Dnr: 153/602/2016

Anvisning till bedömningsorgan för informationssäkerhet
210/2016 O

Versionshistorik

Version	Datum	Beskrivning/ändring	Författare
1.0	7.5.2013	"[Första versionen]"	Laura Kiviharju
2.0	29.1.2015	Kapitel 6, lag om ändring av lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (250/2014) och lag om ändring av lagen om elektroniska recept (251/2014)	Laura Kiviharju
3.0	12.8.2015	4.2.3 Ändring av kompetensområdet; de ändringar i dokumentet som föranleds av Katakri III.	Anna von Fieandt-Lehtonen
4.0	19.2.2016	Avsnitt 1.1 Syfte och tillämpningsområde och kapitel 7 Övervakning och kvalitetssäkring av bedömningsorgan: preciseringar och tillägg.	Anna von Fieandt-Lehtonen
5.0	19.5.2017	Tillägg: 5.4.4 Verifieringsmetoder vid användning av bedömningskriterier; preciseringar: 5.5 Myndighetsgodkännande, fotnot 20 om lagringstider; 5.3.5 innehåll i intyg; 6.1 innehåll i intyg; 7.2.1 innehåll i årlig anmälan; 7.2.2 bedömningsuppgifter som ska anmälas på egen hand; 7.2.3 Bedömningsrapporter och intyg som ska lämnas till Kommunikationsverket	Anna von Fieandt-Lehtonen
6.0	15.11.2017	Fotnoterna 27 och 28; ett nytt avsnitt 4.1 Verksamhet i egenskap av bedömningsorgan; ändring: 5.3.4 Bedömningsrapport och andra handlingar relaterade till bedömningen	Anna von Fieandt-Lehtonen
7.0	23.4.2018	En ny anvisning	Anna von Fieandt-Lehtonen
8.0	24.9.2019	Uppdateringar, preciseringar och riktlinjer gällande Traficom i avsnitten 3.2, 3.3.1, 3.3.5, 3.5, 3.6, 4.2.2 och 4.2.3	Anna von Fieandt-Lehtonen
8.1	28.1.2020	De ändringar som föranleds av lagen om informationshantering, ändring i avsnitt 3.3.1	Anna von Fieandt-Lehtonen
8.2	18.12.2020	Tillägg som lagen om sekundär an-vändning och Findatas föreskrift medför har gjorts i avsnitt 1.1 och 2.2.1 och i fotnot 18. Ett helt nytt avsnitt 3.7 om ämnet har dessutom fogats till.	Eija Alavesa och Anna von Fieandt-Lehtonen

Innehåll

1 Inledning

1.1 Syfte och tillämpningsområde

Lagen om bedömningsorgan för informationssäkerhet (lagen om bedömningsorgan) innehåller bestämmelser om godkännande av och tillsyn över bedömningsorgan och om bedömningsorganens verksamhet. Lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (bedömningslagen), lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (TUVE-lagen), lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (klientuppgiftslagen) och lagen om sekundär användning av personuppgifter inom social- och hälsovården (lagen om sekundär användning) innehåller bestämmelser om uppgifter som ett sådant bedömningsorgan för informationssäkerhet som har godkänts av Transport- och kommunikationsverket kan sköta.

Enligt 4 § i lagen om införande av lagstiftningen om genomförande av ämbetsverksreformen och omorganisering av ämbetsverkens uppgifter inom kommunikationsministeriets förvaltningsområde ska en sådan uppgift inom det uppgiftsområde som avses i 2 och 3 § i lagen om Transport- och kommunikationsverket som enligt bestämmelser någon annanstans i lagstiftningen ska skötas av Trafiksäkerhetsverket, Kommunikationsverket, Trafikverket, Luftfartsförvaltningen, Teleförvaltningscentralen, Bilregistercentralen, Fordonsförvaltningscentralen, Järnvägsverket, Sjöfartsverket eller länsstyrelsen, övergå på Transport- och kommunikationsverket den 1 januari 2019 i enlighet med denna lag. På så sätt är Transport- och kommunikationsverket, Traficom, från och med den 1 januari 2019 en behörig myndighet i frågor som gäller bedömningsorgan för informationssäkerhet.

I denna anvisning beskrivs rollen och uppgifterna för bedömningsorgan för informationssäkerhet i den bedömningsverksamhet som avses i ovannämnda lagar. Med bedömningsorgan avses i anvisningen alltid bedömningsorgan för informationssäkerhet. I anvisningen beskrivs kraven på organens verksamhet och bedömningsförfarandet. Ett godkänt bedömningsorgan ska känna till gällande lagstiftning och övriga krav som berör dess verksamhet.

1.2 Definitioner

Ackreditering ackrediteringstjänsten FINAS fastställande av ett bedömningsorgans kompetens enligt internationellt eller europeiskt harmoniserade bedömningsgrunder.

Bedömningskriterier för informationssäkerhet kriterier som tillämpas vid bedömning av informationssäkerheten och för vilka ett bedömningsorgan kan söka ackreditering och godkännande hos Traficom.

1.3 Bedömningsorgan

Bedömningsorganet gör en uppdragsbaserad bedömning av objektets informationssäkerhetsnivå. Bedömningsorganets bedömning ska klarlägga om de informationssäkerhetskrav som ligger till grund för bedömningen uppfylls

på behörigt sätt i verksamheten på objektet. Om kraven uppfylls kan bedömningsorganet utfärda ett intyg över kravuppfyllelsen för objektet.

Bedömningsorganets verksamhet ska följa kraven i lagstiftningen, tillämpliga ackrediteringsstandarder, Traficoms anvisningar och beslutet om godkännande av organet.

2 Godkännande av bedömningsorgan

2.1 Krav på bedömningsorgan

Godkännande av ett bedömningsorgan för informationssäkerhet förutsätter att det uppfyller kraven enligt 5 § i lagen om bedömningsorgan. Kraven är följande:

1) organet är funktionellt och ekonomiskt oberoende av den som bedömningen gäller,

2) organets personal har god teknisk och yrkesinriktad utbildning samt tillräckligt omfattande erfarenhet av de uppgifter som ingår i verksamheten,

3) organet har den utrustning, de hjälpmedel och de system som behövs i verksamheten,

4) tillförlitligheten hos de ansvariga personerna inom organet har säkerställts och organet har en övervakad metod som bedömts som tillförlitlig och med vars hjälp säkerheten i organets lokaler och databehandling säkerställs,

5) organet har ändamålsenliga anvisningar för sin verksamhet och uppföljningen av den.

2.1.1 FINAS ackreditering

FINAS-tjänsten vid Säkerhets- och kemikalieverket ansvarar för utredningen av att ett bedömningsorgan uppfyller kraven i punkterna 1–3 ovan. Som ett bevis på uppfyllandet av kraven beviljar FINAS bedömningsorganet ett ackrediteringsintyg för fyra år, varefter ackrediteringen kan förlängas med en ny giltighetstid på fyra år. Dessutom övervakar FINAS att ackrediteringskraven uppfylls under intygets giltighetstid.

Vid ackreditering av bedömningsorgan tillämpas kraven i standarderna ISO/IEC 17021-1:2015[1] och ISO/IEC 27006:2015[2]. Dessa standarder specificerar kraven på organ som reviderar och certifierar ledningssystem för informationssäkerhet.

[1] SFS-EN ISO/IEC 17021-1:2015 Bedömning av överensstämmelse. Krav på organ som reviderar och certifierar ledningssystem. Conformity assessment. Requirements for bodies providing audit and certification of management systems

[2] ISO/IEC 27006:2015 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems

2.1.2 Traficoms godkännande av bedömningsorgan för informationssäkerhet

När FINAS har ackrediterat ett bedömningsorgan kan Traficom godkänna organet, om kraven i 5 § 4–5 punkterna i lagen om bedömningsorgan också är uppfyllda.

2.1.2.1 Tillförlitlighet hos de ansvariga personerna och säkerhet i databehandlingen

Bedömningsorganets ansvariga personer ska vara dokumenterat tillförlitliga personer. Som ansvariga personer anses organets högsta ledning och personer angivna på organets handelsregisterutdrag.

I bedömningsverksamheten behandlar bedömningsorganet sekretessbelagd information från bedömningsobjektet och organet ska ha förmåga att behandla sådan information enligt de uppställda skyddskraven. Bedömningsorganet ska ha en dokumenterat tillförlitlig och övervakad metod för säkerställande av att organets lokaler och databehandling är säker.

Kraven på säker behandling av konfidentiell information verifieras med vid var tid gällande version av Katakri[3]. I bedömningsverksamheten ska bedömningsorganet uppfylla kraven på säkerhetsledning, fysisk säkerhet och teknisk informationssäkerhet i Katakri. De tillämpade kraven på bedömningsorganets verksamhet är i princip en säkerhetsklass över den kravnivå som ansökan gäller.[4] När det kompetensområde som ansökan gäller endast är ISO/IEC 27001, verifieras säkerheten i databehandlingen utifrån Katakri III-kraven. Sådan sekretessbelagd information som bedömningsorganet har fått av bedömningsobjekt i anslutning till sina bedömningar får endast behandlas i de informationssystem som har godkänts i processen för godkännande av bedömningsorganet.

I praktiken innebär detta bland annat att organet ska ha fastställt principer för säkerhetsverksamheten, säkerhetsorganisationen och tillhörande ansvar samt ha adekvata metoder för identifiering och bedömning av risker och hantering av incidenter. Organets lokaler ska uppfylla Katakri-kraven på området, fysiska strukturer och säkerhetstekniska system.

Personalsäkerhetskraven innebär bland annat att endast personer som gett relevanta sekretessförbindelser och genomgått adekvata säkerhetsutredningar används i bedömningsverksamheten. Bedömningsorganet ska ansöka om säkerhetsutredningar av personer som deltar i bedömningsverksamheten utifrån vilken säkerhetsklassificerad information respektive person behandlar. I verksamheten kan bedömningsorganet endast använda personer som

[3] Katakri – verktyg för informationssäkerhetsauditering för myndigheter 2015.

[4] Bedömningsorganet ska kunna behandla slutkundernas klassificerade information enligt de fastställda skyddskraven. När bedömningsorganet till exempel bedömer ett slutkundssystem med nivå IV, får organet under processen klassificerad information om systemet från kunden (till exempel nätverksdiagram och uppgifter om kopplingar till andra system). Uppgifter om systemens säkerhetsimplementeringar klassificeras i vissa fall ett steg över den högst klassificerade information som behandlas i systemet. En informationsmängd bestående av olika slutkunders information kan ofta tolkas ha en högre säkerhetsklass än säkerhetsklassen för enskilda uppgifter på grund av den kumulativa effekten.

genomgått en säkerhetsutredning där ingen relevant information för dess syfte har framkommit. Om ett skriftligt meddelande lämnas utifrån en säkerhetsutredning ska bedömningsorganet alltid begära ett skriftligt förhandsutlåtande av Traficom om uppfyllandet av personalkraven innan personen används i bedömningsverksamheten.

När det gäller säker informationsbehandling ska bedömningsorganet även beakta ackrediteringsstandardernas krav på konfidentialitet. Katakri-nivån för skydd av uppgifter ska iakttas till de delar kraven på säkerheten i databehandlingen skiljer sig mellan ackrediteringsstandarderna och Katakri. Dessutom ska bedömningsorganet försäkra sig om att informationsbehandlingskraven iakttas oavsett vilken person eller instans som behandlar sekretessbelagd information för dess räkning. Kraven gäller egen personal och likaså dem som utför bedömningsuppgifter enligt till exempel uppdragsavtal.

2.1.2.2 Behöriga anvisningar för verksamheten och övervakningen

Bedömningsorganet ska ha anvisningar för bedömningsverksamheten och övervakning av den, och uppdatera anvisningarna. Anvisningarna ska beakta lagstadgade och andra krav på bedömningsorganets verksamhet samt innehållet i denna anvisning. Bedömningsorganets anvisningar om informationssäkerheten ska även uppfylla Katakri-kraven.

Organet ska försäkra sig om att personer och instanser som arbetar för dess räkning är medvetna om kraven och skyldigheterna i samband med bedömningsverksamheten. För säkerställande av detta ska anvisningarna till exempel ange hur organet försäkrar sig om att dess personal och andra som arbetar för dess räkning är medvetna om bedömningsorganets allmänna och säkerhetsrelaterade anvisningar och förstår deras innehåll.

2.2 Ansökningsprocessen för bedömningsorgan

2.2.1 Ansökan om ackreditering hos FINAS och kompetensområde

Innan godkännande söks hos Traficom ska bedömningsorganet ansöka om ackreditering, dvs. bedömning av kompetensen, hos FINAS-tjänsten.

När bedömningsorganet ansöker om bedömning av kompetensen ska organet ange vilket kompetensområde ansökan om ackreditering gäller. Kompetensområdena fastställs enligt bedömningskriterium och säkerhetsklass.

Bedömningskriterier för informationssäkerhet:

1) finansministerieriets VAHTI-anvisning om verkställighet av förordningen om informationssäkerheten inom statsförvaltningen (specificeras i bilaga 1), vid var tid gällande versioner
2) Katakri, verktyg för informationssäkerhetsauditering för myndigheter, vid var tid gällande version
3) ISO/IEC 27001, vid var tid gällande version
4) andra publicerade och allmänt eller regionalt tillämpade bestämmelser, föreskrifter eller anvisningar om informationssäkerhet eller informationssäkerhetskrav i en fastställd standard.

Bedömningsorganet ska alltid ansöka om bedömning av kompetensen för delområde 3, dvs. för att kunna godkännas som ett bedömningsorgan för informationssäkerhet ska det ha kompetens för att utföra bedömningar enligt ISO/IEC 27001-standarden.

Om ett bedömningsorgans kompetensområde omfattar finansministeriets anvisning om verkställighet av förordningen om informationssäkerheten inom statsförvaltningen (punkt 1) eller Katakri (punkt 2), kan bedömningsorganet även göra följande bedömningar:

- en bedömning av informationssystemen inom social- och hälsovården och utfärda ett intyg över att de relevanta kraven har uppfyllts (se 3.6 Bedömning av informationssystem inom social- och hälsovården) och

- en bedömning av informationssäkerhet i en informationssäker driftmiljö enligt lagen om sekundär användning av personuppgifter inom social- och hälsovården samt ge ett intyg om att kraven är uppfyllda (se 3.7 Bedömning av informationssäkerhet i en driftmiljö enligt lagen om sekundär användning).

När ett bedömningsorgan ansöker om ackreditering för VAHTI- eller Katakri-kompetensområdet gäller ansökan även säkerhetsklassen.

När ett bedömningsorgan första gången hos Traficom ansöker om godkännande för sin verksamhet, kan bedömningsorganets kompetensområde ackrediteras för högst säkerhetsklass BEGRÄNSAD ANVÄNDNING, dvs. TL IV. Senare kan bedömningsorganet ansöka om högst säkerhetsklass KONFIDENTIELL, dvs. TL III, för sitt kompetensområde.

2.2.2 Ansökan om godkännande hos Traficom

Bedömningsorgan för informationssäkerhet kan ansöka om godkännande av verksamheten genom en fritt formulerad ansökan till Traficom. Uppgifter som behövs för behandling av ärendet ska bifogas ansökan. FINAS-tjänstens ackrediteringsbeslut, som utvisar bedömningsorganets ackrediterade kompetensområde, ska bifogas ansökan. Godkännande förutsätter att bedömningsorganet uppfyller kraven på godkännande i 5 § i lagen om bedömningsorgan.

Ansökan ska innehålla följande uppgifter:

- ansökt kompetensområde och säkerhetsklass (säkerhetsklass ska endast anges om ansökan gäller ackreditering för VAHTI- eller Katakri-kompetensområdet)
- de ansvariga personerna inom bedömningsorganet (vd, styrelsemedlemmar och personer med prokura)
- utredning om bedömningsorganets metod med vilken säkerheten i dess lokaler och databehandling säkerställs
- bedömningsorganets anvisningar för sin verksamhet
- vid behov uppgift om sekretessbelagd information i ansökan.

Om ansökan innehåller sekretessbelagd information, ska sökanden specificera vilka delar som är sekretessbelagda och grunden för sekretessen. Sekretessbelagd information ska helst lämnas i separata bilagor till ansökan. I fråga om avgiften för behandlingen av ärenden som gäller godkännande av bedömningsorgan för informationssäkerhet gäller vad som föreskrivs i lagen om grunderna för avgifter till staten (150/1992) och i kommunikationsministeriets förordning om avgifter som tas ut för Transport- och kommunikationsverkets prestationer som gäller elektronisk kommunikation (1149/2018).

2.3 Ändring av kompetensområdet

När kriterierna för bedömningsorgans godkända kompetensområde förändras till exempel till följd av en ny version av Katakri, ändras kompetensområdet inte automatiskt. Kompetensområdet förblir förenligt med beslutet om godkännande så länge som beslutet gäller. Traficom fastställer ingen viss tidsfrist för när den nya versionen ska börja användas, utan bedömningsorganet får själv bestämma när det vill ansöka om kompetens att tillhandahålla bedömningar enligt de nya kriterierna.

Om ett av Traficom godkänt bedömningsorgan vill ändra sitt kompetensområde, ska bedömningsorganet först hos FINAS ansöka om ändring av kompetensområdet eller ett helt nytt kompetensområde. FINAS utvärderar ändringen och ändrar ackrediteringsbeslutet utifrån utvärderingen. Därefter kan bedömningsorganet hos Traficom ansöka om ett nytt godkännandebeslut där kompetensområdet är ändrat.

3 Verksamhet i egenskap av bedömningsorgan

3.1 Tjänster som tillhandahålls av godkända respektive icke godkända bedömningsorgan

Enligt 2 § i lagen om bedömningsorgan tillämpas lagen på näringsidkare och på enheter som tillhandahåller serviceuppgifter för den offentliga förvaltningen och som på uppdrag bedömer informationssäkerhetens nivå och vill att Traficom ska godkänna deras verksamhet.

Enligt 13 § i den lagen ska ett godkänt bedömningsorgan för informationssäkerhet iaktta förvaltningslagen, lagen om offentlighet i myndigheternas verksamhet och språklagen när bedömningsorganet utför uppgifter som av-

ses i lagen om bedömningsorgan. Med stöd av 3 § 4 mom. i lagen om informationshantering inom den offentliga förvaltningen (informationshanteringslagen) ska bedömningsorganen också tillämpa kapitel 4 (informationssäkerhet) samt 25–28 § när de sköter de uppgifter som avses i lagen om bedömningsorgan.

Bedömningsorgan som har godkänts av Traficom kan även sköta andra bedömningsuppgifter än dem som avses i lagen om bedömningsorgan.[5] Därför ska ett godkänt bedömningsorgan, när organet avtalar om tillhandahållande av sina tjänster, kontrollera om kunden vill använda organets tjänster eller ett icke godkänt bedömningsorgans tjänster[6]. Privata företag får välja bedömningsorgan som har godkänts av Traficom, eller icke godkända bedömningsorgan. I inspektioner av informationssystem får myndigheterna däremot endast anlita Traficom eller bedömningsorgan[7] som har godkänts av Traficom. Det innebär att ett godkänt bedömningsorgans tjänster alltid ska väljas vid bedömning av en myndighets informationssystem. Bedömningsorganet ansvarar för att dess kund informeras på ändamålsenligt sätt så att kunden är medveten om att denne köper tjänster som tillhandahålls av ett av Traficom godkänt bedömningsorgan för informationssäkerhet, eller något annat.

Lagen om bedömningsorgan och Traficoms anvisning till bedömningsorgan för informationssäkerhet gäller endast tjänster som bedömningsorganen tillhandahåller i egenskap av bedömningsorgan som har godkänts av Traficom.

3.2 Bedömningskriterier och tillämpningsanvisningar

Här beskrivs allmänna ramvillkor för kravtolkningspraxisen. I oklara fall ska tolkningsanvisningar begäras hos Traficom.

3.2.1 VAHTI

Skyddskraven på system med nationellt skyddad information beskrevs tidigare i statsrådets förordning om informationssäkerheten inom statsförvaltningen (informationssäkerhetsförordningen). Finansministeriet har utfärdat en VAHTI-anvisning om styrning av verkställigheten av förordningen och uppfyllandet av kraven. Informationssäkerhetsförordningen upphävdes genom informationshanteringslagen som trädde i kraft den 1 januari 2020. VAHTI-anvisningen om styrning av verkställigheten av informationssäkerhetsförordningen finns i bilaga 1. Vid ansökan om myndighetsgodkännande

[5] För ackrediteringen och Traficoms godkännande krävs dock funktionellt och ekonomiskt oberoende.
[6] Exempelvis ISO 27001:2013-bedömningar som görs av FINAS ackrediteringsorgan och som tillhandahålls sådana privata företag som inte behandlar myndigheters sekretessbelagda information.
[7] Lag om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation, 3 §.

baserat på VAHTI-kriterierna ska objektet uppfylla kraven i informationssäkerhetsförordningen och VAHTI-anvisningen i bilaga 1.

VAHTI 2/2014 Tietoturvallisuuden arviointiohje (Anvisning om bedömning av informationssäkerhet) konstaterar följande om bedömning av informationssäkerheten:

"I 4 §[8] i informationssäkerhetsförordningen fastställs tio krav på informationssäkerhetens basnivå. Dessa krav preciseras och kompletteras av VAHTI-anvisningen 2/2010 som innehåller en detaljerad beskrivning av kraven för alla tre informationssäkerhetsnivåer. Dessa krav ställs på förfarandena och processerna, och utifrån kraven går det inte att fatta beslut om tekniska detaljer och lösningar med vilka nivåkraven kan uppfyllas. För att denna omständighet ska kunna korrigeras har informationssäkerhetsnivåerna beaktats i den VAHTI-anvisning som har publicerats efter att förordningen trätt i kraft. Denna anvisning innehåller krav och rekommendationer om lösningar som kan tillämpas på olika informationssäkerhetsnivåer.

Vid uppfyllande och bedömning av kraven på informationssäkerhetsnivå ska hänsyn inte enbart tas till VAHTI 2/2010 utan särskilt även till följande anvisningar:

VAHTI 3/2010 Sisäverkko-ohje (Anvisning om inomhusnät)
VAHTI 3/2011 Valtion ICT-hankintojen tietoturvaohje (Anvisning om informationssäkerhet i statens IKT-upphandling)
VAHTI 3/2012 Teknisen ympäristön tietoturvataso-ohje (Anvisning om informationssäkerhet i teknisk miljö)
VAHTI 1/2013 Sovelluskehityksen tietoturvaohje (Anvisning om informationssäkerhet vid applikationsutveckling)
VAHTI 2/2013 Toimitilojen tietoturvaohje (Anvisning om informationssäkerhet i verksamhetslokaler)
VAHTI 4/2013 Henkilöstön tietoturvaohje (Anvisning till personal om informationssäkerhet)
VAHTI 5/2013 Päätelaitteiden tietoturvaohje (Anvisning om informationssäkerhet i terminalutrustning)".

Traficom tillämpar anvisningarna ovan så att bedömningar som utgår från VAHTI-kriterierna uppfyller kraven i VAHTI-anvisningarna 2/2010, 3/2010, 3/2012, 1/2013, 2/2013 och 5/2013 i tillämpliga delar. När kraven strider mot varandra är Traficoms tolkning att kraven kan uppfyllas om det strängaste kravet är uppfyllt.

För vissa krav hänvisar VAHTI-publikationerna till Katakri. Bedömning av att dessa krav uppfylls ska göras enligt specifikationerna i Katakri.

3.2.2 Katakri – verktyg för informationssäkerhetsauditering för myndigheter

Katakri är ett verktyg för informationssäkerhetsauditering och har tagits fram av den nationella säkerhetsmyndigheten (NSA, National Security Authority) i syfte att bedöma förmågan att behandla myndigheters sekretessbelagda informationsmaterial. Kraven i Katakri har samlats in så att de utgör

[8] Borde vara 5 §.

en tillräcklig helhet som skyddar sekretessbelagd nationell eller internationell information mot obehörigt avslöjande och obehörig behandling.[9]

Katakri kan användas som auditeringsverktyg när syftet är att verifiera om myndigheters eller företags informationssystem och verksamhet uppfyller de nationella eller internationella informationssäkerhetskrav som har ställts på informationssystemen och verksamheten.

Bedömningsorganen har dock inte behörighet att bedöma sådana av myndigheternas informationssystem som behandlar EU:s eller Natos säkerhetsklassificerade information.

3.2.3 Informationssäkerhetskrav baserade på fastställda standarder

ISO/IEC 27001-standarden innehåller krav på ledningssystem för informationssäkerhet. Vid tillämpning av ISO/IEC 27001-standarden och tillhörande bedömningar kan andra standarder i ISO/IEC 27000-serien användas som hjälp.

3.2.4 Bedömningskriterier för säkerheten av molntjänster

Våren 2019 publicerade Traficom bedömningskriterierna för säkerheten av molntjänster (PiTuKri, endast på finska). Traficom kommer att meddela när bedömningsorganen kan ansöka om PiTuKri-kompetens. Än så länge är det inte möjligt att ansöka om PiTuKri-kompetens.

3.3 Bedömningsförfarandets faser

Bedömningsverksamheten syftar till att ge uppdragsgivaren kunskap om huruvida bedömningsobjektet överensstämmer med kraven. Vid bedömningen klarläggs om de informationssäkerhetskrav som ligger till grund för bedömningen uppfylls på behörigt sätt i objektets verksamhet.

3.3.1 Uppdrag

Bedömningsförfarandet initieras alltid av ett uppdrag. Uppdraget innebär att förfarandet vid bedömningen följer ISO/IEC 17021-standarden[10]. Som slutresultat fastställer bedömningsorganet huruvida kraven som ligger till grund för bedömningen uppfylls. Ett intyg kan endast utfärdas om kraven uppfylls.

I princip avser bedömningsuppdraget vid VAHTI- och Katakri-bedömningar en enskild bedömning. I så fall omfattar uppdraget till exempel inga periodiska inspektioner. Å andra sidan kan uppdragsgivaren och bedömningsorganet även avtala om en mera omfattande bedömningstjänst, till exempel ett bredare bedömningsprogram, uppföljningsåtgärder och ombedömningar.

---

[9] Statsrådets förordning om informationssäkerheten inom statsförvaltningen (681/2010), som varit den viktigaste kravkälla för Katakri, upphävdes den 1 januari 2020. Rådets säkerhetsbestämmelser (2013/488/EU) har i första hand använts som internationell källa.

[10] ISO 17021 bilaga E Tredje parters revisions- och certifieringsprocess. Uppföljande revisioner och ombedömningar sker genom VAHTI- och Katakri-bedömningar, om detta avtalas separat mellan parterna.

Om bedömningsorganet utifrån bedömningen utfärdar ett intyg gäller intyget i högst tre år[11]. Intygets giltighet kan förlängas om objektet uppfyller kriterierna utifrån en ny bedömning.

Begäran om bedömning av myndigheters informationssystem eller datakommunikation görs av den myndighet som bestämmer över systemet eller planerar att skaffa det. Med att bestämma över systemet avses att systemet är tillgängligt för myndigheten, till exempel enligt licensavtal, och huruvida myndigheten har rätt att bestämma över drift, utlämning av uppgifter och annan informationsbehandling. Begäran om bedömning av en myndighets informationssystem kan även göras av den som tillhandahåller databehandlingstjänster som allmänt används av olika statsförvaltningsmyndigheter ifall myndigheten bemyndigat denne.

Bedömningsorganet ska upprätta ett skriftligt avtal om bedömningsuppgiften med uppdragsgivaren. Avtalet ska i vart fall innehålla överenskommelser om bedömningsobjektet, eventuella avgränsningar av det, tillämpade bedömningsgrunder och bedömningskriterier, säkerhetsklasser, bedömningens omfattning och längd, bedömningsrapporten till uppdragsgivaren och annat dokumentmaterial samt avgifter för bedömningen.

Enligt 9 § 2 mom. i lagen om bedömningsorgan kan bedömningen även vara partiell. På så sätt är det möjligt att göra bedömningen exempelvis endast utifrån del F i Katakri. Att bedömningen har varit partiell ska dock på ett tydligt sätt framgå av rapporten och ett eventuellt intyg.[12] En partiell bedömning är dock inte allmängiltig enligt VAHTI- eller Katakri 2015-kraven.

Bedömningsorganet ska i uppdragsavtalet försäkra sig om att det har rätt att få behövliga uppgifter och tillträde till berörda lokaler för utförande av bedömningsuppgiften. Dessutom ska bedömningsorganet försäkra sig om att uppgifter om bedömningen i tillräcklig grad är tillgängliga för bedömningsorganet och Traficom även efter att bedömningsuppdraget har slutförts. Bedömningsorganet ska i sex år efter varje bedömning förvara ett sådant relevant bevismaterial om VAHTI- och Katakri-bedömningarna som påverkar bedömningsresultatet.

Bedömningsorganen kan dock inte bedöma sådana informationssystem som behandlar Natos, EU:s eller ESA:s säkerhetsklassificerade information. I Finland har enbart Traficom behörighet att inspektera informationssystem som innehåller internationell säkerhetsklassificerad information. Därför får bedömningsorganen inte ta emot bedömningsuppdrag gällande informationssystem som behandlar internationell säkerhetsklassificerad information.

Enligt 9 § i säkerhetsutredningslagen har Traficom behörighet att som ett led i en säkerhetsutredning av företag göra en utredning om nivån på informat-

[11] Undantaget utgörs dock av de informationssystem inom social- och hälsovården som har tagits fram enligt föreskriften av Institutet för hälsa och välfärd och för vilka intyg kan beviljas för fem år, se 3.6.
[12] Se 3.3.5 Utfärdande av intyg.

ionssäkerheten i informationssystem och datakommunikation. Som grundläggande material är det möjligt att använda den bedömning som bedömningsorganet gjort för testsystem.

Sådana här bedömningar kan användas till exempel om bedömningsorganets bedömning gäller ett separat informationssystem som företaget senare vill ansluta till ett informationssystem eller en databehandlingsmiljö som omfattas av säkerhetsutredning av företag och som en del av säkerhetsutredningen av företag. Då är det dock Traficom som utför den slutliga inspektionen av säkerhetsutredningen av företag. Här är det också att beakta att bedömningsorganen inte kan bedöma sådana informationssystem som behandlar EU:s, Nato:s eller ESA:s säkerhetsklassificerade information eller annan internationellt säkerhetsklassificerad information som endast får behandlas av utsedda myndigheter. Vad gäller internationella data ska man alltid före inspektionen hos Traficom säkerställa huruvida bedömningsorganet kan utföra bedömningen, eftersom utgångspunkten är att det inte kan utföra dem.

3.3.2 Hur informationssäkerhetskrav som ligger till grund för bedömningen uppfylls

När VAHTI eller Katakri används som bedömningskriterier sker bedömningen enligt kraven i 3.3 Bedömningsmetoder. I inspektionen ska bedömningsorganet granska lokalerna hos objektet eller försäkra sig om att en behörig myndighet (Skyddspolisen eller huvudstaben) har inspekterat dem. Ett intyg kan inte utfärdas på grundval av bedömningen utan behörig inspektion av lokalerna.

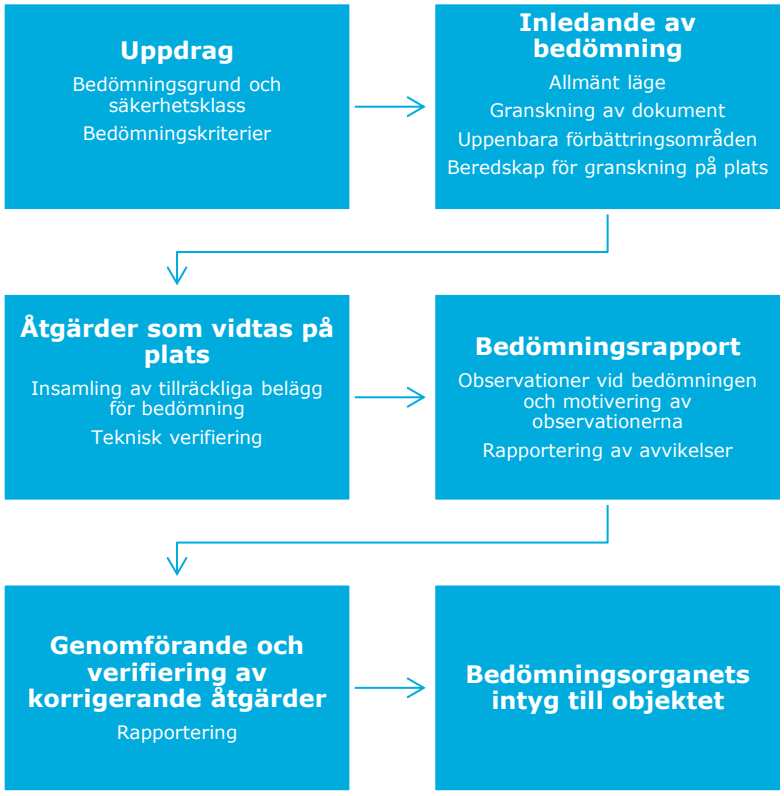
Vissa enskilda informationssäkerhetskrav förutsätter godkännande av den nationella säkerhetsmyndigheten. Sådant godkännande kan krävas till exempel för krypteringsprodukter, gatewaylösningar och motåtgärder mot kompromettерande strålning (TEMPEST)[13]. Bedömningsobjektet ska på förhand skaffa myndighetsgodkännandena inför bedömningen. I bedömningen fastställer bedömningsorganet att godkännande har sökts och att verksamheten på objektet motsvarar kraven och villkoren för godkännandet (till exempel villkoren för användning av krypteringsprodukter). Bedömningsorganet kan ansöka om bedömning av krypteringsprodukter hos Traficom i en så kallad CAA-process.

3.3.3 Tillämpat bedömningsförfarande

Vid förfarandet för bedömning av informationssäkerheten tillämpas processkraven i standarderna ISO/IEC 17021 och ISO/IEC 27006 i tillämpliga delar.

[13] Krypteringslösningar som har godkänts av Traficoms NCSA-verksamhet, guide om gatewaylösningar och principer för förebyggande av informationssäkerhetsrisker via elektromagnetisk strålning, se https://www.kyberturvallisuuskeskus.fi/sv/var-verksamhet/ncsa.

Dessutom kan förfaranden enligt ISO 19011 och ISO/IEC 27007-standarderna tillämpas vid bedömningsförfarandet[14].



Figur 1. Exempel på hur en bedömning av informationssäkerheten fortskrider

3.3.4 Bedömningsrapport och andra handlingar relaterade till bedömningen

En bedömningsrapport om bedömningen av informationssäkerheten och utförda inspektioner ska upprättas enligt kraven i standarderna ISO/IEC 17021 och ISO/IEC 27006. Vid VAHTI- och Katakri-bedömningar ska en kravtabell med bedömningsresultat och motiveringar alltid bifogas rapporten. Rapporten och den bifogade kravtabellen ska ge en tillräckligt omfattande motivering av observationerna och de grunder på vilka enskilda ärendepunkter har godkänts eller underkänts. Traficom ger bedömningsorganen en rapportmall för Katakri-bedömning. En motsvarande rapportmall ska också användas vid VAHTI-bedömningar.

Bedömningsorganet ska dokumentera dokument- och bevismaterial som skapas vid utförandet av bedömningsuppgiften med tillräcklig noggrannhet

[14] ISO 19011:2011 ”Guidelines for auditing management systems”/ SFS-EN ISO 19011 ”Vägledning för revision av ledningssystem”, ISO 27007 Guidelines for information security management systems auditing

så att observationerna kan verifieras i efterhand. För verifiering av observationer i efterhand ska bedömningsorganet dessutom försäkra sig om dokument- och bevismaterialets tillgänglighet.[15]

3.3.5 Utfärdande av intyg

Bedömningsorganet ska utfärda ett intyg för bedömningsobjektet, om objektets verksamhet och lokaler uppfyller de informationssäkerhetskrav som ligger till grund för bedömningen. Ett intyg kan endast beviljas när alla krav har uppfyllts.

Ett intyg kan beviljas när bedömningen har genomförts i informationssystemet så att den har riktats till systemet eller en sådan del av systemet som med tanke på informationssäkerheten kan skiljas åt från andra system eller deras delar. Bedömningsobjektet ska med andra ord avgränsas så att objektet utgör en helhet som med tillräckligt tillförlitliga gränssnitt för den aktuella säkerhetsklassen har skilts åt från de informationssystem som har utelämnats från bedömningen.[16]

På grund av Katakris struktur kan ett intyg endast beviljas för avsnitt T eller avsnitten T och F i en partiell Katakri-bedömning. Ett intyg kan inte utfärdas enbart utifrån en bedömning av avsnitt F eller I.

Intyget ska innehålla åtminstone följande uppgifter:

- Vem intyget har beviljats
- Bedömningens omfattning (avgränsning och specificering av objektet, ange i en separat bilaga var informationssystemet används och eventuella övriga sekretessbelagda ärenden och långa beskrivningar)
- Bedömningsgrunder för informationssäkerhet, dvs. bedömningskriterier
- Tillämpad informationssäkerhetsnivå
- Datum för beviljande av intyget
- Sista giltighetsdag
- Åtagande: ”Bedömningsobjektet ska till intygsutfärdaren anmäla alla förändringar på objektet som kan påverka uppfyllandet av informationssäkerhetskraven. Bedömningsobjektet förbinder sig att behålla informationssäkerhetsnivån för informationssystemet på samma nivå som den var när bedömningen gjordes.”
- 9 § i lagen om bedömningsorgan för informationssäkerhet
- Den huvudsakliga kvalitetsrevisorns underskrift och namnförtydligande
- Utfärdaren av intyget (bedömningsorganets namn och FO-nummer)

[15] Bedömningsorganet ska i sex år efter varje bedömning förvara ett sådant relevant bevismaterial som påverkar bedömningsresultatet.
[16] Se även 3.4.1.5 om avgränsning.

Bedömningsorganet kan även lämna andra uppgifter i intyget.[17]

Bedömningsorganet ska fastställa ett datum för när giltighetstiden för intyget går ut. Intyget får gälla i högst tre år.[18]

3.3.6 Publicering av bedömningsuppgifter

När bedömningskriterierna är andra än ISO/IEC 27001, ska bedömningsorganet endast göra uppgifter som avses i punkterna 8.1.3 och 8.3 i ISO/IEC 17021-standarden offentligt tillgängliga, om myndigheten som begärt bedömningen har gett skriftligt samtycke till detta.

Enligt 13 a § i lagen om bedömningsorgan ska Traficom i registret över säkerhetsutredningar anteckna uppgifter om godkända bedömningsorgan samt uppgifter som ingår i intyg som getts till bedömningsorgan. Ett godkänt bedömningsorgan kan för anteckning i registret över säkerhetsutredningar och för vidarebefordran ur registret lämna Traficom uppgifter om dem som det har bedömt och om innehållet i det intyg som det har utfärdat, om inte den som bedömningen gäller har förbjudit detta. Före underrättelsen ska den som bedömningen gäller informeras om syftet med databehandlingen och den reglering som gäller den.

3.3.7 Uppföljningsåtgärder

Om bedömningsorganet utfärdar ett intyg över att informationssäkerhetskraven uppfylls på bedömningsobjektet, ska intyget förutsätta att objektet anmäler alla förändringar på objektet som kan påverka uppfyllandet av kraven och att objektet förbinder sig att behålla informationssäkerhetsnivån för informationssystemet på samma nivå som den var när bedömningen gjordes. När bedömningsorganet underrättas om en förändring som gör att bedömningsobjektet inte längre uppfyller de krav som har legat till grund för bedömningen, ska organet samråda med innehavaren av intyget och ge innehavaren möjlighet att avhjälpa bristerna. Om bristerna inte har avhjälpts inom skälig tid ska bedömningsorganet återkalla intyget. Bedömningsorganet ska underrätta uppdragsgivaren om att intyget återkallas.

Övriga uppföljningar och ombedömningar utförs av bedömningsorganet på uppdragsbasis.

---

[17] Andra uppgifter kan till exempel vara en uppgift om att bedömningen omfattat en mera omfattande bedömning som även innebär andra metoder än de verifieringsmetoder som är i överensstämmelse med kraven. Beroende på systemet som bedöms ska avsnitten 3.6.2 och 3.7.2 i anvisningen också beaktas i intyget.

[18] Enligt 19 k § i lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården kan intyg vid bedömning av informationssystemen inom social- och hälsovården emellertid gälla i fem år. Också enligt 26 § 3 mom. i lagen om sekundär användning kan bedömningsorganets intyg vara i kraft högst fem år.

3.4 Bedömningsmetoder

3.4.1 Allmänna principer för bedömningsverksamheten

3.4.1.1 Skydd av kunduppgifter

Katakri-skyddskraven ska uppfyllas under hela livscykeln för information vid behandling av kunduppgifter. Vid teknisk inspektion ska man särskilt beakta

- separering av information/kundspecifik dedikering[19]
- inspektionsutrustningens integritet och tillförlitligheten hos mätdata samt
- datatransport och -lagringspraxis.

3.4.1.2 Inspektionsutrustningens integritet och tillförlitligheten hos mätdata

Tillförlitligheten hos inspektionsutrustningens mätdata ska kunna säkerställas. Framförallt ska man säkerställa att

- utrustningen kalibreras från en pålitlig källa före varje inspektionsbesök och
- att mätresultatens riktighet kontrolleras ur flera källor[20].

3.4.1.3 Bedömning av kumulativ effekt

Med kumulativ effekt avses fenomen där kundhelheten i informationssystem som har en stor mängd information med en viss säkerhetsklass ofta får en högre klass än säkerhetsklassen för enskilda uppgifter. En kumulativ effekt gäller vanligen information med nivå IV (till exempel en stor mängd information med TL IV kan sammantaget utgöra en informationsmängd med TL III).

När informationsmängdens säkerhetsklass till följd av den kumulativa effekten tolkas överstiga de enskilda informationsenheternas klass ska de specificerade skyddsmetoderna för informationsmängden genomföras enligt kraven för den högre säkerhetsklassen. Med specificerade skyddsmetoder avses metoder för att begränsa tillgången till enbart en sådan enskild eller begränsad del av informationsinnehållet som behövs i uppgiften, och för att upptäcka obehöriga försök att få tillgång till en större del av informationsinnehållet.

När Katakri används som bedömningsverktyg, ska den kumulativa effekten tolkas så att skyddet av informationsmängden ska uppfylla kraven i punkterna I 13 (applikationsskiktets säkerhet), I 10 och I 11 (spårning och observationsförmåga) samt I 06 (separering av uppgifter) utöver kravet på fysisk säkerhet i informationsmängden i enlighet med den högre nivån. Det bör därför beaktas att en sådan säkerhetsklass för informationsmängden

[19] Utrustning som ansluts till kundens nätverk får inte innehålla andra kunders uppgifter.
[20] Exempel: implementering av uppdateringspraxisen ska verifieras genom att intervjua minst en person, ta del av processbeskrivningar (eller motsvarande), undersöka uppdateringsnivån inifrån systemet (till exempel kontrollera tidsstämplar för installation av säkerhetsuppdateringar i själva systemet) och utföra en extern sårbarhetsskanning.

som har höjts med en klass till följd av den kumulativa effekten inte kräver en godkänd gatewaylösning mellan informationsmängden (till exempel TL III) och terminalutrustningen (till exempel TL IV). När bedömningskriterierna i sin tur är VAHTI ska följande ämnesområden granskas i enlighet med den nivå som har höjts med en klass:

1) applikationsskiktets säkerhet
2) spårning och observationsförmåga
3) separering av uppgifter
4) fysisk säkerhet i informationsmängden.

3.4.1.4 Tillämpliga hotmodeller

System med säkerhetsklass IV ska skyddas mot hot där den som attackerar har allmänna resurser och/eller kunskaper på låg eller mellannivå. Exempel: anslutningspunkter i fjärrlösningar som kan nås från offentliga nät ska hållas strikt på de publicerade säkerhetsuppdateringarnas nivå och utnyttjandet av publicerade 0-dags sårbarheter ska stoppas på andra sätt[21].

System med säkerhetsklass III ska skyddas mot hot där den som attackerar har större resurser och/eller kunskaper. Exempel: behandling av information med säkerhetsklass III ska begränsas till fysiska lokaler som är godkända och uppfyller kraven.

3.4.1.5 Avgränsningar

Informationen ska skyddas enligt kraven under hela livscykeln i alla användningssituationer och användningsmiljöer. Vid till exempel inspektion av arbetsstationer ska man beakta implementeringen av processerna för första installation, uppdaterings- och ändringshantering och avinstallation samt olika användningsmiljöer (till exempel distansarbete). I inspektioner som syftar till ett myndighetsgodkännande eller ett intyg från bedömningsorganet krävs det att inspektionen utvidgas till alla miljöer där den skyddade informationen befinner sig under sin livscykel i användningssituationer där ett godkännande/intyg söks. Om inspektionen till exempel gäller ett informationssystem i ämbetsverk A, ska inspektionen även omfatta alla arbetsstationer och nät där systemet används eller där det är möjligt att på något annat sätt påverka skyddet av informationen. Traficom ger bedömningsorganen närmare anvisningar om specifikationerna av avgränsningen i olika inspektionstyper och användningssituationer.

3.4.2 Minimikrav på administrativ verifiering

Minimikraven på administrativ verifiering beskrivs i tabell 1. Tabellen listar erfordrade verifieringsmetoder och de säkerhetsklasser för vilka metoderna krävs.

[21] Den sårbara komponenten kan till exempel tas ur drift i avvaktan på att säkerhetsuppdateringen har publicerats och installerats.

ID	Verifieringsmetod	Nivå	Observera
A1	Intervjuer	IV och III	Relevanta personer som intervjuobjekt, typiskt företrädare för ledningen, administration/utveckling och slutanvändare
A2	Granskning av dokumentation	IV och III	Omfattar nätverksdiagram, system- och processbeskrivningar o.d.

Tabell 1. Minimikrav på administrativ verifiering:

Denna anvisning beskriver inte tilläggskraven på administrativ verifiering av säkerheten i system på säkerhetsklasserna II–I.

3.4.3 Minimikrav på teknisk verifiering

Minimikraven på teknisk verifiering beskrivs i tabell 2. Tabellen listar erfordrade verifieringsmetoder och de säkerhetsklasser för vilka metoderna krävs.

ID	Verifieringsmetod	Nivå	Observera
T1	Passiv gränssnittsanalys	IV och III	Metoden ska inkludera uppgörande av nätverks-/och systemdiagram och trafikanalyser.
T2	Granskning av systemkonfigurationernas säkerhet	IV och III	Metoden ska täcka alla delområden som påverkar objektets säkerhet[22].
T3	Aktiv gränssnittsanalys	IV och III	Metoden ska inkludera port- och sårbarhetsskanning (kända sårbarheter) och test av driftsäkerhet[23] (okända sårbarheter).
T4	Granskning av applikationssäkerhet per systemtyp	IV och III	Metoden ska omfatta granskning av programkomponenter som påverkar objektets säkerhet, till exempel webbapplikationer, Java-server/klientprogram och ERP-systemens interna åtkomstkontrollmekanismer.
T5	Verifiering av krypteringslösningarnas säkerhet	IV och III	På objekt som använder en krypteringslösning godkänd av Traficoms NCSA-verksamhet ska man bedöma om krypteringsinställningar och administrativa rutiner är tillräckligt säkra.

[22] Typiska delområden är operativsystem för servrar och arbetsstationer samt andra programinstallationer på plattformen, konfigurationer av nätutrustning, databaskonfigurationer och andra program som påverkar systemets säkerhet.

[23] Med test av driftsäkerhet avses i denna anvisning framförallt prov genom inmatning av felaktiga data (fuzz testing). Test av driftsäkerhet krävs bara för säkerhetskritiska systemkomponenter. Exempel på sådana är gatewaylösningar på säkerhetsklass III, gränssnitt mellan olika nätverkstekniker samt åtkomstkontrollmekanismer för stora datamassor (kumulativ effekt).

			Då objektet inte använder en NCSA-godkänd krypteringslösning ska NCSA:s bedömning av lösningens säkerhet inhämtas.
T6	Tillgänglighetsprov (inkl. belastningsprov)	IV och III	Krävs bara för system med höga tillgänglighetskrav (till exempel säkerhetssystem som skyddar människoliv). Bedömningsorganet ska ha kapacitet att utföra stresstester av applikationer, testa förmågan att motstå blockeringsattacker och bedöma objektets förfaranden för kontinuitetshantering/driftsäkerhet.
T7	Verifieringsmetoder för skydd av fysisk säkerhet	IV och III	
T8	Test av gatewaylösningarnas säkerhet	III	På objekt som använder en gatewaylösning enligt Traficoms guide om gatewaylösningar[24] ska man bedöma om lösningen är tillräckligt säker jämfört med de krav som beskrivs i guiden. Då objektet inte använder en ovan avsedd lösning ska NCSA:s bedömning av lösningens säkerhet inhämtas.
T9	Test av förmågan att upptäcka incidenter	IV och III	Metoden ska inkludera test av förmågan att upptäcka obehöriga åtgärder och försök till sådana framförallt i miljöer med säkerhetsklass III.
T10 (*)	Verifiering av skydd mot komprometterande strålning	III	Kravnivån ska kontrolleras hos respektive informationsägare. Krävs till exempel för EU:s säkerhetsklassificerade information på Confidential-nivå.
T11 (*)	Verifiering av existensen av otillåten teknisk utrustning	III	Kravnivån ska kontrolleras objektspecifikt hos respektive informationsägare eller en av ägaren bemyndigad instans. Krävs vanligen inte till exempel för serverlokaler där sekretessbelagd information inte diskuteras.

Tabell 2. Minimikrav på teknisk verifiering:

De verifieringsmetoder som i tabell 2 är markerade med asterisk (*) kan utkontrakteras till en DSA-myndighet[25]. Denna anvisning beskriver inte tilläggskraven på teknisk verifiering av säkerheten i system på nivåerna II–I.

[24] Traficoms ”Guide om planeringsprinciper och lösningsmodeller för gatewaylösningar”, se https://www.kyberturvallisuuskeskus.fi/sv/var-verksamhet/ncsa.
[25] DSA-myndigheterna är Skyddspolisen, huvudstaben, försvarsministeriet och Traficom.

3.4.4 Verifieringsmetoder vid användning av bedömningskriterier

Vid VAHTI- och Katakri-bedömningar krävs en säkring ur flera tillämpliga källor av att de gjorda observationerna är korrekta (jfr avsnitt 3.4.1.2). Vid ansökan om VAHTI- eller Katakri-kompetensområde ska sökanden kunna visa hur denne ska kontrollera att bedömningskriterierna har uppfyllts så att varje kriterium blir verifierat på ett tillräckligt tillförlitligt sätt. I VAHTI- och Katakri-bedömningarna ska bedömningsorganet verifiera uppfyllandet av kraven minst enligt de verifieringsmetoder som avser de aktuella bedömningskriterierna och som har godkänts av Traficom.

3.5 Bedömningsorganets bedömning i förhållande till Traficoms bedömning samt ett så kallat myndighetsgodkännande

Med myndighetsgodkännande avses, till skillnad från intyg som beviljas av bedömningsorgan för informationssäkerhet, av hävd ett sådant intyg som Traficom beviljar med stöd av 8 § i bedömningslagen för informationssystem. Traficom kan bevilja intyget utifrån sin bedömning av informationssystemet eller så att ett bedömningsorgan har gjort en korrekt avgränsad och godkänd bedömning av informationssystemet och sammanställt en tillräcklig rapport om bedömningen.

För att bedömningsobjekt på ett ändamålsenligt sätt ska kunna specificeras i bedömningar som syftar till ett myndighetsgodkännande ska Traficom kontaktas redan i det inledande skedet av bedömningen. En förutsättning för ett myndighetsgodkännande är alltid att alla använda kriterier uppfylls.

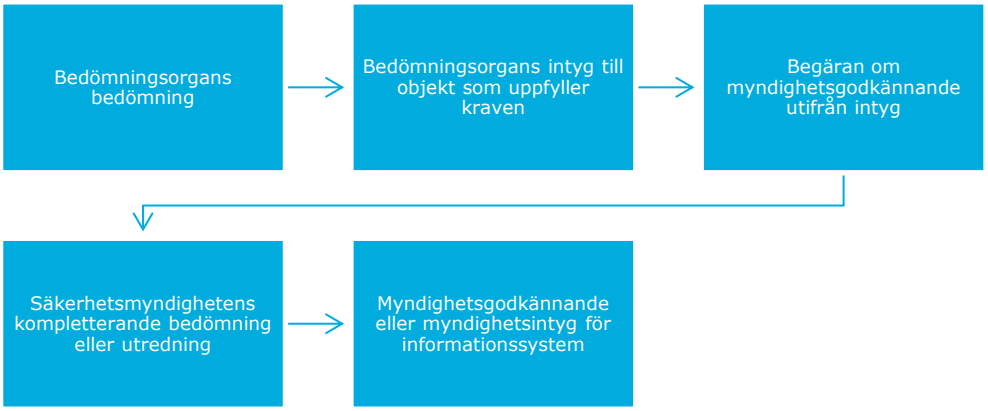


Bild 2. Förfarande för godkännande av objektet

Ansökan om myndighetsgodkännande beskrivs närmare i Traficoms anvisning ”Bedömnings- och godkännandeprocesser av informationssystem utförda av Transport- och kommunikationsverket Traficom – Beställarorganisationens perspektiv”.[26] (på finska)

[26] Se https://www.kyberturvallisuuskeskus.fi/sv/var-verksamhet/ncsa

I fråga om avgiften för myndighetsgodkännande gäller vad som föreskrivs i lagen om grunderna för avgifter till staten (150/1992) och i kommunikationsministeriets förordning om avgifter som tas ut för Transport- och kommunikationsverkets prestationer som gäller elektronisk kommunikation (1149/2018).

3.6 Bedömning av informationssäkerheten i de informationssystem inom hälso- och sjukvården som ansluts till Kanta-tjänsterna

3.6.1 Bedömning av överensstämmelsen med kraven

Med informationssystem inom hälso- och sjukvården avses en programvara eller ett system för elektronisk behandling av klientuppgifter inom socialvården eller hälso- och sjukvården som används för lagring och uppdatering av klient- eller journalhandlingar. Sådana system inom social- och hälsovården som ska bedömas vad gäller informationssäkerheten[27] är även förmedlingsservice varmed klientuppgifter inom socialvården eller hälso- och sjukvården förmedlas till de riksomfattande informationssystemtjänster (Kanta-tjänster) som Folkpensionsanstalten (Fpa) förvaltar. Informationssystemen inom social- och hälsovården omfattas av lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården (klientuppgiftslagen[28]), och lagen fastställer väsentliga krav på informationssystemen och hur kraven verifieras. Enligt lagen om elektroniska recept tillämpas kraven även på de datasystem som används när elektroniska recept görs upp och expedieras och den programvara som stöder systemen, och enligt lagen om klienthandlingar inom socialvården[29] på behandlingen av klientuppgifter inom socialvården.

Enligt 19 b § i klientuppgiftslagen indelas informationssystemen enligt användningsändamål och egenskaper i klasserna A och B. Till klass A hör Kanta-tjänsterna som förvaltas av Fpa, de informationssystem som är avsedda att anslutas till Kanta-tjänsterna antingen direkt eller via en teknisk förmedlingstjänst och den förmedlingsservice som avses i klientuppgiftslagen. Klassificeringen av informationssystemen ankommer på tillverkaren av systemen. Institutet för hälsa och välfärd har utfärdat närmare anvisningar om klassificering av informationssystem.

Bedömningar av informationssäkerheten i system som hör till klass A får endast göras av bedömningsorgan vars kompetensområde är VAHTI eller Katakri. System som hör till klass B beviljas inte sådana överensstämmelseintyg som avses i klientuppgiftslagen.

Bedömningar av system som hör till klass A genomförs enligt bestämmelserna i lagen om bedömningsorgan och klientuppgiftslagen. Institutet för hälsa och välfärd har preciserat de väsentliga kraven på informationssystemen inom social- och hälsovården i sin föreskrift och bilagan till föreskriften.[30]

---

[27] De omfattas dock inte av Fpa:s samtestning.
[28] https://www.finlex.fi/sv/laki/ajantasa/2007/20070159
[29] https://www.finlex.fi/sv/laki/ajantasa/2015/20150254
[30] Föreskrift om väsentliga krav på informationssäkerhet hos informationssystem av klass A inom social- och hälsovården och Bilaga 1 krav på informationssäkerhet hos system av klass A

De förfaranden som beskrivs i denna anvisning och föreskriften från Institutet för hälsa och välfärd ska iakttas i bedömningen. En bedömning enligt klientuppgiftslagen omfattar inte en bedömning och inspektion av vare sig tillverkaren av informationssystemen eller användarens lokaler.

Bedömningsorganet ska i tid ombes göra en bedömning av informationssäkerheten i ett informationssystem. Tillräcklig tid ska reserveras för bedömningen. Bedömningen ska göras redan före Fpa:s samtestning. En förutsättning för beviljande av överensstämmelseintyg är dock alltid att Fpa har utfärdat ett utlåtande om samtestning. Utlåtandet får vara högst fem år gammalt.

Verifiering av överensstämmelse med kraven hos informationssystem som hör till klass A sker[31]

1. genom att tillverkaren av informationssystemet lämnar en redogörelse (systemblankett) för att systemet uppfyller alla krav på informationssystemets funktionalitet (se föreskrift 2/2016 av Institutet för hälsa och välfärd)
2. genom en godkänd samtestning som ordnats av Fpa
3. genom en bedömning av informationssäkerheten gjord av ett bedömningsorgan för informationssäkerhet (kriterierna är föreskrift 1/2015 av Institutet för hälsa och välfärd).

Bedömningsorganet beviljar endast ett överensstämmelseintyg för informationssystemet, om systemet uppfyller kraven 1–3 ovan. Intyget visar att systemet uppfyller de krav som har ställts på informationssystem genom föreskrift av Institutet för hälsa och välfärd, en systemblankett har sammanställts och Fpa har gjort en samtestning av systemet.

3.6.2 Innehåll i överensstämmelseintyget

Minimiinnehållet i bedömningsorganets överensstämmelseintyg beskrivs i avsnitt 3.3.5. Dessutom ska följande anges i separata punkter i överensstämmelseintyg som utfärdas för informationssystem inom social- och hälsovården:

- Det handlar om ett överensstämmelseintyg som har beviljats utifrån klientuppgiftslagen. Intyget visar att informationssystemet uppfyller föreskriften av Institutet för hälsa och välfärd om väsentliga krav på informationssäkerhet hos informationssystem av klass A inom social- och hälsovården (1/2015).
- Tjänster som tillhandahålls via systemet (Recept/Patientdataarkivet/Klientdataarkivet för socialvården/Arkivet över bildmaterial/Datalagret för egna uppgifter).

---

och på systemets användningsmiljöer: https://thl.fi/sv/web/informationshantering-inom-social-och-halsovarden/foreskrifter-och-specifikationer/foreskrifter

[31] 19 d § 1 mom. och 19 k § 2 mom. i klientuppgiftslagen.

- Profiler för de funktionella krav som har genomförts i systemet (som tillverkaren har angett på systemblanketten).
- Preciseringar av hur överensstämmelsen har införts (i situationer där det behövs ytterligare uppgifter om på vilket sätt ett krav har uppfyllts eller ska uppfyllas; om utlåtandet om samtestning innefattar begränsningar ska dessa även ingå i intyget)[32].
- En förteckning eller uppgifter om eventuella krav som har verifierats eller som uppfylls via ett annat system; vid behov ytterligare uppgifter.
- En förteckning eller uppgifter om eventuella krav som endast kan uppfyllas genom särskilda åtgärder vidtagna av organisationer som använder systemet; vid behov ytterligare uppgifter.
- Datum och nummer på utlåtandena om Fpa:s samtestning[33]; utlåtandena ska bifogas överensstämmelseintyget.

Bedömningsorganet kan bevilja ett intyg för ett informationssystem som hör till klass A och som är en del av en mer omfattande systemhelhet i Kanta, så att systemet använder andra delar av helheten för att kunna genomföra Kanta-förbindelserna eller för att kunna uppfylla vissa informationssäkerhetskrav. Sådana faktorer och krav ska beskrivas på ett tydligt sätt i överensstämmelseintyget.

Av överensstämmelseintyg som finns på finska eller svenska ska det på ett tydligt sätt framgå vad som har bedömts och när. Om det finns fel i intyget eller om intyget inte har upprättats enligt denna anvisning, ska intyget rättas till.

Överensstämmelseintyget är giltigt i högst fem år. Efter bedömningsorganets övervägande kan giltighetstiden även vara kortare till exempel om det på grund av informationssystemets utvecklingsskede eller en känd ändring av de väsentliga kraven är uppenbart att systemet inte i fem år uppfyller de väsentliga kraven utan att det görs betydande ändringar i systemet. Bedömningsorganet ska motivera en giltighetstid som är kortare än fem år.

3.6.3 Betydelse av överensstämmelseintyg

Bedömningsorganets överensstämmelseintyg används åtminstone för följande ändamål:

---

[32] Faktorer som ska beaktas i driftmiljön för systemet respektive vid användningen av systemet tillsammans med andra system. Det är inte nödvändigt att redogöra för hur ett visst problem har lösts. Däremot ska nödvändiga ytterligare uppgifter lämnas om hur bedömningsgrunderna har tillämpats. Ett villkor som skrivs i överensstämmelseintyget kan till exempel vara att överensstämmelseintyget har beviljats för en systemhelhet och att överensstämmelsen ska bedömas på nytt om helhetens systemarkitektur har ändras. En begränsning som skrivs i intyget kan till exempel vara att systemet endast genomför anordnarens del, inte producentens del, av funktionen Fullmakt för köpta tjänster.

[33] Intyget ska förses med det senaste överensstämmelseutlåtandet/de senaste utlåtandena som gäller bedömningsobjektet.

– Ett informationssystem som används i produktionen och som hör till klass A ska ha ett giltigt överensstämmelseintyg.

– Uppgifterna i intyget ska lämnas till Valvira, som utifrån uppgifterna uppdaterar uppgifterna i det offentliga registret över informationssystem som hör till klass A.

– Fpa granskar intyget innan en förbindelse till Kanta-tjänsterna öppnas för den tillhandahållare av tjänster som använder systemet.

3.6.4 Uppföljning efter ibruktagandet och bedömningsorganets anmälningsskyldighet

Tillverkaren eller producenten av informationssystemet ska underrätta bedömningsorganet om ändringar i systemet och betydande avvikelser som har upptäckts i produktionen av systemet.[34] Institutet för hälsa och välfärd har utfärdat en anvisning om anmälan om ändringar i informationssystem av klass A inom social- och hälsovården (Anvisningar för anmälan av ändringar i informationssystem av klass A inom social- och hälsovården 2/2018). Bedömningsorganets överensstämmelseintyg ska förnyas om betydande ändringar har gjorts i informationssystemet eller om de väsentliga kraven har förändrats. Om bedömningsorganet konstaterar att ett informationssystem inte längre uppfyller de krav som har ställts på informationssystem eller att ett överensstämmelseintyg inte borde ha beviljats, ska organet uppmana tillverkaren eller producenten av informationssystemet att avhjälpa bristerna. Bedömningsorganet får återkalla intyget för viss tid eller helt och hållet eller bevilja intyget med begränsningar, om inte tillverkaren avhjälper bristerna inom den skäliga tid som organet satt ut[35]. Begränsningen kan röra till exempel intygets giltighetstid eller uppgifter som får behandlas i systemet.

Ett bedömningsorgan ska underrätta Valvira och Fpa om alla överensstämmelseintyg som har utfärdats, ändrats eller kompletterats eller som har återkallats för viss tid eller helt och hållet eller förvägrats. Dessutom ska bedömningsorganet på begäran ge Valvira all behövlig ytterligare information om de informationssystem för vilka organet har beviljat överensstämmelseintyg.[36]

3.7 Bedömning av informationssäkerhet i en driftmiljö enligt lagen om sekundär användning

3.7.1 Bedömning av överensstämmelsen med kraven

Tillståndsmyndigheten för social- och hälsovårdsuppgifter Findata förvaltar en informationssäker driftmiljö i enlighet med lagen om sekundär användning av personuppgifter inom social- och hälsovården (552/2019, lagen om

[34] 19 g § i klientuppgiftslagen.
[35] När tidsfristens längd bestäms ska det beaktas att en skälig tid behövs för att ändra informationssystemet.
[36] 19 m § i klientuppgiftslagen.

sekundär användning).[37] De datamaterial som Findata beviljat dataanvändningstillstånd, lämnas i regel ut för tillståndshavarens behandling i Findatas driftmiljö. Om datamaterial begärts för behandling i en annan driftmiljö än i Findatas informationssäkra driftmiljö, får Findata eller en annan myndighet som avses i lagen om sekundär användning lämna ut uppgifter till sökanden endast om driftmiljön uppfyller villkoren i 30 § 2 mom. och i 21–29 §. Sökanden ska dessutom iaktta de allmänna informationssäkerhetskrav som krävs i 18 § i lagen om sekundär användning där det anges att när personuppgifter behandlas med stöd av denna lag ska en tillräcklig informationssäkerhet för behandlingen säkerställas genom riskhantering, åtkomsthantering, aktiv övervakning och genom iakttagande av föreskrifter och anvisningar från den myndighet som svarar för förverkligandet och övervakningen av informationssäkerhet och dataskydd. Särskild uppmärksamhet ska fästas vid att användningsbegränsningar och sekretessplikten iakttas.

Enligt 24 § 2 mom. i lagen om sekundär användning meddelar Findata närmare föreskrifter om de krav som ska ställas på andra tjänsteleverantörers informationssäkra driftmiljöer. Findata har enligt 24 § 2 mom. i lagen om sekundär användning meddelat förskriften 1/2020[38] om krav som ska ställas på andra tjänsteleverantörers informationssäkra driftmiljöer. Enligt lagen om sekundär användning är det tillåtet att analysera datamaterial på individnivå endast i de driftmiljöer som uppfyller föreskriftens krav. Kraven förutsätter informationssäkerhet på motsvarande nivå som i Findatas egen driftmiljö.

I praktiken ska informationssäkerheten i driftmiljön påvisas genom ett intyg från ett bedömningsorgan för informationssäkerhet.[39] Bedömningsorganet ska i tid ombes göra en bedömning av informationssäkerheten i ett informationssystem. Tillräcklig tid ska reserveras för bedömningen. Ett bedömningsorgan för informationssäkerhet bedömer i enlighet med lagen om sekundär användning, på ansökan om driftmiljön uppfyller kraven på informationssäkerhet. Som bedömningskriteriet ska användas Findatas föreskrift 1/2020.[40]

Om driftmiljön uppfyller informationssäkerhetskraven enligt Findatas föreskrift 1/2020, ska bedömningsorganet för informationssäkerhet ge tjänsteleverantören ett intyg över sin bedömning och en anknytande kontrollrapport.[41] Efter detta kan Findata överväga och lämna ut datamaterial till sökanden för behandling i en annan driftmiljö än sin egen driftmiljö.

[37] 20 § 1 mom. i lagen om sekundär användning.
[38] Föreskrift 1/2020 av Tillståndsmyndigheten för användning av social- och hälsovårdsdata: Krav som ska ställas på andra tjänsteleverantörers informationssäkra driftmiljöer.
[39] 25 § 1 mom. i lagen om sekundär användning.
[40] 26 § 1 mom. i lagen om sekundär användning.
[41] 26 § 2 mom. i lagen om sekundär användning.

3.7.2 Innehållet i intyget över överensstämmelse med krav och kontrollrapport

Bedömningsorganet beviljar intyget till leverantören av en driftmiljö.[42] Minimiinnehållet i bedömningsorganets överensstämmelseintyg beskrivs i avsnitt 3.3.5. Utöver minimiinnehållet ska följande anges i separata punkter i överensstämmelseintyg som utfärdas för en driftmiljö enligt lagen om sekundär användning:

- Det är fråga om ett överensstämmelseintyg som utfärdats på basis av lagen om sekundär användning och påvisar att informationssystemet uppfyller kraven i Findatas föreskrift 1/2020: Krav som ska ställas på andra tjänsteleverantörers informationssäkra driftmiljöer
- Identifierande uppgifter omfattar överensstämmelseintygets nummer/ID, namnet på tjänsteleverantörens driftmiljö[43] samt FO-nummer/Registreringsbeteckning
- Om bedömningen eller en förnyad bedömning gäller endast en del av driftmiljön, ska det i bedömningsorganets intyg tydligt antecknas vilken del av driftmiljön som har bedömts. [44] I intyget ska också finnas en motivering till varför en del av driftmiljön inte har bedömts.
- Begränsningar som bedömningsorganet för informationssäkerhet ställt för driftmiljön eller tjänsteleverantören.[45]
- Allmän beskrivning av driftmiljön och dess användningsändamål
- Är det fråga om en första bedömning eller en förnyad bedömning (om förnyad bedömning, identifieringskod för det gamla och det nya intyget, om de avviker från varandra)
- Om det vid bedömningen av överensstämmelse har använts gällande certifikat ska de räknas upp och nämnas till vilken del varje certifikat tolkas motsvara kraven för ett visst delområde och hur länge certifikaten är i kraft.

Bedömningsorganets intyg är i kraft högst fem år. Bedömningsorganet för informationssäkerhet kan av tjänsteleverantören kräva alla de uppgifter som förutsätts för bedömningen och för uppgörandet och upprätthållandet av intyget.

---

[42] Med tjänsteleverantör avses den organisation, för vilket intyget utfärdas och från vilket Valvira tar emot registreringsanmälan om driftmiljön. Om verksamheten omfattar flera organisationer, utfärdas intyget dock endast för en organisation som ska ha avtal om verksamheten med de övriga organisationerna. I Valviras register tas emot en anmälan endast av en aktör vars driftmiljö även kan vara ett föremål för myndighetens tillsynsåtgärder.

[43] Driftmiljön ska ha ett individuellt namn i ett sådant format som används när driftmiljön tillhandahålls kunden. Intyget utfärdas för samma driftmiljö som Valvira registrerat på basis av en registreringsanmälan.

[44] 26 § 2 mom. i lagen om sekundär användning.

[45] 27 och 28 § i lagen om sekundär användning.

På utfärdandet av intyg tillämpas i övrigt 9 § 3 mom.[46] i lagen om bedömningsorgan för informationssäkerhet enligt vilket det godkända bedömningsorganet för informationssäkerhet utfärdar på basis av utredningarna och granskningen ett intyg, om lokalerna och verksamheten hos den som bedömningen gäller är förenliga med de bedömningsgrunder som legat till grund för utredningen. De grunder för bedömning av informationssäkerheten som använts vid bedömningen och bedömningens omfattning ska specificeras i intyget.

3.7.3 Betydelse av överensstämmelseintyg

Bedömningsorganets överensstämmelseintyg används åtminstone för följande ändamål:

- Driftmiljöer utanför Findata där det behandlas datamaterial med personuppgifter i enlighet med lagen om sekundär användning ska ha ett giltigt intyg över överensstämmelse med krav som förutsätts i lagen om sekundär användning.

- Bedömningsorganet skickar uppgifterna i intyget över överensstämmelse med krav samt kontrollrapporten till Valviras registratorskontor via säker e-post (kirjaamo[at]valvira.fi). Valvira för ett offentligt register över de driftmiljöer som uppfyller kraven och som anmälts till verket.

3.7.4 Uppföljning efter ibruktagandet och bedömningsorganets anmälningsskyldighet

Tjänsteleverantören ska genom ett uppdaterat och systematiskt förfarande följa upp och utvärdera erfarenheterna av den informationssäkra driftmiljön under den tid den används för produktion. Tjänsteleverantören ska ge akt på ändringar i lagen om sekundär användning och justera driftmiljön i enlighet med ändringarna. Väsentliga förändringar i driftmiljön ska anmälas till bedömningsorganet för informationssäkerhet. Bedömningsorganets intyg ska förnyas, om betydande förändringar görs i driftmiljön eller om minimikraven på driftmiljön har ändrats på ett sätt som förutsätter en förnyad bedömning.[47]

Tjänsteleverantören ska bevara uppgifterna om överensstämmelse med kraven och övriga uppgifter som tillsynen kräver i minst fem år efter det att den informationssäkra driftmiljön inte längre används för produktion.[48]

Om ett bedömningsorgan för informationssäkerhet konstaterar att en driftmiljö inte har uppfyllt eller inte längre uppfyller kraven i lagen om sekundär användning och i Findatas föreskrift 1/2020 eller att ett intyg av någon annan orsak inte borde ha beviljats, ska organet uppmana tjänsteleverantören att avhjälpa bristerna och underrätta Valvira om detta. Bedömningsorganet får återkalla intyget för viss tid eller helt och hållet eller bevilja intyget med begränsningar, om inte tjänsteleverantören avhjälper bristerna inom den

[46] 26 § 3 mom. i lagen om sekundär användning.
[47] 29 § 1 mom. i lagen om sekundär användning.
[48] 29 § 2 mom. i lagen om sekundär användning.

skäliga tid som organet satt ut. När tidsfristens längd bestäms ska det beaktas att en skälig tid behövs för att ändra användningsmiljön.[49]

Bedömningsorgan för informationssäkerhet ska underrätta Valvira om alla intyg som har utfärdats, ändrats eller kompletterats eller som har återkallats för viss tid eller helt och hållet eller förvägrats samt om de uppmaningar och begränsningar som avses i 27 § i lagen om sekundär användning. Dessutom ska bedömningsorgan för informationssäkerhet på begäran ge Valvira all behövlig ytterligare information i ärendet.[50]

4 Övervakning och kvalitetssäkring av bedömningsorgan

4.1 Styrning och övervakning av bedömningsorgan

Traficom styr och övervakar godkända bedömningsorgan för informationssäkerhet i syfte att trygga en kvalificerad och tillförlitlig bedömningsverksamhet och säkerställa att organen har enhetliga tillvägagångssätt. Styr- och övervakningsmedel är anvisningar och myndighetsrådgivning till bedömningsorgan, fastställande av villkor och begränsningar för godkännande och övervakning av bedömningsorganens verksamhet, till exempel inspektioner av deras verksamhet och utfallen. Inspektioner kan göras periodiskt eller genom stickprov på objekt som ska myndighetsgodkännas eller andra objekt.

Bestämmelser om Transport- och kommunikationsverkets inspektionsrätt finns i 7 § lagen om bedömningsorgan och bestämmelser om återkallelse av godkännande av bedömningsorgan i 6 §.

4.2 Bedömningsorganets informations- och anmälningsskyldighet

4.2.1 Årlig anmälan

Som en del av övervakningen av bedömningsorgan vid Traficom ska godkända bedömningsorgan lämna en årlig anmälan till Traficoms registratorskontor (registrator[at]traficom.fi) före utgången av mars det år som följer på anmälningsåret. **En årlig anmälan ska göras om den verksamhet som bedömningsorganet har bedrivit i egenskap av ett av Traficom godkänt bedömningsorgan.**[51] Anmälan ska göras med Traficoms blankett.

4.2.2 Bedömningsuppgifter och uppgifter om lägesbilden som ska anmälas i förväg

Traficom ska i förväg underrättas om en bedömning som ett av Traficom godkänt bedömningsorgan avser att göra i sin egenskap och där bedömningskriterierna är VAHTI eller Katakri.

---

[49] 27 § i lagen om sekundär användning.
[50] 28 § i lagen om sekundär användning.
[51] Traficom övervakar inte verksamhet som bedrivs utanför bedömningsorgan för informationssäkerhet och som beskrivs i avsnitt 2.1.

Anmälan ska lämnas till Traficom per säker post på ncsa[at]traficom.fi och arviointilaitokset[at]traficom.fi så att rubriken börjar med ordet ”Bedömningsorgan:” eller via wiki för bedömningsorgan.

En tabell om lägesbilden i excel-format ska lämnas in för alla bedömningar som under innevarande år är under arbete (inklusive uppdrag som har inletts redan under tidigare år) under första veckan **varje månad**.

Vid ett nytt projekt ska **tabellen om lägesbilden uppdateras** med uppgifterna om det nya projektet, och tabellen ska lämnas in **inom två veckor efter att projektet har inletts**. Datumet för när ett projekt inleds är datumet för när kunden har kvitterat att ett anbud godkänts, eller någon annan motsvarande bekräftelse av att projektet inleds.

Anmälan ska innehålla

- uppgifter om bedömningsobjektet och de kriterier som ska användas
- bedömningstidpunkt
- det godkända bedömningsorganets kontaktperson av vem ytterligare information kan begäras

I anslutning till uppdraget ska bedömningsorganet informera bedömningsobjektet om att

- Traficom kommer att underrättas om bedömningen
- Traficom vid behov får delta i bedömningen
- bedömningsrapporten och bedömningsintyget kommer att lämnas till Traficom för kännedom och registrering.

4.2.3 Bedömningsrapporter och intyg som lämnas till Traficom

För att Traficom ska kunna utföra sin övervakningsuppgift ska bedömningsorganet lämna Traficom kopior av de **bedömningsrapporter** och eventuella **intyg** som organet i egenskap av ett av Traficom godkänt bedömningsorgan har lämnat till kunden. Intyg och rapporter krävs dock inte för bedömningar där kriterierna är andra än VAHTI eller Katakri.

Handlingarna ska lämnas in på ett USB-medium av en personkurir eller alternativt genom att använda en av Traficom godtagen TC-kryptering enligt III, tilläggsskyddade per säker post på arviointilaitokset[at]traficom.fi och ncsa[at]traficom.fi.

Samtidigt ska bedömningsorganet till Traficom ange om uppgifterna i intyget med kundens samtycke får antecknas i registret över säkerhetsutredningar i enlighet med 13 a § i lagen om bedömningsorgan.[52]

4.2.4 Uppgifter om ändringar

Ett av Traficom godkänt bedömningsorgan ska underrätta Traficom om sådana ändringar i sin verksamhet som har betydelse för de skyldigheter som organet har. Meddelandet ska skickas per e-post på ncsa[at]traficom.fi och

[52] Se 3.3.6 Publicering av bedömningsuppgifter

arviointilaitokset[at]traficom.fi så att rubriken börjar med ordet ”Arviointilaitos:”.

I oklara fall finns det skäl att informera om ändringarna, varvid myndigheten som gett godkännandet avgör om ändringen har betydelse för organets skyldigheter.

Om ett bedömningsorgan lägger ned sin verksamhet eller verksamheten överlåts till ett annat företag till exempel genom företagsförvärv, är det fråga om en sådan ändring som avses i paragrafen ovan och som Traficom ska underrättas om. Eftersom en sådan ändring har betydelse ska Traficom underrättas om ändringen utan dröjsmål.

Andra fall som ett bedömningsorgan ska underrätta Traficom om är till exempel förändringar i organets ledning eller kvalitetsrevisorer eller i företagets lokaler (till exempel nya lokaler eller en väsentlig strukturell ändring i de gamla lokalerna).

När Traficom har tagit emot anmälan bedömer Traficom om bedömningsorganet fortfarande uppfyller de krav som har ställts på godkännande, och uppmanar vid behov organet att avhjälpa bristerna inom utsatt tid.

5 Anlitande av bedömningsorgans tjänster

Enligt 3 § i bedömningslagen får statsförvaltningsmyndigheterna för bedömning av informationssäkerheten i sina informationssystem och sin datakommunikation bara använda sig av ett sådant bedömningsorgan som har godkänts av Traficom.

Bedömningsorgan får också sälja sina bedömningstjänster till andra organisationer än myndigheterna. I så fall kan det vara fråga om bedömningsorganets tjänster i egenskap av ett godkänt bedömningsorgan eller externa tjänster (se 3.1).

Avsnitt 3.3.1 beskriver det uppdrag som ett bedömningsorgan får av en kund. Avsnitt 3.3.6 beskriver förutsättningarna för publicering av bedömningsuppgifter. Avsnitt 3.3.7 handlar om uppföljningsåtgärder efter en bedömning.

Bedömningsorganen bör beakta Traficoms övervakningsverksamhet. Därför ska bedömningsorganen lämna Traficom kopior av de rapporter som organen har sammanställt och av de intyg som de har beviljat i egenskap av godkända bedömningsorgan (se 4.2.3). Uppgifterna i intyget antecknas även med samtycke av bedömningsorganets kund i registret över säkerhetsutredningar (se 4.2.3). Dessutom har Traficoms tjänstemän möjlighet att övervaka bedömningsorganets bedömning hos kunden (se 4.2.2).

6 Anvisningens ikraftträdande

Denna anvisning träder i kraft den 18 december 2020.

Helsingfors den 18 december 2020

Tf. överdirektör Sauli Pahlman

Direktör Aki Tauriainen

Denna handling har i stället för underskrifter verifierats så att av den framgår föredragandens och beslutsfattarens namn. Beslutet har föredragits för beslutsfattaren per e-post. Detta exceptionella verifieringssätt är tillfälligt i bruk med anledning av åtgärderna för att begränsa spridningen av coronaviruset, varför den tjänsteman som behandlar ärendet arbetar på distans och det normala sättet att underteckna handlingar inte är möjligt.

7 BILAGOR

1. Viktigaste styrande normer för bedömningsverksamheten

Bilaga 1: Viktigaste styrande normer för bedömningsverksamheten

Denna bilaga listar de viktigaste normerna för verksamheten i bedömningsorgan för informationssäkerhet, vilka personer som arbetar för dess räkning ska känna till.

I Lagstiftning

- **Lag om offentlighet i myndigheternas verksamhet (621/1999)**

  Offentlighetslagen innehåller bestämmelser om offentlighet för myndigheternas handlingar och grunderna för sekretessbeläggning samt andra för skyddande av allmänna och enskilda intressen nödvändiga begränsningar av rätten att ta del av handlingar.

- **Lag om informationshantering inom den offentliga förvaltningen (906/2019)**

- **Statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019)**

- **Lag om bedömningsorgan för informationssäkerhet (1405/2011)**

  Lagen innehåller bestämmelser om kraven och förfarandet för godkännande av bedömningsorgan samt om bedömningsorganens uppgifter och skyldigheter.

- **Lag om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011)**

  Lagen innehåller bestämmelser om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation samt om bedömningsgrunder för informationssäkerhet.

- **Lag om elektronisk behandling av klientuppgifter inom social- och hälsovården (159/2007)**

  Lagen innehåller bestämmelser om kraven på informationssäkerhet i informationssystem som används vid behandling av klientuppgifter inom social- och hälsovården, verifiering av kraven och uppgifter som ankommer på godkända bedömningsorgan för informationssäkerhet.

- **Lag om sekundär användning av personuppgifter inom social- och hälsovården (552/2019)**

  I lagen finns bestämmelser om sekundär användning av personuppgifter inom social- och hälsovården, krav på driftmiljöer och uppgifter som ankommer på godkända bedömningsorgan för informationssäkerhet.

- **Lag om elektroniska recept (61/2007)**

  Lagen innehåller bestämmelser om elektroniska recept, när de informationssystem som används vid uppgörandet och expedieringen av elektroniska recept ska utvärderas enligt lagen om elektronisk behandling av klientuppgifter inom social- och hälsovården innan systemen tas i bruk.

- **Dataskyddslag (1050/2018)**

  Europaparlamentets och rådets förordning (EU) 2016/679 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

- **Lag om internationella förpliktelser som gäller informationssäkerhet (588/2004)**

  Lagen innehåller bestämmelser om säkerhetsåtgärder för skydd av särskilt känsligt material för att uppfylla internationella förpliktelser som gäller informationssäkerhet.

- **Säkerhetsutredningslag (726/2014**)

  Lagen innehåller bland annat bestämmelser om förutsättningarna för säkerhetsutredningar av person och företag och om förfarandet vid genomförande av sådana, giltigheten av säkerhetsutredningar och intyg över säkerhetsutredningar som har utfärdats utifrån utredningarna samt om återkallelse av intyg.

II Beslut

- FINAS-tjänstens ackrediteringsbeslut inklusive villkor
- Traficoms beslut om godkännande inklusive villkor

III Föreskrifter, anvisningar, rekommendationer mm.

- Traficoms anvisning till bedömningsorgan för informationssäkerhet
-
- Katakri 2015 – Verktyg för informationssäkerhetsauditering för myndigheter

- Anvisning om verkställighet av förordningen om informationssäkerheten inom statsförvaltningen (VAHTI 2/2010)
- Sisäverkko-ohje (VAHTI 3/2010 Anvisning om inomhusnät)
- Teknisen ICT-ympäristön tietoturvataso-ohje (VAHTI 3/2012 Anvisning om informationssäkerhet i teknisk miljö)
- Sovelluskehityksen tietoturvaohje (VAHTI 1/2013 Anvisning om informationssäkerhet vid applikationsutveckling)
- Valtionhallinnon toimitilojen tietoturvaohje (VAHTI 2/2013 Anvisning om informationssäkerhet i statsförvaltningens lokaler)
- Päätelaitteiden tietoturvaohje (VAHTI 5/2013 Anvisning om informationssäkerhet i terminalutrustning)

För vissa krav hänvisar VAHTI-publikationerna till Katakri. Bedömning av att dessa krav uppfylls ska göras enligt specifikationerna i Katakri. Observera att villkoret för myndighetsgodkännande utöver administrativ säkerhet alltid är att de tekniska skyddskraven uppfylls.

- Föreskrift av Institutet för hälsa och välfärd om väsentliga krav på system inom social- och hälsovården.

- Tolkningsriktlinjer och andra anvisningar som listas på Traficoms webbplats eller i övrigt delgetts bedömningsorganen.

- Föreskrift 1/2020 av Tillståndsmyndigheten för användning av social- och hälsovårdsdata: Krav som ska ställas på andra tjänsteleverantörers informationssäkra driftmiljöer