VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Tiedonhallintalautakunta
Informationshanteringsnämnden

Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet

Nämnder

Finansministeriets publikationer – 2020:77

Finansministeriets publikationer 2020:77

Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet

Finansministeriet, Helsingfors 2020

Finansministeriet

ISBN PDF: 978-952-367-519-3

Layout: Statsrådets förvaltningsenhet, publikationsverksamheten

Helsingfors 2020

Presentationsblad

Utgivare	Finansministeriet		20.10.2020
Författare	Informationshanteringsnämnden		
Publikationens titel	Rekommendationssamling om tillämpningen av vissa bestämmelser om informationssäkerhet		
Publikationsseriens namn och nummer	Finansministeriets publikationer 2020:77		
Diarie-/ projektnummer	-	**Tema**	Nämnder
ISBN PDF	978-952-367-519-3	**ISSN PDF**	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-367-519-3		
Sidantal	72	**Språk**	svenska
Nyckelord	nämnder, informationshanteringsnämnden, lagen om informationshantering inom den offentliga förvaltningen, informationssäkerhet, den offentliga förvaltningen, riskhantering, livscykel, loggfiler		

Referat

Denna rekommendationssamling som utfärdats av informationsförvaltningsnämnden ger vägledning när det gäller att uppfylla de krav som ställs i lagen om informationshantering inom den offentliga förvaltningen.

Kapitel 4 i informationshanteringslagen innehåller de krav på informationssäkerhet som alla myndigheter som hör till tillämpningsområdet för lagen om informationshantering inom den offentliga förvaltningen ska uppfylla. För att se till att informationssäkerhetskraven uppfylls har informationshanteringsnämnden gett rekommendationer som gäller informationssäkerhet.

Informationshanteringsnämnden godkände rekommendationssamlingen den 26 mars 2020 och kompletteringen den 23 juni 2020.

Ersätter versionen som publicerades den 1 april 2020 (Finansministeriets publikationer 2020:21).

Förläggare	Finansministeriet
Distribution/ beställningar	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: vnjulkaisumyynti.fi

Kuvailulehti

Julkaisija	Valtiovarainministeriö		20.10.2020
Tekijät	Tiedonhallintalautakunta		
Julkaisun nimi	Suosituskokoelma tiettyjen tietoturvallisuussäännösten soveltamisesta		
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisuja 2020:77		
Diaari/hankenumero	-	**Teema**	Lautakunnat
ISBN PDF	978-952-367-519-3	**ISSN PDF**	1797-9714
URN-osoite	http://urn.fi/URN:ISBN:978-952-367-519-3		
Sivumäärä	72	**Kieli**	ruotsi
Asiasanat	lautakunnat, tietoturva, julkinen hallinto, riskienhallinta, elinkaari, lokitiedostot, tiedonhallintalautakunta, tiedonhallintalaki		

Tiivistelmä

Tämä tiedonhallintolautakunnan antama suosituskokoelma opastaa tiedonhallintalain asettamien erinäisten vaatimusten täyttämisessä.

Tiedonhallintalain luku 4 sisältää tietoturvallisuutta koskevat vaatimukset, jotka kaikkien tiedonhallintalain soveltamisalaan kuuluvien viranomaisten tulee täyttää. Tietoturvallisuusvaatimusten toteuttamiseksi tiedonhallintalautakunta on antanut tietoturvallisuutta koskevia suosituksia.

Tiedonhallintalautakunta hyväksyi suosituskokoelman 26.3.2020 ja täydennyksen 23.6.2020.

Korvaa 1.4.2020 julkaistun version (Valtiovarainministeriön julkaisuja 2020:21).

Kustantaja	Valtiovarainministeriö
Julkaisun jakaja/myynti	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: vnjulkaisumyynti.fi

Description sheet

Published by	Ministry of Finance		20 October 2020
Authors	Information Management Board		
Title of publication	Collection of recommendations on the application of certain information security provisions		
Series and publication number	Publications of the Ministry of Finance 2020:77		
Register number	-	**Subject**	Board
ISBN PDF	978-952-367-519-3	**ISSN (PDF)**	1797-9714
Website address (URN)	http://urn.fi/URN:ISBN:978-952-367-519-3		
Pages	72	**Language**	Swedish
Keywords	board, Information Management Board, Information Management Act, Boards, information security, public administration, risk management, lifecycle, log files		

Abstract

This collection of recommendations issued by the Information Management Board provides guidance on the fulfilment of a number of requirements set out in the Information Management Act.

Chapter 4 of the Information Management Act lists the information security requirements that must be met by all authorities covered by the Information Management Act. To ensure that the information security requirements are fulfilled, the Information Management Board has issued various recommendations on information security.

The Information Management Board approved the collection of recommendations on 26 March 2020 and the supplement on 23 June 2020.

Replaces the version published on 1 April 2020 (Publications of the Ministry of Finance 2020:21).

Publisher	Ministry of Finance
Distributed by/ Publication sales	Online version: julkaisut.valtioneuvosto.fi Publication sales: vnjulkaisumyynti.fi

Innehåll

1 Inledning

Informationshanteringsnämnden har utfärdat denna samling rekommendationer som handledning för uppfyllande av de särskilda kraven i lagen om informationshantering inom den offentliga förvaltningen (906/2019, nedan informationshanteringslagen).

Kapitel 4 i informationshanteringslagen innefattar informationssäkerhetskrav som ska uppfyllas av alla myndigheter som omfattas av lagens tillämpningsområde. Informationssäkerhetsnämnden har gett rekommendationer för uppfyllande av informationssäkerhetskraven.

Allmänna iakttagelser om innehållet i rekommendationerna:

- Rekommendationerna har utfärdats för att de ska stödja utvecklingen av informationshanteringsenheternas respektive myndigheternas verksamhet. De är inte avsedda att användas som revisionskriterier eller bedömningskriterier.
- Rekommendationerna gäller information i alla former, både analogt och elektroniskt format.
- Rekommendationerna hänvisar inte till några allmänna standarder eller referensramar och ger inga anvisningar om tekniska lösningar, som kan förändras till och med snabbt. Utifrån en riskbedömning som görs från fall till fall ska varje myndighet välja tillräckligt säkra tekniska lösningar som är lämpliga i den aktuella situationen.
- Rekommendationerna beskriver rekommendationer och bästa praxis och är inte bindande på samma sätt som lagstiftningen.

Vid behandling av säkerhetsklassificerad information ska statsförvaltningsmyndigheterna beakta rekommendationerna angående både informationshanteringslagen och statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019).

2 Minimikrav på informationssäkerhet

Den offentliga förvaltningen ska iaktta följande minimikrav på informationssäkerhet och rekommendationer för uppfyllande av kraven:

1. Uppgifter som förutsätter särskild tillförlitlighet hos personer som utför uppgifterna ska ha identifierats, 12 §.

2. Informationssäkerhetens tillstånd i enhetens verksamhetsmiljö ska följas upp, 13 § 1 mom.

3. Informationssäkerheten under informationens livscykel ska säkerställas, 13 § 1 mom.
   13 § Hänsyn till livscykeln vid informationsbehandling; rekommendationen beskriver på vilket sätt informationssäkerheten ska beaktas i de olika skedena av informationens livscykel.
   13 § Hänsyn till livscykeln i informationssystem; rekommendationen beskriver på vilket sätt informationssäkerheten ska beaktas i de olika skedena av informationssystemens livscykel.

4. Hanteringen av informationsrisker och de därpå baserade informationssäkerhetsåtgärderna ska vara ordnade, 13 § 1 mom.
   13 § Riskhantering; rekommendationen beskriver på vilket sätt hanteringen av informationsrisker kan genomföras i informationshanteringsenheterna.

5. Informationssystemens feltolerans och funktionella användbarhet ska ha säkerställts, 13 § 2 mom.

6. Offentlighets- och sekretesstrukturen ska ha beaktats i informationslagrens strukturer, 13 § 3 mom.

7. De informationssystem som ska upphandlas ska ha lämpliga säkerhetsåtgärder, 13 § 4 mom.
   Kort 13 § Informationssäkerhet vid upphandlingar; rekommendationen beskriver på vilket sätt informationssäkerheten ska beaktas på ett tillräckligt sätt vid upphandlingar.

8. När sekretessbelagd information överförs i det allmänna datanätet ska informationen vara skyddad, 14 § 1 mom.

9. Säkerheten i fråga om informationsmaterial ska ha säkerställts, 15 §.
   15 § Skydd mot skador; rekommendationen beskriver på vilket sätt information och informationssystem kan skyddas mot tekniska och fysiska skador.
10. Informationsmaterial ska behandlas i tillräckligt säkra lokaler, 15 § 2 mom.
11. Användarrättigheterna för informationssystem ska ha definierats och administrerats, 16 §.
12. Den logginformation som behövs ska ha insamlats om användning av informationssystem och om utlämnande av information, 17 §.
    17 § Insamling av logginformation; rekommendationen beskriver vilka faktorer som ska beaktas vid insamlingen av logginformation.
13. De säkerhetsklassificerade handlingarna och behandlingen av handlingarna ska ha ombesörjts, 18 §.

Myndigheten ska bedöma vad en viss planerad ändring i informationshanteringsmodellen innebär för varje minimikrav eller vad som ska beaktas för varje minimikrav vid utvecklingen.

Vid upphandling av nya informationssystemtjänster utgörs kraven på informationssäkerhet av minimikraven och eventuella andra krav som har identifierats utifrån en riskbedömning. Förfarandet för uppfyllande av varje krav ska utvärderas i en riskbedömningsprocess.

3 Riskhantering (13 § 1 mom. i informationshanteringslagen)

En informationshanteringsenhet ska följa upp informationssäkerhetens tillstånd i sin verksamhetsmiljö och säkerställa informationsmaterialens och informationssystemens informationssäkerhet under hela deras livscykel. Informationshanteringsenheten ska identifiera relevanta risker som är förenade med informationsbehandlingen och dimensionera informationssäkerhetsåtgärderna utifrån riskbedömningen.

3.1 Analys och hantering av informationsrisker

Informationshanteringsenheternas goda praxis är att ombesörja riskhanteringen för informationsmaterial, informationslager och informationssystem (1):

- genom att identifiera och värdera relevanta risker
- genom att minska sannolikheten för risker och riskernas konsekvenser till en acceptabel nivå
- genom att upprätthålla den uppnådda nivån eller
- alternativt genom att acceptera alla eller en del av de kvarstående riskerna.

Syftet med riskhanteringen är att genomföra en kombination av informationssäkerhetsåtgärder i syfte att säkerställa en tillräcklig informationssäkerhetsnivå för informationsmaterial och informationssystem och skapa en tillfredsställande balans mellan användarnas krav, kostnader och den kvarstående risken för säkerheten. En proportionerlig riskhanteringsnivå kan uppnås när konsekvenserna för informationen och informationssystemen har identifierats genom en konsekvensanalys och sannolikheten för att riskerna realiseras har beaktats. Säkring av kvaliteten på informationen och informationsmaterialet är en del av riskhanteringen, eftersom oriktig information i sig kan utgöra en stor risk.

Hantering av informationsrisker är kontinuerlig verksamhet. Informationshanteringsenheterna bör beskriva målsättningen, principerna, ansvarsområdena och de relevanta förfarandena för hantering av informationsrisker. Ledningen ansvarar för organiseringen och resursfördelningen för hanteringen av informationsrisker. Hanteringsprocessen påverkar bedömningen och planeringen av informationshanteringsenhetens verksamhet och målsättning. De risker som har upptäckts vid hanteringen av informationsrisker påverkar enhetens åtgärder under hela den tiden enheten är verksam.

Vid hanteringen av informationsrisker används förfaranden som har valts utifrån informationshanteringsenhetens uppgifter och informationsmaterialets omfattning. I små organisationer kan en enda person ha tilldelats ansvaret för samordningen av informationsrisker och samordningen sköts i samarbete mellan ledningen och några personer. Behovet av resurser som krävs för hantering av informationsrisker påverkas av organisationens storlek samt av uppgifternas och informationsmaterialets art. Vanliga kontorsprogram kan användas i processen.

I större organisationer, och särskilt i organisationer som ansvarar för IKT-produktionen, behövs såväl arbetsinsatser av flera experter, mellanledningen och den högre ledningen som särskilda riskhanteringsprogram vid riskhanteringen. I alla organisationer ska ledningen minst en gång om året behandla informationsrisker som en del av den övriga riskhanteringen.

Åtgärderna för att behandla informationsrisker ska dimensioneras till en nivå som har fastställts och accepterats av organisationen. Organisationens ledning har helhetsansvar för riskhanteringen och den acceptabla risknivån. De kvarstående riskerna och de informationssäkerhetsåtgärder som har vidtagits ska följas upp regelbundet. Uppföljningen av informationsrisker ska fortsätta under informationsmaterialets och informationssystemens hela livscykel. I uppföljningen ska det granskas att riskbehandlingsplaner har gjorts upp och att informationssäkerhetsåtgärderna har haft effekt.

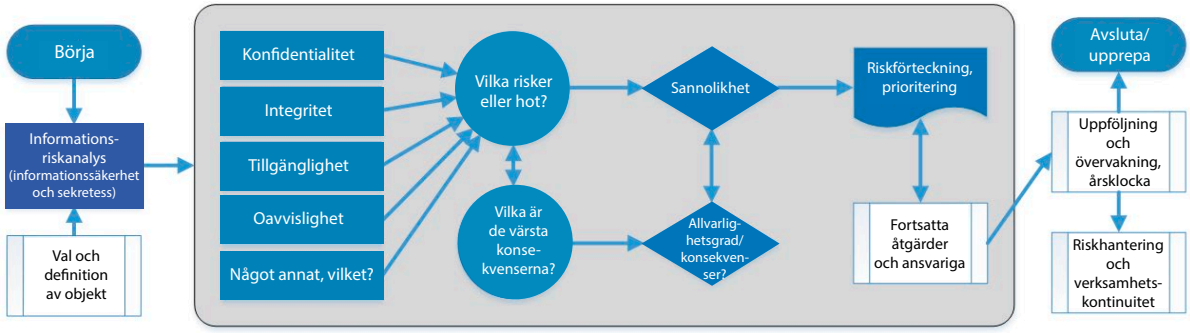
Vid hantering av informationsrisker är det viktigt att föra in alla potentiella informationsrisker i ett riskregister och att bedöma sannolikheten för sådana risker och riskernas konsekvenser. Alla relevanta personer bör delta i kartläggningen av informationsriskerna för bedömningsobjektet och i riskbedömningen för att riskregistret ska bli omfattande och olika experters syner beaktade. Det är också bra att anteckna orsakerna till informationsriskerna och konsekvenserna av en eventuell realisering av riskerna. Ofta är det enklare att ta itu med orsaken till en informationsrisk än med själva risken. Närmare anvisningar om bedömning av sannolikheten för risker och riskernas konsekvenser finns i Anvisningen för riskhantering (Finansministeriets publikationer 22/2017).

Vid sidan av kartläggningen och bedömningen av informationsrisker är det bra att föra in de riskhanteringsåtgärder som redan inletts eller genomförts och potentiella nya åtgärder.

Ägaren till informationsrisken beslutar vilka hanteringsåtgärder som ska genomföras, vilka risker som kan accepteras och vem som ansvarar för åtgärderna och tidsplanen för åtgärderna. Utifrån en riskbedömning ska hanteringsåtgärderna dimensioneras till hoten och konsekvenserna för informationen och informationssystemen.

Riskerna och hanteringsåtgärderna ska också beaktas vid kontinuitetsplaneringen i syfte att säkerställa en tillräcklig tillgång till information eller informationssystem.

Det är bra att på ett systematiskt sätt, till exempel en gång per månad eller minst fyra gånger om året, kontrollera att de överenskomna hanteringsåtgärderna har vidtagits och tidsplanerna följts. En bedömning av informationsriskerna bör göras på nytt när en eller flera hanteringsåtgärder har genomförts.



Figur 1. **Processchema för informationsriskanalys (2)**

3.2 Hantering av kvarstående risker

Risker som fortfarande föreligger efter att hanteringsåtgärder vidtagits och som man inte kan eller vill påverka längre kallas kvarstående risker. Kvarstående risker uppstår till exempel när hanteringsåtgärderna är för dyra eller omfattande i förhållande till riskens konsekvenser. Organisationen ska ha en metod för att behandla kvarstående risker och vid behov även ta upp kvarstående risker i ledningsgruppen. Metoden ska ha godkänts på ledningsgruppsnivå.

3.3 Informationsmaterial som behövs vid hantering av informationsrisker

God praxis är att informationshanteringsenheterna följer upp säkerheten i verksamhetsmiljön utifrån myndighetskällor, myndighetskontakter och mediebevakning samt genom att kontinuerligt övervaka informationssystemen och informationslagren. Vid uppföljningen ska hänsyn tas till eventuell speciallagstiftning, uppförandekoder och annan informationsstyrning, resultatstyrning och ekonomiska resurser. Relevanta myndighetskällor är Cybersäkerhetscentrets rapporter och, i brottmål, polisen.

Vid den egna beredskapen bör den offentliga förvaltningen ta hänsyn till VAHTI-anvisningarna om informationssäkerhet. En anvisning är bland annat att en anmälan om informationssäkerhetsincident ska göras till Cybersäkerhetscentret så fort som möjligt för att den myndighet som berörts av incidenten ska få hjälp för att återställa verksamheten efter situationen. Dessutom rekommenderas alltid en polisanmälan, om vissa brottsrekvisit är uppfyllda. Åtgärder som vidtas i rätt tid är till fördel för både den offentliga förvaltningen och medborgarna.

Vid hantering av informationsrisker utnyttjas både metadata om informationssystem och metadatabeskrivningar för informationsmaterial och informationslager samt för prioritetsklassificeringar av informationslagren och informationssystemen. Metadata om informationssystem ska uppdateras av informationshanteringsenheten och metadatabeskrivningarna ska ingå i en informationshanteringsmodell. Särskild uppmärksamhet ska ägnas åt var informationssystemen och informationslagren är fysiskt belägna och vilka informationsrisker det eventuellt orsakar, med hänsyn till verksamheten och det aktuella informationsmaterialet.

Informationshanteringsenheterna ska administrera informationsmaterialet, som består av riskbedömningarnas resultat och riskbehandlingsplaner. Dessutom ska enheterna göra regelbundna bedömningar av om materialet är helt eller delvis sekretessbelagt eller säkerhetsklassificerat. Myndigheterna ska klassificera informationsmaterialet om informationsrisker som sekretessbelagt om det krävs i sekretessbestämmelserna och, om kraven på säkerhetsklassificering är uppfyllda, även helt eller delvis säkerhetsklassificera materialet.

3.4 Allmänna krav

Följande allmänna krav bör beaktas vid riskhantering:

- Har myndigheten identifierat och dokumenterat all information och alla informationssystem som myndigheten ansvarar för?
- Har de nyckelpersoner som administrerar och använder informationen och informationssystemen identifierats?
- Har eventuella riskfaktorer för informationen, informationssystemen och nyckelpersonerna identifierats?
- Har en konsekvensanalys för informationen och informationssystemen gjorts så att det är möjligt att bedöma om riskhanteringsåtgärderna är proportionerliga eller inte?
- Är riskhanteringsåtgärderna proportionerliga jämfört med konsekvenserna av och sannolikheten för att risken realiseras?
- Förs ett riskregister och görs regelbundna granskningar av att riskhanteringsåtgärderna har effekt?

3.5 Bestämmelser och tilläggsinformation

(1) ISO 31000 Riskhantering

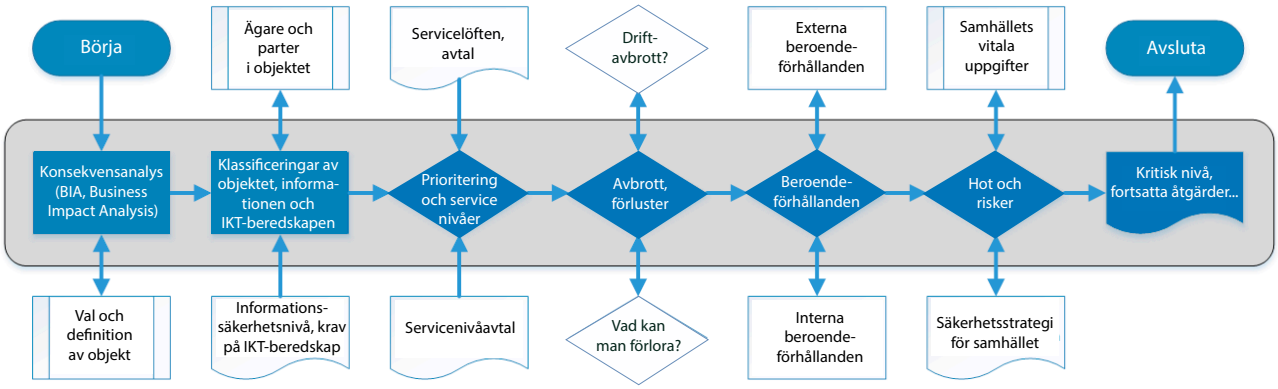
(2) Anvisning för riskhantering – Bilagorna 1–6 (Finansministeriets publikationer 22/2017) (på finska)

Ordnande av riskhantering (finansministeriets webbsidor)

Modell för riskhanteringspolitik (finansministeriets webbsidor)

Anvisning för riskhantering (Finansministeriets publikationer 22/2017) (på finska)

Mer information om metadata och beskrivningar av metadata i Riksarkivets SÄHKE2-bestämmelse.



Figur 2. Processchema för konsekvensanalys (2)

4 Hänsyn till livscykeln vid informationsbehandling (13 § 1 mom. i informationshanteringslagen)

En informationshanteringsenhet ska följa upp informationssäkerhetens tillstånd i sin verksamhetsmiljö och säkerställa informationsmaterialens och informationssystemens informationssäkerhet under hela deras livscykel.

En enskild uppgifts livscykel börjar när uppgiften produceras eller tas emot och slutar när uppgiften överlämnas till ett arkiv för varaktig förvaring eller destrueras. Livscykeln omfattar med andra ord alla skeden i behandlingen av uppgiften, dvs. att **producera** eller **ta emot, förvara, använda, dela, överföra** och arkivera eller **destruera uppgiften**. Livscykeltänkandet utgår från att information behandlas och hanteras på ett systematiskt och riskbaserat sätt som en del av informationshanteringsenhetens verksamhet.

En informationshanteringsenhet ska säkerställa informationsmaterialets informationssäkerhet under informationens hela livscykel genom att identifiera riskerna för behandlingen av informationsmaterialet och genom att dimensionera informationssäkerhetsåtgärderna utifrån riskbedömningen. Informationsmaterialets informationssäkerhet ska uppfylla de minimikrav som fastställs i informationshanteringslagen.

Med tanke på en enskild uppgifts livscykel är det viktigt att beakta att ett informationsmaterial behandlas på många olika ställen och i många informationssystem eller enheter där uppgiften kan ha en egen livscykel, och att uppgiftens livscykel i regel är längre än ett enskilt informationssystems livscykel.

4.1 Informationssäkerhet genom en enskild uppgifts livscykel

Informationssäkerhet under ett enskilt informationsmaterials livscykel utgör en helhet som omfattar **klassificering av informationen, riskbedömning, planering av informationssäkerhetsåtgärder** utifrån identifierade risker och **genomförande av informationssäkerhetsåtgärder**. En informationshanteringsenhet ska bedöma risker för informationsmaterialet regelbundet under materialets hela livscykel och vid informationssäkerhetsplanerna och genomförandet av informationssäkerheten beakta de åtgärder som krävs när riskerna har förändrats. Innan information produceras eller tas emot ska hänsyn tas till definitionen av information och då ska kännetecknande drag för informationen, säkerheten och metadata analyseras. Utifrån definitionen av information skapas principer för behandlingen av informationen under informationens hela livscykel.

I fråga om en enskild uppgift gäller det att identifiera och definiera vad behandlingen av uppgiften bygger på och vilket som är syftet med behandlingen av uppgiften. Dessutom gäller det att se till att det planerade syftet med behandlingen av uppgiften uppfylls under uppgiftens livscykel. I alla skeden av livscykeln gäller det att säkerställa att uppgiften behandlas enligt de krav som föranleds av behandlingsgrunden, med hänsyn till riskerna för uppgiften och enligt informationssäkerhetskraven på uppgiften. Från första början ska informationssäkerhet vara en del av planeringen och genomförandet av de rutiner och behandlingsmiljöer som används i anslutning till behandlingen av informationsmaterial.

Informationshanteringsenheten ska ha kännedom om rutinerna, behandlingsmiljöerna och andra faktorer som har samband med behandlingen, så att enheten kan genomföra en ändamålsenlig informationshantering och bedöma riskerna för informationsbehandlingen. Information behandlas enligt planerna i alla skeden av informationens livscykel. Mer information om behandling av säkerhetsklassificerad information finns i bland annat anvisningen om hantering av internationellt säkerhetsklassificerat informationsmaterial.

En enskild uppgifts livscykel börjar när behandling av uppgiften inleds i anslutning till att uppgiften produceras eller tas emot, och slutar när uppgiften överlämnas för varaktig förvaring i form av arkivering eller destrueras. Livscykeln omfattar med andra ord alla skeden i behandlingen av uppgiften, vilka vanligen är att **producera** eller **ta emot, förvara, använda, dela, överföra** och **arkivera** eller **destruera uppgiften**. Livscykeltänkandet utgår från att information behandlas och hanteras på ett systematiskt och riskbaserat sätt som en del av informationshanteringsenhetens verksamhet.

En informationshanteringsenhet ska säkerställa informationsmaterialets informationssäkerhet under informationens hela livscykel genom att identifiera riskerna för behandlingen av informationsmaterialet och genom att dimensionera informationssäkerhetsåtgärderna

utifrån riskbedömningen. Informationsmaterialets informationssäkerhet ska uppfylla de minimikrav som fastställs i informationshanteringslagen.

Med tanke på en enskild uppgifts livscykel är det viktigt att beakta att ett informationsmaterial behandlas på många olika ställen och i många informationssystem eller enheter där uppgiften kan ha en egen livscykel, och att uppgiftens livscykel i regel är längre än ett enskilt informationssystems livscykel.

Nedan finns viktiga frågor som gäller ett informationsmaterials livscykel:

- Har grunden och användningsändamålet med behandling av informationsmaterialet identifierats och definierats?
- Har en eventuell ändring av informationens användningsändamål beaktats vid informationsbehandlingen?
- Har grunden för informationsbehandling, bland annat de krav som personuppgifter och särskilda kategorier av personuppgifter ställer, identifierats?
- Har riskerna för informationsmaterialet bedömts för informationens hela livscykel? Följs riskerna upp regelbundet?
- Har informationshanteringsenheten kännedom om de rutiner, behandlingsmiljöer och andra faktorer som har samband med behandlingen (en informationshanteringsmodell, dessutom har ministerierna en informationshanteringskarta)?

4.2 Produktion och mottagande av information

Med produktion av information avses det behandlingsskede där ny information produceras eller informationsmaterialet uppdateras. Med mottagande av information avses det behandlingsskede där informationshanteringsenheten tar emot informationsmaterial som har producerats någon annanstans.

När information produceras eller tas emot ska grunderna och syftet med behandlingen av information identifieras och beskrivas. När information produceras eller tas emot gäller det att identifiera de särskilda krav som fastställts på behandling av informationen i lagstiftningen eller i en annan organisations kriterier. Särskilda krav fastställs till exempel i lagen om dataskydd och dataskyddsförordningen gällande personuppgifter. När information produceras och tas emot gäller det att slå fast en preliminär tidsperiod under vilken informationsmaterialet ska förvaras. Den preliminära förvaringstiden kan ännu ändras i olika skeden av informationens livscykel.

Nedan finns viktiga frågor som gäller produktion och mottagande av information:

- Har grunden och användningsändamålet med behandling av informationsmaterialet identifierats och definierats?
- Har de särskilda kraven på det informationsmaterial som ska behandlas, bland annat kraven på personuppgifter, identifierats?

4.3 Förvaring av informationsmaterial

I fråga om förvaring definieras och genomförs ett tillräckligt skydd för den aktuella informationen enligt de krav, de hanteringsmetoder och den risknivå som har fastställts för informationen. Genom skydd av informationen går det att säkerställa informationens fortsatta konfidentialitet och integritet samt informationens tillgänglighet. Skyddet ska omfatta tekniska och administrativa metoder.

När information förvaras gäller det att säkerställa att informationen är tillgänglig och bevaras samt att den är användbar under hela förvaringstiden även om tekniker byts. När förvaringen av ett informationsmaterial planeras och genomförs gäller det att förbereda sig för de hotsituationer som har identifierats i riskbedömningar. Förberedelserna ska ske på den nivå som krävs med tanke på riskerna, bland annat genom lämplig kryptering och kontinuitetshantering. En förvaringstid har fastställts för informationsmaterialet och efter förvaringstiden ska materialet arkiveras eller destrueras. För destruering av informationsmaterial används en dokumenterad process. Mer information om krypteringsmetoder finns bland annat i Vahti-anvisning 2/2015 (på finska).

För förvaring av informationsmaterial används endast förvaringsmiljöer som har accepterats för förvaringssyfte och som uppfyller förvaringskraven och principerna i kapitel 5.

Nedan finns viktiga frågor som gäller förvaring av informationsmaterial:

- Är det informationsmaterial som ska förvaras klassificerat (säkerhetsklassificerat)? Om ja, har förvaringskraven identifierats och uppfylls kraven? Har olika perspektiv, såsom informationssystem, sekretess, informationssäkerhet, verksamhetsprocesser och informationsarkitektur, beaktats vid klassificeringen av informationen?
- Förvaras informationsmaterialet på det sätt att det endast är behöriga personer som har tillgång till materialet?
- Har förvaringen av informationsmaterialet planerats så att materialet också är användbart och tillgängligt under undantagsförhållanden, om det krävs utifrån riskbedömningen?

- Har en förvaringstid fastställts för den information som ska förvaras, så att informationen arkiveras eller destrueras på behörigt sätt efter förvaringstiden?

4.4 Användning av information

Behörig användning av informationsmaterial ska möjliggöras och obehörig användning av materialet förhindras så att rollbaserade fysiska och logiska användarrättigheter och åtkomstbehörigheter fastställs och kontrolleras utifrån enskilda personers arbetsuppgifter. Identiteten hos dem som använder informationsmaterialet ska kontrolleras på ett tillräckligt sätt i förhållande till riskerna och den information som används.

Användningen av informationsmaterialet följs upp och övervakas enligt riskbedömningen. I informationssystemen ska loggar skapas åtminstone om inloggningar och försök till inloggning. I flera situationer ska en händelselogg också skapas i systemet. Logginformation om användning av informationsmaterial ska samlas in och användningen övervakas utifrån en behovsbedömning på det sätt som krävs med tanke på informationens användningsändamål och riskerna med ändamålet. Den ansvariga för denna tjänst ska utreda huruvida logginformation om tjänsten får samlas in eller inte.

Informationsmaterial ska användas i informationssystem, enheter och behandlingsmiljöer som överensstämmer med de uppställda kraven och har accepterats för användningssyfte.

Nedan finns viktiga frågor som gäller användning av informationsmaterial:

- Har användarrättigheterna och åtkomstbehörigheterna för informationsmaterial fastställts utifrån enskilda personers arbetsuppgifter?
- Övervakas användningen av informationsmaterialet enligt riskbedömningen?
- Kan ni vara säkra på att informationsmaterialet endast används för det syfte som materialet (ursprungligen) är avsett för?
- Insamlas logginformation om inloggningar i informationssystemen?
- Kan ni vara säkra på att informationsmaterialet endast behandlas i sådana informationssystem, enheter och behandlingsmiljöer som överensstämmer med de uppställda kraven och har accepterats för behandlingssyfte?

4.5 Delning, överföring och utlämnande av information

Med delning av informationsmaterial avses åtgärder för att bestämma mottagare, verifiera mottagarnas informationsbehov och rätt och förmåga att behandla det informationsmaterial som ska delas. Med överföring av informationsmaterial avses åtgärder för att överföra informationsmaterialet till vissa fastställda parter eller andra informationssystem. Informationsmaterial kan överföras till exempel per post eller e-post, med elektroniska lagringsmedier, genom dataöverföring mellan olika informationssystem eller beviljande av behandlingsrättigheter. Vid delning och överföring av icke offentlig eller säkerhetsklassificerad information gäller det att komma ihåg att vanliga e-postadresser i regel inte är krypterade och säkra kanaler för förmedling av information. Vid överföring av sådan information gäller det särskilt att säkerställa att den metod som används är krypterad och tillräckligt säker. Med utlämnande av information avses att information lämnas till den part som har begärt informationen. Offentlig information lämnas ut enligt lagen om offentlighet i myndigheternas verksamhet.

Vid delning, överföring och utlämnande av information gäller det alltid att på ett tillförlitligt sätt kontrollera identiteten hos en eventuell mottagare och att överföra informationen med lämplig kryptering och skydd i förhållande till de risker som har identifierats. På så sätt är det möjligt att säkerställa att obehöriga inte kommer över informationen och att informationsmaterialet endast delas eller lämnas ut till dem som har rätt till materialet baserat på sina arbetsuppgifter. Mer information om säkerheten i krypteringslösningar finns i kapitel 0, i de krypteringslösningar som Cybersäkerhetscentret har godkänt (på finska) för skydd av säkerhetsklassificerade uppgifter, i tabellerna över krypteringsstyrka (på finska) och i anvisningarna om bedömning (på finska) och säker utveckling av krypteringsprodukter.

När informationsmaterial delas eller överlämnas mellan olika myndigheter, ska hänsyn tas till (den separata) Rekommendationen för tekniska gränssnitt och elektroniska förbindelser. Nedan finns viktiga frågor som gäller delning, överföring och utlämnande av information:

- Kan identiteten hos mottagare verifieras på en tillräcklig nivå när informationsmaterial delas, överförs och lämnas ut?
- Används en lämplig kryptering vid överföring av information?
- Har det vid utlämnande av information kontrollerats att utlämnandet av information är lagenligt och att mottagaren har rätt och förmåga att behandla informationsmaterialet enligt kraven?

4.6 Arkivering av informationsmaterial

Med arkivering av informationsmaterial avses förfaranden för att kontrollera att informationen förblir oförändrad under hela den fastställda livscykeln. Informationsmaterialet ska destrueras eller arkiveras på ett säkert sätt efter att förvaringstiden har gått ut.

Vid arkivering ska hänsyn tas till hur lång tid informationsmaterialet ska förvaras, var och på vilket sätt. Dessutom ska informationens användbarhet och läsbarhet säkerställas under informationens hela förvaringstid. Arkiveringen bygger på bestämmelserna om arkivering och på planer som har gjorts upp utifrån bestämmelserna. Mer information om arkiveringskraven finns på Riksarkivets webbsidor för styrning.

Nedan finns viktiga frågor som gäller arkivering av informationsmaterial:

- Har hänsyn vid arkivering tagits till hur lång tid informationsmaterialet ska förvaras, var och på vilket sätt?
- Har informationens användbarhet och läsbarhet säkerställts under informationens hela förvaringstid?
- Bygger arkiveringen på bestämmelserna om arkivering och på planer som har gjorts upp utifrån bestämmelserna?

4.7 Destruering av information

Med destruering av information avses åtgärder för att avsiktligen destruera informationsmaterial när materialets förvaringstid har gått ut och användningsbehovet upphört eller när utrustning som innehåller information tas ur bruk, sänds för underhåll eller överlämnas för materialåtervinning.

Information ska destrueras på ett tillräckligt tillförlitligt sätt i förhållande till de risker som har identifierats, när den fastställda förvaringstiden har gått ut eller användningsbehovet upphört. Förvaringstiderna för informationsmaterialet ska beaktas vid planeringen av hur informationen ska destrueras. Kopior, utkast och temporära datafiler om informationsmaterialet ska destrueras när de inte behöver användas längre.

Då används metoder som förhindrar att informationen återskapas helt eller delvis. Flera olika metoder och verktyg kan användas för att destruera sekretessbelagd information, beroende på bland annat i vilket format informationen finns och vilka lösningar som finns tillgängliga. I stället för eller förutom att förstörelsemaskinen till exempel tuggar sönder informationsmaterialet eller hårddisken raderas kan materialet brännas och disken smältas.

Särskilt förfarandena för tillförlitlig destruering av elektroniskt material ska gälla alla enheter där sekretessbelagd information har sparats under enheternas livscykel. Särskilt när delar av enheter (hårddiskar, minnen, minneskort osv.) tas ur bruk, sänds för underhåll eller överlämnas för materialåtervinning, ska sekretessbelagd information destrueras på ett tillförlitligt sätt. Om en tillförlitlig radering (till exempel genom en raderingsmetod som godkänts av myndigheten) (på finska) inte är möjlig, ska delar som innehåller sekretessbelagd information inte överlämnas till tredje part. När minnet eller motsvarande inte kan raderas på ett tillförlitligt sätt innan underhållsåtgärder vidtas, bör de underhållsåtgärder som vidtas av tredje part övervakas. Dessutom gäller det att kontrollera att sekretessbelagd information inte tas bort i anslutning till åtgärderna. Om information destrueras av en serviceproducent, ska myndigheten på ett tillförlitligt sätt säkerställa att informationen destrueras på rätt sätt.

Nedan finns viktiga frågor som gäller destruering av information:

- Sker destrueringen av information på ett tillräckligt tillförlitligt sätt när den utsatta tiden har gått ut eller användningsbehovet upphört? Används då metoder för att förhindra att informationen återskapas helt eller delvis?
- Gäller förfarandena för tillförlitlig destruering alla enheter där sekretessbelagd information har sparats under enheternas livscykel?

4.8 Bestämmelser och tilläggsinformation

EU:s allmänna dataskyddsförordning

Arkivlag

De krypteringslösningar som har godkänts av Cybersäkerhetscentret (på finska)

De raderingsmetoder som har godkänts av Cybersäkerhetscentret (på finska)

Cybersäkerhetscentrets anvisning: Kryptografiska krav av konfidentialitet – nationella skyddsnivåer (på finska)

4.9 Sammanfattning av rekommendationen

Tabell 1. Sammanfattning av rekommendationen.

Hela livscykeln	Riskerna för informationsmaterialet ska bedömas regelbundet. Grunden och användningsändamålet med behandling av informationsmaterial ska identifieras och definieras. Det ska säkerställas att de krav som föranleds av behandlingsgrunden samt riskerna för informationen och informationssäkerhetskraven på informationen beaktas i alla skeden av informationsbehandlingen. Det ska säkerställas att kraven på informationen, informationsmaterialet och informationsbehandlingen beaktas när informationssystem och miljöer planeras och olika lösningar genomförs. Informationshanteringsenheten ska ha kännedom om de rutiner, behandlingsmiljöer och andra faktorer som har samband med informationsbehandlingen (en informationshanteringsmodell, dessutom har ministerierna en informationshanteringskarta).
Produktion och mottagande av information	Grunden och syftet med behandlingen ska identifieras och beskrivas. Särskilda krav på informationsbehandling (till exempel i lagstiftningen eller i en annan organisations kriterier) ska identifieras.
Förvaring av informations-material	Informationsmaterial som förvaras ska skyddas enligt de krav, de hanteringsmetoder och den risknivå som har fastställts för informationen. Bevarandet och tillgången till information som förvaras har säkerställts. Användbarheten av information som förvaras har säkerställts under informationens hela livscykel. En förvaringstid har fastställts för informationsmaterialet och efter förvaringstiden ska materialet arkiveras eller destrueras. För förvaring av informationsmaterial används endast förvaringsmiljöer som har accepterats för förvaringssyfte och som uppfyller uppställda krav.
Användning av information	Användarrättigheterna och åtkomstbehörigheterna för informationsmaterial ska bygga på enskilda personers arbetsuppgifter. Logginformation om användning av informationsmaterial ska samlas in utifrån riskerna. Informationsmaterialet ska användas för det syfte som materialet (ursprungligen) är avsett för. Informationsmaterial ska endast användas i informationssystem, enheter och behandlingsmiljöer som överensstämmer med uppställda krav och som har accepterats för användningssyfte.
Delning, överföring och utlämnande av information	När information delas, överförs och lämnas ut ska identiteten hos mottagare verifieras på en tillräcklig nivå. Vid överföring av information används en lämplig kryptering. Vid utlämnande av information ska det kontrolleras att utlämnandet av information är lagenligt och att mottagaren har rätt och förmåga att behandla informationsmaterialet enligt kraven.
Arkivering av informations-material	Vid arkivering ska hänsyn tas till hur lång tid informationsmaterialet ska förvaras, var och på vilket sätt. Informationens användbarhet och läsbarhet har säkerställts under informationsmaterialets hela förvaringstid. Arkiveringen bygger på bestämmelserna om arkivering och på planer som har gjorts upp utifrån bestämmelserna.
Destruering av information	Information ska destrueras på ett tillräckligt tillförlitligt sätt när den fastställda förvaringstiden har gått ut eller användningsbehovet upphört. Då används metoder som förhindrar att informationen återskapas helt eller delvis. Förfarandena för tillförlitlig destruering av elektroniskt material gäller alla enheter där sekretessbelagd information har sparats under enheternas livscykel?

5 Hänsyn till livscykeln i informationssystem (13 § 1 mom. i informationshanteringslagen)

En informationshanteringsenhet ska följa upp informationssäkerhetens tillstånd i sin verksamhetsmiljö och säkerställa informationsmaterialens och informationssystemens informationssäkerhet under hela deras livscykel.

5.1 Informationssystem

Med **informationssystem** avses system vars syfte är att betjäna, underlätta och effektivisera en verksamhet genom att behandla information. Ett informationssystem består av program, informationslager, enheter och tjänster. Ett informationssystems livscykel börjar från en därtill relaterad behovsanalys och slutar när systemet tas ur bruk. Livscykeln omfattar alla skeden av denna tidsperiod, dvs. **definition** och **planering**, **konkurrensutsättning** och **upphandling**, **genomförande** och **utveckling, ibruktagande, underhåll** och **urbruktagande**. Vad gäller informationssystem utgår livscykeltänkandet från hänsynstagande till den behandlade informationens livscykel i systemet och från en systematisk och riskbaserad hantering av system som en del av informationshanteringsenhetens verksamhet.

En informationshanteringsenhet säkerställer informationssystemens informationssäkerhet under systemens hela livscykel genom att identifiera **riskerna** för systemen och genom att dimensionera informationssäkerhetsåtgärderna utifrån riskbedömningen. Vid riskbedömning identifieras relevanta risker som kan påverka informationssystemens användbarhet och tillgänglighet eller informationssäkerheten och riktigheten i det informationsmaterial som behandlas i systemen.

Informationssäkerhet under enskilda informationssystems livscykel utgör en helhet som omfattar riskbedömning, planering av informationssäkerhetsåtgärder utifrån identifierade risker och genomförande av informationssäkerhetsåtgärder. Informationshanteringsenheten bedömer risker för informationssystemen regelbundet under systemens hela livscykel

och beaktar vid planeringen och genomförandet av informationssäkerheten de åtgärder som krävs när riskerna har förändrats. Vid bedömning av riskerna för informationssystemen tas hänsyn till verksamhetsmiljön och informationssäkerhetskraven på systemen.

5.2 Definition och planering

Innan definition och planering inleds görs en behovsanalys. I analysen identifieras och definieras ett informationssystem, vilka frågor som ska beaktas vid ett nytt system eller ett uppdaterat system och vilka krav som ställs på systemet. Under definitions- och planeringsskedet identifieras frågor som är relevanta med tanke på informationssäkerheten och som ska beaktas i de senare skedena av genomförandet. Till sådana frågor hör alltid minimikraven på informationssäkerhet i informationshanteringslagen, se kapitel 3.

Vid definition och planering identifieras gränssnitten mellan informationssystemet och andra system samt beroendeförhållandena och informationsflödena mellan gränssnitten. De ska dokumenteras som en del av arkitektur- och integrationsplanerna. I enlighet med planerna genomförs nödvändiga integrationer i den övriga miljön så att integrationernas informationssäkerhet också är säkerställd. Frågorna ovan kan identifieras redan när en behovsanalys görs, och de blir mer precisa under utvecklingsarbetet.

Vid definition och planering beskrivs informationssystemets användningsändamål och verksamhetsmiljö, exempelvis användare, styrande lagstiftning och andra externa krav, det informationsmaterial som ska behandlas i systemet, och gränssnitten till andra system. Utifrån beskrivningen görs en riskbedömning och dessutom ska det fastställas hur kritiskt informationssystemet är och vilken informationssäkerhetsnivå som behövs. Utgående från den kritiska nivån och informationssäkerhetsnivån identifieras de informationssäkerhetskrav som ska beaktas under informationssystemets hela livscykel. De funktionella kraven på informationssystemet ska beskrivas och utifrån kraven skapas kriterier för godkännande av informationssystemet. Beskrivningen och kriterierna innefattar även planer och krav på informationssäkerhet och dessa krav ska fastställas genom användning av nödvändig informationssäkerhetskompetens. Vid definition och planering tas hänsyn till preciseringarna i kapitel 6 av planeringen och beredningen av upphandlingen.

Vid definition av ett informationssystem eller delar av ett informationssystem görs en bedömning för hela systemet och olika delar av systemet gällande risker som kan äventyra ett säkert genomförande av systemet eller delarna. Delar som endast kan genomföras eller underhållas på ett säkert sätt med en stor mängd resurser bör inte integreras i systemet. Dessutom är det viktigt att vid bedömning av informationsrisker ägna uppmärksamhet åt alla parter och deras miljöer i hela service- och leveranskedjan så att riskerna

för informationssystemet kan hanteras på ett övergripande sätt. Organisationens ledning förbinder sig att genomföra informationssäkerheten baserat på hanteringen av informationsrisker redan från och med definitions- och planeringsskedet. Dessutom är det ändamålsenligt att ge ledningen en realistisk bild av de resurser som behövs för att bygga upp och underhålla informationssäkerheten.

Före upphandlingen eller genomförandet uppgörs i planeringsskedet en preliminär plan för uppgifter, ansvarsområden och tidsscheman gällande informationssäkerhet för den tid under vilken upphandlingen och genomförandet pågår. Vid definition och planering är det också bra att säkerställa och planera tillräckliga resurser för en säker drift av informationssystemen, exempelvis uppdatering av informationssäkerheten, under systemens hela livscykel.

5.3 Konkurrensutsättning och upphandling

Vid konkurrensutsättning och upphandling planeras och genomförs en upphandling angående informationssystemet enligt kapitel 6.

Då är det viktigt att upphandlingskraven, anbudsbegäran och avtalen också innefattar informationssäkerhetskrav. Kraven ska gälla såväl det system som ska upphandlas som genomföraren respektive tillhandahållaren av systemet.

5.4 Genomförande

Innehållet i genomförandeskedet beror på vilket informationssystem som ska upphandlas och vilken genomförandemodell som ska tillämpas. Det kan till exempel vara fråga om ett helt kundanpassat system och ett därtill relaterat mer omfattande utvecklingsprojekt eller en färdig programvara som endast förses med vissa konfigurationer i genomförandeskedet.

I genomförandeskedet görs en ombedömning av den riskbedömning som har gjorts i definitionsskedet. Nödvändiga preciserande hotmodelleringar och riskbedömningar ska göras i genomförandeskedet så att riskerna och hotscenarierna för informationssystemet kan identifieras. De fastställda informationssäkerhetskraven ska planeras och dokumenteras i form av informationssäkerhetskontroller, som ska utföras i detta skede.

Informationssystem består ofta av flera, eventuellt decentraliserade komponenter som har skapats av många olika parter. Vid hantering av informationsrisker är det då bra att fästa

vikt vid hur gränssnitten samt dataöverföringen mellan ett servicesystem och ett bakomliggande system hanteras.

I genomförandeskedet utförs planerade granskningar och tester utifrån en riskbedömning och en behovsprövning, bland annat en arkitekturgranskning, en kodgranskning och tester av funktioner, missbruk/informationssäkerhet och prestanda.

I genomförandeskedet tas hänsyn till de planer och faser som har skapats för systemet i förväg. Syftet är att de åtgärder som behövs ska genomföras utifrån risker och på ett systematiskt sätt så att en ändamålsenlig informationssäkerhet kan inbyggas i systemet.

De informationssäkerhetskontroller och lösningar som genomförts ska dokumenteras som en del av beskrivningen av informationssystemets säkerhet och annan dokumentation som utarbetats.

I genomförandeskedet är oklarheter i ansvarsfördelningen i fråga om informationssäkerhet ett vanligt problem, särskilt i en miljö där flera leverantörer är verksamma. Det är möjligt att förbereda sig för sådana oklarheter genom att kontinuerligt hantera informationsrisker och genomföra åtgärder som syftar till att hantera risker, särskilt med hänsyn till de mål och åtgärder för riskhantering som har skrivits in i avtal. Vanliga risker som är kopplade till avtal är IPR-frågor, upphovsrätt, licenser, allt material som ännu inte har identifierats och som omfattas av immateriella rättigheter, byte av ägare, fusioner och nedläggning av verksamhet.

5.5 Ibruktagande

Med tanke på ibruktagandet uppgörs en plan för införande av ett informationssystem i produktionsmiljön. Som ett led i ibruktagandet av ett informationssystem utförs ett godkännande av ibruktagandet och då kontrolleras det att informationssystemet är förenligt med de tidigare beskrivna kraven. För att systemet ska kunna godkännas ska nödvändiga funktioner och informationssäkerhetskontroller verifieras. Informationssystem, enheter och program ska installeras enligt en fastställd process och anvisningar med hänsyn till bland annat organisationens arkitekturprinciper, kompatibiliteten mellan systemen och den övriga miljön samt de fastställda skyddskraven och härdningen. För att dessa ska kunna genomföras har formbundna konfigurationer av olika inställningar och parametrar specificerats och onödiga tjänster har lagts ner. För en härdad installation som inbegriper vissa definierade informationssäkerhetsinställningar är det till exempel möjligt att utnyttja en underhållen betrodd diskavbild (golden image). Dessa diskavbilder ska granskas, testas och uppdateras regelbundet i syfte att kontrollera att de är lämpliga. Dessutom ska en

regelbunden granskning och övervakning av konfigurationer i själva informationssystemen, enheterna och programmen planeras så att de är en del av underhållet.

Vid ibruktagande ska nödvändiga ändringar göras i beskrivningen av informationssäkerheten i informationssystem.

5.6 Underhåll

Som ett led i underhållet ska det identifieras hur ändringarna i behandlingsmiljön eller i kraven påverkar informationssystemet och vilka ändringar som behöver göras i informationssäkerhetskontrollerna med anledning av ändringarna i behandlingsmiljön eller i kraven. De fastställda förfarandena för hantering av ändringar ska följas när ändringar görs. Regelbundna riskbedömningar och bedömningar av skyddsnivåns lämplighet ska göras i informationssystemet i syfte att kontrollera att riskerna och kraven på systemet har beaktats. I bedömningarna utnyttjas bland annat granskningar och både automatiska och manuella informationssäkerhetstester. Beroende på genomförandemetod görs nödvändiga revisioner även för leverantören av informationssystemet, och leverantören kan förutsättas ha en uppföljning av systemets säkerhetsnivå och lämna rapporter om uppföljningen. Ett av syftena med underhållet är att baserat på planerna kontrollera att de fastställda informationssäkerhetskraven och skyddsmetoderna är uppdaterade och att verksamheten är ändamålsenlig, samt att uppdatera dokumentationen och beskrivningarna av dessa kontroller.

Vid underhåll av informationssystem ska organisationen iaktta fastställda processer och rutiner, såsom hantering av ändringar, incidenter och risker, i anslutning till hantering av sårbarheter, uppdatering, säkerhetskopiering, hantering och härdning av konfigurationer, skydd mot skadeprogram och övervakning av informationssystem. Vid underhåll gäller det även att för informationssystemet göra upp en återställningsplan som behövs för att säkerställa verksamhetskontinuitet och att testa planen.

Som ett led i underhållet av informationssystemen genomförs en nödvändig kontroll och uppföljning bland annat i syfte att följa upp och upprätthålla funktionen, prestandan och informationssäkerheten i systemen. Kontrollen och uppföljningen ska dock vara planerad i definitions- och planeringsskedet.

Säkerhetskopior ska tas enligt planen med hänsyn till de uppgifter som har specificerats utifrån organisationens verksamhet och behandlad information och som ska säkerhetskopieras, metoderna och frekvensen för säkerhetskopiering och metoderna för skydd av säkerhetskopior. Säkerhetskopiering ska ske

- genom att använda en lösning för säkerhetskopiering,
- genom att samla in logginformation om säkerhetskopierade uppgifter och tidpunkter och objekt för säkerhetskopiering samt genom att göra ändamålsenliga anteckningar om säkerhetskopiorna,
- genom att se till att säkerhetskopieringen har lyckats och återställts till exempel genom rapporter och återställningstester, och
- genom att skydda säkerhetskopior mot skador och missbruk, bland annat så att de inte raderas, ändras eller destrueras, både medan kopiorna överförs och medan de lagras.

Vid hantering av sårbarheter i program iakttas en fastställd process som specificerar identifieringen och observationen av uppdateringsbehov, verksamhetsmodellerna för installation av uppdateringar (med hänsyn till olika typer av informationssystem och miljöer samt särskilda behov som systemen och miljöerna eventuellt medför), rutinerna vid misslyckade uppdateringar och återställning, rutinerna för uppföljning av uppdateringar och rapportering om uppföljningen samt de alternativa skyddsmetoderna och åtgärderna när sårbarheter inte kan åtgärdas genom uppdatering (till exempel när en uppdatering ännu inte har offentliggjorts eller när något program inte fungerar i en uppdaterad version).

Verksamhetsmodellerna för skydd mot skadeprogram har specificerats bland annat genom att beskriva installationen och konfigurationen av lösningar för skydd mot skadeprogram, uppdateringsrutinerna, uppdateringen av lösningarna och säkringen av att lösningarna fungerar.

Underhållsanslutningar och underhållsrättigheter följer principen om lägsta behörighet, dvs. det används lägsta möjliga behörigheter att vidta underhållsåtgärder. Underhållsanslutningarna i informationssystemen ska vara krypterade. Den logiska respektive fysiska åtkomsten ska begränsas.

5.7 Urbruktagande

Med tanke på urbruktagandet görs en riskbedömning och de risker som identifieras i bedömningen ska beaktas vid urbruktagandet. En plan för urbruktagande ska göras upp. I planen ska hänsyn tas till bland annat migration av det informationsmaterial som förvaras, rening av lagringsmedier och destruering av delar i informationssystem som tas ur bruk.

Vid urbruktagande ska informationsmaterialet destrueras på ett tillräckligt tillförlitligt sätt i förhållande till de risker som har identifierats. Då används metoder som förhindrar att

informationen återskapas helt eller delvis. Vad gäller informationsmaterialets livscykel beaktas principerna i kapitel 4.

När informationssystem tas ur bruk, kan uppgifterna i systemen arkiveras i stället för att de destrueras. Vid arkiveringen ligger fokus på att uppgifterna ska bevaras och vara användbara och tillförlitliga.

5.8 Bestämmelser och tilläggsinformation

JHS 166 Avtalsvillkor för IT-upphandlingar inom den offentliga sektorn (JIT 2015) (på finska)

Tilastoinnin yleinen prosessimalli (GSBPM) (processmodellen för den allmänna statistikproduktionen, GSBM) (på finska)

5.9 Sammanfattning av rekommendationen

Tabell 2. Sammanfattning av rekommendationen

Hela livscykeln	Riskerna för informationsmaterialet ska bedömas regelbundet. En uppgifts livscykel ska planeras i sin helhet så att exempelvis urbruktagandet kan genomföras enligt planerna. Under utvecklingsarbetet ska planerna uppdateras under uppgiftens livscykel.
Definition och planering	Informationssystemets betydelse för informationshanteringsenhetens verksamhet och verksamhetskontinuiteten samt den information som ska behandlas i systemet, och betydelsen av informationen, ska identifieras. Externa krav på informationssystemet ska identifieras. Riskerna för informationssystemet ska bedömas. Hur kritiskt informationssystemet är och vilken informationssäkerhetsnivå som behövs ska fastställas. Informationssäkerhetskrav som ställs på informationssystemet och som bygger på externa krav, en intern klassificering och identifierade risker ska fastställas och beskrivas. Kriterier för godkännande av informationssystemet ska fastställas. Informationssäkerhetsuppgifter som ska utföras medan upphandlingen och genomförandet pågår, och ett tidschema för utförande av uppgifterna, ska planeras.

Konkurrens-utsättning och upphandling	Upphandling som rör informationssystemet ska göras på ett planmässigt sätt. Vid upphandlingen beaktas principerna i kapitel 0. De krav, anbudsbegäranden och avtal som har samband med konkurrensutsättningen och upphandlingen ska också innefatta informationssäkerhetskrav. Hänsyn tas till att informationssäkerhetskraven ska gälla såväl det system som ska upphandlas som genomföraren respektive tillhandahållaren av systemet.
Genomförande	En hotmodell ska tas fram och riskerna och hotscenarierna för informationssystemet identifieras. Informationssäkerhetskontroller ska väljas och dokumenteras. Gränssnitten mellan informationssystemet och andra system samt beroendeförhållandena mellan gränssnitten ska identifieras som en del av helhetsarkitekturen. De informationssäkerhetskontroller som har valts ska genomföras som ett led i utvecklingen av informationssystemet. De granskningar och tester som fastställts genomförs (en arkitekturgranskning, en kodgranskning och tester av funktioner, missbruk/informationssäkerhet och prestanda). En beskrivning av säkerheten i informationssystemet och annan dokumentation utarbetas.
Ibruktagande	En plan för ibruktagande ska göras upp. Nödvändiga integrationer och gränssnitt mellan systemet och den övriga miljön genomförs och integrationernas informationssäkerhet kontrolleras. Godkännandetester av informationssystemet genomförs. Ibruktagandet av systemet godkänns.
Underhåll	Risker och skyddsnivåns lämplighet ska granskas och bedömas regelbundet. Det ska identifieras hur ändringarna i behandlingsmiljön respektive kraven påverkar informationssystemet och vilka ändringar som behöver göras i informationssäkerhetskontrollerna med anledning av ändringarna i behandlingsmiljön respektive kraven. De fastställda förfarandena för hantering av ändringar ska följas när ändringar görs. Informationssystemet ska underhållas enligt planerna. I anslutning till underhållet sköts bland annat uppdatering, säkerhetskopiering, hantering av konfigurationer, härdning och skydd mot skadeprogram. Dokumentationen och beskrivningarna av informationssystemet ska uppdateras i enlighet med de ändringar som har gjorts i systemet. Informationssystemet ska övervakas kontinuerligt med tanke på de risker som har identifierats.
Urbruktagande	En plan för urbruktagande ska göras upp och godkännas. Migration av informationsmaterial som förvaras planeras och genomförs. Enheter som ska destrueras renas så att de uppgifter som finns i enheterna raderas på ett tillförlitligt sätt. Delarna i informationssystem som ska tas ur bruk destrueras.

6 Skydd mot skador (15 § 1 mom. i informationshanteringslagen)

Myndigheterna ska genom adekvata säkerhetsåtgärder säkerställa att
2) informationsmaterialen har skyddats mot tekniska och fysiska skador.

Myndigheterna ska vara säkra på att ett system eller information som ska behandlas har skyddats mot fysiska skador, såsom brand, vattenskada och skadegörelse, och sådana fysiska skador som har orsakats genom elektroniska metoder, såsom skada i utrustning. Informationen eller systemet ska skyddas genom adekvata åtgärder som är ändamålsenliga utifrån riskbedömningen. Mer information om bedömning av effekter och risker för system finns i kapitel 2.

För respektive informationsmaterial bör myndigheterna fastställa acceptabla utrymmen där material och informationslager som finns i elektroniskt format eller i pappersform kan behandlas och också förvaras. När utrymmen fastställs ska hänsyn tas till på vilket sätt olika tjänster tillhandahålls, bland annat serviceproducenter, molntjänster och det fysiska rum där information behandlas.

Vanligen är det serviceproducenterna som förvarar och underhåller fysiska lokaler och enheter som behövs vid behandling av information och informationssystem, eller avtal om upphandling av informationssystem, som molntjänster. Då gäller det att kontrollera med serviceproducenterna att kraven på fysisk säkerhet uppfylls. Myndigheterna ska beakta att olika informationsmaterial (till exempel sekretessbelagd information eller personuppgifter) omfattas av olika skyddskrav som ger upphov till ytterligare krav på serviceproducenten och/eller myndigheten.

Myndigheterna ska beakta följande faktorer för fysisk säkerhet i informationsmaterial och informationssystem:

- Konstruktiv säkerhet: Lokalernas konstruktioner ska uppfylla de krav som har ställts på konstruktionerna. Mer information om konstruktionsrekommendationer finns i del F i de nationella auditeringskriterierna. Mer information om bestämmelser och krav på arkivutrymmen för dokumentär information som ska förvaras varaktigt finns i Riksarkivets Föreskrift och anvisningar angående arkivutrymmen.
- Säkerhetsområden: Verksamhetslokalerna ska vara uppdelade i säkerhetsområden, om det förutsätts enligt kraven på det informationsmaterial som förvaras i lokalerna. Syftet med säkerhetsområdena är att förhindra eller i tillräcklig utsträckning försvåra att obehöriga kommer över informationen eller informationssystemet.
- Skydd av sekretessbelagd information skapas genom konstruktiva, tekniska och administrativa metoder. Till de administrativa skyddsmetoderna hör exempelvis åtkomstbehörigheter för sekretessbelagd information och adekvata metoder för att behandla sekretessbelagd information. Dessutom kan tillträdet till kritiska lokaler eller uppgifter begränsas till exempel genom säkerhetsutredningar och förbindelser om tystnadsplikt.
- Kontroll av förhållanden: Lokalerna ska förses med kontroll av förhållanden. Kontrollen ska vara tillräcklig i förhållande till kraven på informationssystem och det informationsmaterial som förvaras, till exempel i händelse av brand, vattenskada, gasläckage, damm och vibrationer. Organisationen ska fastställa en tillräcklig nivå för kontroll av förhållanden utifrån resultaten av riskbedömningen.
- Personalsäkerhet: Personalen ska ges utbildning i behandling av uppgifter och organisationens besöksrutiner. Besöksrutinerna ska inbegripa bland annat instruktioner i vilka områden i organisationens lokaler utomstående får besöka och hur anställda ska göra om de upptäcker obehöriga utan ledsagare i lokaler.
- Reservström och UPS: Informationssystemen ska vara försedda med UPS-lösning i händelse av oförväntade strömtoppar eller elavbrott. Genom lösningen kan systemet drivas tills det kan läggas ner på ett kontrollerat sätt och organisationen kan övergå till en verksamhet enligt kontinuitetsplanen.

Mer information om instruktioner och krav på säkerhet i verksamhetslokaler finns i Vahti-anvisningen 2/2013 – Toimitilojen tietoturvaohjeesta (Informationssäkerhet i verksamhetslokaler).

Kritiska system bör dubbleras så att verksamheten kan fortsätta från en annan datahall eller ett annat ställe när verksamheten i det primära underhållsstället är förhindrad. I fråga om informationsmaterial ska hänsyn tas till de krav som ställs på behandling och förvaring av information genom säkerhetsklassificering av information, och kraven ska uppfyllas på ett adekvat sätt.

6.1 Allmänna krav

Följande allmänna krav bör beaktas vid skydd mot skador:

- Uppfyller serviceproducenten informationssäkerhetskraven vad gäller fysisk säkerhet, när hänsyn har tagits till säkerhetsklassificeringen av information och till hur kritiskt informationssystemet är?
- Har åtkomsten till skyddad information endast begränsats till personer som har rätt att behandla informationen?
- Har de kritiska systemen dubblerats så att verksamheten kan fortsätta om det primära underhållsstället inte kan användas?
- Om myndigheten underhåller informationssystemen själv, har de krav som beror på säkerhetsklassificeringen av informationen och/eller systemets kritiska roll beaktats och uppfyllts?
  - Har de fysiska lokalerna uppdelats i säkerhetszoner?
  - Är de konstruktiva lösningarna för lokalerna tillräckliga?
  - Är lokalerna försedda med kontroll av förhållanden i händelse av brand och fuktskador?
  - Används en reservströmlösning som garanterar en tillräcklig drift av systemet medan systemet läggs ner på ett kontrollerat sätt?

6.2 Bestämmelser och tilläggsinformation

Nationella auditeringskriterier Katakri 2015 – verktyg för informationssäkerhetsauditering för myndigheter (på finska)

Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) (Bedömningskriterier för säkerheten av molntjänster) (EI LÖYDY)

VAHTI 2/2014 – Tietoturvallisuuden arviointiohje (Vahti-anvisning 2/2014 om bedömning av informationssäkerhet) (på finska)

VAHTI 2/2013 – Toimitilojen tietoturvaohje (Vahti-anvisning 2/2013 om informationssäkerhet i verksamhetslokaler) (på finska)

VAHTI 2/2012 – ICT-varautumisen vaatimukset (Vahti-anvisning 2/2012 om krav på IKT-beredskap) (på finska)

Riksarkivets Föreskrift och anvisningar angående arkivutrymmen

7 Insamling av logginformation (17 § i informationshanteringslagen)

En myndighet ska ombesörja att logginformation insamlas om användning av dess informationssystem och om utlämnande av information från dem, om användningen förutsätter identifiering eller annan registrering. Syftet med logginformationen är uppföljning av användningen och utlämnandet av information från informationssystem samt utredning av tekniska systemfel.

7.1 Utgångspunkter

Syftet med logginformationen är uppföljning av användningen och utlämnandet av information från informationssystem samt utredning av tekniska systemfel. Utifrån logginformationen är det möjligt att utreda fel och övervaka användningen av informationssystem i syfte att säkerställa rättsskydd, återställa verksamheten efter störningar, verifiera tjänsteansvar och känna igen störningar och incidenter som utgör en risk. Med logginformation avses händelseinformation som skapas i informationssystem automatiskt. Logginformation är händelseinformation som skapas i informationssystem, program eller enheter och som till exempel beskriver inloggningar eller utloggningar, behandling av information (att se, lägga till, ändra eller radera information) eller åtgärder som vidtas av brandväggen.

Logginformation behövs både under normala förhållanden och vid incidenter. Under normala förhållanden kan loggar användas bland annat vid uppföljning av att verksamheten bedrivs störningsfritt, övervakning av användningen, statistikföring och fakturering. I undantagssituationer används loggar bland annat vid utredning av orsaker, normalisering av läget och identifiering av händelser och parter i händelserna. Ett av syftena med behandlingen av logginformation är med andra ord att kontrollera parterna i olika händelser, händelseförloppet och oavvisligheten i händelsekedjan samt att kunna upptäcka och hantera intrångsförsök, incidenter, störningar och problem med prestandan. Dessutom

kan logginformation utnyttjas vid uppföljning och visualisering av nuläget, identifiering av trender, prognoser för framtida utveckling och stöd vid beslut och verksamhet.

Logginformationen är inte nödvändigtvis alltid elektronisk logginformation som skapas i informationssystem, eftersom behandling och utlämnande av informationsmaterial även kan ske manuellt och röra informationsmaterial i pappersform. Då ska rekommendationerna beaktas i tillämpliga delar när uppföljningen av behandlingen av pappersmaterial planeras och genomförs.

7.2 Logginformation

Logginformationen beskriver en viss händelse vid en viss tidpunkt. Logginformationen ska kunna presentera nödvändiga uppgifter om händelserna så att det är möjligt att skapa en tillförlitlig händelsekedja (audit trail). Logginformation samlas in om olika åtgärder, bland annat användning av informationssystem, utlämnande av information, underhåll av informationssystem, teknisk drift av informationssystem och fel i informationssystem.

Insamling av logginformation är bunden till hur nödvändig informationen är, vilket bedöms utifrån risker. Det är särskilt nödvändigt att samla in logginformation om användning av informationssystem och utlämnande av information när sekretessbelagd information behandlas i informationssystemen. Om sekretessbelagd information eller personuppgifter lämnas ut från ett informationssystem genom gränssnitt eller åtkomst till uppgifter, ska logginformation om utlämnande av information samlas in i systemet så att det är möjligt att kontrollera att det finns en lagenlig grund för utlämnande av information. Behovet att samla in logginformation om användning av information bedöms särskilt utgående från om logginformationen behövs för att utreda fel eller för att säkerställa individers intressen, rättigheter och skyldigheter samt rättsskydd eller tjänsteansvar. Logginformation om underhåll av informationssystem beskriver ändringar i informationssystem och användarrättigheter, och tekniska systemloggar och felloggar bland annat tekniska fel och driftstörningar.

7.3 Planering och styrning av logghanteringen

Insamling och behandling av loggar bygger på lag. I organisationen ska logghanteringen och behandlingen av logginformation beskrivas och styras i loggprinciper och en loggplan. Principerna och planen ska beskriva roller och ansvarsområden i loggbehandlingen, olika skeden i loggbehandlingens livscykel (hur logginformation samlas in, behandlas och

lagras), behandlingsbehov och behandlingsgrund samt tekniskt genomförande av logghanteringen.

Logginformation ska samlas in och behandlas efter ett visst fastställt behov enligt loggprinciperna och loggplanen och inte summariskt. Innan ett informationssystem och därtill hörande loggfunktioner genomförs, gäller det att utreda och beskriva på vilket sätt systemet och funktionerna ska användas och hur nödvändig den information som ska samlas in och behandlas är. Dessutom fastställer lagstiftningen skyldigheter att skydda information, särskilt personuppgifter. Det innebär att behoven att skydda information ska identifieras och beaktas när loggbehandlingen, informations- och loggsystemen och upphandlingen av systemen planeras.

Som ett led i planeringen av logghantering och upprättandet av den dokumentation som styr planeringen gäller det att:

- identifiera externa krav som fastställs på logginformation och loggbehandling i lagstiftningen, föreskrifterna och eventuella avtal,
- fastställa rutiner för logghantering och loggbehandling,
- specificera en process, metoder, roller och ansvarsområden för loggbehandling,
- specificera en process för regelbunden bedömning av lämpligheten och lagenligheten i logghanteringen och loggbehandlingen,
- identifiera varför och för vilket syfte enskilda loggar behandlas,
- identifiera informationssystem och utrustning som ska producera logginformation, bland annat kritiska informationssystem och informationssystem för behandling av sekretessbelagd information,
- bedöma hur nödvändig den information som ska lagras är,
- identifiera informationstyper som kommer att lagras i loggarna, särskilt personuppgifter och identifieringsuppgifter,
- identifiera behov att skydda informationstyper som lagras,
- fastställa skyddsbehov och metoder för att skydda loggar (såsom kryptering, säkerhetskopiering, åtkomsthantering),
- säkerställa att behovet att skydda information tillgodoses vid genomförande av system och behandling av information,
- beakta behovet av samarbetsförfarande enligt lagen om integritetsskydd i arbetslivet, om det är fråga om en teknisk övervakning,
- utöver samarbetsförfarandet beakta annan information till användare, registrerade eller andra parter,

- beakta kraven på behandling av personuppgifter i lagstiftningen (såsom dataskyddsförordningen och lagen om dataskydd), om loggarna innehåller personuppgifter,
- planera och dokumentera förvaringsbehovet och säkerställa att behovet tillgodoses i praktiken,
- specificera konfigurationer av insamling av logginformation i informationssystem och annan utrustning.

Krav på loggar ska fastställas och också förutsättas att bli uppfyllda i anslutning till systemutveckling, upphandling eller utkontraktering genom att de ingår i kravspecifikationer, planer och avtal om systemutveckling, upphandling eller utkontraktering. Producenter ska ha beskrivningar av insamling, lagring och analys av logginformation i de system eller funktioner som de ansvarar för. När avtal ingås gäller det även att fastställa krav och rutiner för behandling av loggar, den organisation som äger logginformationen och ägarens möjligheter att använda logginformation, om det behövs. Organisationen kan även samla in logginformation om informationssystem och tjänster som organisationen använder och som leverantören äger.

Speciallagstiftningen och olika föreskrifter och standarder kan innefatta krav på behandling av logginformation och särskilt på insamling, förvaring och förvaringstider för logginformation. Sådana krav ska identifieras och beaktas som ett led i logghanteringen.

7.4 Insamling av logginformation

Logginformation ska produceras och samlas in om användning av informationssystem och utlämnande av information. I vilken omfattning och vilken logginformation som får produceras och samlas in bygger på en behovsbedömning enligt informationshanteringslagen. På behovsbedömningen bygger grunden och omfattningen av insamlingen av logginformation (vilken logginformation som samlas in) samt syftet med logginformationen och behandlingens omfattning (hur logginformation behandlas och av vem). Behovsbedömningen påverkas även av kraven på de tekniska och organisatoriska åtgärder som enligt den allmänna dataskyddsförordningen ska genomföras för att skydda personuppgifter. Behovsbedömningen ska göras av den myndighet som ansvarar för informationssystemet.

Behovet att använda logginformation avgör vilken information som samlas in som logginformation i ett visst informationssystem. I enlighet med behovsbedömningen ska varje loggуppgift som samlats in innehålla tillräcklig information så att det är möjligt att skapa en sådan tillförlitlig händelsekedja som behövs och att övervaka och analysera händelser. Hur användbar en logg är beror på om den information som samlats in i loggen är

tillräcklig med tanke på syftet med loggen. Logginformationen ska alltid i tillräcklig omfattning beskriva varje händelse för loggarna, dvs. när, var, vem och vad:

- När (när ägde händelsen rum?)
  - Tidsstämpel, dvs. datum och klockslag för logginformationen
  - Tidsstämpel, dvs. datum och klockslag för händelsen (tidsstämpeln för logginformationen kan ibland också vara en annan än tidsstämpeln för händelsen)
  - Identifieringsuppgifter om händelsen
- Var (vilken information och/eller vilket system byggde händelsen och åtgärden på?)
  - Identifieringsuppgifter om föremålet för händelsen (informationssystemet, enheten, programmet), bland annat namn, destinationsadress, enhetens identitet och identifieringsuppgifter, kontaktmetod, använt protokoll och position
  - Uppgifter som beskriver föremålet för händelsen, bland annat vilken del av ett informationssystem, ett program eller en tjänsthändelse har drabbat samt vilket element eller vilken uppgift
- Vem (aktör, dvs. vem eller vilket har orsakat händelsen och vilken var källan till händelsen?)
  - Identifieringsuppgifter om källan till händelsen (användaren är en fysisk person eller en enhet), bland annat namn, källadress, personens eller enhetens identitet, identifieringsuppgifter och position
  - Med vilka rättigheter och behörigheter händelsen orsakades
- Vad (vad hände och lyckades händelsen?)
  - Typ av händelsen, exempelvis att ett objekt skapades, ett objekt ändrades, någon loggade in eller systemet kraschade
  - Status för händelsen (lyckades eller misslyckades händelsen och varför misslyckades händelsen eventuellt?)
  - Händelsens betydelse eller prioritering
  - Beskrivning av händelsen

Följande information ska i regel inte samlas in i en logg:

- personbeteckningar
- särskilda kategorier av personuppgifter (så kallade känsliga personuppgifter)
- kreditkortsnummer
- lösenord (inte ens i form av kondensat)
- donglar eller hemligheter mellan system
- information om fullmakter
- innehåll i kommunikationen mellan personer
- källkoder

- information som kräver en högre säkerhetsnivå än nivån i logghanteringssystemet.

Loggkällor är informationssystem, program eller enheter som producerar logginformation. Sådana loggkällor kan vara bland annat

- program
- operativsystem
- servrar
- terminaler
- nätutrustning
- brandväggar
- åtkomsthantering
- intrångsförhindrande system (IPS)
- intrångsdetekteringssystem (IDS)
- antivirusprogram

Vid användning av flera loggar är det bra att möjliggöra en enkel kombination av loggar med tanke på analysbehov. Genom att synkronisera klockorna för loggkällor som producerar logginformation kan det säkerställas att logginformation som produceras i olika system är sinsemellan enhetlig och kan bilda en sammanhängande händelsekedja. Särskilt tidsstämplarna för loggkällor ska visa samma tid. Tiden i system som producerar logginformation kan synkroniseras med NTP (Network Time Protocol). Dessutom är det bra att spara information om loggarnas tidszoner. UTC-tiden bör användas för alla källor.

Vanligen är det klokt att planera informationsinnehållet i loggar om användning och utlämnande när informationsinnehåll och användningssituationer fastställs för hela systemet, men på så sätt att det går lätt att lägga till och radera logghändelser i alla skeden av systemets livscykel. Om sekretessbelagda uppgifter eller personuppgifter lämnas ut från ett informationssystem genom gränssnitt eller åtkomst till uppgifter, ska logginformation om utlämnande av information samlas in i systemet så att det är möjligt att kontrollera att det finns en lagenlig grund för utlämnande av information. Om informationsmaterial lämnas ut i pappersform via en annan kanal än i informationssystem, ska registrering av loggar om sådant utlämnande av information också planeras.

När insamlingen av logginformation om användning, ändring och utlämnande specificeras ska bland annat behovet av följande typer av information bedömas:

- information om att spara, ändra, radera eller se eller andra åtgärder som riktas mot information, inbegripen information om bland annat
  – att lägga till och radera informationsinnehåll (kan även kallas ändringslogg),

  - ändringar i informationsinnehållet och misslyckade registreringar (kan även kallas ändringslogg),
  - åtkomsthändelser och information om förfrågningar, inbegripet sökvillkor, i databaser,
  - utskrifter, och
  - utlämnande av information

- information om inloggningar och utloggningar per användare, grupp och program (kan även kallas åtkomstkontrollogg).

Informationsinnehåll i tekniska loggar är vanligen mindre noggrant specificerat än informationsinnehåll i händelseloggar. Särskild uppmärksamhet ska dock ägnas åt att tekniska loggar inte innehåller sådan sekretessbelagd information som är onödig för utredning om användningen av system. Sådan information kan till exempel vara närmare beskrivningar av ett behandlat informationsinnehåll eller information om särskilda kategorier av personuppgifter, såsom hälsouppgifter. När insamling av logginformation om åtgärder för att underhålla informationssystem och om tekniska system- och felinformation specificeras ska bland annat behovet av följande typer av information bedömas:

- ändring, radering och tillägg av användarrättigheter,
- ändringar i system,
- ändring av systemparametrar och inställningsfiler i system,
- fel som upptäckts i informationssystem eller i händelser som ska följas upp,
- hantering av fel i användningen, och
- upptäckta fel och avbrott.

Betydelsen av insamling, uppföljning och logginformation om användning av informationssystem betonas särskilt när sekretessbelagd information behandlas i informationssystem. Syftet med logginformationen är också att dokumentera utlämnande av information från informationssystem och att samtidigt kontrollera att det finns en lagenlig grund för utlämnande av information. Detta är särskilt viktigt om sekretessbelagd information eller personuppgifter lämnas ut från ett informationssystem genom gränssnitt eller åtkomst till uppgifter.

Det är bra att skapa olika loggar för ett system så att logginformation kan kombineras och sorteras. Om olika kategorier av logginformation har samlats in i en logg, bör informationen vara i ett sådant format att intressanta händelser om användning kan följas upp så att till exempel det tekniska loggmaterialets stora omfattning inte försvårar uppföljningen.

Logginformation är en del av informationssäkerhetsarrangemangen för myndigheternas informationssystem. Därför är logginformationen sekretessbelagd utifrån 24 § 1 mom. 7 punkten i lagen om offentlighet i myndigheternas verksamhet, om det inte är uppenbart att utlämnandet av information inte äventyrar genomförandet av syftet med skyddsarrangemangen.

7.5 Förvaring av logginformation

När förvaringen av logginformation planeras fastställs en förvaringstid och en förvaringsplats. Förvaringstiden beror alltid på syftet med logginformationen. Det är bra att myndigheterna identifierar den logginformation som vanligen ska förvaras i minst fem år med anledning av de straffrättsliga preskriptionstiderna. Speciallagstiftningen kan innehålla särskilda bestämmelser om förvaringstider för logginformation, särskilt om logginformation förvaras längre än vad som behövs för att myndigheterna ska kunna fullgöra sina förpliktelser. Det är viktigt att kontrollera att logginformationen bevaras och är tillgänglig under hela den fastställda förvaringstiden, och informationen ska raderas efter förvaringstiden.

Förvaringstiden för tekniska loggar ska vara tillräckligt lång för att loggarna ska kunna användas vid utredning av problem med driften av system. Informationssäkerhetshändelser (bland annat missbruk eller obehörig användning av information) kan vara händelser som upptäcks först lång tid efter att händelsen inträffat. Detta faktum ska beaktas vid förvaring av loggar så att till exempel tekniska loggar som endast innehåller information om tekniska problem bör förvaras i minst sex månader, men att denna förvaringstid oftast är otillräcklig för utredning av dataintrång. Dessutom kan det vara omöjligt att försäkra sig om att en logg om användning och utlämnande av information är oförändrad, om relevanta tekniska loggar inte förvaras under lika lång tid som loggarna om användning av information. För att ovannämnda krav ska kunna uppfyllas bör relevanta tekniska loggar i regel förvaras i minst fem år.

Behovet att förvara loggar kan förutsätta längre förvaringstider än vad till exempel det program eller det informationssystem som producerar logginformation, och lagringskapaciteten, stöder. Det innebär att loggarna behöver arkiveras. Med långtidsförvaring av loggar avses att loggar förvaras under förlängd tid. Loggar kan överföras exempelvis till en särskild loggserver eller en annan förvaringsenhet för långvarig förvaring så att loggarna inte destrueras förrän förvaringstiden enligt normal loggcykel har gått ut. I princip rekommenderas dock alltid en central logghantering, där loggar överförs från källsystem till ett separat centralt logghanteringssystem. På så sätt möjliggörs även en mer effektiv uppföljning och analys av loggar.

Nödvändiga verksamhetsmodeller och en infrastruktur för att samla in logginformation ska ha tagits fram så att loggarna har ett tillräckligt lagringsutrymme i förhållande till mängden och förvaringstiden för logginformation. Vid planeringen och genomförandet av lagringsutrymmet har hänsyn även tagits till att insamlingen av logginformation inte ska stanna när loggen eller loggutrymmet har blivit fullt. Lagringskapaciteten för loggar ska följas upp och det är viktigt att skapa larm om problem med kapaciteten.

När behandlingen av logginformation inte längre behövs och förvaringstiden för informationen har gått ut ska informationen raderas eller anonymiseras. Raderingen av logginformation har automatiserats så att all logginformation där förvaringstiden har gått ut raderas från loggarna automatiskt. Härvid är det anmärkningsvärt att loggar också vanligen har lagrats på säkerhetskopieringsband eller andra motsvarande lagrings- och arkiveringsmedier där informationen också vid behov ska raderas. Vid radering av information ska hänsyn tas till huruvida radering är möjlig utan att den äventyrar informationens integritet. När information som är lagrad på säkerhetskopieringsband eller andra motsvarande lagrings- och arkiveringsmedier raderas ska hänsyn tas till att säkerhetskopieringens integritet bevaras.

7.6 Uppföljning och analys av logginformation

Logginformation ska följas upp och analyseras regelbundet i syfte att skapa en behövlig observationskapacitet och upprätthålla denna kapacitet. Syftet med uppföljningen och analysen av logginformation samt med larmen är att skapa en så aktuell observationskapacitet som möjligt, särskilt vad gäller kritiska objekt och kritisk information, så att nödvändiga åtgärder kan vidtas fort.

Uppföljning och övervakning av logginformation betjänar även den uppföljning av informationssäkerhetens tillstånd som förutsätts i 13 § 1 mom. i informationshanteringslagen.

Vid analys och förståelse av loggar är det viktigt att förstå den normala, typiska verksamheten i ett system som producerar logginformation och bland dem som använder systemet. Syftet är att skapa en bild av normala händelser som skapar logginformation för att det ska vara möjligt att få ett jämförelseobjekt till ovanliga logghändelser. Med tiden kan man identifiera hur ett system fungerar normalt, och särskilja ovanliga logghändelser som skiljer sig från det normala.

Följande har specificerats i fråga om uppföljning och analys av logginformation:

- vilken logginformation som ska följas upp och analyseras och hur ofta,
- vem som har åtkomst till logginformation och vilken logginformation som organisationen själv ska producera om behandling av logginformation,
- vilka åtgärder organisationen ska vidta när den har upptäckt incidenter som kräver åtgärder (anslutningen mellan logghanteringen och till exempel processen för hantering av incidenter),
- hur logginformation och den information som har tagits fram utifrån logginformationen utnyttjas i verksamheten samt vid styrningen och utvecklingen av verksamheten eller underhållet av informationssystem, och

- hur organisationen ska förebygga att konfidentiell information, såsom lösenord, känsliga personuppgifter och ett känsligt innehåll i kommunikationen, avslöjas och på vilket sätt ett oavsiktligt avslöjande av sådan information ska behandlas.

Eftersom det är arbetskrävande och till och med omöjligt att manuellt analysera logginformation gällande omfattande miljöer, är syftet med verktyg och lösningar för logghantering att automatisera uppföljningen och analysen av logginformation. Syftet ska vara att händelser som avviker från den normala användningen ska identifieras och filtreras så att det går att åtgärda händelserna genom larm, manuella åtgärder och automatiska informationssäkerhetskontroller. Dessutom möjliggör filtreringen prioritering av en manuell analys när det går att på ett effektivt och enkelt sätt endast fokusera på logghändelser som har identifierats vara betydelsefulla händelser.

För att det ska vara möjligt att effektivisera uppföljningen, analysen och skyddet av logginformation ska centrala logghanteringslösningar utnyttjas. Sådana lösningar stöder identifieringen och filtreringen av incidenter från normala händelser, observationen av kränkningar av informationssäkerheten, hanteringen av otydliga och vilseledande data och det effektiva åtgärdandet. De lösningar som används ska utnyttja regler och gränsvärden som har fastställts vid analysen av logginformation och händelser, samt beteendemodeller som har tagits fram om normal användning, individers agerande och informationssystems funktion jämfört med logginformationen om sådana händelser och åtgärder genom identifiering av anomalier, dvs. incidenter och händelser som avviker från det normala.

I syfte att skapa larm och prioritera analys har en modell för att filtrera och prioritera logginformation tagits fram. Modellen ska beakta bland annat följande:

- typ av loggregistrering, såsom den kategori som beskriver händelsen,
- hur sällsynt eller avvikande en loggregistrering är (en helt ny typ av loggregistrering),
- föremål för loggregistrering (till exempel ett kritiskt informationssystem eller en kritisk uppgift),
- hur avvikande en händelse är (till exempel en avvikande tidpunkt eller en avvikande förekomst av händelsen).

För att kunna följa upp och analysera logginformation och åtgärda avvikande situationer har organisationen reserverat tillräckliga och kompetenta resurser för att genomföra åtgärderna. Både interna resurser och resurser som har köpts som tjänster kan användas vid uppföljning och analys av loggar samt hantering av incidenter. Uppföljningen och analysen av loggar har anslutits till organisationens övriga processer, såsom processen för hantering av incidenter så att denna startar till exempel när en informationssäkerhetsincident har upptäckts genom logghantering.

7.7 Utlämnande av logginformation

Logginformation kan lämnas bland annat till olika myndigheter för utredning av informationssäkerhets överträdelse och brott. Rätten att få logginformation avgörs utifrån lagen om offentlighet i myndigheternas verksamhet eller speciallagar. I vissa branscher kan speciallagstiftningen tillåta bland annat att vissa personer lämnar begäran om logginformation och begäran om granskning. Då ska organisationen ha en process och verksamhetsmodeller för att svara på begäran.

Organisationen ska se till att logginformation samlas in och är tillgänglig enligt avtalet, om informationssystemet har byggts upp som köpt tjänst och serviceproducenten ansvarar för insamlingen och administrationen av logginformationen. Rätten att lämna ut logginformation bygger då på avtalet och på att parterna i utlämnandet har en ställning som faktiska ägare till informationen.

7.8 Skydd av logginformation

I loggar insamlas olika typer av information som alla har särskilda skyddsbehov. Detta skyddsbehov, som orsakas av riskerna för informationen och loggarna, samt de externa kraven på loggarna har identifierats så att ett adekvat skydd av logginformation har kunnat skapas för hela logghanteringsmiljön. För att logginformationen ska vara tillförlitlig ska informationens integritet, dvs. oföränderlighet, kunna garanteras så att en obehörig ändring eller destruering av logginformation har förhindrats medan informationen förvaras och överförs. Dessutom ska loggarnas konfidentialitet säkerställas bland annat genom adekvat åtkomsthantering. I syfte att garantera tillgången till logginformation gäller det bland annat att säkerställa att informationen ska bevaras och kunna användas under hela den tid som informationen förvaras.

Loggar utgör ett informationsmaterial i ett informationssystem. Säkerheten i loggarna bör säkerställas åtminstone på samma sätt som säkerheten i det övriga informationsmaterialet som finns i systemet. Säkerheten kan säkerställas till exempel genom att logginformationen överförs till ett annat skyddat system som har åtskilts från det informationssystem som har skapat logginformationen. En väl uppbyggd loggmiljö är en databas som har åtskilts från andra informationssystem och vars integritet har säkerställts genom att redigering av loggar är förhindrad.

När behandlingen av logginformation har planerats och genomförts har det säkerställts att skrivbehörigheten i logginformationen endast tillkommer den process som skapar logginformation. Andra processer, användare av informationssystemet och administratörer

ska inte ha skrivbehörigheter i logginformationen. Användarrättigheterna för loggar skiljer sig från användarrättigheterna för det egentliga informationsinnehållet i informationssystemet. Åtkomsthantering och användarrättigheterna för loggar har specificerats och iakttagandet av rättigheterna övervakas enligt samma principer som användarrättigheterna för övrigt informationsinnehåll i systemet. Vid logginformation ska hänsyn särskilt tas till farliga arbetskombinationer så att användaren av systemet eller administratören inte har behörighet att behandla loggar om den egna användningen. Vanligen krävs då begränsning av användarrättigheterna på både administrativ nivå och teknisk nivå. Det innebär bland annat att farliga arbetskombinationer ska identifieras och specificeras samt beaktas när roller och användarrättigheter beviljas. Det är bra att farliga arbetskombinationer även åtskiljs genom en teknisk tvångsfunktion. Då begränsas beviljandet av roller som utgör farliga arbetskombinationer till en och samma användare.

7.9 Bestämmelser och tilläggsinformation

Statsrådets förordning om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019), 14 §

EU:s allmänna dataskyddsförordning

Lag om dataskydd (1050/2018)

Lag om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018)

Vahti-anvisning (3/2009) (på finska)

Cybersäkerhetscentret: Näin kerää ja käytät lokitietoja (Så här insamlar och använder du logginformation) (på finska)

Viestintäviraston ohje 4/2016 Lokien keräys ja käyttö (Kommunikationsverkets anvisning 4/2016 Insamling och användning av logginformation) (på finska)

Katakri, del I10 (på finska)

8 Informationssäkerhet vid upphandlingar av IT-system (13 § i informationshanteringslagen)

Myndigheten ska vid sina upphandlingar säkerställa att de aktuella informationssystemen har lämpliga säkerhetsåtgärder. Angående bedömning av informationssäkerheten i myndigheters informationssystem och datakommunikation föreskrivs särskilt.

8.1 Reglering av informationssäkerhetsåtgärder vid upphandlingar

I 4 kap. i informationshanteringslagen föreskrivs om minimikraven för informationssäkerhetsåtgärder. Bestämmelserna avser främst informationsmaterial och IT-system. För att säkerställa informationssäkerhetsåtgärdernas ändamålsenlighet i myndighetsverksamhet ska informationssäkerhetsåtgärderna definieras redan när upphandling av IT-system och andra IKT-tjänster planeras.

13.4 § i informationshanteringslagen ålägger den myndighet som svarar för upphandlingen att säkerställa att IT-system har lämpliga informationssäkerhetsåtgärder.

Lagen föreskriver inte om konkreta åtgärder relaterade till IT-system eller informationsmaterial, utan de ska definieras och vidtas utifrån den behandlade informationens kvalitet och art. Dessutom påverkas definitionen och vidtagandet av informationssäkerhetsåtgärder av det upphandlade IT-systemets betydelse i myndighetsverksamheten, fullgörandet av lagstadgade skyldigheter och verksamheten i samhället.

I 13.1 § i informationshanteringslagen föreskrivs att en informationshanteringsenhet ska följa upp informationssäkerhetens tillstånd i sin verksamhetsmiljö och säkerställa informationsmaterialens och informationssystemens informationssäkerhet under hela deras livscykel.

I 13.1 § föreskrivs också om informationshanteringsenhetens skyldighet att identifiera relevanta risker som är förenade med informationsbehandlingen och anpassa informationssäkerhetsåtgärderna till de krav som gäller för informationssäkerheter enligt informationshanteringslagen. I upphandlingsskedet gäller det också att utreda hur informationssäkerheten följs upp när IT-systemet används.

I Europeiska unionens allmänna dataskyddsförordning (EU) 2016/679 föreskrivs om inbyggt dataskydd och dataskydd som standard. Enligt skäl 78 i dataskyddsförordningen bör principerna om inbyggt dataskydd och dataskydd som standard också beaktas vid offentliga upphandlingar. När upphandlingar planeras gäller därför att utreda de dataskyddskrav som påverkar definitionen av informationssäkerhetsåtgärderna i handlingarna om anbudsförfrågan vid upphandlingar.

Enligt artikel 25.2 dataskyddsförordningen ska den personuppgiftsansvarige genomföra lämpliga informationssäkerhetsåtgärder (tekniska och organisatoriska åtgärder) för att säkerställa att dataskyddsprinciperna enligt dataskyddsförordningen iakttas i behandlingen av personuppgifter. Informationssäkerhetsåtgärderna ska vidtas så att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas i standardfallet. Denna skyldighet gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.

Enligt 5.3 § i informationshanteringslagen hör bedömningen av förändringar i informationssäkerhetsarrangemang till följd av upphandlingar av IT-system till konsekvensbedömningen av informationshanteringen. Enligt bestämmelsen ska informationshanteringsenheten vid planeringen av väsentliga administrativa reformer som har konsekvenser för innehållet i informationshanteringsmodellen och i samband med att informationssystem tas i bruk bedöma de förändringar som hänför sig till åtgärderna och deras konsekvenser i förhållande till bland annat informationssäkerhetskraven och -åtgärderna enligt 4 kap. I bestämmelsen avses med ibruktagande av IT-system antingen anskaffning av nya IT-system eller förändringar i befintliga system som påverkar innehållet i informationshanteringsmodellen. Ibruktagande av IT-system innebär enligt informationshanteringslagen konsekvensbedömning av förändringar i bland annat informationssäkerhetsåtgärder redan i upphandlingsfasen. I konsekvensbedömningen av förändringar bedöms risker som hänför sig till den operativa miljön och planeras relevanta informationssäkerhetsåtgärder i förhållande till de föreskrivna informationssäkerhetskraven.

Eftersom informationshanteringslagen föreskriver om informationshanteringsenhetens skyldighet att säkerställa att informationssäkerhetsåtgärderna är relevanta både vid upphandlingar av IT-system och under IT-systemens livscykel, ska informationshanteringsenheten

planera tillräckliga kontrollåtgärder för såväl upphandlingsförfarandet och de olika faserna i införandet av IT-system som för användningen av IT-systemen. Säkerhets- och kontrollåtgärderna vid upphandlingar och införandeprojekt ska också uppfylla säkerhetskraven för systemet.

Planeringen och dokumentationen av informationssäkerhetsåtgärder vid upphandlingar av IT-system kan indelas på följande sätt:

- Upphandlingsanvisningar
- Anbudsförfrågan
- Bedömning av anbudens innehåll
- Upprättande av upphandlingskontrakt
- Genomförande av upphandlingskontrakt.

8.2 Informationssäkerhet i upphandlingsanvisningar

En informationshanteringsenhet kan ha flera handlingar som styr upphandlingarna. Exempel på dem är upphandlingsregler, ekonomistadgor, upphandlingsanvisningar, upphandlingsstrategier och riktlinjer för IT-systems arkitektur. I handlingar som styr upphandlingar gäller det att precisera hur upphandlingsförfarandet uppfyller kraven för informationssäker hantering av upphandlingsdokument enligt informationshanteringslagen. Allmänna upphandlingsprinciper som påverkar planeringen av informationssäkerhetsåtgärder för upphandlingsobjekt omfattar även adekvat dokumentation som styr upphandlingsprocessen. Eftersom de informationssäkerhetsprinciper som informationshanteringsenheten iakttar kan fastställas i informationshanteringsmodellen, kan även de påverka planeringen av upphandlingar.

De dokument som styr upphandlingar bör innehålla:

- anvisningar för hantering av upphandlingsdokument, av vilka de informationssäkerhetsåtgärder som ska iakttas när upphandlingsdokument hanteras inom informationshanteringsenheten framgår
- en mall för anbudsförfrågan med information om allmänna informationssäkerhetsåtgärder som iakttas inom informationshanteringsenheten oberoende av upphandlingsobjekt
- en avtalsmall, enligt vilken den person som ansvarar för planeringen av upphandlingen upphandlingsspecifikt ska beskriva de relevanta informationssäkerhetskraven och -åtgärderna relaterade till personer, datakommunikation, IT-system, informationsmaterial och lokaler.

När offentliga upphandlingar genomförs ska även olika aktörers roller vara klara. Informationshanteringslagen innehåller bestämmelser om informationshanteringsenheter. Den är en myndighetsorganisation, till exempel ett statligt ämbetsverk eller en kommun. En informationshanteringsenhet kan bestå av flera myndigheter, som i sin tur kan vara en upphandlande enhet som avses i upphandlingslagen. I denna rekommendation används termen informationshanteringsenhet, eftersom den i sista hand är upphandlingskontraktets avtalspart, såsom en kommun som juridisk person som kan företrädas av en kommunal upphandlande myndighet som upphandlande enhet.

8.3 Informationssäkerhetskrav i anbudsförfrågan

När informationssäkerhetskraven och -åtgärderna för anbudsförfrågningar definieras ska man beroende på upphandlingsobjekt beakta de principer om vilka föreskrivs i 3 § i lagen om offentlig upphandling och koncession (1397/2016), 2 § i lagen om offentlig försvars- och säkerhetsupphandling (1531/2011) och 6 § i förvaltningslagen. Informationssäkerhetskraven och de relaterade åtgärdskraven ska anpassas till det upphandlade IT-systemets informationsinnehåll och betydelse för myndighetsverksamheten. När informationssäkerhetskraven för anbudsförfrågan definieras gäller det att se till att kraven anknyter till det IT-system som är föremål för upphandlingen och övriga relaterade tjänster som upphandlas. Även informationssäkerhetskraven ska beakta kraven på likvärdig och icke-diskriminerande behandling av anbudsgivare enligt ovan nämnda lagar. Dessutom förutsätter lagstiftningen att kraven är skäliga i förhållande till det upphandlade IT-systemet.

Färdiga kravlistor eller kriterier för vidtagande av informationssäkerhetsåtgärder rekommenderas för upprättande av anbudsförfrågningar, men innehållet i dem ska anpassas till det upphandlade IT-systemet och den information som behandlas i systemet. När krav som överskrider minimikraven enligt informationshanteringslagen definieras gäller det att bedöma deras lämplighet och anpassa dem till upphandlingsobjektet, eftersom överdimensionerade och onödiga krav kan orsaka extra kostnader och påverka upphandlingsobjektets användbarhet och effektivitet. Kraven ska vara motiverade och sakligt definierade.

I anbudsförfrågan gäller det också att tydligt skilja mellan ovillkorliga krav för IT-systemets informationssäkerhet och de definitioner som innehåller informationssäkerhetsåtgärder som är kriterier relaterade till IT-systemets kvalitet och som eventuellt används i anbudsjämförelsen. De krav som ställs på anbudsgivarna och de kriterier som används i anbudsjämförelsen ska vara tydligt åtskilda. En otydlig anbudsförfrågan kan leda till att den måste upprättas på nytt.

Informationssäkerhetskraven ska vara så tydliga och förståeliga att en professionell och relativt insatt anbudsgivare inom branschen förstår dem. Anbudsförfrågningar med krav ska upprättas på ett sätt som gör det möjligt för anbudsgivare att komma med tydliga och entydiga svar avseende såväl uppfyllandet av kraven som kriterierna i anbudsjämförelsen. En otydlig anbudsförfrågan med otydliga bifogade blanketter som ska fyllas i kan leda till att informationshanteringsenheten inte får jämförbara anbud. Genom hanteringen av anbud bör informationshanteringsenheten kunna bedöma om kraven för IT-systemet enligt anbudsförfrågan uppfylls.

Det är viktigt att utifrån anbud säkerställa att informationssäkerhetskraven uppfylls även med tanke på dataskyddet, eftersom den personuppgiftsansvarige enligt artikel 28.1 i dataskyddsförordningen endast får anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i förordningen och säkerställer att den registrerades rättigheter skyddas. En informationshanteringsenhet som upphandlar ett IT-system ska alltså säkerställa att leverantören av IT-systemet (i egenskap av till exempel personuppgiftsbiträde) uppfyller de krav som fastställts i anbudsförfrågan för att skydda personuppgifter i anslutning till informationssäkerhetsåtgärderna. Informationshanteringsenheten kan inte välja en sådan anbudsgivare till leverantör av IT-systemet som inte med säkerhet uppfyller kraven för informationssäkerhetsåtgärderna.

När anbudsförfrågan upprättas är det viktigt att beakta vissa krav relaterade till obligatoriska informationssäkerhetsarrangemang för IT-system enligt informationshanteringslagen:

1. överföring av sekretessbelagd information via allmänna datanät ska ske via en krypterad eller på annat sätt skyddad dataöverföringsförbindelse.
2. IT-systemets användarrättigheter ska fastställas utifrån användningsbehovet i användarens arbetsuppgifter, och funktionerna för beviljande av användarrättigheter ska bidra till att administrationen av användare och användarrättigheter är aktuell.
3. nödvändig logginformation enligt 17 § i informationshanteringslagen ska gå att insamla om användningen av IT-systemet och om utlämnande av information från det.
4. IT-systemens gränssnitt ska uppfylla kraven enligt 22 § i informationshanteringslagen och öppnande av elektroniska förbindelser som uppfyller kraven enligt 23 § i lagen.

Kraven för informationssäkerhetsåtgärder i anbudsförfrågan om IT-system inom statsförvaltningen kan också bestå av krav enligt förordningen om säkerhetsklassificering av handlingar inom statsförvaltningen (1101/2019). Anbudsförfrågan kan också innehålla

säkerhetsklassificerad information, vilket innebär att man i hanteringen av anbudsförfrågan måste beakta kraven för hantering av säkerhetsklassificerade handlingar enligt ovan nämnda förordning.

Rekommendation om innehållet i anbudsförfrågan:

- I anbudsförfrågan beskrivs de informationssäkerhetskrav som ställs på IT-systemet. Kraven kan även inkludera beskrivningar av åtgärder som ska vidtas, såsom tekniska lösningar, eller anbudsgivare kan ges en möjlighet att erbjuda informationssäkerhetsåtgärder för att uppnå kraven. Då ska anbudsgivaren kunna visa att den föreslagna informationssäkerhetsåtgärden obestridligen uppfyller informationssäkerhetskraven. Om man inte vill jämföra eller bedöma olika tekniska informationssäkerhetsåtgärder, är det bra att ange kraven för informationssäkerhetsåtgärderna i anbudsförfrågan. Beskrivningen av informationssäkerhetsåtgärder får inte förutsätta användning av ett visst varumärke.

- När det gäller informationssäkerhetskraven rekommenderas också information om huruvida informationshanteringsenheten kommer att låta utföra en säkerhetsutredning av tjänsteleverantören och dess namngivna personer.

- Informationssäkerhetskraven kan kopplas till leverantörens eventuella informationssäkerhetscertifikat eller något annat sätt (t.ex. revision som utförs av en oberoende informationssäkerhetsrevisor) genom vilket leverantören kan intyga organisationens informationssäkerhetsnivå.

- Informationssäkerhetskraven omfattar också krav på servicenivån, som bör beskrivas tydligt i anbudsförfrågan, eftersom servicenivån även påverkar anskaffningspriset på IT-systemet och tjänstens lämplighet. Servicenivån kan variera avsevärt mellan olika IT-system beroende på deras användningssyfte och betydelse för myndighetsverksamheten.

- Det rekommenderas också att anbudsförfrågan innehåller kriterier för uppfyllandet av informationssäkerhetskraven under serviceproduktionen av IT-systemet och krav på regelbundet säkerställande av feltoleransen åtminstone när det gäller IT-system som väsentligt inverkar på myndighetsverksamheten, eftersom 13.2 § i informationshanteringslagen förutsätter det.

- Anbudsförfrågan bör dessutom innehålla en beskrivning av hur IT-systemets produktionsbruk säkerställs i undantagssituationer, om IT-systemet är väsentligt för myndighetens uppgifter eller samhällets funktion.

- Anbudsförfrågan bör också beskriva hur bland annat olika avvikelser och observerade informationssäkerhetskränkningar ska rapporteras till informationshanteringsenheten samt hur och hur snabbt man ska agera i sådana avvikande situationer.

- Anbudsförfrågan bör även innehålla beskrivningar av förändringshanteringen oberoende av om förändringarna gäller uppdatering av informations-säkerhetsåtgärderna eller någon annan form av administration.

- Av anbudsförfrågan bör dessutom framgå sanktionsförfarandet, om leverantören av IT-systemet inte iakttar de definierade informationssäkerhetskraven.

- Anbudsförfrågan ska också innehålla villkor och förfaranden, enligt vilka informationshanteringsenheten har rätt att genom revisioner säkerställa att informationssäkerhetsåtgärderna uppfyller kraven i IT-systemets funktion och produktion. När det gäller revisioner ska man beskriva principerna för kostnadsfördelningen och den tid inom vilken revisionen kan utföras efter meddelandet. Kontrollpunkter relaterade till säkerställandet bör kopplas till IT-systemets utvecklings- eller införandemodell.

- Anbudsförfrågan bör också innehålla skadeståndsprinciper, om informations-hanteringsenheten orsakas skada på grund av leverantörens försummelser relaterade till informationssäkerhetsåtgärder. Det är särskilt viktigt att införliva skadeståndsprinciperna i sådana anbudsförfrågningar där upphandlingsobjektet är ett IT-system som används för behandling av personuppgifter. Eftersom lagen om behandling av personuppgifter i brottmål och vid upprätthållandet av den nationella säkerheten (1054/2018) föreskriver om skadeståndsansvar för den personuppgiftsansvarige, rekommenderas att informationshanteringsenheten säkerställer att skadeståndsansvaret till följd av en leverantörs behandling av personuppgifter i sista hand kan påföras leverantören.

- Anbudsförfrågan kan också innehålla kvalitetskriterier relaterade till informationssäkerheten som används i anbudsjämförelsen. Uppställandet av sådana kriterier förutsätter dock att informationshanteringsenheten har tillräcklig kompetens att bedöma och jämföra olika informationssäkerhetslösningar. Därför bör användningen av informationssäkerhetsåtgärder som jämförelsekriterier alltid prövas från fall till fall, och detta påverkas också av arten hos den information som behandlas i IT-systemet och den tekniska utvecklingen. Den eftersträvade miniminivån för informationssäkerheten bör dock alltid fastställas som ett ovillkorligt krav.

- Anbudsförfrågan eller de bifogade avtalsmallarna bör även beskriva de förfaranden och krav genom vilka informationshanteringsenhetens verksamhet säkerställs i slutet av IT-systemets livscykel och hur informationen i IT-systemet (inklusive logginformation) överförs till ett nytt system eller en ny kund. Dessutom bör man beskriva de förfaranden genom vilka man säkerställer att system som avvecklas inte innehåller informationsmaterial som uppstått under användningen.

- Innan anbudsförfrågan upprättas ska immaterialrättsliga behov (rätt till innehav, ändring och överlåtelse) relaterade till IT-systemet bedömas med beaktande av säkerhetskraven för IT-systemet och utvecklingsbehoven under livscykeln. Dessa immaterialrättsliga behov införlivas vid behov som krav i anbudsbegäran.

Informationssäkerhetskraven i anbudsförfrågan utgör en del av upphandlingskontraktet. Det rekommenderas att ett kontraktsutkast inklusive bilagor fogas till anbudsförfrågan i syfte att säkerställa uppfyllandet av kraven för den valda leverantörens verksamhet och det upphandlade IT-systemet enligt både informationshanteringslagen och dataskyddsförordningen. Informationssäkerhetskravens företräde i kontraktsutkastet bör säkerställas genom i kontraktsbilagornas giltighetsordning.

8.4 Bedömning av innehållet i anbud

Efter mottagandet av anbuden ska man kontrollera att de uppfyller kraven i anbudsförfrågan. Enligt upphandlingslagen (74.1 §, 104.2 §) ska en anbudsgivare i sitt anbud visa att den vara, tjänst eller byggentreprenad som erbjuds överensstämmer med kraven i anbudsförfrågan och de andra upphandlingsdokumenten. Den upphandlande enheten ska ur anbudsförfarandet utesluta anbud som inte motsvarar anbudsförfrågan eller villkoren för anbudsförfarandet. Anbud med ofullständiga uppgifter om informationssäkerhetskraven i anbudsförfrågan ska enligt upphandlingslagen uteslutas ur anbudsjämförelsen.

Om bristen dock är teknisk till sin karaktär, till exempel om ett kryss saknas i en förteckning över krav, kan informationshanteringsenheten begära att anbudsgivaren kompletterar anbudet. Då får endast den observerade bristen av teknisk karaktär kompletteras. I övrigt får innehållet i anbudet inte ändras. Enligt upphandlingslagen (74.2 §, 104.2 §) kan den upphandlande enheten be anbudsgivaren eller anbudssökanden lämna, komplettera, förtydliga eller färdigställa informationen eller dokumentationen om anbudet eller anbudsansökan inom en tidsfrist som den upphandlande enheten sätter ut. Vid

färdigställande gäller det dock att särskilt beakta kravet på likvärdig och icke-diskriminerande behandling av anbudsgivarna.

Vid handläggningen av anbud rekommenderas att

- tillräckliga och sakkunniga resurser tilldelas för att säkerställa att informationssäkerhetsåtgärderna i anbuden motsvarar informationssäkerhetskraven för IT-systemet och leveransen av det i anbudsförfrågan.

- flera informationssäkerhetssakkunniga anlitas för att bedöma lösningarna för informationssäkerhetsåtgärder, om de används som jämförelsekriterier. Anlitandet av flera sakkunniga skapar en grund för en adekvat bedömning av anbuden för att säkerställa en likvärdig och icke-diskriminerande behandling. I bedömningen ska man använda kriterier och skalor som på förhand definierats i anbudsförfrågan, så att bedömningen av lösningarna för informationssäkerhetsåtgärderna inte bildar en obegränsad prövningsmarginal för bedömningen av anbuden.

8.5 Upprättande och genomförande av upphandlingskontrakt

Upphandlingsförfaranden är kumulativa processer. Anbudsförfrågan, upphandlingsannonsen och anbuden bildar upphandlingskontraktshelheten. Om mallar för upphandlingskontraktet och dess bilagor har fogats till anbudsförfrågan kan de endast kompletteras till den del som de lämnats öppna i anbudsförfrågan eller innehåller variabler relaterade till anbud. De krav som även i anbudsförfrågan angetts som informationssäkerhetskrav bör även framgå av kontraktet eller dess bilagor. Eftersom ett anbud utgör en del av upphandlingskontraktet, är den valda leverantörens föreslagna informationssäkerhetsåtgärder som motsvarar informationssäkerhetskraven bindande för leverantören. Vid behov kan ett säkerhetskontrakt fogas till upphandlingskontraktet, men ett sådant kontrakt ska antingen ha ingått i anbudsförfrågan eller motsvarande krav ha angetts i anbudsförfrågan. Eftersom innehållet i säkerhetskontraktet kan påverka leveransen och prissättningen av IT-systemet, kan säkerhetskontraktet inte betraktas som ett separat dokument som inte tillhör upphandlingsförfarandet. Mallarna för säkerhetskontrakt rekommenderas när säkerhetskontrakt upprättas, men deras ändamålsenlighet och lämplighet visavi upphandlingsobjektet bör bedömas först.

Vid upphandlingar av IT-system och sakkunnigtjänster används i allmänhet sekretessavtal som upprättats av informationshanteringsenheterna. Sekretessavtalen är inte signifikanta utom när man avtalsrättsligt fastställer vite eller grunder för hävning av avtal på grund

av till exempel brott mot tystnadsplikten. I 23 § i lagen om offentlighet i myndigheternas verksamhet (621/1999) föreskrivs om tystnadsplikt och förbud mot utnyttjande. Enligt bestämmelsen omfattar tystnadsplikten och förbudet mot utnyttjande även den som verkar på uppdrag av en myndighet eller som utför ett myndighetsuppdrag. Med bestämmelsen avses att till exempel anställda hos och eventuella underleverantörer till leverantören av IT-systemet har tystnadsplikt som direkt föreskrivs i lag. Brott mot den lagstadgade tystnadsplikten medför straffrättsligt ansvar. Om sekretessavtal ingås rekommenderas att de utgör en del av det egentliga upphandlingskontraktet.

Innan upphandlingskontrakt ingås bör informationshanteringsenheten säkerställa att upphandlingskontraktet eller dess bilagor innehåller alla de beskrivningar och krav relaterade till informationssäkerhetsåtgärder som ingått i anbudsförfrågan och anbudet..

8.6 Genomförande av upphandlingskontrakt

Under genomförandet av ett upphandlat IT-system eller en produkt och under projekt- och starttidpunkten för en tjänst säkerställs processens framskridande och resultatens kvalitet. De olika faserna i IT-systemets utvecklings- eller införandeprocess bör ha kontrollpunkter där man bland annat bedömer om IT-systemets informationssäkerhetsåtgärder uppfyller kraven.

Om det inträffar förändringar i den operativa miljöns informationssäkerhet under utvecklingsarbetet, bör de vid behov beaktas i form av ändringsbegäran till leverantören för att säkerställa en relevant och tillräcklig informationssäkerhet innan systemet går i produktion.

Ännu i samband med testningen för godkännande före införandet bör man utföra en systematisk testning av informationssäkerheten för att säkerställa att informationssäkerhetskraven i anbudsförfrågan uppfylls och dessutom separat förrätta syn över de olika testningsfaserna för att säkerställa att informationssäkerhetskraven har beaktats i alla relevanta testfaser.

När det gäller IT-system som väsentligt inverkar på verksamheten vid informationshanteringsenheten och dess myndigheter bör man beakta att feltoleransen och den funktionella användbarheten ska testas regelbundet enligt 13.2 § i informationshanteringslagen. I praktiken innebär detta att informationshanteringsenheten och leverantören av IT-systemet ska skapa en process för kvalitetskontroll för att säkerställa feltoleransen hos ett IT-system i produktion med hjälp av testning. IT-systemens funktionella användbarhet bör säkerställas redan när IT-systemet utvecklas och införs och när uppdateringar som väsentligt påverkar IT-systemets funktion och användarnas verksamhet görs. I säkerställandet av

den funktionella användbarheten rekommenderas både teknisk användbarhetstestning och användbarhetstestning som utförs av användare eller heuristiska sakkunnigbedömningar.

8.7 Bestämmelser och tilläggsinformation

Lag om offentlig upphandling och koncession (1397/2016)

Lag om offentlig försvars- och säkerhetsupphandling (1531/2011)

Förvaltningslag (434/2003)

Lag om offentlighet i myndigheternas verksamhet (621/1999)

ENISA, Security Guide for ICT Procurement

Anvisning för försvarskritiska upphandlingar, Finansministeriets publikationer – 2019:7

ISO/IEC 27036

ISO/IEC 28000

ISO/IEC 27001 och 27002

9 Ordlista

Ordlista om cybersäkerhet (Säkerhetskommittén)

Ordlista om övergripande säkerhet (Terminologicentralen TSK rf)

Begrepp i VAHTI 2/2014 – Tietoturvallisuuden arviointiohje (Vahti-anvisning 2/2014 om bedömning av informationssäkerhet) (på finska)

Valtionhallinnon tietoturvasanasto (VAHTI 8/2008, finansministeriet) (Ordlista om informationssäkerhet inom statsförvaltningen) (på finska)

Med **anonymisering** avses behandling av personuppgifter så att enskilda personer inte längre kan identifieras utifrån uppgifterna. Uppgifterna kan till exempel förgrovas till en generell nivå (aggregeras) eller ändras till en statistisk form så att uppgifterna om enskilda personer inte längre är i identifierbar form. Identifiering ska vara förhindrad på ett oåterkalleligt sätt så att den personuppgiftsansvarige eller andra externa parter inte längre med de uppgifter som de förfogar över kan ändra uppgifterna till en identifierbar form igen.

Bakomliggande system omfattar system som stöder driften av det egentliga systemet.

Med **bedömning** avses utredning av om ett visst objekt, sett till de olika delarna av objektet, uppnår en fastställd målbild (krav, rekommendationer och bästa praxis). Bedömningsprocessen är ofta en delprocess i en godkännandeprocess.

Med **behandling av logginformation** avses åtgärder som vidtas under en loggs hela livscykel, allt från insamling till förvaring och arkivering av logginformation och från övervakning och analys till utlämnande och radering av loggar.

Med **diskavbild** eller image avses en fil som omfattar hela innehållet och strukturen i ett masslagringsmedium.

Med **granskning** avses en bedömning av ett objekts tillstånd i syfte att identifiera skillnaderna mellan tillståndet och målbilden och att åstadkomma utvecklingsförslag.

Med **gränssnitt** avses en anslutning som möjliggör dataöverföring mellan utrustning, program eller användare.

Hantering av informationssäkerhetsincidenter omfattar åtgärder för att förbereda sig och ingripa i informationssäkerhetsincidenter i syfte att begränsa skadorna och återställa verksamheten efter skadorna.

Med **händelsekedja** och verifieringskedja avses en sammanhängande kedja av källdokument, indata och utskrifter så att det är möjligt att verifiera alla skeden där en enskild uppgift har behandlats.

Med **identifiering och dokumentation av skyddade objekt** avses identifiering av alla uppgifter och system som administreras av en informationshanteringsenhet samt av andra skyddade objekt, såsom nyckelpersoner.

Med **immateriella rättigheter** avses bland annat upphovsrätt, patenträtt, mönsterrätt, rätt till varumärke och rätt till firma.

Informationshanteringsenheter är till exempel statliga och kommunala organisationer, bland annat finansministeriet, Statens center för informations- och kommunikationsteknik Valtori, Lantmäteriverket och Helsingfors stad.

Med **informationsrisk** avses sannolikhet för en olägenhet eller en skada som drabbar information eller orsakas av information samt konsekvenser av en sådan olägenhet eller skada. Informationsrisk anges vanligen i form av en kombination av riskkällor och eventuella händelser samt konsekvenser och sannolikhet för händelser.

Informationsrisker kan till exempel orsakas av mänskliga fel, brister i anvisningar eller underlåtenhet att följa anvisningar, stöld eller skadegörelse, fel eller driftstörningar i utrustning, system eller program, spridning av skadeprogram, destruering av informationsmaterial eller fel eller försummelser hos en underleverantör eller en aktör i ett partnerskapsnätverk.

Med **informationssystem** avses ett system som omfattar individer, databehandlingsutrustning, dataöverföringsutrustning och program och som syftar till att effektivisera eller underlätta en viss verksamhet eller att göra en verksamhet möjlig samt ett abstrakt system som utgörs av information och regler för behandling av information.

Med **informationssäkerhetshot** avses en oavsiktlig eller avsiktlig faktor som har samband med informationsmaterial eller informationssystem och som äventyrar ett informationsmaterials konfidentialitet, integritet eller användbarhet, användningen av informationssystem eller feltoleransen i informationssystem.

Informationssäkerhetshot kan till exempel orsakas av mänskliga fel, brister i anvisningar eller underlåtenhet att följa anvisningar, stöld eller skadegörelse, fel eller driftstörningar i utrustning, system eller program, spridning av skadeprogram, destruering av informationsmaterial eller fel eller försummelser hos en anställd inom organisationen, en underleverantör, en serviceproducent eller en aktör i ett partnerskapsnätverk.

Med **informationssäkerhetshändelse** avses en händelse i ett informationssystem eller i organisationens funktioner som har lett till att status för uppgifter eller tjänster har förändrats, och som kan påverka informationssäkerheten. Informationssäkerhetshändelser kan till exempel följas upp genom identifiering av förändringar eller incidenter (på engelska: anomalies) i data eller i informationssystemets funktion. Förändringar och incidenter följs främst upp genom gallring med tekniska verktyg.

Med informationssäkerhetsincident avses en eller flera oförväntade och icke önskade informationssäkerhetshändelser som äventyrar informationssäkerheten i olika uppgifter och tjänster och påverkar organisationens verksamhet negativt. Informationssäkerhetsincidenter är skadliga händelser, avsiktliga eller oavsiktliga händelser eller tillstånd som leder till att integritet, konfidentialitet eller en ändamålsenlig användbarhetsnivå i uppgifter och tjänster som organisationen ansvarar för har eller kan ha äventyrats.

Inspektion inför godkännande omfattar åtgärder för att konstatera huruvida en produkt eller ett arbetsresultat uppfyller uppställda krav.

IPR-frågor (Intellectual Property Rights), dvs. frågor gällande immateriella rättigheter, rör upphovsrätt, varumärken, patent, firmanamn och affärshemligheter.

Med **it-angrepp eller nätangrepp** avses en gärning eller åtgärd som sker via ett datanät och som syftar till obehörig användning av eller en skada på datanätet, informationssystem, utrustning eller data. It-angrepp kan till exempel göras i form av överbelastningsangrepp eller med hjälp av skadeprogram.

Med **kodning** avses att någon använder en metod för att ändra presentationen av information så att det ursprungliga innehållet i informationen endast kan utredas genom samma metod eller genom en lämplig omvänd metod. Kodning sker med en krypteringsnyckel enligt en viss krypteringsalgoritm.

Med **komponent** avses en fristående programvaruenhet som tillhandahåller olika tjänster genom ett väl specificerat gränssnitt.

Med **konsekvensanalys** avses identifiering av hot som avbryter verksamheten eller stör verksamhetskontinuiteten, och av beroendeförhållanden i verksamheten. Med tanke på

informationssäkerheten och cybersäkerheten ska bland annat följande granskas vid konsekvensanalysen, särskilt vad gäller verksamheten inom statsförvaltningen eller i någon annan offentlig organisation:

- konsekvenser för den egna operativa funktionsförmågan
- konsekvenser för skötseln av lagstadgade uppgifter (jämför även samhällets vitala uppgifter)
- konsekvenser för samhället
- beroendeförhållanden och deras konsekvenser:
  - den egna organisationens beroendeförhållande till en annan part eller tjänst eller andra organisationer eller tjänster
  - en annan organisations eller tjänsts beroendeförhållande till en tjänst eller verksamhet som tillhandahålls av den egna organisationen.

Med **kontroll** avses ett mål, ett medel eller en metod för riskhantering, en systematisk, kontinuerlig verksamhet, en engångsåtgärd eller en återkommande åtgärd för att förbereda eller gardera sig mot kränkningar mot (informations)säkerheten eller skadliga händelser. Kontroller är förebyggande, upptäckande (avslöjande) eller korrigerande.

Med **krav** avses ett enskilt mål som har ställts på ett objekt och som objektet ska kunna uppfylla.

Med **kriterium** avses en bedömningsgrund för att konstatera att ett visst mål har uppnåtts.

Med **krypterad förbindelse** avses en förbindelse som används mellan olika informationssystem och som är skyddad mot externa parter.

Med **kryptering** avses att information, till exempel ett meddelande till en annan person, behandlas så att externa parter inte kan komma över informationen, meddelandet eller den information som meddelandet innehåller. Med kryptering avses även kodning eller dess resultat.

Med **krypteringsmetod** avses en metod som används för kryptering och avkryptering.

Med **kränkning av informationssäkerheten** avses en obehörig åtgärd som riktas mot information eller ett informationssystem. De vanligaste kränkningarna av informationssäkerheten är missbruk av användarnamn och lösenord, dataintrång, överbelastningsangrepp, informationsstöld och riktade sabotageprogram.

Med **källkod** avses datorprogram i den form som programmerare har skrivit programmet i och som programmet kan administreras i.

Med **logg** avses en fil där händelser och orsaker till händelserna registreras i kronologisk ordning. I regel skapas en logg automatiskt och ett system kan ha flera loggar, till exempel fellogg, faktureringslogg och säkerhetslogg.

Med **logginformation** avses händelseinformation som skapas i informationssystem automatiskt. Logginformation kan innehålla olika identifieringsuppgifter och röra bland annat vem som har använt ett system eller hur och när ett system har använts, samt information om olika felsituationer.

Med **migration av information** avses att information överförs till ett annat system för att informationens äkthet, integritet, tillförlitlighet och användbarhet ska kunna säkerställas.

Myndigheterna ska kunna identifiera alla uppgifter och informationssystem som de ansvarar för, och beakta nyckelpersoner som administrerar och använder uppgifterna och systemen. Riskerna för varje identifierat objekt och riskernas eventuella konsekvenser ska bedömas och föras in i ett riskregister som förs av organisationen själv.

Med **nätövervakning** eller nätverksövervakning avses verksamhet där datakommunikationen i egna datanät följs upp och analyseras. Organisationerna kan följa upp och analysera datakommunikationen i sina egna datanät till exempel för att kunna upptäcka tekniska fel eller garantera informationssäkerheten.

Med **penetrationstest** avses att informationssystem testas i händelse av informationssäkerhetsrisker. Penetrationstest används i syfte att upptäcka svagheter och sårbarheter i skyddsmekanismer i informationssystem.

Med **plattform** avses en teknisk verksamhetsmiljö för en programvara eller ett informationssystem. Med plattform avse i sin enklaste form utrustning och systemprogramvara. Mer generellt kan vi med plattform avse en viss mer omfattande körmiljö för program, inbegripet stödprogramvaror, databaser och datakommunikationskapacitet.

Med **protokoll** eller procedur avses ett vedertaget förfarande för kommunikation mellan två parter samt, i fråga om datakommunikation, regler som ska följas av den sändande enheten och den mottagande enheten för att dataöveringen ska lyckas på önskat sätt. Protokoll är regler som fastställer vilka kontaktmetoder, koder och överförings-, styr- och återställningsförfaranden som ska tillämpas genom dataförbindelse.

Med **rening av lagringsmedier** avses att önskade uppgifter eller material som finns på lagringsmedier raderas eller renas.

Med **revision** avses ett oberoende organs utredning av ett objekt, dess verksamhet och verksamhetsresultat, en utredning som i regel utförs regelbundet för att utreda om objektet är förenligt med de krav som har ställts på objektet.

I ett **riskregister** införs identifierade risker, bedömningar av identifierade risker och planerade hanteringsåtgärder.

Med **serviceelement** avses en funktion eller uppgift som finns i ett servicesystem och vars användning man vill övervaka separat.

Med **servicesystem** avses informationssystem som tillhandahåller användare programtjänster.

Med **skadeprogram** avses program som avsiktligt i ett informationssystem eller i en del av ett informationssystem skapar händelser som är icke önskade för användaren av systemet eller enheten. Skadeprogram är exempelvis virus, maskar och trojaner samt kombinationer av dessa. Utpressningsprogram är skadeprogram som krypterar eller manipulerar uppgifter som finns i en enhet och som vanligen kräver lösen av användaren för avkryptering.

Med **skydd** avses bekämpning eller förebyggande av skadliga externa effekter.

Med **skyddat objekt** avses objekt som är viktiga för en organisations verksamhet och som organisationen vill skydda mot risker. Skyddade objekt kan vara exempelvis information, informationssystem, processer, fysiska lokaler, enskilda dokument eller arbetsstationer.

Med **störning** avses en situation eller en händelse som gör att ett system inte fungerar normalt, eller en skadlig variation i en viss delfaktor för verksamheten så att verksamheten trots variationen i huvudsak kan fortsätta.

Med **sårbarhet** avses utsatthet för säkerhetshotande faktorer, brister och svagheter i säkerhetsåtgärder och skydd. Sårbarheter i informationssäkerheten är säkerhetsäventyrande svagheter i ett informationssystem eller i en del av ett informationssystem. Sårbarhet kan vara en följd av ett programfel eller av att någon specialsituation inte har beaktats. Skadeprogram utnyttjar sårbarheter i informationssäkerheten när de sprider sig.

Med **sårbarheter i informationssäkerheten** avses säkerhetsäventyrande svagheter i ett informationssystem eller i en del av ett informationssystem. Sårbarhet kan vara en följd av ett programfel eller av att någon specialsituation inte har beaktats. Skadeprogram utnyttjar sårbarheter i informationssäkerheten när de sprider sig.

Med **sårbarhetsskanning** avses automatisk sökning av kända sårbarheter i tjänster som tillhandahålls i målsystemet i datanätet, till exempel genom intrångsförsök eller genom att undersöka den programversion som finns på servern.

Med **säkerhetsbeskrivning** avses till exempel en beskrivning av säkerheten i ett system och genomförandet av säkerheten.

Med **testning** avses en serie av åtgärder för att utreda funktionen, användbarheten, prestandan, överensstämmelsen med specifikationerna eller någon annan funktion i ett system.

Med **tidsstämpel** avses information som är bifogad till händelseinformation eller ett meddelande och som anger tidpunkten för utskick, inkommande eller behandling av informationen och eventuellt parterna i händelsen. Genom tidsstämpel blir utskicket eller mottagandet av ett meddelande oavvisligt.

En **upptäckande kontroll** försöker upptäcka konsekvenser av en kvarstående risk som har lyckats tränga sig genom ett skyddslager. Kontrollen kan inte längre förhindra en skada, utan gör endast skadan synlig.

Med **utredning av kränkning av informationssäkerheten** avses åtgärder som inleds för att utreda en kränkning av informationssäkerheten efter att kränkningen avslöjats. Utredning av kränkning av informationssäkerheten kan omfatta bland annat tryggande av bevismaterial, forensik, analys av skadeprogram, logganalys eller en generell utredning av kränkningens konsekvenser och omfattning.

Med **verifiering av part** avses en metod eller process där part i kommunikationen verifieras.

Återställning återspeglar återställning av funktionsförmågan efter kris, specialsituation, störning eller undantagsförhållanden, eller återställning av verksamheten efter kris eller katastrof.

Med **återställningsplanering** avses uppgörande och uppdatering av en återställningsplan. En återställningsplan är en del av en kontinuitetsplan eller beredskapsplan och innehåller anvisningar om återställning av verksamhet efter katastrof, fortsättning av verksamhet och återgång till normal verksamhet. Planen fastställer krav på reservsystem för viktiga informationssystem, ansvarsområden och åtgärder för att skapa beredskap, och innehåller anvisningar om verksamhet i undantagssituationer. Planen ska inte enbart innehålla krav utan även konkreta överenskomna åtgärder, förfaranden och tekniska reservlösningar.

Åtkomsthantering omfattar förfaranden för att säkerställa att användare, utrustning, program och system enligt sin respektive roll ska ha tillgång till den information som finns i informationssystem.

Åtkomstkontroll omfattar information, funktioner och förfaranden som gör det möjligt att endast behöriga användare får använda ett servicesystem eller olika serviceelement i ett servicesystem.

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

FINANSMINISTERIET
Snellmansgatan 1 A
PB 28, 00023 STATSRÅDET
Telefon 0295 160 01
finansministeriet.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-519-3 (pdf)

Oktober 2020