisationen har avtal med serviceproducenterna (t.ex. bränsle för reservelverk), e) organisationen har giltiga säkerhetsavtal med en bevakningsfirma (säkerhetstjänster) och en firma för fastighetstjänster (luft, vatten, el, bränsle, städning), f) utryckningstiden vid larm är så kort att risken att åka fast är stor, g) organisationen har skriftligt beskrivit för personalen vilka åtgärder som vidtas under underhållsåtgärder och vilka som utförs inför andra avbrott, h) monterings- och servicearbeten som hänför sig till säkerhetssystemen utförs av ett företag som organisationen själv valt och vars personal har genomgått säkerhetsutredning, i) städning utförs en gång i månaden eller efter behov. Städarna har genomgått säkerhetsutredning. Städarna är försedda med ID-kort med foto.

FT-05	Beredskap och kontinuitetshantering
Krav	1) Utrymmen eller byggnader som innehåller information, informationssystem eller annan nätinfrastruktur av sekretessbelagd eller kritisk natur är skyddade via fysiska, tekniska och organisatoriska skyddsåtgärder mot eldsvåda, vattenskador, explosioner, oroligheter och andra hot förorsakade av människan eller naturen. 2) Skyddet av viktig infrastruktur omfattar åtminstone följande: a) Fysiska skyddsåtgärder: Fysiskt brandskydd (brandsäkra vägg-, golv-, tak- och dörr-/fönsterkonstruktioner samt genomföringar tätade med produkter som uppfyller kraven för brandklassen i fråga). b) Tekniska säkerhetsåtgärder: i. Utrymmet eller byggnaden är kopplad till ett automatiskt system som förmedlar larm om brand till nödcentralen. ii. Utrymmet är försett med ett ventilationssystem som är avskilt från den övriga fastigheten och med automatiska brandstopp (t.ex. automatiska rökspjäll). iii. Beroende på den skyddade informationen har tillräckliga miljö-, temperatur- och fuktsensorer (nät- eller tryckvariationer, hetta/kyla, vattenläckage) installerats. iv. Det finns automatiska släcksystem som upptäcker t.ex. brand i ett tidigt skede och påbörjar släckningen. v. Jämn elförsörjning är tryggad med hjälp av anläggningar för detta ändamål (UPS, reservkraft). vi. Säkrad datakommunikation och dubblerat kylsystem. c) Organisatoriska säkerhetsåtgärder: i. Organisationen har en räddningsplan. ii. Organisationen har en ansvarsperson eller ansvarig instans som informeras när ett larm går. iii. Organisationen har regelbundna räddningsövningar och brandskyddsinspektioner för att kontrollera att brandskyddsföreskrifterna följs. iv. Kontinuitetsplanering
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Molntjänstens datorhallar (och motsvarande anläggningar) är skyddade mot vanliga risker för att säkra kontinuiteten.
Ytterligare information	Säkerhetsåtgärder som är till stöd för kontinuiteten omfattar typiskt följande: Fysiskt skydd: - Brandsektioner som avgränsar brand eller läckage - Brandfasta material, t.ex. 60 eller 90 min - Brandstopp som förhindrar att rök- och brandgaser sprids till andra utrymmen Tekniskt skydd: - Regelbundna och dokumenterade funktionstester av anläggningarna - Fungerande processer och information som når de rätta instanserna eller personerna - Reservkablar och förbindelser, dubblerade system, säkerhetskopiering med tillräckliga intervall och i tillräcklig omfattning - Kontinuitetsplanering med avseende på störningar som innebär att a) lokaler b) system c) personal inte är tillgängliga till hundra procent. Organisatoriskt skydd: - Syftet med räddningsplanen och kontinuitetshanteringen är att beskriva åtgärder med vilka man förebygger, minimerar, begränsar och återhämtar sig från funktionsstörningar, olyckor, skador och exceptionella händelser. - Planerna borde ses över åtminstone årligen. Kritiska servrar och anordningar ska identifieras och säkerhetskopieras enligt vad driftskraven förutsätter. Jfr TJ-05 (Kontinuitetshantering) och KT-03 (Säkerhets- och returprocesser). Om driftskraven är höga måste systemen säkras mot inbrott, vandalism, brand, värme, gas, damm, vibrationer, vatten och elavbrott. Fjärråtkomst har förhindrats för VVS-automatiken i kritiska serverutrymmen och tekniska utrymmen. Miljösensorerna i kritiska serverutrymmen och tekniska utrymmen skyddas och övervakas. Den viktigaste molninfrastrukturen bör vara fördelad på minst två separata utrymmen.

Delområde 5: Datatrafikens säkerhet

TT-01	Datanätets uppbyggnad
Krav	1) Molntjänstmiljön är frånskild från andra miljöer. 2) Innanför molnets utkant är molntjänstmiljön indelad i olika områden (zoner, segment, mikrosegment eller motsvarande). 3) Trafiken begränsas och övervakas så att endast trafik som godkänts separat och som är nödvändig tillåts (default-deny) i molntjänstmiljöns utkant och mellan de interna områdena.
Tillämplighet	Internetbrandväggar (eller motsvarande nätverksenheter, t.ex. routrar), programbrandväggar för arbetsstationer och servrar, övriga system som hör till molntjänstmiljön (inkl. administration).
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Syftet med att begränsa trafiken så att endast nödvändig trafik tillåts i miljön där molntjänsten produceras är att minimera riskerna för angrepp från oskyddade nät och att avgränsa det område som ska skyddas så att det är hanterbart. Syftet med filtreringen mellan olika interna områden är att begränsa skadan av eventuella informationssäkerhetsincidenter (inkl. dataintrång) eller försök till sådana och att hjälpa upptäcka incidenter.
Ytterligare information	Att skärma av databehandlingsmiljöer är en av de mest effektiva åtgärderna i skyddet av sekretessbelagd information. Syftet med avskärmningen är att avgränsa behandlingsmiljön för sekretessbelagd information till en kontrollerbar helhet och i synnerhet att kunna avgränsa behandlingen av sekretessbelagd information till endast tillräckligt säkra miljöer. En korrekt konfigurerad brandvägg eller motsvarande nätverksenhet ska användas för att skärma av utkanten av databehandlingsmiljön. Brandväggen (eller motsvarande nätverksenhet) som används för att skärma av utkanten ska också skyddas mot obehörig åtkomst. För att komplettera och stöda skyddsåtgärderna kan även den så kallade Zero Trust-metoden användas. Med den kan olika aktörers verksamhetsmöjligheter begränsas och övervakas i synnerhet utifrån identifiering och verifiering av aktörer och funktioner. Att kopplingar och konfigurationer fungerar säkert ska kontrolleras regelbundet, jfr MH-01 (Ändringshantering). En lämplig lösning som tryggar tillgången och en tillräcklig dokumentering är ofta att brandväggsreglerna och brandväggskonfigurationerna säkerhetskopieras, och att säkerhetskopiorna förvaras tillräckligt skyddat. Detta krav bör tolkas mot bakgrund av ansvarsfördelningen mellan molnleverantören och kunden. Om avsikten är att få en heltäckande överblick över skyddet av sekretessbelagd information för att bedöma skyddet borde bedömningen i princip omfatta både molnleverantörens och kundens ansvar under informationens hela livscykel. Saker att beakta är bl.a. att molnleverantören i IaaS-lösningar typiskt inte kan ta ställning till säkerheten i de programbrandväggskonfigurationer som kunden har ansvar för. Kunden kan å andra sidan inte påverka skyddet för molnleverantörens IaaS-infrastruktur. Om kunden inte har satt upp en programbrandvägg med den programkomponent som molnleverantören har tillhandahållit kan kunden i vanliga fall endast påverka brandväggsskyddet genom den konfigurering som kunden själv har gjort och hur säker den är. I detta användningsfall bör det därför helst kontrolleras att molnleverantören tar ansvar för säkerheten för sina programkomponenter också i situationer där säkerhetsbrister som har betydelse för skyddet av kundens sekretessbelagda uppgifter upptäcks i komponenterna i fråga. Rekommendationen i sådana situationer är att man också kontrollerar ansvaren för åtgärdande av säkerhetsbrister och skadestånd. Om infrastrukturen eller till exempel trafikfiltreringen är säkerhetsmässigt beroende av programkoden är åtkomst- och versionshanteringen av programkoden ett särskilt viktigt område. Jfr MH-01 (Ändringshantering), MH-02 (Systemutveckling) och IP-03 (Administrativ åtkomst). En lösning som är beroende av programkoden kan med vissa förbehåll möjliggöra en beskrivning av miljön och bedömning av dess säkerhet med versionshanteringen som stöd. Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kundens andel. Kraven lämpar sig i allmänhet direkt för situationer där ett kundsystem som kunden ansvarar för har inrättats i en molnplattform som tillhandahålls med IaaS-servicemodellen.

TT-02	Skydd mot allmänna nätattacker
Krav	1) Det finns en riskbedömning i organisationen som omfattar skydd mot allmänna nätattacker. 2) Skyddet har dimensionerats så att allmänna internetattacker inte äventyrar tjänsten eller konfidentialiteten och integriteten för eller tillgången till den information som behandlas i den.
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Tillgången till informationen som behandlas i tjänsten förhindras inte och deras konfidentialitet eller integritet äventyras inte till följd av allmänna nätattacker.
Ytterligare information	Alla anslutna informationssystem ska behandlas som icke-pålitliga och det ska finnas beredskap för allmänna nätattacker. I beredskapen för allmänna nätattacker ingår till exempel att endast nödvändiga funktioner körs. Med andra ord bör det finnas ett specifikt operativt behov för varje funktion som körs. Funktionaliteten bör begränsas till den snävaste uppsättningen som fyller de operativa kraven (till exempel begränsad synlighet för funktionaliteterna). Viktigt att beakta är också att adressförfalskning (spoofing) förhindras och att nätverkens synlighet begränsas. Särskilt internetgränssnitt bör skyddas bl.a. mot (distribuerade) denial-of-service-attacker (DoS-attacker, överbelastningsattacker). I vissa interna gränsytor kan risken för DoS-attacker ligga inom acceptabla gränser utan särskilt skydd. Detta krav bör tolkas mot bakgrund av ansvarsfördelningen mellan molnleverantören och kunden. I en IaaS-lösning kan molnleverantören till exempel inte ta ställning till bl.a. feltoleransen i kundsystemets applikationslager eller till exempel hur säkert programbrandväggarna som ligger på kundens ansvar är konfigurerade. I en SaaS-lösning har å andra sidan molnleverantören ofta ett omfattande ansvar för bl.a. riskhanteringen när det gäller DoS-attacker.

Delområde 6: Hantering av identitet och tillträde

IP-01	Behörighetshantering
Krav	1) Användarrättigheterna administreras enligt principen om minsta möjliga behörighet: a) Det finns en definierad process för skapande, godkännande och administration av användarkonton. b) Användare av databehandlingsmiljön ska ges endast de uppgifter, rättigheter eller behörigheter som är nödvändiga för uppgifterna som de ska utföra. c) En lista förs över systemanvändarna. Varje beviljad användarrättighet antecknas. d) När användarrättigheter beviljas kontrolleras att personen hör till personalen eller är behörig av annan orsak. e) Det finns direktiv för hantering och beviljande av användarrättigheter. f) Användar- och åtkomsträttigheterna hålls uppdaterade. Onödiga användarkonton och rättigheter tas bort när de inte längre behövs (till exempel när användaren lämnar organisationen eller när ett användarkonto inte har använts under en angiven tid). g) Det finns en klar och fungerande metod för hur man informerar berörda parter om ändringar i personalen, och en fungerande metod för att genomföra ändringarna. h) Användar- och åtkomsträttigheterna granskas regelbundet, åtminstone med sex månaders mellanrum.
Tillämplighet	Nätverksutrustning, servrar, informationssystem, arbetsstationer och andra terminaler.
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Användarrättigheterna administreras enligt principen om minsta möjliga behörighet: Användarkoder beviljas och överlåts endast åt dem som är behöriga och som behöver dem på grund av sin uppgift eller roll. Användarrättigheterna omfattar endast nödvändiga funktionaliteter, program, apparater och nätverk.
Ytterligare information	Det centrala syftet för hanteringen av användarrättigheter är att säkerställa att endast behöriga användare har tillgång till databehandlingsmiljön och den skyddade information som den innehåller. Det rekommenderas att användarrättigheterna baserar sig på ett avtal eller någon annan verifierbar dokumenterad grund (t.ex. anställningsförhållande, avtal om arbete i miljön). Man ska se till att livscykeln för användarnamnen är sådan att endast nödvändiga användarnamn är i kraft och aktiva och att onödiga användarnamn omedelbart avlägsnas. Användarrättigheterna ska begränsas endast till den uppsättning som det funktionella behovet förutsätter. Onödigt omfattande rättigheter ger onödigt stora handlingsmöjligheter för användaren, processen eller ovan beskrivna attackerare. Genom att begränsa användarrättigheterna så att de överensstämmer med principen om minimirättigheter kan riskerna minimeras för både avsiktliga och oavsiktliga gärningar, liksom också för till exempel skadliga program. Särskild uppmärksamhet ska fästas vid att underhållsrättigheter endast används för underhållsåtgärder. Ett användarkonto med underhållskod ska inte användas till exempel för webbläsare eller e-post. För att åtkomsträttigheterna ska vara aktuella förutsätts i allmänhet regelbunden kontroll, till exempel med sex månaders mellanrum, av åtkomst- och användarrättigheterna för alla anställda, leverantörer och externa användare. Vid ändringar i befattningsbeskrivningen och särskilt i samband med att ett anställningsförhållande upphör ska det finnas en tydlig och överenskommen rutin för att ändra och ta bort rättigheterna. Detta kan till exempel ske så att chefen på förhand meddelar ansvarspersonerna om ändringarna, varvid alla rättigheter kan hållas aktuella. Detta kan innebära att användar- och åtkomsträttigheter tas bort/ändras separat i det centraliserade administrationssystemet eller i enskilda system. Kravet bör tillämpas med beaktande av ansvarsfördelningen mellan molnleverantör och kund. I typiska fall är molnleverantören administratör för användarrättigheterna till systemet med vilket molntjänsten produceras, medan kunden administrerar användarrättigheterna för den del av helheten som är förankrad i leverantörens servicekoncept (IaaS, PaaS eller Saas). Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

IP-02	Identifiering av användare
Krav	1) Innan de får åtkomst till skyddad information ska administratörer hos molnleverantören och kunden, som jobbar med molntjänsten, samt användare av tjänsten identifieras och verifieras på tillförlitligt sätt: a) Alla användare har individuella och personliga användar-ID:n. b) Alla användare identifieras och verifieras. c) Identifieringen och verifieringen ska ske enligt en betrodd, pålitlig teknik eller ordnas på annat pålitligt sätt. d) Ett användar-ID ska låsas om identifieringen misslyckas för många gånger efter varandra. e) Administratörskoderna för systemen och applikationerna är personliga. Om detta inte är tekniskt möjligt i alla system eller applikationer måste det finnas överenskommen och dokumenterad hanteringspraxis som gör det möjligt att identifiera användaren för gemensamma användar-ID. f) Verifieringen av användare kräver minst tvåfaktorsautentisering (till exempel lösenord + token). Förbindelsen ska krypteras enligt vad användningssituationen kräver. För detta ändamål ska man företrädesvis använda krypteringslösningar/-protokoll vars tillförlitlighet bygger på validering och standardisering. Jfr SA-01. i. Ett undantag är en situation där verifieringen görs inom ett fysiskt skyddat säkerhetsområde (jfr FT-01) minst med hjälp av lösenord. Om autentisering sker med lösenord ska följande villkor uppfyllas: 1. användarna har fått direktiv om vad som utgör ett säkert lösenord och hur man använder det säkert. 2. det övervakande programmet ställer vissa minimisäkerhetskrav på lösenorden och tvingar användaren att byta lösenord med lämpliga mellanrum. 2) I situationer där förbindelsen går utanför ett fysiskt skyddat säkerhetsområde (jfr FT-01), till exempel mellan molnleverantörens maskinhall och underhållets/kundens terminal, skyddas informationen/datakommunikationen med en myndighetsgodkänd krypteringslösning. 3) Innan de ges åtkomst till skyddad information ska terminaler och system som används av administratörer hos molnleverantören och kunden för att producera molntjänsten identifieras på tillförlitligt sätt.
Tillämplighet	Nätverksutrustning, servrar, informationssystem, arbetsstationer och andra terminaler.
Datatyper	1: Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa) 2-3: SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Endast behöriga användare har åtkomst till information och tjänster.
Ytterligare information	En pålitlig identifiering och autentisering innebär följande: 1) att autentiseringsmetoden är skyddad mot man-i-mitten-attacker (man-in-the-middle), 2) ingen onödig information avslöjas vid inloggning, före autentisering, 3) de identifierande uppgifter som används för autentisering är alltid krypterade om de sänds över nätet, 4) autentiseringsmetoden är skyddad mot återuppspelningsattacker (replay attacks), och 5) autentiseringsmetoden är skyddad mot uttömmande attacker (brute force attacks). I situationer där man vid identifiering i molntjänsten utnyttjar federerad identitetshantering och/eller identitets- och åtkomsthanteringssystem (organisationens egna system eller till exempel system som produceras av molnleverantören) ska särskild uppmärksamhet fästas vid tillförlitligheten hos identifieringstjänsten (Identity Provider, IdP) och attributens förmedlingskedja. För behandling av sekretessbelagd information lämpar sig endast sådana identifieringstjänster som erbjuder en identitet som grundar sig på stark första identifiering och vars attribut kan förmedlas på ett tillräckligt säkert sätt till en tjänst som stöder sig på identifiering (Relying Party, RP eller Service Provider, SP). Eftersom skyddet av sekretessbelagd information i allmänhet är direkt beroende av identifieringstjänstens tillförlitlighet, hör det nästan utan undantag till bedömningen av molntjänstens säkerhet att se till att identifieringstjänsten är säker. Till exempel är det vanligen skäl att bedöma det krypteringstekniska skyddet vid förmedling av attribut i samma riktning som förmedlingen av nycklarna till krypteringslösningen som tillämpas på skyddet av datatypen i fråga (jfr SA-01, SA-02 och SA-03). Av identitetshanteringsmodellerna lämpar sig en organisationsorienterad modell (organization-centric identity management) i allmänhet bättre än till exempel en användarcentrerad modell (user-centric) för att skydda sekretessbelagd information, där man också ska beakta att användaren är bunden till en viss organisation och att säkerhetsutförandet är tillförlitligt. Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

IP-03	Administrativ åtkomst
Krav	1) Administrativ åtkomst sker via avgränsade, kontrollerade och övervakade punkter i molntjänstmiljön (till exempel hoppmaskiner, kontrollportaler och motsvarande). De punkter som möjliggör administrativ åtkomst separeras åtminstone så att molnleverantörens och de olika kundernas kontrollpunkter samt de tjänster som nås via dem är tillförlitligt åtskilda från varandra (jfr JT-03). 2) Administrativ åtkomst förutsätter stark autentisering som baserar sig på minst tvåfaktorsverifiering (t.ex. lösenord + token). 3) Den administrativa trafiken ska krypteras enligt vad användningssituationen kräver. För detta ändamål ska man företrädesvis använda krypteringslösningar/-protokoll vars tillförlitlighet bygger på validering och standardisering. Jfr SA-01. 4) Terminaler med kunddata och andra datamedier (hårddiskar, USB-minnen och motsvarande) som exporteras utanför godkända fysiskt skyddade säkerhetsområden (jfr FT-01) förvaras krypterade enligt användningssituationen. För detta ändamål ska man företrädesvis använda krypteringslösningar vars tillförlitlighet bygger på validering och standardisering, eller också lämnas datamedier inte oövervakade. Jfr SA-01 och FT-01. 5) Det är möjligt att hantera säkerhetsklassificerad myndighetsinformation endast från terminaler och miljöer enligt säkerhetsklassen i fråga samt inom fysiska områden (jfr FT-01). 6) Åtkomst för hantering av säkerhetsklassificerad myndighetsinformation är möjlig endast via fjärranslutning som krypterats med en myndighetsgodkänd metod. 7) Krypteringen av terminaler och andra datamedier som innehåller säkerhetsklassificerad information (hårddiskar, USB-minnen och motsvarande) är myndighetsgodkänd.
Tillämplighet	System som används för fjärradministration av molntjänstmiljön, inkl. till exempel nätverksutrustning, servrar samt arbetsstationer och andra terminaler. Innefattar både molnplattformen och kundsystemet som är förankrat i den.
Datatyper	1–4: Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa) 5–7: SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Den administrativa anslutningen har ett tillräckligt omfattande skydd så att den som använder den inte får obehörig åtkomst till kunddata eller till molntjänsten.
Ytterligare information	I molntjänstmiljöer är fjärradministration vanligtvis den mest typiska administrationsmetoden, både för själva molnplattformen och för kundens system. Som fjärradministration räknas till exempel underhåll utfört av molnleverantören när det sker från utsidan av en fysiskt skyddad datorhall. Som fjärradministration räknas också underhåll som utförs av en kund hos molntjänsten på de systemdelar som kunden ansvarar för. En särskild fråga att beakta då man utvärderar skyddet av en administrativ anslutning är i vilken mån informationen som behandlas i molntjänsten är sårbar via anslutningen i fråga. De flesta administrativa anslutningar ger åtkomst till information, antingen direkt (exempel: den som administrerar en databas kommer vid behov oftast åt innehållet i databasen) eller indirekt (exempel: den som administrerar nätverksenheter kan oftast ändra brandväggsreglerna som skyddar datasystemet). Som administrativa anslutningar räknas i princip alla anslutningar genom vilka det går att påverka skyddet av sekretessbelagd information. Administrativa anslutningar innefattar i typiska fall även webbkonsoler/-portaler och motsvarande administrativa fjärranslutningar som molntjänsten erbjuder sina kunder. När en administrativ anslutning ger direkt eller indirekt åtkomst till sekretessbelagd information är det särskilt viktigt att anslutningen och de använda terminalerna begränsas till att användas på en skyddsnivå som i princip är samma som databehandlingsmiljön i fråga. På grund av den administrativa trafikens säkerhetskritiska natur är det i princip inte möjligt att administrera en miljö som används för behandling av säkerhetsklassificerad information från miljöer eller terminaler med svagare skydd. Administrativ åtkomst till en molnplattform som innehåller säkerhetsklassificerad information ska begränsas till datorer som uppfyller säkerhetsklassens krav. Observera att även administrationslösningar för terminaler och andra bakgrundssystem som är kopplade till dem ska uppfylla kraven för säkerhetsklassen i fråga, liksom även fysiska utrymmen/områden där hanteringen utförs. Vid skydd av terminaler och tillhörande bakgrundssystem (till exempel katalog- och administrationstjänster) ska man särskilt beakta TT-01 (Datanätets struktur), IP-01 (Behörighetshantering), IP-02 (Identifiering av användare), IP-03 (Administrationsförbindelser), JT-01 (Spårbarhet och upptäcktskapacitet), JT-02 (Systemhärdning), JT-04 (Skydd mot skadeprogram), JT-05 (Flytt och förstöring av skyddade objekt), SA-01 (Kryptering och nyckelhantering), SA-02 (Kryptering utanför fysiskt skyddat säkerhetsområde), KT-04 (Hantering av sårbarheter), MH-01 (Ändringshantering) och SI-02 (Förstöring av informationsmaterial). Då terminaler och tillhörande bakgrundssystem skyddas och då skyddet bedöms kan också referensramen Katakri 2015 användas. Som en följd av masseffekten ska man i administrationslösningarna för informationsmängder i säkerhetsklass III dessutom särskilt beakta att de terminaler som används för administrationen är tillförlitligt åtskilda från näten som är kopplade till internet. Tillräcklig spårbarhet kan åstadkommas till exempel med hjälp av en s.k. hoppmaskin så att alla administrativa handlingar genomförs och registreras (loggförs) via hoppmaskinen. Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

Delområde 7: Informationssystemets säkerhet

JT-01	Spårbarhet och upptäcktskapacitet
Krav	1) Organisationen har tillförlitliga spårbarhetsmetoder för händelser av säkerhetsrelevans. Följande är särskilt viktigt: a) De dokument som uppstår är tillräckligt omfattande för verifiering av utförda dataintrång eller försök till sådana. b) Viktiga dokument förvaras i minst 6 månader såvida inte lagstiftningen eller avtalen kräver en längre förvaringstid. c) Logguppgifter och inloggningstjänster skyddas från obehörig åtkomst (administration av användarrättigheter, logisk åtkomstkontroll) enligt principen om lägsta behörighet. d) Metoden med vilken logguppgifter sänds mellan loggkällorna och loggsamlaren är skyddad. Avsändaren och mottagaren identifieras. Logguppgifterna som översänds ska krypteras enligt vad användningssituationen kräver. För detta ändamål ska man företrädesvis använda krypteringslösningar/-protokoll vars tillförlitlighet bygger på validering och standardisering. Jfr SA-01. Logguppgifter kan också överföras via ett särskilt administratörsnätverk. e) Klockor är synkroniserade med en överenskommen tidskälla. f) För datamassa i säkerhetsklass III dessutom: Viktiga dokument förvaras i minst 24 månader såvida inte lagstiftningen eller avtalen kräver en längre förvaringstid. g) För datamassa i säkerhetsklass III dessutom: Viktig logginformation styrs vidare från loggkällorna till en särskild loggsamlare (eller flera). 2) Molnleverantören förser kunden med logguppgifter för de systemkomponenter som ingår i molnleverantörens ansvar på kundens begäran, i den utsträckning de är relevanta för kunden och i ett sådant format att kunden kan undersöka fall av intresse. 3) Molnleverantören erbjuder möjlighet till (ett tekniskt gränssnitt för) informationsutbyte med kunden i realtid för att förmedla händelser med anknytning till säkerheten (logguppgifter, händelseuppgifter, informationssäkerhetsobservationer). 4) Det finns tillförlitliga metoder för upptäckt av säkerhetsincidenter. Följande är särskilt viktigt: a) Det finns ett förfarande för observation av incidenter i insamlade dokument (jfr KT-04), i synnerhet försök att olovligt använda informationssystemet ska kunna observeras. b) Vad som utgör normal nätverkstrafik (trafikvolymer, protokoll och anslutningar) har definierats. c) Det finns en procedur vars syfte är att identifiera händelser som avviker från normal nätverkstrafik (till exempel icke-normala anslutningar eller försök till sådana). d) Det finns en procedur genom vilken avvikelser kan observeras i de servrar och andra objekt (hosts) som hör till molntjänsten. e) För datamassa i säkerhetsklass III dessutom: Det finns en procedur genom vilken man försöker upptäcka försök att obehörigen få tillgång till en större del av informationsinnehållet. 5) Det finns en procedur för återställande av normaliteten efter upptäckta incidenter.
Tillämplighet	Den levererade tjänstens säkerhet i övergripande mening
Datatyper	1a–e, 2-3, 4a–d, 5: Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa) 1f-g, 4e: SK III (datamassa)
Mål för skyddet	Att upptäcka och utreda olovlig ändring av uppgifter och annan olovlig eller obehörig behandling av uppgifter, medräknat att undersöka dataintrång och att fungera som stöd då återställande åtgärder planeras.

JT-01	Spårbarhet och upptäcktskapacitet
Ytterligare information	Spårbarhet avser att händelser i systemmiljön dokumenteras så att man i händelse av en incident kan utreda vad som gjorts i miljön, vem som gjort det och vilka konsekvenserna har varit. Typiskt viktiga dokument är logguppgifterna för viktiga nätverksenheter och servrar. Samma gäller väldigt ofta logguppgifterna för till exempel datorer och motsvarande. Omfattningen kan i de flesta fall tillgodoses så att man säkerställer att loggföringen är aktiverad åtminstone i datorer, servrar, nätverksenheter (särskilt brandväggar, medräknat datorernas programbrandväggar) och motsvarande enheter. Viktigt är också att man med hjälp av loggarna för nätverksenheterna kan utreda vilka administrativa åtgärder som har utförts på dem, när de har utförts och vem som har utfört dem. Det bör föras händelseloggar över systemets funktion, användaraktivitet, händelser av säkerhetsrelevans och incidenter. Det rekommenderade sättet att säkra loggarna är att viktig logginformation styrs till en eller flera starkt skyddade loggservrar som säkerhetskopieras regelbundet. En rekommendation med tanke på administratörernas rättskydd och undersökningen av misstänkta dataintrång är att funktionen att administrera logguppgifter åtskiljs från övriga administrationsfunktioner. Det är också viktigt att programvaran som lagrar och övervakar logguppgifter övervakas för att säkerställa att den fungerar korrekt. Behoven i användningsfallet i fråga ska beaktas i förvaringstiderna för logguppgifterna. Till exempel i myndighetsverksamhet kan straffrättsliga preskriptionstider vanligen leda till förvaringstider på minst fem år. I de flesta miljöer krävs det i praktiken automatiserade observations- och larmverktyg för att missbruk ska upptäckas. Att granska logguppgifterna manuellt räcker i allmänhet till bara i miljöer där loggvolymerna är mycket små och det finns tillräckliga personresurser att anvisa för detta ändamål. För att återställa en databehandlingsmiljö till skyddad status inom rimlig tid krävs det vanligtvis planerade och beskrivna processer och tekniska metoder som körts in genom utbildning och inövning. Det finns många olika sätt att övervaka nätverkstrafik och begränsa effekterna av upptäckta attacker, allt från övervakning vid viktiga nätverksnoder till sensorer på enskilda datorer och servrar, och kombinationer av dessa. Oberoende av vilken nätverksenhet och vilka leverantörer som används måste man känna till vad som utgör normal status i nätverkstrafiken för att kunna övervaka denna i praktiken. Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

JT-02	Systemhärdning
Krav	1) Detta tillvägagångssätt innebär att systemen installeras enligt ett systematiskt mönster så att slutresultatet är en härdad installation. 2) En härdad installation innehåller endast sådana komponenter, tjänster, användarrättigheter och processrättigheter som är nödvändiga för att driftskraven ska uppfyllas och säkerheten kunna garanteras.
Tillämplighet	Hårdvara och mjukvara som används för att producera molntjänsten. Om det som behandlas är säkerhetsklassificerad myndighetsinformation ingår även de använda terminalerna med tillhörande back-end-system (t.ex. kataloger).
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Att sänka risken för programfel och felkonfigurationer genom att onödiga funktionaliteter tas bort.
Ytterligare information	Det har visat sig vara svårt att skapa en säker programkod. Ju mer programkod en miljö innehåller, desto fler är möjligheterna till programfel, dvs. sårbarheter. Ju fler tjänster det finns som är beroende av programkodens säkerhet, desto sannolikare är det att tjänsterna innehåller sårbarheter. Riskerna kan sänkas genom att den sårbara ytan minskas, det vill säga genom att endast nödvändiga tjänster exponeras för möjligheten till attack. Det är vanligt att system är fulla till bredden av funktionaliteter. Dessa är oftast förinställt aktiverade och lätta att ta i bruk, men med inställningar som brukar vara onödigt osäkra. Genom att låta onödiga funktionaliteter vara kvar gör man dem tillgängliga för illvilliga aktörer, och genom att tjänster som är nödvändiga tillåts ha onödigt osäkra inställningar blir också dessa tillgängliga för sådana aktörer. Förinställningarna i ett system inbegriper ofta till exempel administratörslösenord, färdigt installerade onödiga program och onödiga användarkonton. Att härda ett system betyder allmänt att inställningarna ändras så att systemet blir mindre sårbart. Den allmänna regeln är att endast väsentliga funktioner, enheter och tjänster i systemet ska vara aktiverade. Till automatiska processer ska man endast ge de uppgifter, rättigheter eller behörigheter som är nödvändiga för att de ska kunna utföra sin uppgift. På så sätt begränsas den möjliga skadan av olyckor, fel eller obehörig användning. Ofta går det att använda verktyg för konfigurationshantering för härdning och underhåll av den härdade installationen. Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

JT-03	Åtskild information
Krav	1) Kundernas sekretessbelagda information som förvaras i gemensamma virtuella och fysiska system hålls tillförlitligt åtskilda från varandra.
Tillämplighet	Nätverksapparater, virtualiseringsplattformar, lagringssystem, minnen, överföringsmedier och motsvarande som används för behandling av sekretessbelagda kunddata.
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Endast kunden som äger den sekretessbelagda informationen har tillgång till den.
Ytterligare information	Den logiska och/eller fysiska åtskillnadslösning som används måste vara tillräckligt tillförlitlig. En vanlig åtskillnadslösning för till exempel gemensamma nätverksenheter och lagringssystem är kryptering. Kryptering av datatrafik (data-in-transit) och kryptering vid lagring (data-at-rest) utförs med kundspecifika nycklar och är ett pålitligt skydd också för andra ändamål, till exempel säker förstöring av enheter. Jfr SA-03 (Kryptering innanför ett fysiskt skyddat säkerhetsområde) och KT-03 (Säkerhets- och returprocesser). Om samma maskinvara används för att behandla flera kunders information samtidigt måste man säkerställa att en tillräcklig fysisk och logisk åtskillnad görs mellan de olika kundernas information. Om detta inte kan säkerställas i tillräcklig grad måste separata fysiska enheter användas för behandlingen. Till exempel kan säkerhetsklassificerad information förvaras fysiskt på en egen virtualiseringsplattform där endast personer som har behörighet att behandla säkerhetsklassificerad information har tillgång exempelvis till gränssnitt där processorsårbarheter kan förekomma. Om samma enheter används för att behandla flera kunders uppgifter så att behandlingen inte sker samtidigt måste man även säkerställa att den föregående kundens uppgifter har tagits bort på ett tillräckligt säkert sätt (inbegripet alla delar, BIOS, cacheminnen i andra enheter). Om detta inte kan säkerställas i tillräcklig grad måste separata fysiska enheter användas för behandlingen. Jfr SI-02 (Förstöring av informationsmaterial). Ägare av säkerhetsklassificerad, sekretessbelagd information kan förbehålla sig rätten att granska alla nätverk/system där deras data behandlas. Granskning kräver ofta fysisk och logisk åtkomst, vilket innebär att granskaren tekniskt sett har möjlighet att komma åt den information som behandlas i systemet. Om information som tillhör flera olika ägare måste behandlas i samma miljö är det särskilt viktigt att nätverket/systemet är upplagt så att granskning kan utföras utan att man kommer åt information som tillhör andra. I leveransformerna IaaS och PaaS i synnerhet måste åtskillnaden av den sekretessbelagda informationen säkerställas med hjälp av separata nätverk eller virtuella eller programbaserade lokala nätverk som krypteras. Jfr SA-03 (Kryptering innanför ett fysiskt skyddat säkerhetsområde).

JT-04	Skydd mot skadeprogram
Krav	1) Molntjänsten, inbegripet systemmiljöerna som används för att administrera den, förses med tillförlitliga lösningar för förebyggande, förhindrande och upptäckt av, samt försvar mot skadlig programvara, och för återställande av systemet.
Tillämplighet	Systemen som används för att producera molntjänsten, inbegripet de systemmiljöer som används för att administrera den.
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Kundinformationen är tillräckligt skyddad i fråga om integritet, konfidentialitet och tillgänglighet mot de vanliga riskerna förknippade med skadeprogram.
Ytterligare information	Systemen kan skyddas mot skadeprogram till exempel genom härdning (jfr JT-02), med avgränsningar av användarrättigheter (jfr IP-01), genom att hålla systemen på nivån för säkerhetsuppdateringar (jfr CT-04), med kapacitet att observera avvikelser (jfr JT-01), genom att se till att personalen har säkerhetsmedvetenhet (jfr HT-04) och även genom att använda program för bekämpning av skadliga program. Riskerna kan också minskas genom att sårbara miljöer skiljs åt från produktionsmiljöerna och regler definieras för användning av bl.a. flyttbar media (t.ex. USB-minnen). Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde. Till exempel om det är möjligt att ladda ner filer i ett kundsystem som kunden har ansvar för, finns det vanligtvis riskhanteringsmässiga grunder för skydd mot skadliga program.

JT-05	Flytt och förstöring av skyddade objekt
Krav	1) Enheter, programvara, överföringsmedier och motsvarande får inte flyttas utanför fysiskt skyddade lokaler utan ett specifikt tillstånd för ändamålet. 2) Flytt och behandling som sker utanför fysiskt skyddade lokaler måste ske enligt de regler (den klassificering) som gäller för skyddsobjektet i fråga. 3) När sekretessbelagda kunddata flyttas utanför ett fysiskt skyddat säkerhetsområde (jfr FT-01) är informationen krypterad (jfr SA-02) eller skyddsobjektet står under fortlöpande övervakning av molnleverantörens personal. 4) För skydd av säkerhetsklassificerad myndighetsinformation används myndighetsgodkända krypteringsmetoder, -styrkor och -produkter (jfr SA-01).
Tillämplighet	Enheter som innehåller kunddata.
Datatyper	1–3: Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa) 4: SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Skyddade kunddata äventyras inte i situationer där de flyttas utanför fysiskt skyddade områden (till exempel maskinhallar).
Ytterligare information	Viktigt: • Att informationen raderas på ett säkert sätt och datamediet förstörs, jfr SI-02 (Förstöring av informationsmaterial) • Datamedierna som flyttas krypteras • Informationen flyttas till ett nytt datamedium när det gamla ska ersättas Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att om sekretessbelagd och/eller säkerhetsklassificerad information överförs från en del som hör till kundens ansvar exempelvis till eller från kundens terminaler, ska informationen/datakommunikationen vara krypterad tillräckligt tillförlitligt.

Delområde 8: Kryptering

SA-01	Kryptering och nyckelhantering
Krav	1) Det finns planerade, införda och beskrivna krypteringsregler och hanteringsprocesser för krypteringsnycklar. 2) Endast behöriga användare och processer har krypteringsnycklarna. Processerna förutsätter minst a) kryptografiskt starka nycklar, b) säker nyckelutdelning, c) säker nyckelförvaring, d) regelbundna nyckelbyten, e) utbyte av gamla eller avslöjade nycklar, och f) att obehöriga nyckelbyten har förhindrats. 3) För skydd av säkerhetsklassificerad myndighetsinformation används myndighetsgodkända krypteringsmetoder, -styrkor och -produkter.
Tillämplighet	Direkt eller indirekt skydd av kunddata i situationer där skyddsmetoden är kryptering.
Datatyper	1–2: Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa) 3: SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Krypteringsmetoderna ger ett tillräckligt skydd.
Ytterligare information	I synnerhet om trafiken går via ett offentligt eller något annat mindre skyddat nät är kryptering ofta det enda sättet att skydda konfidentialiteten och vanligen också integriteten hos sekretessbelagd information. Eftersom det ofta är ytterst utmanande att ersätta eventuella brister i krypteringen med annat skydd, ska särskild uppmärksamhet fästas då krypteringslösning väljs och att den används på ett säkert sätt. Det är skäl att beakta att krypteringen i synnerhet inom molntjänster ofta även har en roll i skilja åt olika kunders information (jfr JT-03) i gemensam infrastruktur samt till exempel i att förstöra information (jfr SI-02) på ett tillförlitligt sätt. Särskilt när det gäller skyddet av säkerhetsklassificerad information betonas vikten av att använda krypteringslösningar för vilka det finns tillförlitliga bevis på säkerheten. Flera olika faktorer måste tas i beaktande då krypteringslösningar jämförs. Förutom krypteringsstyrkan som måste vara den rätta och krypteringslösningen som måste fungera ska man ska beakta hotnivån i användningsmiljön i fråga. I trafik som sker till exempel över internet är hotnivån en helt annan än i trafik inom ett kontrollerat och skyddat fysiskt område (till exempel trafik mellan två säkerhetsområden via ett administrativt område). Andra faktorer att beakta i valet av krypteringslösning är till exempel användningsfallet och vilka kraven är i fråga om sekretesstid och integritet. Olika informationsmaterial innebär olika risker. Till exempel kan man generellt anse att säkerhetsklassificerad myndighetsinformation ska skyddas med den nationella säkerheten (det allmänna bästa) i åtanke. Det kan dessutom antas att säkerhetsklassificerad information intresserar andra aktörer än till exempel personuppgifter som inte omfattas av någon säkerhetsklass. Skillnaderna i risker bör beaktas även i valet av krypteringslösningar. Krypteringens skyddande effekt kan gå helt eller delvis förlorad om obehöriga har möjlighet att utnyttja svagheter i nyckelhanteringen. Rutinen för hantering av krypteringsnycklarna ska vara planerad, utförd och beskriven/instruerad. Särskilt när det gäller krypteringslösningarna ska även säkerheten i leveranskedjorna beaktas. Även om krypteringslösningen är tillräckligt säker till exempel hos leverantören av den, kan brister i leveranskedjan möjliggöra manipulation av krypteringslösningen och därmed leda till att en osäker krypteringslösning införs i informationssystemet eller tjänsten. Jfr SA-02 (Kryptering utanför ett fysiskt skyddat säkerhetsområde) och SA-03 (Kryptering innanför ett fysiskt skyddat säkerhetsområde). Cybersäkerhetscentret har mer information. Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

SA-02	Kryptering utanför ett fysiskt skyddat säkerhetsområde
Krav	1) När sekretessbelagda kunddata flyttas utanför godkända fysiska säkerhetsområden (till exempel leverantörens maskinhall, jfr FT-01) eller via ett nätverk med lägre säkerhetsnivå, ska informationen krypteras enligt vad användningssituationen kräver. För detta ska man företrädesvis använda krypteringslösningar/-protokoll vars tillförlitlighet bygger på (validering och) standardisering. Jfr SA-01. 2) Överföringen ska ordnas så att mottagaren verifieras eller identifieras på ett tillräckligt säkert sätt innan mottagaren får tillgång till den sekretessbelagda informationen. 3) Kryptering av säkerhetsklassificerad myndighetsinformation ska utföras enligt den metod som myndigheten i fråga har godkänt (jfr. SA-01).
Tillämplighet	Krypteringslösningar mellan datorhallar, krypteringslösningar för trafik över nätverk med svagare skydd.
Datatyper	1–2: Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa) 3: SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Konfidentialiteten eller integriteten för kunddata äventyras inte i situationer där den överförs via osäkra nätverk.
Ytterligare information	Internet, MPLS-nätverk som operatörer erbjuder och bl.a. svart fiber (dark fiber) tolkas som offentliga nätverk. Då man använder radiogränssnitt över ett trådlöst nätverk (t.ex. WLAN, 4G) tolkas det som att man lämnar det fysiskt skyddade säkerhetsområdet. Det är alltså jämförbart med att sända data över ett offentligt nät, vilket är viktigt att beakta särskilt när informationen krypteras. Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

SA-03	Kryptering innanför ett fysiskt skyddat säkerhetsområde
Krav	1) När sekretessbelagda kunddata flyttas utanför ett fysiskt skyddat säkerhetsområde (jfr FT-01) och innanför ett nät av överensstämmande säkerhetsgrad kan kryptering på lägre nivå eller icke-krypterad överföring användas om informationen kan skyddas i tillräcklig grad med fysiska metoder. Jfr JT-03. 2) Om gemensam utrustning används ska sekretessbelagda kunddata krypteras innan de sparas i molntjänsten. Jfr JT-03. 3) Krypteringsnycklarna ska åtskiljas kundspecifikt. 4) Kryptering av säkerhetsklassificerad myndighetsinformation ska utföras enligt den metod som myndigheten i fråga har godkänt (jfr. SA-01).
Tillämplighet	Alla miljöer i molntjänsten där kunddata behandlas, inbegripet till exempel diskbaserade lagringssystem och lösningar för säkerhetskopiering.
Datatyper	1–3: Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa) 4: SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Att förstärka det skydd som åstadkoms via åtskillnad av olika kunders data. Används i situationer där olika kunders data behandlas på enheter som är i gemensam användning. Ett flernivåförsvar som är till stöd för säkerheten över informationens hela livscykel.
Ytterligare information	2: Gäller inte metadata som har samband med fakturering eller annan administration av kundrelationen. Viktigt att komma ihåg är att molnleverantören i vanliga fall har tillgång till data som behandlas i tjänsten och som under någon del av sin livscykel är okrypterad (till exempel i form av en bild som visas för kunden). System baserade på egna nycklar dvs. BYOK (Bring Your Own Keys) eller på att maskinvaran i molnleverantörens fysiska datorhall förses med särskilda säkerhetsmoduler (HSM, Hardware Security Module) är exempel på lösningar som begränsar molnleverantörens åtkomst till den data som behandlas i tjänsten, men de hindrar den inte i typiska fall. Man kan dock använda kryptering som kompletterande skydd, till exempel tillsammans med åtskillnad av kunddata, förstöring av skyddsobjekt eller åtskillnad av funktioner. Jfr JT-03 (Åtskild information). Kryptering är ofta att rekommendera i synnerhet som komplement till skalbarhet och åtskillnad av kunddata. I bedömningen av kundens ansvarsområde rekommenderas att man särskilt beaktar att i flera molntjänster är det delvis kunden som ansvarar för krypteringen av kunddata och som kan konfigurera den.

Delområde 9: Användarsäkerhet

KT-01	Systembeskrivning till stöd för kontinuitet och driftssäkerhet
Krav	1) Det finns heltäckande systembeskrivningar av molntjänsten och direktiv för ett säkert underhåll och en säker administration av tjänsten. Beskrivningarna och direktiven är så väl gjorda att man baserat på dem tillförlitligt kan undvika driftsfel och vara säker på att tjänsten kan återställas efter incidenter på ett sätt som tillgodoser avtalsförpliktelserna. 2) Systembeskrivningarna och direktiven hålls aktuella. 3) Systembeskrivningarna och anvisningarna är bekanta och tillgängliga för personalen i enlighet med respektive roller.
Tillämplighet	Molntjänsten i sin helhet.
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Att driftsfel ska kunna undvikas och att det ska finnas beredskap för återställning efter incidenter i överensstämmelse med avtalsvillkoren.
Ytterligare information	I situationer där en viktig systemkomponent får ett fel är det särskilt viktigt att det finns tillräckligt omfattande systembeskrivningar som stöd till reparationsarbetet. Beskrivningarna ska finnas tillgängliga för de personer som behöver dem för att återställa normalläget. Beskrivningarna är också till stöd i situationer där nyckelpersoner är förhindrade från att reparera felet i samband med en incident. Beskrivningar och direktiv av tillräcklig omfattning är viktiga också i situationer där kunden eller en tredje part med fullmakt av kunden ska underhålla eller utveckla det kundsystem som drivs på molnplattformen. Det går också att ha automatiserade felreparationsfunktioner (till exempel omstart av containrar) som stöd för kontinuiteten. Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

KT-02	Administration av kapacitet
Krav	1) Molntjänstens kapacitet dimensioneras så att den servicenivå som överenskoms i serviceavtalen kan erbjudas tillförlitligt. Dimensioneringen görs utifrån bl.a. en uppföljning av kapacitetsbehovet och prognoser av kommande kapacitetsbehov. 2) Molnleverantören ska se till att kunden kan följa upp användningen av systemresurserna (t.ex. databehandlings- eller lagringskapacitet).
Tillämplighet	Molntjänsten i sin helhet.
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Målet är att en servicenivå enligt serviceavtalen ska kunna tryggas.
Ytterligare information	Uppföljningen av kapacitetsbehovet utgör ett stöd för att optimera resursanvändningen, bedöma framtida behov och tillgodose skyldigheterna i servicenivåavtalen.

KT-03	Säkerhets- och returprocesser
Krav	1) Det finns planerade, genomförda, testade och beskrivna processer för säkerhetskopiering och återskapande som en del av kontinuitetsplanen, för att säkra att förpliktelserna enligt serviceavtalen och lagen samt de övriga affärsmässiga kraven som ställs på molntjänsten kan tillgodoses. Viktigt: a) Att säkerhetskopieringsfrekvensen är tillräcklig med hänsyn till hur kritisk informationen är. Detta förutsätter klarhet i hur mycket data man kan tillåta sig att förlora (recovery point objective, RPO). b) Återskapandeprocessen är tillräckligt snabb med hänsyn till kraven på verksamheten. Detta förutsätter klarhet i hur lång tid man kan tillåta att återskapandet tar (recovery time objective, RTO). c) Säkerhetskopieringen och återskapandeprocessen testas regelbundet. d) Den fysiska förvaringsplatsen för säkerhetskopiorna är åtskild i tillräcklig grad från själva systemet (skilda ras-/brandutrymmen, avstånd mellan säkerhetskopian och det egentliga utrymmet). 2) Säkerhetskopiorna skyddas under hela deras livscykel med metoder som motsvarar åtminstone den skyddsnivå som den ursprungliga informationen har haft. En stor mängd information kan innebära att ett starkare skydd behövs (masseffekten). Viktigt: a) Tillgången till säkerhetskopior har begränsats enligt principen om minsta behörighet så att endast godkända personer eller roller har tillgång till dem. b) Säkerhetskopierings- och återskapandeprocesserna är spårbara (de loggförs) och övervakas så att otillåtna åtgärder (till exempel obehörigt återskapande) upptäcks i mån av möjlighet. c) Om säkerhetskopior förvaras på en annan fysisk plats har denna åtminstone motsvarande fysisk och logisk åtkomstkontroll. d) I situationer där säkerhetskopior flyttas utanför ett fysiskt skyddat säkerhetsområde (jfr FT-01), till exempel till en annan av molnleverantörens maskinhallar, eller via nätet, ska informationen krypteras enligt vad användningssituationen kräver. För detta ska man företrädesvis använda krypteringslösningar/-protokoll vars tillförlitlighet bygger på validering och standardisering. Jfr SA-02 och SA-03. e) I situationer där säkerhetskopior flyttas utanför ett fysiskt skyddat säkerhetsområde (jfr FT-01) med ett överföringsmedium (t.ex. säkerhetsband eller -diskar), flyttas överföringsmedierna under konstant övervakning. Kryptering är att rekommendera för överföringsmediet eller informationen som den innehåller. f) Säkerhetsmedierna förstörs på ett tillförlitligt sätt (jfr SI-02). 3) Även följande bör observeras när det är fråga om säkerhetskopior som innehåller säkerhetsklassificerad myndighetsinformation: a) I situationer där säkerhetskopior flyttas utanför ett fysiskt skyddat säkerhetsområde (jfr FT-01), till exempel till en annan maskinhall som är molnleverantörens, via nätet, skyddas informationen/datakommunikationen med en myndighetsgodkänd krypteringslösning. b) Om samma säkerhetskopieringsmetod används för information som tillhör olika ägare måste abonnemangen till säkerhetskopieringssystemet och lagringsmediet hållas åtskilda (till exempel genom kryptering och/eller fysiskt separata lagringssystem och -medier). Jfr JT-03 och SA-03.
Tillämplighet	Molntjänstens processer för säkerhetskopiering och återskapande. Obs! Det finns fall där vissa processer är beroende av hur kundsystemet är upplagt, vilket bör beaktas.
Datatyper	1–2: Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa) 3: SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Att skydda kundinformationens tillgänglighet, integritet och konfidentialitet i samband med säkerhetskopiering och återskapande.
Ytterligare information	Man kan också köra automatiserade tester av återskapandeprocesserna, till exempel en gång i veckan. Återskapad information ska skyddas med minst motsvarande skydd som den ursprungliga informationen. SI-02). Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde. I vissa användningsfall kan det till exempel utifrån behovet av beredskap vara motiverat att den information och/eller infrastruktur som behandlas i kundsystemet säkrats/kopierats även i en miljö som helt administreras av kunden.

KT-04	Hantering av sårbarheter
Krav	1) Molntjänsten förses med tillförlitliga metoder för hantering av programsårbarheter som överspänner tjänstens hela livscykel. Viktigt: a) Molnleverantören följer med myndigheternas, maskin- och programtillverkarnas och motsvarande instansers informationsbrev om säkerhet och utför kontrollerad installation av de säkerhetsuppdateringar som bedöms vara nödvändiga baserat på en riskanalys (jfr MH-01). b) En automatisk systemkontroll för att upptäcka kända sårbarheter ska köras minst varje månad. Om man har avvikit från de planerade inställningarna eller den planerade säkerhetsuppdateringsnivån ska orsakerna analyseras och avvikelserna rättas till eller dokumenteras i enlighet med hanteringsprocessen för incidenter (se TJ-04). c) Komponenter som är kritiska för säker drift av molntjänsten ska kontrolleras regelbundet, åtminstone en gång om året, genom penetrationstester utförda av en utomstående part. Avsevärda fel ska rättas till omedelbart. d) Molnleverantören informerar sina kunder om betydande sårbarheter och hur de påverkar skyddet för kundernas data. Informationen är särskilt viktig i situationer där åtgärder förutsätts av både molnleverantör och kund för att hantera sårbarheterna.
Tillämplighet	Program- och maskinvaran som ingår i molntjänsten.
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Att hålla riskerna kopplade till programsårbarheter på acceptabel nivå.
Ytterligare information	Det har visat sig vara svårt att skapa en säker programkod. I många typer av angrepp ingår utnyttjande av programfel, dvs. sårbarheter. Ansvarsfulla leverantörer rättar till de sårbarheter som hittas i deras programvara. Riskerna kan minskas genom att man installerar reparationer. Att hantera sårbarheter är bl.a. att ha program- och systemmiljön under kontinuerlig övervakning och utveckling så att de reparationer som programleverantörerna kommer med för att åtgärda upptäckta sårbarheter kan installeras så snabbt som möjligt. Det stöd som leverantörerna kommer med för de använda programversionerna är också viktigt. För föråldrade programversioner publiceras inga regelbundna uppdateringar vilket gör det omöjligt att åtgärda sårbarheter i programvaran. När man åtgärdar sårbarheter måste man tänka på hur reparationerna påverkar servicen. Om reparationerna innebär ett serviceavbrott för kunden bör det helst utföras vid en tidpunkt som är minst oläglig eller under ett i förväg överenskommet serviceavbrott. Om man vill försäkra sig om att uppdateringarna inte förorsakar oväntade ändringar i tjänsten kan man testa reparationerna, till exempel i en testmiljö. Aktiva åtgärder för hantering av sårbarheter är • att fastställa ansvaren och arbetsfördelningen i fråga om reparation av sårbarheter, • att följa med systemutvecklingen och informationssäkerheten för de program som används för att producera servicen, och • att ha rutiner för fortlöpande övervakning, t.ex. kontinuerlig skanning av den egna miljön för att upptäcka kända sårbarheter. B: En granskning omfattar alla system med gränssnitt till helheten. Granskningen kan bygga på till exempel automatiserade sårbarhetsskanningar eller konfigurationshanteringsdatabaser (CMDB, configuration management database). Säkerhetsuppdateringar kan också köras baserat på en gyllene kopia (golden image) som är en tillförlitlig skivavbildning av t.ex. de virtuella datorerna försedd med alla de senaste säkerhetsuppdateringarna. Avbildningen används i detta fall regelbundet för att helt återskapa de virtuella datorerna. I denna lösning är det särskilt viktigt att det finns ordentliga rutiner för att säkra att skivavbildningen bibehåller sin integritet. Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

Delområde 10: Flyttbarhet och kompatibilitet

SI-01	Flyttbarhet och kompatibilitet
Krav	1) API:na (Application Programming Interface) för programmeringsgränssnitten i molntjänsten är publicerade så att det finns möjlighet till kompatibilitet med olika programkomponenter och program. 2) Molntjänsten stöder de vanligaste lösningarna för överföring av programvara (till exempel Open Virtualization Format, Docker, Kubernetes eller motsvarande). 3) Molnleverantören erbjuder ett tekniskt gränssnitt eller någon annan metod för att tillhandahålla kundens information i en för kunden lämplig, användbar och allmänt kompatibel form. Formaten har beskrivits i tillräcklig detalj i de avtal som ingås med kunden. 4) För import och export av data samt administration av tjänsten används säkra, etablerade nätverksprotokoll så att konfidentialiteten, integriteten och tillgängligheten är säkrad. 5) Vid överföring av säkerhetsklassificerad myndighetsinformation används myndighetsgodkända krypteringslösningar.
Tillämplighet	Molntjänsten i sin helhet.
Datatyper	1–4: Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa) 5: SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Kunder kan byta molnleverantör och använda flera olika molnleverantörer för sin service. Konfidentialiteten, integriteten eller tillgången till kunddata äventyras inte när sådana data överförs.
Ytterligare information	I situationer där servicen som är förankrad i molntjänsten använder molnplattformens egenskaper bör flyttbarhetskravet övervägas från fall till fall. A priori är det dock alltid motiverat att kräva att kunddata (till exempel kundregister lagrade i en databas) ska kunna flyttas i ett maskinellt lättbehandlat format. När kundens ansvarsområde bedöms rekommenderas att man särskilt beaktar krypteringen av data/datakommunikation i situationer där sekretessbelagd information importeras/exporteras till/från tjänsten.

SI-02	Förstöring av informationsmaterial
Krav	1) Informationsmaterial förstörs på ett tillräckligt tillförlitligt sätt. 2) Då det gäller sekretessbelagd information ska förstöringen omfatta alla delar av livscykeln under vilka informationen har funnits i molntjänsten. 3) Särskilt i följande fall krävs en tillförlitlig metod för förstöring av sekretessbelagda kunddata: a) Om kunden begär att informationen förstörs. b) När avtalet med kunden upphör. c) I samband med service, underhåll eller byte av enheter (till exempel då en trasig disk som innehåller sekretessbelagda kunddata byts ut). 4) Då säkerhetsklassificerat informationsmaterial förstörs används metoder som förhindrar att uppgifter helt eller delvis kan återställas.
Tillämplighet	Lagringsmedia och motsvarande som har innehållit sekretessbelagda data som tillhör kunden.
Datatyper	1–3: Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa) 4: SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Att bibehålla konfidentialiteten för sekretessbelagda kunddata i situationer där lagringsmedier och motsvarande system som använts för att behandla kundinformationen tas ur bruk, eller kundinformationen måste tas bort från molntjänsten av annan orsak.
Ytterligare information	**Hur tillförlitlig förstöringen är** Placeringen av olika informationsmaterial i molntjänsten under sin livscykel påverkar i hög grad hur tillförlitlig förstöringen av materialen är. Att till exempel tillförlitligt förstöra säkerhetsklassificerat informationsmaterial som har lagrats i klartext kan förutsätta att lagringsmedierna förstörs fysiskt. Tillförlitlig förstöring kan också förutsätta att informationsmaterialets fysiska och logiska placering kan utredas under informationsmaterialets livscykel. Om sekretessbelagd information som inte omfattas av säkerhetsklassificering däremot har sparats i molntjänsten i en krypterad form som bedöms vara endast tillräckligt tillförlitlig (jfr SA-03: Kryptering innanför ett fysiskt skyddat säkerhetsområde), kan restriskerna vara godtagbara om nyckeluppsättningen som använts för krypteringen tillförlitligt kan förstöras. Metoden kan även vara till nytta då personuppgifter förstörs efter den lagstadgade förvaringstiden. **Förstöring genom att strimla** Dokument kan strimlas till exempel enligt följande: – papper strimlas till en remsstorlek på högst 30 mm2 (DIN 66399/P5 eller DIN 32757/DIN 4), – hårddiskar strimlas till en storlek på högst 320 mm2 (DIN 66399/H-5), – SSD-diskar och USB-minnen strimlas till en storlek på högst 10 mm2 (DIN 66399/E-5), och – optisk media hårddiskar strimlas till en storlek på högst 10 mm2 (DIN 66399/O-5), Om ovan nämnda dimensioner används kan det strimlade avfallet slängas med det övriga kontorsavfallet. **Förstöring genom överskrift** Minnesområden med sekretessbelagda kunddata kan förstöras genom överskrivning. Viktigt att komma ihåg är att den valda överskrivningsmetoden måste vara lämplig för lagringsmediet i fråga och att processen samt ansvaren måste vara definierade. Cybersäkerhetscentret ger närmare anvisningar på finska för hur elektroniska dokument ska förstöras i följande direktiv: (www.ncsa.fi > Ohjeita > ”Kiintolevyjen elinkaaren hallinta - Ylikirjoitus ja uusiokäyttö”). **Förstöring genom att kombinera olika metoder** Förstöring kan kompletteras med andra metoder som säkerställer att informationen inte kan återställas (till exempel att strimlade dokument bränns eller att hårddiskar smälts ner). En annan faktor som påverkar hur lätt det är att återställa data är hur mycket strimlat avfall som kommer i utomstående händer. Kryptering är också en lösning som avsevärt sänker riskerna för sekretessbelagd information i olika faser av informationens och behandlingsenheternas livscykel. **Viktigt vid förstöring av elektroniskt material** I fråga om elektroniskt material är det särskilt viktigt att tillförlitlig förstöring utförs på alla anläggningar där sekretessbelagd information har lagrats under sin livscykel. Särskilt då delar av anläggningarna (hårddiskar, minnen, minneskort osv.) tas ur bruk, skickas på service eller återanvänds måste all sekretessbelagd information i dem förstöras på ett tillförlitligt sätt. Om det inte är möjligt att genomföra en tillförlitlig tömning (till exempel överskrivning godkänd av myndigheten) får delen som innehåller sekretessbelagd information inte överlämnas åt tredje man. I situationer där anläggningens minne eller motsvarande inte kan tömmas på ett tillförlitligt sätt före enheten överlämnas till tredje man för service bör servicearbetet övervakas i syfte att säkerställa att sekretessbelagd information inte kommer i utomstående händer i samband med servicen. Jfr möjligheterna till kryptering för att minska restriskerna (SA-03: Kryptering innanför ett fysiskt skyddat säkerhetsområde). Vid bedömningen av kundens ansvarsområde rekommenderas att man särskilt beaktar att om förstöringen till vissa delar stöder sig på kryptering, ska krypteringsnycklarna förstöras tillräckligt tillförlitligt.

Delområde 11: Ändringshantering och systemutveckling

MH-01	Ändringshantering
Krav	1) Det finns en rutin för hantering av ändringar som görs i molntjänsten. Rutinen tar hänsyn till de relevanta säkerhetsaspekterna. Ändringshanteringen beaktar också överensstämmelse med kraven (jfr TJ-07) samt avtalsförpliktelser. 2) Riskerna kopplade till ändringarna analyseras och godkänns av de relevanta instanserna. 3) Ändringar testas innan de införs i produktionsmiljö. 4) Testmiljöerna är åtskilda från produktionsmiljöerna. 5) Tester planeras och genomförs så att de ger en tillförlitlig bild av konsekvenserna av ändringar innan de tillämpas i produktionsmiljö.
Tillämplighet	Molntjänsten i sin helhet.
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Konfidentialiteten och integriteten för och tillgängligheten till information som behandlas i molntjänsten äventyras inte som en följd av ändringar i tjänsten.
Ytterligare information	Överensstämmelse med kravet kan kontrolleras och påvisas enligt följande: 1) Det finns definierade processer för upphävning av ändringar på grund av fel eller säkerhetsproblem och för återställande av de system eller tjänster som har påverkats. 2) Innan en ändring införs i produktionsmiljö ska man kontrollera att de planerade testerna har utförts framgångsrikt och de godkännanden som krävs har getts. 3) I nödfall (till exempel vid omfattande maskinfel eller dataintrång) kan man följa en förenklad ändringshantering under förutsättning att säkerhetsföljderna av ändringarna utreds i efterhand och i en omfattning som motsvarar den normala ändringshanteringsprocessen (i typiska fall inom högst en vecka). 4) Test- och produktionsmiljöerna hålls åtskilda genom antingen fysiska eller logiska metoder för att undvika obehörig åtkomst och obehöriga ändringar i produktionsmiljön och produktionsdata. Produktionsdata överförs inte till utvecklings- eller testmiljöer i syfte att skydda konfidentialiteten. 5) Rutinerna för ändringshantering omfattar rollbaserade rättigheter ämnade att säkerställa att tillbörlig åtskillnad av uppgifter iakttas då ändringar utvecklas, införs och flyttas från en miljö till en annan. Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

MH-02	Systemutveckling
Krav	1) Program och programmeringsgränssnitt (API) planeras, utvecklas, testas och införs i överensstämmelse med beprövade säkerhetsmodeller. Gränssnitten ska tåla allmänna angrepp utan att konfidentialiteten, integriteten eller tillgängligheten för den information som behandlas äventyras. 2) Produktionsmiljön är åtskild från övriga miljöer (till exempel, utvecklingsmiljöer, testmiljöer och kvalitetskontrollmiljöer). 3) I versionshanteringen har säkerheten beaktats åtminstone genom att det har säkerställts att obehöriga versioner inte kan överföras till produktionsmiljön. 4) Reglerna för säker programutveckling har införts i varje del av organisationen som har att göra med programmet i fråga. 5) Om planeringen, utvecklingen, testningen, eller provisioneringen av källkoden för molntjänsten (eller en del av den) läggs ut på entreprenad är följande särskilt viktigt i entreprenadavtalen: a) krav på en säker programutvecklingsprocess (i synnerhet planering, utveckling och testning), b) bevis på tillräcklig testning, c) testning för godkännande i enlighet med operativa och icke-operativa krav, och d) rätten att testa utvecklingsprocessen och övervakningen, inklusive via stickprov.
Tillämplighet	Systemutvecklingen kopplad till molntjänsten
Datatyper	Sekretessbelagd, personuppgifter, SK IV & KV-R, SK III (datamassa)
Mål för skyddet	Konfidentialiteten och integriteten för eller tillgängligheten till informationen som behandlas i molntjänsten äventyras inte till följd av systemutvecklingen av tjänsten.
Ytterligare information	1: Exempel på säkerhetsmodeller är OWASP för webbapplikationer och livscykelmodellerna för systemutveckling (SDLC, Systems Development Life Cycle). 5: Jfr TJ-08 (Säkerheten för tjänsteleverantörer och andra leverantörer) Det rekommenderas att man i bedömningen av kundens ansvarsområde särskilt beaktar att motsvarande krav även gäller kunden och eventuella tjänsteleverantörer som har anknytning till kundens ansvarsområde.

Bilaga 1: Exempel på fördelning av kravpunkter

I denna bilaga finns exempel på hur kraven som beskrivs i PiTukro ska fördelas. Exemplen har delats in enligt servicemodell i kundens och molnleverantörens ansvar. Den fiktiva molntjänst som används i exemplen har byggts upp i enlighet med den allmänna ansvarsmodellen som presenteras i bild 3.

Obs: I praktiken skiljer sig molntjänster från varandra både vad gäller tekniska lösningar och ansvarsfördelning. Till exempel kan ansvaret för skyddet av en molnplattform som producerats med PaaS-servicemodellen och ett kundsystem som förankrats i den skilja sig avsevärt mellan olika tjänsteleverantörer. En meningsfull bedömning förutsätter att särdragen hos molnleverantören och kundsystemet i fråga samt ansvarsfördelningen beaktas.

Servicemodell IaaS

I det här exemplet beskrivs hur kraven i PiTuKri fördelas ansvarsvis i en situation där kundsystemet ha förankrats i en plattform som byggts upp enligt IaaS-servicemodellen.

ID	Underpunkt	Ansvar/Kundmiljöns andel	Ansvar/Molnleverantörens andel
EE-01	1 a-g	-	x
EE-02	1	-	x
	2	x (lämplighetsbedömning)	x
	3	-	x
	4	x (lämplighetsbedömning)	x
TJ-01	1-3	x	x
TJ-02	1-3	x	x
TJ-03	1-7	x	x
TJ-04	1-3	x	x
	4	-	x
TJ-05	1 a–d	x (i tillämpliga delar)	x
TJ-06	1-6	x	x
TJ-07	1-4	x	x
TJ-08	1 a–d	x	x
HT-01	1	x	x
HT-02	1-2	x	x
HT-03	1	x	x
HT-04	1-5	x	x
HT-04	1-5	x	x
HT-05	1-4	x	x
FT-01	1-4	-	x
FT-02	1	-	x
FT-03	1-2	-	x
FT-04	1-4	-	x
FT-05	1-2	-	x
TT-01	1-3	x	x
TT-02	1-2	x	x
IP-01	1 a-h	x	x
IP-02	1-3	x	x
IP-03	1	-	x
	2-7	x	x

ID	Underpunkt	Ansvar/Kundmiljöns andel	Ansvar/Molnleverantörens andel
JT-01	1	x	x
	2-3	-	x
	4-5	x	x
JT-02	1-2	x	x
JT-03	1	- (Om inte kunddata med olika sorterings-behov fortfarande finns i kundsystemet.)	x
JT-04	1	x	x
JT-05	1-4	-	x
SA-01	1-3	x	x
SA-02	1-3	x	x
SA-03	1	-	x
	2-4	x	x
KT-01	1-3	x	x
KT-02	1	-	x
	2	-	x
KT-03	1	x	x
	2 a-c	x	x
	2 d	X (om kunden gör överföringen via kund-miljön)	x
	2 e-f	-	x
	3	x	x
KT-04	1 a-b	x	x
	1 c-d	-	x
SI-01	1-2	-	x
	3	x (för avtalets del)	x
	4-5	x (kan lämpa sig för kundens konfigure-ringsmöjligheter)	x
SI-02	1-2	x	x
	3	-	x
	4	x	x
MH-01	1-5	x	x
MH-02	1-5	x	x

Servicemodell PaaS

I det här exemplet beskrivs hur kraven i PiTuKri riktas ansvarsvis i en situation där kundsystemet är förankrat i en plattform som byggts upp enligt PaaS-servicemodellen.

ID	Underpunkt	Ansvar/Kundmiljöns andel	Ansvar/Molnleverantörens andel
EE-01	1 a-g	-	x
EE-02	1	-	x
	2	x (lämplighetsbedömning)	x
	3	-	x
	4	x (lämplighetsbedömning)	x
TJ-01	1-3	x	x
TJ-02	1-3	x	x
TJ-03	1-7	x	x
TJ-04	1-3	x	x
	4	-	x
TJ-05	1 a–d	x (i tillämpliga delar)	x
TJ-06	1-6	x	x
TJ-07	1-4	x	x
TJ-08	1 a–d	x	x
HT-01	1	x	x
HT-02	1-2	x	x
HT-03	1	x	x
HT-04	1-5	x	x
HT-05	1-4	x	x
FT-01	1-4	-	x
FT-02	1	-	x
FT-03	1-2	-	x
FT-04	1-4	-	x
FT-05	1-2	-	x
TT-01	1-3	x	x
TT-02	1-2	x	x
IP-01	1 a-h	x	x
IP-02	1-3	x	x
IP-03	1	-	x
	2-7	x	x

ID	Underpunkt	Ansvar/Kundmiljöns andel	Ansvar/Molnleverantörens andel
JT-01	1	x	x
	2-3	-	x
	4-5	x	x
JT-02	1-2	- (Obs: Variation i ansvarsgränserna per tjänsteleverantör, till exempel i fråga om tillämpningar.)	x
JT-03	1	- (Om inte kunddata med olika sorterings-behov fortfarande finns i kundsystemet.)	x
JT-04	1	- (Obs: Variation i ansvarsgränserna per tjänsteleverantör.)	x
JT-05	1-4	-	x
SA-01	1-3	x	x
SA-02	1-3	x	x
SA-03	1	-	x
	2-4	x	x
KT-01	1-3	x	x
KT-02	1	-	x
	2	-	x
KT-03	1	x	x
	2 a-c	x	x
	2 d-f	-	x
	3	x	x
KT-04	1 a-b	X (Obs: Variation i ansvarsgränserna per tjänsteleverantör, till exempel brandväggs-programmet för en eventuell kundspecifik del och eventuella IAM-system som kun-den ansvarar för.)	x
	1 c-d	-	x
SI-01	1-2	-	x
	3	x (för avtalets del)	x
	4-5	x (kan lämpa sig för kundens konfigure-ringsmöjligheter)	x
SI-02	1-2	x	x
	3	-	x
	4	x	x
MH-01	1-5	x	x
MH-02	1-5	x (Obs: Variation per tjänsteleverantör.)	x

Servicemodell SaaS

I det här exemplet beskrivs hur kraven i PiTuKri fördelas ansvarsvis i en situation där kunden utnyttjar en applikation som tagits fram med molnleverantörens SaaS-servicemodell.

ID	Underpunkt	Ansvar/Kundmiljöns andel	Ansvar/Molnleverantörens andel
EE-01	1 a-g	-	x
EE-02	1	-	x
	2	x (lämplighetsbedömning)	x
	3	-	x
	4	x (lämplighetsbedömning)	x
TJ-01	1-3	x	x
TJ-02	1-3	x	x
TJ-03	1-7	x	x
TJ-04	1-3	x	x
	4	-	x
TJ-05	1 a–d	x (i tillämpliga delar, till exempel verksamhet i situationer där nätanslutning till molntjänsten inte är tillgänglig)	x
TJ-06	1	-	x
	2	x	x
	3-4	-	x
	5	X (ägaren/den ansvariga instansen för andelarna som kunden ansvarar för i de tillämpningar som används)	x
	6	x (bokföring och ändringshantering av de applikationer som används och de andelar som kunden ansvarar för)	x
TJ-07	1-4	x (bedömning av överensstämmelse och dataskydd vid användning av applikationer)	x
TJ-08	1 a–d	x	x
HT-01	1	x	x
HT-02	1-2	x	x
HT-03	1	x	x
HT-04	1-5	x	x
HT-05	1-4	x	x
FT-01	1-4	-	x
FT-02	1	-	x
FT-03	1-2	-	x
FT-04	1-4	-	x
FT-05	1-2	-	x
TT-01	1-3	-	x
TT-02	1-2	-	x

ID	Underpunkt	Ansvar/Kundmiljöns andel	Ansvar/Molnleverantörens andel
IP-01	1 a-h	x	x
IP-02	1-3	X (i allmänhet med fokus på konfigurering av säkra inställningar utifrån tjänstens inställningar samt på kundens terminalutrustning)	x
IP-03	1	-	x
	2-7	x (i allmänhet med fokus på konfigurering av säkra inställningar utifrån tjänstens inställningar samt på kundens terminalutrustning)	x
JT-01	1-5	-	x
JT-02	1-2	-	x
JT-03	1	-	x
JT-04	1	-	x
JT-05	1-4	-	x
SA-01	1-3	x (kan lämpa sig för kundens konfigureringsmöjligheter)	x
SA-02	1-3	x (kan lämpa sig för kundens konfigureringsmöjligheter)	x
SA-03	1	-	x
	2-4	x (kan lämpa sig för kundens konfigureringsmöjligheter)	x
KT-01	1-2	-	x
	3	x	x
KT-02	1	-	x
	2	-	x
KT-03	1-3	-	x
KT-04	1 a–d	-	x
SI-01	1-2	-	x
	3	x (för avtalets del)	x
	4-5	x (kan lämpa sig för kundens konfigureringsmöjligheter)	x
SI-02	1-4	- (kan lämpa sig för kundens konfigureringsmöjligheter)	x
MH-01	1-2	x (betoning i allmänhet på administrativa förfaranden)	x
	3-5	- (kan lämpa sig för skräddarsydda applikationer där kunden eventuellt också behöver delta i testningen)	x
MH-02	1-5	-	x

Bilaga 2: Exempel på tillämpning av kriterierna för bedömning av överensstämmelse med kraven

Exempel 1: Bedömning av om skyddet av sekretessbelagd information överensstämmer med kraven

Här finns ett exempel på hur kriterierna kan tillämpas på bedömning av överensstämmelse med kraven för skydd av sekretessbelagda uppgifter utan säkerhetsklassificering i förhållande till kraven i informationsförvaltningslagen (906/2019). I exemplet är kunden myndighet A, som vill bedöma om skyddet av ett nytt datasystemet som planeras är tillräckligt för att behandla sekretessbelagd information som inte säkerhetsklassificerats.

Myndighet A har identifierat följande överensstämmelser mellan informationshanteringslagen och kraven i PiTuKri:

- 12 § Identifiering av uppgifter som kräver tillförlitlighet och säkerställande av tillförlitligheten: HT-02 (Pålitlighetsbedömning av personalen); HT-03 (Avtal om sekretess och tystnadsplikt)

- 14 § Informationsöverföring i datanät: SA-02 (Kryptering utanför ett fysiskt skyddat säkerhetsområde)/Objekt 1-2; SA-01/Objekt 1-2.

- 16 § Kontroll av användarrättigheter för informationssystem: IP-01 (Behörighetshantering)

- 17 § Insamling av logginformation: JT-01 (Spårbarhet och upptäcktskapacitet) punkterna 1–3

- 21 § Definition av behovet att förvara informationsmaterial (förstöring efter att förvaringstiden har löpt ut): SI-02 (Förstöring av informationsmaterial)

Att definiera ansvaret i anslutning till systemmiljön enligt kravkortet TJ-02 (Säkerhetsansvar), att se till att direktiven är aktuella enligt kravkortet HT-04 (säkerhetsmedvetenhet) samt övervakningen enligt kravkortet TJ-07 (Överensstämmelse med krav och dataskydd) är i stor utsträckning förenliga med ordnandet av informationshanteringen (4 §). Å andra sidan lämpar sig kravkortet TJ-03 (Hantering av säkerhetsrisker) direkt för identifiering av risker i samband med informationsbehandling och för riskbedömningsbaserad dimensionering av informationssäkerhetsåtgärder.

Myndighet A har dessutom i sin egen riskhantering (13 §) identifierat att man till exempel för att uppnå tillräcklig feltolerans och funktionell användbarhet kan stöda sig på kravkorten TJ-05 (Kontinuitetshantering), KT-03 (Säkerhets- och returprocesser), MH-01 (Ändringshantering) och MH-02 (Systemutveckling), liksom även TT-02 (Skydd mot allmänna nätattacker). JT-01 (Spårbarhet och upptäcktskapacitet) stöder direkt uppföljningen av informationssäkerheten (13 §). Å andra sidan är till exempel ett hållbart skydd av livscykeln väsentligt förknippat med KT-04 (Hantering av sårbarheter) och SI-02 (Förstöring av informationsmaterial). Å ena sidan har A identifierat att för att kunna fungera tillförlitligt förutsätter administrationen av användarrättigheterna även användaridentifiering (IP-02), och å andra sidan är till exempel de nättekniska avgränsningarna (TT-01) och systemhärdningarna (JT-02) för att minska systemets sårbarhet nödvändiga utifrån riskerna. Eftersom systemets säkerhet stöder sig direkt på administrationsförbindelserna (IP-03), ser A även dessa som kritiska skydd som förutsätts av systemet.

Myndighet A har i sin riskbedömning (13 §) dessutom identifierat att ett tillförlitligt tryggande av säkerheten för informationsmaterialet (15 §) även förutsätter att den fysiska säkerheten (FT-01–FT-05) beaktas i tillämpliga delar. För att myndighet A ska försäkras om kontinuiteten i säkerhetsarbetet kan även delområdet säkerhetsledning utnyttjas i tillämpliga delar.

Myndighet A har i sin riskhantering medvetet valt att om det senare skulle vara nödvändigt att överföra informationssystemet som utvecklas till en annan molnplattform, kan detta orsaka betydande kostnader och kräva att systemet byggs om i betydande utsträckning. A godkänner riskerna förknippade med överförbarheten och tillämpar till exempel inte kravkort SI-01 (Överförbarhet) för detta system.

Exempel 2: Bedömning av om skyddet av sekretessbelagd information överensstämmer med kraven

Här finns ett exempel på hur kriterierna kan tillämpas för att bedöma överensstämmelsen med kraven för skydd av sekretessbelagd information utan säkerhetsklassificering i förhållande till kraven i informationsförvaltningslagen (906/2019) och förordningen om säkerhetsklassificering (1101/2019). I exemplet är kunden myndighet B, som vill bedöma om ett nytt informationssystem som ännu planeras är tillräckligt skyddat för behandling av sekretessbelagd information i säkerhetsklass IV (ANVÄNDNING BEGRÄNSAD).

Myndighet B har konstaterat motsvarande överensstämmelser mellan informationshanteringslagen (906/2019) och kraven i PiTuKri som myndighet A i exempel 1. Myndigheten B har dessutom konstaterat följande överensstämmelser mellan förordningen om säkerhetsklassificering (1101/2019) och kraven i PiTuKr, som direkt gäller B:s systemmiljö:

- 6 §: Förutsättningar för utlämnande av en säkerhetsklassificerad handling: EE-01 (Systembeskrivning); EE-02 (Lagstiftningsrelaterade risker)
- 8 §: Behandlingsrättigheterna och förteckningen över dem: HT-05 (Behov av information och åtskiljande mellan funktioner)/punkterna 1–3; HT-04 (Säkerhetsmedvetenhet); HT-03 (Avtal om sekretess och tystnadsplikt)
- 9 §: Säkerhetsområden: FT-01 (Skydd och riskhantering baserade på flernivåförsvar)/punkt 2; FT-03 (Förhindrande av obehörigt tillträde)
- 10 §: Skydd av dokumenthantering och informationssystem med hjälp av säkerhetsområden: FT-01 (Skydd och riskhantering baserade på flernivåförsvar), FT-02 (Konstruktioner och säkerhetssystem), FT-03 (Förhindrande av obehörigt tillträde), FT-04 (Serviceproducenter och besökare), FT-05 (Beredskap och kontinuitetshantering); IP-03 (Administrationsförbindelser); JT-05 (Flytt och förstöring av skyddade objekt)
- 11 §: Krav som gäller informationssystem och datakommunikationsarrangemang/punkt 1: TT-01 (Datanätets uppbyggnad)/punkterna 1 och 3
- 11 §: Krav som gäller informationssystem och datakommunikationsarrangemang/punkt 3: IP-01 (Behörighetshantering)/punkt b.
- 11 §: Krav som gäller informationssystem och datakommunikationsarrangemang/punkt 5: IP-02 (Identifiering av användare)
- 11 §: Krav som gäller informationssystem och datakommunikationsarrangemang/punkt 6: JT-02 (Systemhärdning)
- 11 §: Krav som gäller informationssystem och datakommunikationsarrangemang/punkt 7: SA-01 (Kryptering och nyckelhantering)
- 12 §: Överföring av en handling via datanätet: SA-02 (Kryptering utanför ett fysiskt skyddat säkerhetsområde); SA-03 (Kryptering innanför ett fysiskt skyddat säkerhetsområde); SA-01 (Kryptering och nyckelhantering)
- 15 §: Förstöring av handling: SI-02 (Förstöring av informationsmaterial)

De centrala skydden mot elektroniska meddelanden, till exempel skadliga program som bifogats ett e-postmeddelande och även mer direkta attacker mot applikationssäkerheten i molntjänsten (1101/2019 ,11 §, punkt 2) utgörs av TT-01 (Datanätets struktur), TT-02 (Skydd mot allmänna nätattacker), KT-04 (Hantering av sårbarheter), JT-04 (Skydd mot skadeprogram), JT-02 (Systemhärdning), MH-02 (Systemutveckling) och naturligtvis även JT-01 (Spårbarhet och upptäcktskapacitet).

Å andra sidan är den centrala metoden för att skydda informationssystemets integritet (1101/2019, 11 §, punkt 4) fysisk säkerhet. För detta lämpar sig direkt punkterna FT-01 (Skydd och riskhantering baserade på flernivåförsvar), FT-02 (Konstruktioner och säkerhetssystem), FT-03 (Förhindrande av obehörigt tillträde), FT-04 (Serviceproducenter och besökare) och FT-05 (Beredskap och kontinuitetshantering). Utanför det fysiska skyddet ska man i integritetsskyddet förutom kryptering (SA-02) även beakta bland annat IP-03 (Administrationsförbindelser) och JT-05 (Flytt och förstöring av skyddade objekt).

Myndighet B har också tydligt noterat att ett flernivåförsvar (1101/2019, 7 §) förutsätter skydd som stöder varandra både för säkerhetsledningen och den fysiska och datatekniska säkerheten, till exempel att datakommunikationsnätets struktur delas och övervakas i flera steg (TT-01: Datanätets struktur/punkterna 2–3).

Bilaga 3: Myndighetsbedömning och ackreditering

Bakgrund

I lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation [36] föreskrivs att myndigheterna för bedömning av informationssäkerheten i sina datasystem får använda sig av Transport- och kommunikationsverket Traficom eller av ett bedömningsorgan för informationssäkerhet som Traficom har godkänt [37]. Myndigheter kan använda säkerhetskriterierna för molntjänster (PiTuKri) för att utreda hur informationssäkerheten för ett molnbaserat datasystem som de har kontroll över eller planerar att skaffa är ordnad mot bakgrund av behovet att skydda nationell eller internationell information [38].

I denna bilaga beskrivs olika användningsfall för säkerhetskriterierna för molntjänster (PiTuKri) vid bedömning av molnbaserade datasystem. Användningsfallen som beskrivs är en säkerhetsbedömning för företag och en bedömning av myndigheters datasystem, med Traficom som behörig myndighet. Beskrivningen är indelad i processen för bedömning och godkännande samt processen för ackreditering. Beskrivningen tar inte upp andra användningsfall, till exempel den användning som sker inom ramen för organisationens interna säkerhetsarbete.

Bedömningsprocessen

Första steget i säkerhetsbedömningsprocessen för ett datasystem (L 1406/2011) är att den aktör som ska bli bedömd ber Traficom att utföra bedömningen. Andra viktiga steg i processen är planeringen av bedömningen, inspektionerna och rapporteringen. Bild 4 visar en förenklad överblick över bedömningsprocessen. En bedömningsprocess kan också användas som stöd för det interna säkerhetsarbetet i organisationen så att denna ansvarar helt och hållet för bl.a. kvarstående risker. Bedömningsprocessen beskrivs närmare på finska i anvisningen "NCSA-toiminnon suorittamat tietoturvallisuustarkastukset – Tilaajaorganisaation näkökulma" [39].

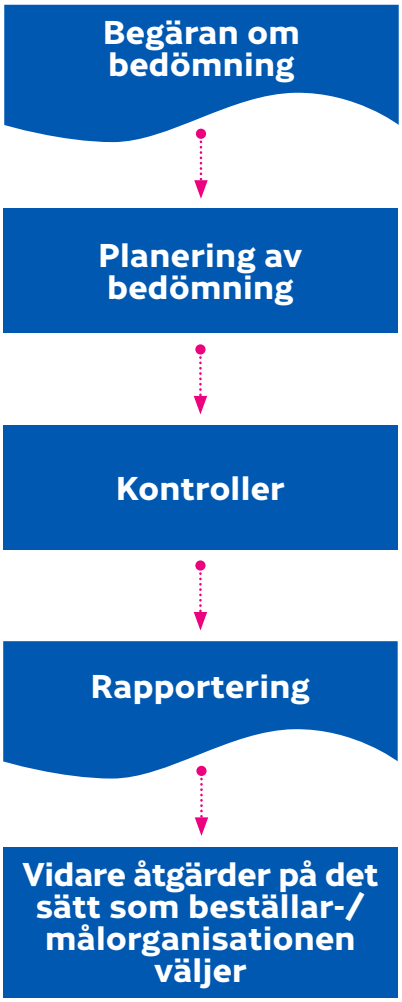


Bild 4. Bedömningsprocessen förenklad

[36] Lagen om bedömningsorgan för informationssäkerhet (L 1405/2011), https://www.finlex.fi/sv/laki/ajantasa/2011/20111405.

[37] Lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011), https://www.finlex.fi/sv/laki/alkup/2011/20111406. Lagen om införande av lagstiftningen om verkställande av myndighetsreformen inom kommunikationsministeriets förvaltningsområde och om omorganisering av ämbetsverkens uppgifter (937/2018), https: //www.finlex.fi/sv/laki/smur/2018/20180937.

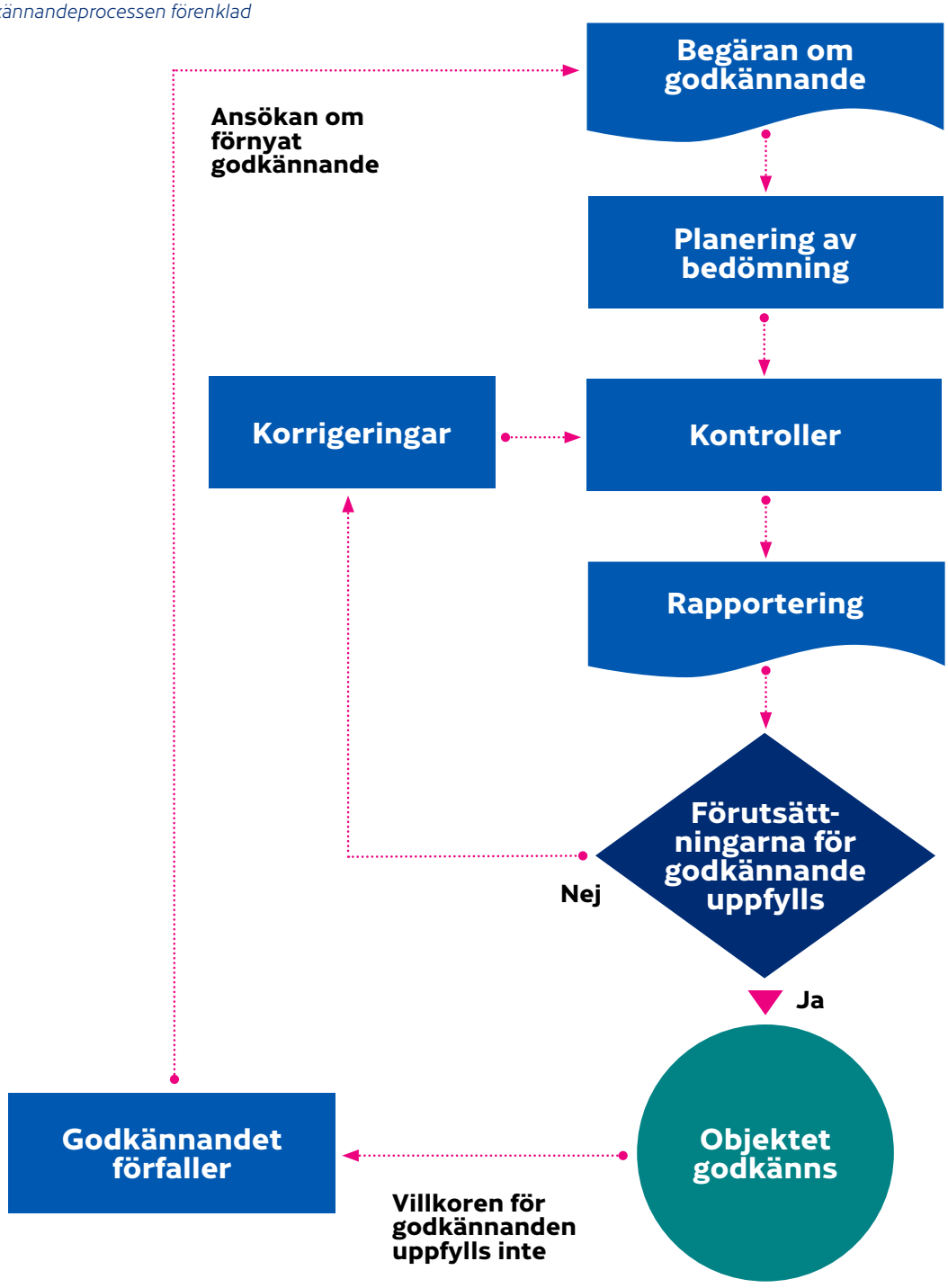
[38] Lagen om internationella förpliktelser som gäller informationssäkerhet (588/2004), https://www.finlex.fi/sv/laki/alkup/2004/20040588. Säkerhetsutredningslagen (726/2014), https://www.finlex.fi/sv/laki/alkup/2014/20140726.

[39] Cybersäkerhetscentret. 2019. URL: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/regulation/ohje_NCSA-toiminnon_suorittamat_tietoturvallisuustarkastukset.pdf.

Godkännandeprocessen

Processen som utmynnar i Trafik- och kommunikationsverket Traficoms godkännande (L 726/2014 eller L 1406/2011) börjar när organisationen i fråga sänder Traficom en begäran om godkännande. Processen löper enligt liknande mönster som bedömningsprocessen med det centrala undantaget att eventuella brister som hittas under inspektionerna måste vara åtgärdade på verifierat sätt innan godkännandet kan ges. Bild 5 visar en förenklad överblick över godkännandeprocessen. Att inhämta godkännande av Traficom är ett alternativ till exempel för organisationer som vill påvisa att deras datasystem har ett tillfredsställande skydd. Riskanalysen i godkännandeprocessen utförs utifrån både den bedömda organisationens och Traficoms analyser. Godkännandeprocessen beskrivs närmare på finska i anvisningen "NCSA-toiminnon suorittamat tietoturvallisuustarkastukset - Tilaajaorganisaation näkökulma".

Bild 5. Godkännandeprocessen förenklad



Ackreditering

Trafik- och kommunikationsverket Traficom kan ackreditera system som används för att behandla nationell eller internationell säkerhetsklassificerad information. Ett villkor för ackreditering är att organisationen åtar sig att upprätthålla säkerheten i den omfattning som ackrediteras. Ett typiskt krav för ackreditering [40] är också att systemet är helt och hållet underkastat finsk lagstiftning.

Ackrediteringen förlorar sin giltighet om det inträffar avsevärda förändringar av säkerhetsrelevans i organisationen. Sådana är till exempel avsevärda förändringar i nätverksstrukturen, personalen, säkerhetsrutinerna eller verksamhetslokalerna. Förändringar som hänger samman med ordinarie administration, till exempel installation av säkerhetsuppdateringar, medför inte att ackrediteringens giltighet upphör. När ackrediteringen upphör att gälla definieras fall för fall då ackrediteringen utfärdas. Avsevärda förändringar måste godkännas av Traficom i förväg.

[40] Ett undantag är till exempel systemprojekt i anslutning till internationellt myndighetssamarbete, där man mellan säkerhetsmyndigheterna i de medlemsländer som deltar i myndighetssamarbetet separat har kommit överens om behörigheten och ansvaret för granskning och godkännande av systemhelheternas delar.

Transport- och kommunikationsverket Traficom
Cybersäkerhetscentret
PB 320, 00059 TRAFICOM
t. 029 534 5000

traficom.fi/sv

Transport- och kommunikationsverket
Cybersäkerhetscentret