



VALTIOVARAINMINISTERIÖ  
FINANSMINISTERIET

# Genomförandeplanen för digital säkerhet inom den offentliga förvaltningen 2020–2023 (Haukka)

Offentliga förvaltningens ICT

Finansministeriets publikationer 2020:46



Finansministeriets publikationer 2020:46

## Genomförandeplanen för digital säkerhet inom den offentliga förvaltningen 2020–2023 (Haukka)

Tuija Kuusisto (redaktör)

Finansministeriet

ISBN PDF: 978-952-367-284-0

Layout: Statsrådets förvaltningsenhet, publikationsverksamheten

Helsingfors 2020

## Presentationsblad

<b>Utgivare</b>	Finansministeriet	8.6.2020	
<b>Författare</b>	Tuija Kuusisto (redaktör)		
<b>Publikationens titel</b>	Genomförandeplanen för digital säkerhet inom den offentliga förvaltningen 2020–2023 (Haukka)		
<b>Publikationsseriens namn och nummer</b>	Finansministeriets publikationer 2020:46		
<b>Diarie-/ projektnummer</b>	VN/1465/2020	<b>Tema</b>	Offentliga förvaltningens ICT
<b>ISBN PDF</b>	978-952-367-284-0	<b>ISSN PDF</b>	1797-9714
<b>URN-adress</b>	<a href="http://urn.fi/URN:ISBN:978-952-367-284-0">http://urn.fi/URN:ISBN:978-952-367-284-0</a>		
<b>Sidantal</b>	38	<b>Språk</b>	engelska
<b>Nyckelord</b>	IKT inom den offentliga förvaltningen, informationspolitik, riskhantering, cybersäkerhet, beredskap, dataskydd, digitalisering		
<b>Referat</b>	<p>I statsrådets principbeslut om digital säkerhet inom den offentliga förvaltningen (finansministeriets publikationer 2020:24) fastställs principerna för utvecklingsarbetet och de centrala tjänsterna med syftet att främja säkerhet i en digital verksamhetsmiljö. Målet är att inom referensramen för den övergripande säkerheten skydda medborgarna, sammanslutningarna och samhället mot de risker och hot som kan riktas mot information, tjänster och samhällets verksamhet i en digital miljö. I genomförandeplanen för digital säkerhet inom den offentliga förvaltningen 2020-2023 (Haukka) beskrivs hur principbeslutet ska verkställas.</p> <p>För Haukka-genomförandeplanen har man valt 19 uppgifter med vilka man ska utveckla de centrala tjänsterna för digital säkerhet inom den offentliga förvaltningen. Genomförandeplanen stöder också den beredning och det genomförande av utvecklingsprogrammet inom cybersäkerhetsstrategin 2019 som har inletts samt bidrar till verkställandet av statsrådets beslut om målen för försörjningsberedskapen (1048/2018).</p> <p>Genomförandeplanen bereddes i en förvaltningsövergripande samordningsgrupp tillsatt av finansministeriet. Verkställandet sker under ledning av finansministeriet. Kostnaderna för genomförandet uppgår vid finansministeriet till 600 000 euro, vid Myndigheten för digitalisering och befolkningsdata till 2 280 000 euro och vid Transport- och kommunikationsverket till 780 000 euro, dvs. sammanlagt till 3 660 000 euro.</p>		
<b>Förläggare</b>	Finansministeriet		
<b>Distribution/ beställningar</b>	Elektronisk version: <a href="http://julkaisut.valtioneuvosto.fi">julkaisut.valtioneuvosto.fi</a> Beställningar: <a href="http://vnjulkaisumyynti.fi">vnjulkaisumyynti.fi</a>		

## Kuvailulehti

<b>Julkaisija</b>	Valtiovarainministeriö	8.6.2020
<b>Tekijät</b>	Tuija Kuusisto (toim.)	
<b>Julkaisun nimi</b>	Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka)	
<b>Julkaisusarjan nimi ja numero</b>	Valtiovarainministeriön julkaisuja 2020:46	
<b>Diaari/hankenumero</b>	VN/1465/2020	<b>Teema</b> Julkisen hallinnon ICT
<b>ISBN PDF</b>	978-952-367-284-0	<b>ISSN PDF</b> 1797-9714
<b>URN-osoite</b>	<a href="http://urn.fi/URN:ISBN:978-952-367-284-0">http://urn.fi/URN:ISBN:978-952-367-284-0</a>	
<b>Sivumäärä</b>	38	<b>Kieli</b> ruotsi
<b>Asiasanat</b>	Julkisen hallinnon ICT, tietopoliittika, riskienhallinta, kyberturvallisuus, varautuminen, tietoturva, digitalisaatio	
<b>Tiivistelmä</b>	<p>Valtioneuvoston periaatepäätöksessä julkisen hallinnon digitaalisesta turvallisuudesta (Valtiovarainministeriön julkaisuja 2020:23) määritetään kehittämisen periaatteet ja keskeiset palvelut turvallisuuden edistämiseksi digitaalisessa toimintaympäristössä. Tavoitteena on kokonaisturvallisuuden viitekehyksessä suojata kansalaisia, yhteisöjä ja yhteiskuntaa niiltä riskeiltä ja uhkilta, jotka voivat kohdistua tietoihin, palveluihin ja yhteiskunnan toimintaan digitaalisessa toimintaympäristössä. Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelmassa 2020-2023 (Haukka) kuvataan periaatepäätöksen toteuttaminen.</p> <p>Haukka-toimeenpanosuunnitelmaan on valittu 19 tehtävää, joiden avulla kehitetään keskeisiä julkisen hallinnon digitaalisen turvallisuuden palveluita. Toimeenpanosuunnitelmalla tuetaan myös käynnistymässä olevaa kyberturvallisuusstrategian 2019 kehittämissuunnitelman valmistelua ja toteuttamista, sekä osaltaan pannaan täytäntöön valtioneuvoston päätöstä huoltovarmuuden tavoitteista (1048/2018).</p> <p>Toimeenpanosuunnitelma valmisteltiin valtiovarainministeriön asettamassa poikkihallinnollisessa koordinaatioryhmässä. Sen toteuttamista ohjaa valtiovarainministeriö. Toteuttamisen kustannukset ovat valtiovarainministeriössä 600 000 euroa, Digi- ja väestötietovirastossa 2 280 000 euroa, sekä Liikenne- ja viestintävirastossa 780 000 euroa, yhteensä 3 660 000 euroa.</p>	
<b>Kustantaja</b>	Valtiovarainministeriö	
<b>Julkaisun jakaja/myynti</b>	Sähköinen versio: <a href="http://julkaisut.valtioneuvosto.fi">julkaisut.valtioneuvosto.fi</a> Julkaisumyynti: <a href="http://vnjulkaisumyynti.fi">vnjulkaisumyynti.fi</a>	

## Description sheet

<b>Published by</b>	Ministry of Finance	8 June 2020	
<b>Authors</b>	Tuija Kuusisto (Ed)		
<b>Title of publication</b>	Implementation plan for digital security in the public sector		
<b>Series and publication number</b>	Publications of the Ministry of Finance 2020:46		
<b>Register number</b>	VN/1465/2020	<b>Subject</b>	Public Sector ICT
<b>ISBN PDF</b>	978-952-367-284-0	<b>ISSN (PDF)</b>	1797-9714
<b>Website address (URN)</b>	<a href="http://urn.fi/URN:ISBN:978-952-367-284-0">http://urn.fi/URN:ISBN:978-952-367-284-0</a>		
<b>Pages</b>	38	<b>Language</b>	Swedish
<b>Keywords</b>	public administration ICT, information policy, risk management, cyber security, preparedness, data security, digitalisation		
<p><b>Abstract</b></p> <p>The Government Resolution on digital security in the public sector (Publications of the Ministry of Finance 2020:24) defines the development principles and key services for advancing security in the digital environment. Within the framework of comprehensive security, the goal is to protect citizens, communities and society from the risks and threats that may affect information, services and the functioning of society in the digital environment. The implementation plan for digital security in public administration 2020–2023 (Haukka) describes how the resolution is to be put to practice.</p> <p>The 19 tasks selected to the implementation plan aim to develop the key services in terms of digital security in the public sector. The implementation plan also supports the preparation and implementation of the development programme for the Cyber Security Strategy 2019 that is getting started, and contributes to the implementation of the Government Decision on the Objectives of Security of Supply (1048/2018).</p> <p>The implementation plan was prepared in a cross-sectoral coordination group appointed by the Ministry of Finance, which will also lead the implementation process. The implementation costs at the Ministry of Finance will be EUR 600,000, at the Digital and Population Data Services Agency EUR 2,280,000, and at the Finnish Transport and Communications Agency EUR 780,000, which gives the grand total of EUR 3,660,000.</p>			
<b>Publisher</b>	Ministry of Finance		
<b>Distributed by/ Publication sales</b>	Online version: <a href="http://julkaisut.valtioneuvosto.fi">julkaisut.valtioneuvosto.fi</a> Publication sales: <a href="http://vnjulkaisumyynti.fi">vnjulkaisumyynti.fi</a>		





# Innehåll

<b>Inledning</b> .....	9
<b>1 Nationell och internationell samarbetsmodell för den digitala säkerheten inom den offentliga förvaltningen</b> .....	11
1.1 Den strategiska ledningsgruppen för digital säkerhet inom den offentliga förvaltningen.....	11
1.2 Samarbets- och hanteringsmodell för digital säkerhet inom den offentliga förvaltningen.....	12
1.3 Nationell operativ utveckling av den digitala säkerheten inom den offentliga förvaltningen .....	13
1.4 Samarbete kring digital säkerhet inom den offentliga förvaltningen på det internationella planet.....	14
<b>2 Hantering av risker i samband med digital säkerhet inom den offentliga förvaltningen</b> .....	16
2.1 Strategisk riskanalys av den digitala säkerheten inom den offentliga förvaltningen.....	16
2.2 Effektivitets-/kostnadsmodell för digital säkerhet inom den offentliga förvaltningen.....	17
<b>3 Gemensamma tjänster för kommunerna för främjande av den digitala säkerheten</b> .....	19
3.1 Säkerheten hos datanäten i kommunerna.....	19
3.2 Kommunernas gemensamma tjänster för digital säkerhet.....	20
<b>4 Hantering av digital identitet</b> .....	21
<b>5 Utveckling av medborgarnas och de anställdas kompetens</b> .....	22
5.1 Utbildningstjänster inom digital säkerhet för medborgare och anställda.....	22
5.2 Körkort i digital säkerhet för medborgare och anställda .....	23
<b>6 Sakkunnigtjänster i anslutning till digital säkerhet inom den offentliga förvaltningen</b> .....	24
6.1 Ordandet av sakkunnigtjänster för digital säkerhet .....	24

<b>7</b>	<b>Bedömning av den digitala säkerheten hos tjänsterna och tjänsteproduktionen inom den offentliga förvaltningen</b> .....	26
7.1	Bestämmelser om bedömning av informationssäkerheten.....	26
7.2	Bestämmelser om bedömning av förutsättningarna och beredskapen för digitala tjänster .....	27
<b>8</b>	<b>Skydd av den digitala infrastruktur som den offentliga förvaltningen behöver</b> .....	28
8.1	Säkerhetsarkitekturen inom den offentliga förvaltningen.....	28
8.2	Observations-, reaktions- och analyseringsförmågan inom den offentliga förvaltningen.....	30
8.3	Den offentliga förvaltningens molntjänster .....	31
<b>9</b>	<b>Säker utveckling av autonoma och lärande system och tjänster inom den offentliga förvaltningen</b> .....	33
9.1	Övervakning av autonoma och lärande system inom den offentliga förvaltningen.....	33
9.2	Säker serviceutveckling inom den offentliga förvaltningen .....	34
<b>10</b>	<b>Sammanfattning av kostnaderna</b> .....	36

## INLEDNING

I Statsrådets principbeslut om digital säkerhet inom den offentliga förvaltningen beskrivs vilka områden den digitala säkerheten ska utvecklas på och enligt vilka principer samt viktiga tjänster för digital säkerhet som stöder verksamheten och processerna inom den offentliga förvaltningen. I denna genomförandeplan har man utifrån en utredning om nuläget för den digitala säkerheten inom den offentliga förvaltningen och en internationell jämförelse valt ut ett antal uppgifter för varje tjänst. För varje uppgift fastställs mål och en tidsplan, beskrivs de åtgärder som behövs för att uppnå målen, anges hur utfallet av åtgärderna ska mätas samt uppskattas kostnader och nytta. Genomförandeplanen stöder och är också avsedd att integreras i beredningen av utvecklingsprogrammet för cybersäkerhetsstrategin 2019. Genomförandeplanen uppdateras vid behov i enlighet med förändringarna i omvärlden och de krav som ställs i utvecklingsprogrammet för cybersäkerhetsstrategin 2019.

Finansministeriet tillsatte 29.8.2019 en koordineringsgrupp att under tiden 1.9.2019–28.2.2020 bereda riktlinjer för digital säkerhet inom den offentliga förvaltningen. Koordineringsgruppen bestod av företrädare för olika aktörer inom den offentliga förvaltningen. Koordineringsgruppen beredde utkastet till principbeslut om digital säkerhet inom den offentliga förvaltningen jämte bilagor samt denna genomförandeplan för åren 2020–2023. De var på remiss i utlåtandetjänsten 24.1–19.2.2020. Utifrån utlåtandena lades sista handen vid genomförandeplanen – först i koordineringsgruppen och därefter på finansministeriet.

För genomförandeplanen 2020–2023 ansvarar följande aktörer:

**Finansministeriet**

- Den strategiska ledningsgruppen för digital säkerhet inom den offentliga förvaltningen, ordförande understatssekreterare Päivi Nerg: Övervakar verkställandet av genomförandeplanen och kommunernas digitala färdplan för digital säkerhet.
- Offentliga förvaltningens ICT; ICT-direktör, överdirektör Anna-Maija Karjalainen: Styr verkställandet av genomförandeplanen Haukka samt instruerar Myndigheten för digitalisering och befolkningsdata.
- Projektchef Tuija Kuusisto: Leder verkställandet av projektet Haukka.

**Myndigheten för digitalisering och befolkningsdata**

- Vahti-ledningsgruppen: Tar fram en lägesbild och en grund för riskbedömning, styr Vahti-sakkunnignätverket.
- Genomför de uppgifter som tilldelats Myndigheten för digitalisering och befolkningsdata i genomförandeplanen Haukka, i huvudsak inom ramen för utvecklingsprojektet för digital säkerhet inom den offentliga förvaltningen (JUDO), för vilket myndigheten har tillsatt en ledningsgrupp.

**Traficom/Cybersäkerhetscentret**

- Genomför de uppgifter som tilldelats Traficom/Cybersäkerhetscentret i genomförandeplanen Haukka inom ramen för Myndigheten för digitalisering och befolkningsdatas JUDO-projekt.

**Övriga ministerier, Kommunförbundet och kommuner**

- Genomför i samarbete med finansministeriet de uppgifter som beskrivs i genomförandeplanen.

# 1 Nationell och internationell samarbetsmodell för den digitala säkerheten inom den offentliga förvaltningen

Genom det nationella och internationella samarbetet effektiviseras samordningen av den digitala säkerheten och dess effektivitet samt främjas Finlands konkurrenskraft. Ministerierna inom respektive förvaltningsområde, kommunerna och sammanslutningarna bidrar aktivt till en positiv utveckling av den digitala säkerheten i EU och centrala internationella organisationer, såsom FN och OECD.

## 1.1 Den strategiska ledningsgruppen för digital säkerhet inom den offentliga förvaltningen

**Mål:** Att främja digitaliseringen och den digitala säkerheten på ett balanserat sätt

**Ansvar:** Finansministeriet

**Kommunikation:** Kommunikationsministeriet utarbetar en kommunikationsplan och informerar om verksamheten i den strategiska ledningsgruppen för digital säkerhet.

**Målgrupp:** Offentlig förvaltning

**Tidsplan:** 2020–2024

**Åtgärder:** Finansministeriet tillsätter en strategisk ledningsgrupp för digital säkerhet. Till gruppen hör statsrådets kansli, utrikesministeriet, inrikesministeriet, försvarsministeriet, kommunikationsministeriet, social- och hälsovårdsministeriet, arbets- och näringsministeriet, Säkerhetskommittén, Kommunförbundet, en representant för kommunerna, Försörjningsberedskapscentralen, en representant för universiteten

och i egenskap av sakkunnig myndigheten för digitalisering och befolkningsdata. Gruppen samordnar den strategiska riskbedömningen av den digitala säkerheten inom den offentliga förvaltningen, skapar och samordnar en samarbetsmodell för digital säkerhet samt gör en strategisk lägesbedömning av den digitala säkerheten inom den offentliga förvaltningen och de viktigaste tjänsterna för digital säkerhet som bör utvecklas, ställer upp riktlinjer för centrala frågor inom digital säkerhet, såsom mål för den digitala säkerheten, samt övervakar verkställandet av denna genomförandeplan för digital säkerhet och kommunernas färdplan för digital säkerhet.

**Mätning:** Den strategiska ledningsgruppen för digital säkerhet inom den offentliga förvaltningen tillsattes 2020 och gruppen är verksam. Den strategiska riskbedömningen har behandlats och resurser har utifrån den allokerats till de utvecklingsobjekt som har största effekt.

**Kostnad/nytta:** Arbetet inom den strategiska ledningsgruppen för digital säkerhet inom den offentliga förvaltningen utförs som tjänstearbete. De aktörer som deltar i gruppen ansvarar för sina representanters rese- och övriga kostnader. Om gruppens arbete utfaller väl har det en betydande inverkan på förebyggandet av centrala strategiska risker för digital säkerhet inom den offentliga förvaltningen, vilket minskar omfattande avbrott och störningar i förvaltningens processer och funktioner samt de nackdelar som dessa medför för verksamhetens kontinuitet i samhället. Det minskar även skadorna på ryktet och förtroendet inom förvaltningen och bland sammanslutningarna och medborgarna. Om gruppen lyckas med sitt arbete främjar det även Finlands konkurrenskraft och möjliggör innovationer och tillväxt.

## 1.2 Samarbets- och hanteringsmodell för digital säkerhet inom den offentliga förvaltningen

**Mål:** Att finansministeriet tillsammans med de övriga ministerierna, kommunerna och sammanslutningarna ska arbeta i enlighet med en samarbets- och hanteringsmodell avsedd att effektivisera den digitala säkerheten inom den offentliga förvaltningen.

**Ansvar:** Finansministeriet

**Kommunikation:** Finansministeriet utarbetar en kommunikationsplan och informerar organisationer inom den offentliga förvaltningen och medborgarna om samarbets- och hanteringsmodellen för digital säkerhet.

- Målgrupp:** Den offentliga förvaltningen, medborgarna
- Tidsplan:** 2021–2023
- Åtgärder:** Finansministeriet och de övriga ministerierna, kommunerna och sammanslutningarna skapar och samordnar tillsammans, med stöd från Vahti-verksamheten, en nationell strategisk samarbetsmodell för digital säkerhet i syfte att utveckla verksamheten, ekonomin och kompetensen. Vid beredningen av samarbetsmodellen behandlas statens, samkommunernas och kommunernas uppgifter och ansvar, vilka tjänster för digital säkerhet inom den offentliga förvaltningen som ska tillhandahållas medborgarna samt forskningsarbetet. Ansvar och arrangemangen för den operativa ledningen fastställs med beaktande av myndigheternas befogenheter, och den nationella cyberlägesbilden förtydligas med beaktande av olika aktörer i samhället och internationella samarbetspartner. Finansministeriet och de övriga ministerierna informerar om målen för digital säkerhet och inkluderar dem i den offentliga förvaltningens operativa mål.
- Mätning:** Samarbetsmodellen har beskrivits och tagits i bruk. Ekonomiplanerna innehåller konkreta mål för att förbättra delområdena inom digital säkerhet.
- Kostnad/nytta:** Utredning av samarbetsmodellen: 80 000 euro. Samordningen av genomförandet utförs i huvudsak som tjänstearbete. Kostnaderna för genomförandet uppskattas i närmare detalj i samband med utredningsarbetet. Nyttan består i att det effektivare samarbetet möjliggör en strategisk och operativ utveckling av den digitala säkerheten samt kompetensutveckling.

### 1.3 Nationell operativ utveckling av den digitala säkerheten inom den offentliga förvaltningen

- Mål:** Att VAHTI-ledningsgruppen ska främja och utveckla samarbetet och samordningen av genomförandet av den digitala säkerheten inom hela den offentliga förvaltningen.
- Ansvar:** Myndigheten för digitalisering och befolkningsdata
- Kommunikation:** Myndigheten för digitalisering och befolkningsdata utarbetar en kommunikationsplan och informerar om VAHTI-ledningsgruppens verksamhet.
- Målgrupp:** Den offentliga förvaltningen, det internationella samarbetet
- Tidsplan:** 2020–2024

- Åtgärder:** Myndigheten för digitalisering och befolkningsdata tillsätter VAHTI-ledningsgruppen som en operativ tväradministrativ styrgrupp. Den nya VAHTI-ledningsgruppen avses bestå av de centrala ämbetsverkens och de centrala sammanslutningarnas och förvaltningsorganens ledningar. Ledningsgruppen ska främja den nationella och internationella kompetensutvecklingen. I VAHTI-verksamheten utnyttjas den lägesbild av digital säkerhet som tagits fram av flera olika myndigheter.
- Mätning:** Den operativa ledningsgruppen för den offentliga förvaltningen/VAHTI-ledningsgruppen har tillsatts och är verksam.
- Kostnad/nytta:** Arbetet inom VAHTI-ledningsgruppen utförs som tjänstearbete. De aktörer som deltar i gruppen ansvarar för sina representanters rese- och övriga kostnader. Om gruppens arbete utfaller väl har det en betydande inverkan på förebyggandet av centrala operativa risker för den digitala säkerheten inom den offentliga förvaltningen, vilket minskar kostnaderna för störningssituationer och dataskyddskränkningar samt skadorna på ryktet och förtroendet inom förvaltningen och bland sammanslutningarna och medborgarna.

## 1.4 Samarbete kring digital säkerhet inom den offentliga förvaltningen på det internationella planet

- Mål:** Att utveckla tekniska lösningar enligt EU:s regelverk och se till att den offentliga förvaltningens tjänster omfattas av tillräckliga krav på digital säkerhet. Det internationella samarbetet stärker även Finlands konkurrenskraft på detta område.
- Ansvar:** Varje ministerium ansvarar för sitt område
- Kommunikation:** Varje ministerium informerar de andra ministerierna samt organisationerna om det internationella samarbetet kring digital säkerhet.
- Målgrupp:** Internationellt samarbete
- Tidsplan:** 2021–2023
- Åtgärder:** Varje ministerium främjar i fråga om sitt ansvarsområde tillsammans med de övriga ministerierna och under samordning av statsrådets kansli i EU-ärenden och utrikesministeriet i andra internationella ärenden utvecklingen av tekniska lösningar i enlighet med EU:s regelverk och ser till att den offentliga förvaltningens tjänster omfattas av tillräckliga krav på digital säkerhet.



Finansministeriet inleder i samarbete med de övriga ministerierna och aktörerna en utredning av om rapporteringen i internationella ärenden kan centraliseras så att en enda aktör i Finland sammanställer och rapporterar de finländska data som behövs för internationella analyser av digital säkerhet och av olika internationella organisationer.

Finansministeriet stärker tillsammans med Vahti-verksamheten vid Myndigheten för digitalisering och befolkningsdata samarbetet kring digital säkerhet inom den offentliga förvaltningen med de baltiska och de nordiska länderna. Samarbetet samordnas med de internationella åtgärderna för digital säkerhet vid utrikesministeriet och statsrådets kansli.

**Mätning:** För det internationella samarbetet inom den offentliga förvaltningen har uppställts mål som ska följas upp. Den centraliserade rapporteringen till de internationella organisationerna har planerats och genomförs som bäst. Samarbetet kring digital säkerhet mellan finansministeriet och de baltiska och nordiska länderna resulterar i ny information till stöd för beslutsfattandet.

**Kostnad/nytta:** Det internationella samarbetet och planeringen av den centraliserade rapporteringen utförs som tjänstearbete. De deltagande aktörerna ansvarar för sina representanters rese- och övriga kostnader. Om arbetet utfaller väl har det en betydande inverkan på den offentliga förvaltningens möjligheter att upphandla digitala tjänster och på deras produktionsmodeller samt på den fortgående effektiviseringen av tjänsternas, infrastrukturens och uppgifternas säkerhet, eftersom dessa inte kan utvecklas enbart med hjälp av åtgärder i Finland.

**Totalt 80 000 euro för de anskaffningar som gäller utredningsarbetet i punkt 1.**

## 2 Hantering av risker i samband med digital säkerhet inom den offentliga förvaltningen

Med hjälp av bedömningen av nuläget för den digitala säkerheten och de riskanalyser och konsekvensbedömningar som produceras utifrån helhetsbilden väljs utvecklingsobjekt som tilldelas resurser.

### 2.1 Strategisk riskanalys av den digitala säkerheten inom den offentliga förvaltningen

- Mål:** Att tillgängliggöra en riskanalys som grundar sig på en nulägesanalys och en strategisk helhetsbild av den digitala säkerheten.
- Ansvar:** Finansministeriet, myndigheten för digitalisering och befolkningsdata
- Kommunikation:** Finansministeriet informerar om den strategiska riskanalysen. Myndigheten för digitalisering och befolkningsdata utarbetar en kommunikationsplan och informerar organisationerna inom den offentliga sektorn om tjänsterna för riskhantering i fråga om digital säkerhet.
- Målgrupp:** Offentlig förvaltning
- Tidsplan:** 2020–2021
- Åtgärder:** Myndigheten för digitalisering och befolkningsdata utreder och genomför en process och tjänster med vilka den centraliserat sammanställer information om hoten, riskerna och mognadsnivån för den digitala säkerheten i organisationerna samt delar information som behövs för att utveckla den digitala säkerheten. Statsrådet controller och den övriga offentliga förvaltningen är samarbetspartner.

Finansministeriet utreder och genomför processen tillsammans med myndigheten för digitalisering och befolkningsdata och upprätthåller med myndighetens hjälp en långsiktig strategisk riskbedömning för digital säkerhet samt skapar långsiktiga riktlinjer för utvecklingen. Finansministeriet samordnar genomförandeprogrammet Haukka, som verkställer riktlinjerna, och utvärderar regelbundet utfallet av riktlinjerna.

- Mätning:** En riskbedömning som baserar sig på helhetsbilden har skapats, genomförts och tillgängliggjorts.
- Kostnad/nytta:** Utredning av processerna för riskidentifiering och underhåll 80 000 euro samt en första riskanalys av de strategiska hoten mot den digitala säkerheten uppskattningsvis 60 000 euro. Upprätthållandet av riskbilden i samband med tjänsten för digital säkerhetsutblick uppskattningsvis 100 000 euro. Kostnaderna för genomförandet uppskattas i närmare detalj i samband med utredningen. Den interna riskhanteringen i organisationerna utförs som tjänstearbete. Nyttan beskrivs i punkt 1.1.

## 2.2 Effektivitets-/kostnadsmodell för digital säkerhet inom den offentliga förvaltningen

- Mål:** Att främja modeller och förfaranden för bedömning av kostnaderna för och effekterna av den digitala säkerheten inom den offentliga förvaltningen.
- Ansvar:** Finansministeriet
- Kommunikation:** Finansministeriet utarbetar en kommunikationsplan och informerar organisationerna inom den offentliga förvaltningen om utvecklingen av effektivitets-/kostnadsmodellen och hur den kan användas och utnyttjas inom den offentliga förvaltningen. Myndigheten för digitalisering och befolkningsdata informerar om användningen av modellen som en del av tjänsten för digital säkerhetsutblick.
- Målgrupp:** Organisationerna inom den offentliga förvaltningen
- Tidsplan:** 2020–2021
- Åtgärder:** Finansministeriet skapar tillsammans med Myndigheten för digitalisering och befolkningsdata en effektivitets-/kostnadsmodell och process för digital säkerhet. En metod planeras för bedömning av effekterna av och kostnaderna för hanteringen och utvecklingen av den digitala säkerheten inom den offentliga förvaltningen och i kommunerna. Målet är att den offentliga förvaltningen ska avsätta ett anslag motsvarande fem procent av ICT-utgifterna på digital säkerhet. Modellen ska pilottestas och utifrån

erfarenheterna tas i bruk som en uppdaterad version år 2021. Lämpliga delen av modellen tas i bruk som en del av Myndigheten för digitalisering och befolkningsdatas tjänst för digital säkerhetsutblick.

**Mätning:** Modellen har skapats och genomförts. Effektivitetsbedömningen har tillgängliggjorts.

**Kostnad/nytta:** Utredning av utformningen av modellen och processen: 60 000 euro. Gränssnitt för dataöverföring till statliga aktörer 50 000 euro som en del av tjänsten för digital säkerhetsutblick samt offerering av användargränssnittet till kommunerna 50 000 euro. I denna uppskattning ingår inte underhållskostnaderna för produktionsmiljön. Kostnaderna för genomförandet, inbegripet arbetet i kommunerna, preciseras i samband med upprättandet av modellen och processen. Modellen och processen behövs för att den strategiska ledningen av digital säkerhet ska basera sig på information. Nyttan av den strategiska ledningen av digital säkerhet behandlas i punkt 1.1.

**Totalt 140 000 euro för de anskaffningar som gäller utredningsarbetet i punkt 2 samt 260 000 euro för anskaffningarna för genomförande och underhåll.**

## 3 Gemensamma tjänster för kommunerna för främjande av den digitala säkerheten

Att upprätthålla och följa upp genomförandet av kommunernas färdplan för utveckling av digital säkerhet.

### 3.1 Säkerheten hos datanäten i kommunerna

- Mål:** Att öka kommunernas observations- och reaktionsförmåga.
- Ansvar:** Myndigheten för digitalisering och befolkningsdata, Kommunförbundet, kommuner
- Kommunikation:** Myndigheten för digitalisering och befolkningsdata utarbetar en kommunikationsplan och informerar kunderna om åtgärderna för att förbättra observations- och reaktionsförmågan.
- Målgrupp:** Kommunerna
- Tidsplan:** 2020–2022
- Åtgärder:** Under finansministeriets ledning samlar Myndigheten för digitalisering och befolkningsdata tillsammans med Traficom, Kommunförbundet och kommunerna en grupp för att utreda och samordna kommunernas observations- och reaktionsförmåga och förbättra den. En möjlig tjänst är att bereda Havarotjänsten för kommunsektorn. Åtgärden hänför sig till punkt 8.2.
- Mätning:** Kommunerna har tillgång till tjänster som ökar observations- och reaktionsförmågan.
- Kostnad/nytta:** Utredning 60 000 euro. Genomförandet beskrivs i punkt 8.2. Under utredningen väljer man ut de kommuner som ska anlita tjänsterna och själva tjänsterna samt uppskattar kostnaderna för genomförandet i kommunerna. De som anlitar tjänsten svarar för kostnaderna för att ta i bruk och anlita tjänsten samt för nödvändiga licensavgifter. En snabbare

reaktionsförmåga tryggar kontinuiteten och säkerheten hos de tjänster som medborgarna anlitar och minskar kostnaderna för störningssituationer och dataskyddskränkningar. Det minskar även skadorna på ryktet och förtroendet inom förvaltningen och bland sammanslutningarna och medborgarna.

## 3.2 Kommunernas gemensamma tjänster för digital säkerhet

- Mål:** Att upprätthålla och följa upp genomförandet av kommunernas gemensamma färdplan för utveckling av digital säkerhet.
- Ansvar:** Myndigheten för digitalisering och befolkningsdata, Kommunförbundet, kommuner
- Kommunikation:** Myndigheten för digitalisering och befolkningsdata utarbetar en kommunikationsplan tillsammans med Kommunförbundet och informerar kommunerna om genomförandet av färdkartan för utveckling av digital säkerhet och om kommunernas uppgifter när det gäller att utveckla den digitala säkerheten.
- Målgrupp:** Kommunerna
- Tidsplan:** 2021–2023
- Åtgärder:** Under finansministeriets ledning samlar Myndigheten för digitalisering och befolkningsdata tillsammans med Kommunförbundet och kommunerna en arbetsgrupp för att utreda behovet och genomförandet av gemensamma utvecklingsprojekt för digital säkerhet i kommunerna. Utredningen grundar sig på denna genomförandeplan, vilken utgör grunden för kommunernas färdplan för utveckling av digital säkerhet. Vidare kartläggs en övervakningsfunktion för de digitala verksamhetsmiljöerna (kommunernas gemensamma cyber- och informationssäkerhetsövervakning). Övervakningsfunktionen kunde skapas som en gemensamt tillgänglig övervakningstjänst så att varningsuppgifterna kan användas som stöd för kommunledningens beslut.
- Mätning:** En arbetsgrupp har tillsatts och utredningarna genomförts. Kommunernas färdplan för digital säkerhet hålls uppdaterad.
- Kostnad/nytt:** Utredning: 100 000 euro. I utredningen fastställs vilka förutsättningar en tjänst ska uppfylla för att den ska kunna ansluta sig till övervakningstjänsten och preciseras kostnaderna för genomförandet. Servicebehovet inom de valda tjänsterna ska vara samma inom alla eller flertalet kommuner. Om kommunerna skapar och utreder tjänster skilt för sig går offentliga resurser förlorade.

**Totalt 160 000 euro för de anskaffningar som gäller utredningsarbetet i punkt 3.**

## 4 Hantering av digital identitet

Finska medborgare och alla invånare i Finland ska ges möjlighet till elektronisk identifiering. Utveckling av fungerande elektroniska identifieringslösningar, som möjliggör användningen av olika slags verktyg, ska främjas.

- Mål:** Att den offentliga förvaltningen ska garantera en pålitlig, användbar elektronisk identitet för varje medborgare och invånare. Staten ska på ett heltäckande och icke-diskriminerande sätt möjliggöra en digital identifieringslösning för medborgarna och invånarna och garantera att de kan bestyrka sin identitet i den digitala världen.
- Ansvar:** Finansministeriet
- Kommunikation:** Finansministeriet utarbetar en kommunikationsplan och informerar medborgarna om läget beträffande hantering av digital identitet.
- Målgrupp:** Medborgare
- Tidsplan:** 2020–2023
- Åtgärder:** Finansministeriet samordnar tillsammans med de andra ministerierna de nödvändiga lagstiftningsändringarna och de uppgifter som behövs vid myndigheten för digitalisering och befolkningsdata.
- Mätning:** Lagstiftningsändringarna har gjorts och de nödvändiga uppgifterna fastställts. Användningen av e-tjänster ökar, inkl. hantering av ärenden åt någon annan och fullmakter (m.a.o. ökning i antalet personer som har möjlighet att använda e-tjänster)
- Kostnad/nytt:** Servicehelheten genomförs som ett separat projekt, inom vilket man bedömer kostnaderna och nyttan och ansvarar även för att ordna finansiering för servicehelheten.

## 5 Utveckling av medborgarnas och de anställdas kompetens

Färdigheterna i och medvetenheten om digital säkerhet i alla persongrupper inom den offentliga förvaltningen och sammanslutningarna samt hos de enskilda medborgarna utvecklas.

### 5.1 Utbildningstjänster inom digital säkerhet för medborgare och anställda

- Mål:** Att öka kunskapen om digital säkerhet.
- Ansvar:** Myndigheten för digitalisering och befolkningsdata
- Kommunikation:** Myndigheten för digitalisering och befolkningsdata utarbetar en kommunikationsplan och informerar organisationerna inom den offentliga förvaltningen och medborgarna om till buds stående utbildningar i digital säkerhet.
- Målgrupp:** Medborgarna, de anställda och ledningen
- Tidsplan:** 2022–2023
- Åtgärder:** Myndigheten för digitalisering och befolkningsdata producerar tillsammans med undervisnings- och kulturministeriet utbildning inom digital säkerhet för medborgarna och för anställda och personer i ledande ställning hos staten och kommunerna. Kompetensutvecklingen fortsätter som planerats inom ramen för JUDO-projektet för åren 2019–2021. Övningar som en form av kompetensutveckling och förbättringar i serviceattityden tas i beaktande. Undervisnings- och kulturministeriet utvecklar medborgarnas kunskaper om digital säkerhet på ett heltäckande sätt som en del av det finländska utbildningssystemet.
- Mätning:** Utbildningshelheterna har skapats och distributionskanalen tagits i bruk.



**Kostnad/nytt:** Kostnaderna uppgår till uppskattningsvis 80 000 euro per år. Som distributionskanal för utbildningen kan befintliga plattformar användas, varför kostnaderna för licenser och ibruktagande är måttliga. Kostnaderna hänför sig till produktionen av nytt material samt underhåll, licenser och serviceavgifter för utbildningsmaterial och licenser för webbplatsen och serviceplattformen (t.ex. årliga kostnader för molnplattformen). Genom att utveckla kompetensen tryggas säkerheten och driftssäkerheten för förvaltningens tjänster samt medborgarnas och invånarnas möjligheter att anlita förvaltningens tjänster.

## 5.2 Körkort i digital säkerhet för medborgare och anställda

- Mål:** Att utveckla ett förfarande för identifiering av medborgarnas och personalens kompetens i syfte att öka förtroendet och identifiera kompetensen.
- Ansvar:** Myndigheten för digitalisering och befolkningsdata
- Kommunikation:** Myndigheten för digitalisering och befolkningsdata utarbetar en kommunikationsplan och informerar medborgarna och personalen inom den offentliga sektorn om förfarandet för att identifiera kompetens.
- Målgrupp:** Offentlig förvaltning
- Tidsplan:** 2021–2022
- Åtgärder:** Myndigheten för digitalisering och befolkningsdata utreder förfaringsätt som tagits fram för att påvisa medborgarnas kompetens i digital säkerhet, som körkort i cybersäkerhet, samt förfaringsätt som tagits fram för att påvisa anställdas baskunskaper i digital säkerhet. I utredningen presenteras alternativa sätt att gå vidare för att genomföra/utvidga förfaringsätten.
- Mätning:** Utredningen om förfaringsätten för att påvisa kompetensen i digital säkerhet har gjorts. Utifrån utredningen har det föreslagits genomförandemodeller som efter behov gjorts till pilotprojekt. Planer har gjorts för främjandet av förfaringsätten.
- Kostnad/nytt:** Utredning 40 000 euro, genomförande uppskattningsvis 40 000 euro. Medborgare och anställda vid den offentliga förvaltningen kan påvisa att de iakttar säkra förfaringsätt i den digitala omvärlden. Fördelen är att medvetenheten om digital säkerhet ökar bland medborgarna och de anställda.

**Totalt 40 000 euro för anskaffningar som gäller utredningsarbetet i punkt 5, 40 000 för anskaffningar för genomförandet av dem samt 80 000 per år i två års tid, dvs. totalt 240 000 euro.**

## 6 Sakkunnigtjänster i anslutning till digital säkerhet inom den offentliga förvaltningen

Centraliserade sakkunnigtjänster för digital säkerhet utvecklas och tillhandahålls på bred front inom hela den offentliga förvaltningen.

### 6.1 Ordandet av sakkunnigtjänster för digital säkerhet

<b>Mål:</b>	Att ordna gemensamma sakkunnigtjänster för digital säkerhet för den offentliga förvaltningen.
<b>Ansvar:</b>	Myndigheten för digitalisering och befolkningsdata
<b>Kommunikation:</b>	Myndigheten för digitalisering och befolkningsdata utarbetar en kommunikationsplan och informerar organisationerna inom den offentliga förvaltningen om hur man anlitar sakkunnigtjänster för digital säkerhet.
<b>Målgrupp:</b>	Offentlig förvaltning
<b>Tidsplan:</b>	2020–2021 beredning, 2022–2023 tjänsterna börjar tillhandahållas
<b>Åtgärder:</b>	Myndigheten för digitalisering och befolkningsdata utreder och utvecklar tillsammans med Hansel konsulterings- och kvalitetsrevisionstjänsterna för digital säkerhet inom den offentliga förvaltningen samt upphandlingsförfarandena kring dem. Utredningen gäller tjänsteleverantörernas enhetliga möjligheter att ta del av serviceutbudet, behovet av konsultering och kvalitetsrevisioner inom digital säkerhet i den offentliga förvaltningens organisationer samt alternativa modeller för upphandling av sakkunnigtjänsterna. Utifrån utredningen skapar myndigheten för digitalisering och befolkningsdata en sakkunnigtjänst för digital säkerhet inom den offentliga förvaltningen och verktyg som stöd för den.

**Mätning:** Sakkunnigtjänsten och verktygen har tagits i bruk.

**Kostnad/nytta:** Tjänsterna ordnas som tjänstearbete. De som använder tjänsterna bekostar användningen av dem. Nyttan består i att tjänsterna är tillgängliga för hela den offentliga förvaltningen.

## 7 Bedömning av den digitala säkerheten hos tjänsterna och tjänsteproduktionen inom den offentliga förvaltningen

Utvärdering och certifiering av digitala tjänster och tjänsteproducenter som baserar sig på normer och standarder främjas.

### 7.1 Bestämmelser om bedömning av informations säkerheten

- Mål:** Att utreda behovet av att revidera lagen om bedömning av informations säkerheten i myndigheternas informationssystem och datakommunikation (1406/2011) och lagen om bedömningsorgan för informations säkerhet (1405/2011) och utifrån slutsatserna genomföra den eventuella lagberedningen.
- Ansvar:** Finansministeriet
- Kommunikation:** Finansministeriet informerar om lagberedningen i enlighet med kommunikationsprinciperna för detta.
- Målgrupp:** Offentlig förvaltning
- Tidsplan:** 2021–2022
- Åtgärder:** Finansministeriet utreder tillsammans med kommunikationsministeriet, Traficom samt de övriga ministerierna och eventuellt kommunerna nuläget och behovet av revidering år 2021. Lagberedningen sker utifrån slutsatserna 2021–2022. De eventuella nya lagförslagen överlämnas till riksdagen i början av hösten 2022.
- Mätning:** Utredningarna har gjorts. De fortsatta åtgärder som föranletts av utredningarna har vidtagits.

**Kostnad/nytta:** Utredningarna och en eventuell lagberedning görs som tjänstearbete. I beredningen ingår en konsekvensbedömning och en bedömning av de ekonomiska effekterna. Traficoms arbete ingår inte i kostnadsberäkningen.

## 7.2 Bestämmelser om bedömning av förutsättningarna och beredskapen för digitala tjänster

**Mål:** Behovet av lagstiftning i anslutning till förutsättningarna och beredskapen för och kraven på de digitala tjänsterna och infrastrukturen samt förfarandet för att utvärdera dem ska bedömas och eventuell lagberedning genomföras.

**Ansvar:** Finansministeriet

**Kommunikation:** Finansministeriet informerar om lagberedningen i enlighet med kommunikationsprinciperna för detta.

**Målgrupp:** Offentlig förvaltning

**Tidsplan:** 2021–2022

**Åtgärder:** Finansministeriet utreder tillsammans med kommunikationsministeriet, Traficom samt de övriga ministerierna och eventuellt kommunerna nuläget och behovet av revidering år 2021. Lagberedningen sker utifrån slutsatserna 2021–2022. De eventuella nya lagförslagen överlämnas till riksdagen i början av hösten 2022.

**Mätning:** Utredningarna har gjorts. De fortsatta åtgärder som föranletts av utredningarna har vidtagits.

**Kostnad/nytta:** Utredningarna och en eventuell lagberedning görs som tjänstearbete. I beredningen ingår en konsekvensbedömning och en bedömning av de ekonomiska effekterna. Traficoms arbete ingår inte i kostnadsberäkningen.

## 8 Skydd av den digitala infrastruktur som den offentliga förvaltningen behöver

Säkerheten i centrala gemensamma tekniker och tjänster främjas så att kontinuiteten och informationen i den offentliga förvaltningens verksamhet, processer och tjänster är tryggad.

### 8.1 Säkerhetsarkitekturen inom den offentliga förvaltningen

- Mål:** Att med hjälp av säkerhetsarkitekturen inom den offentliga förvaltningen styra utvecklingen av den digitala infrastrukturen.
- Ansvar:** Myndigheten för digitalisering och befolkningsdata
- Kommunikation:** Tillsammans med Myndigheten för digitalisering och befolkningsdata utarbetar finansministeriet en kommunikationsplan och informerar organisationerna inom den offentliga förvaltningen om utvecklingen av säkerhetsarkitekturen och hur man drar fördel av den.
- Målgrupp:** Offentlig förvaltning
- Tidsplan:** Utredning 2020–2021, genomförande 2021–2023
- Åtgärder:** Under finansministeriets ledning utarbetar Myndigheten för digitalisering och befolkningsdata tillsammans med Traficom, FPA, andliga statliga ämbetsverk och inrättningar samt kommunerna en säkerhetsarkitektur för den offentliga förvaltningen. Här drar man fördel av de informationshanteringskartor och -modeller som utarbetas i samband med verkställandet av informationshanteringslagen samt finansministeriets anvisningar om kompatibilitet. I uppgiften samarbetar man med program som syftar till att utveckla beredskapen inom kritisk infrastruktur med fokus på centrala delområden av denna, som Försörjningsberedskapscentralens program Digital säkerhet 2030.

- a. Man beskriver på vilken nivå den nationella kompetensen ska byggas upp och vilka kritiska digitala tjänster, data och infrastrukturer som behöver särskilda nationella krav på administration och säkerhet. Offentligt tillgänglig information kan i sig utgöra en risk, eller så kan en risk uppkomma när enstaka offentliga uppgifter sammanförs (information kumuleras). Scheman över elnätet eller konstruktionsritningar till broar är exempel på sådan information. All offentlig information behöver inte vara tillgänglig digitalt. Man bereder riktlinjer om till vilken del tjänsterna ska produceras och infrastrukturen byggas upp med hjälp av nationella åtgärder och till vilken del man kan stödja sig exempelvis på gemensam utveckling inom EU eller annat internationellt samarbete samt hur man i synnerhet inom den offentliga förvaltningen bör och kan utnyttja olika nya servicemodeller och tekniska möjligheter i produktionen av offentliga digitala tjänster.
- b. Man skapar och tar i bruk ett klassificeringssystem för kritiska tjänster och datasystem inom den offentliga förvaltningen, bedömer behovet av ett dataregister och analyserar nuläget för kritiska tjänster, datasystem och kommunikationslösningar samt deras kravenlighet.
- c. Man bereder en förteckning över tekniker som rekommenderas inom den offentliga förvaltningens digitala tjänster. Man bereder även en förteckning över tekniker som bör undvikas och eventuellt bedömas ur ett riskhanteringsperspektiv, exempelvis i fråga om föråldrad teknik.
- d. Man utarbetar en plan för att utveckla analysen av tjänsternas och servicenätverkens säkerhet i anslutning till punkt 7.

Åtgärder för att iaktta villkoren för arkitekturen:

- e. Man sammanställer ett informationsunderlag över de långsiktiga utvecklingsbehoven för kritiska datasystem, datalager och datanät samt utarbetar en plan för att inleda ett utvecklingsprogram med centraliserad finansiering. I anslutning till detta kartläggs sårbarheter i synnerhet i kritiska gamla informationssystem och deras livscykelplanering ses över.
- f. Man utarbetar en långsiktig utvecklingsplan för att förbättra kravenligheten hos kritiska tjänster, informationssystem och kommunikationslösningar och hantera den befintliga reparationsskulden.

**Mätning:** Punkt a–d har genomförts. Punkt e–f har genomförts i fråga om den offentliga förvaltningens och statsförvaltningens gemensamma tjänster.

**Kostnad/nytta:** Utredning av nuläget och kartläggning av brister: 60 000 euro. Beskrivning/utredning av utvecklingsbehoven inom säkerhetsarkitekturen, inbegripet kriterierna i punkt a–d: 100 000 euro. Utformning av tekniska

riktlinjer: 120 000 euro. För genomförandet av de tekniska riktlinjerna och skapandet av en miljö enligt dem ansvarar respektive myndighet i fråga om punkt e–f, och dessa kostnader uppskattas separat för varje projekt. Om varje myndighet separat ska bereda de frågor som hör till säkerhetsarkitekturen kommer nivån på säkerhetsarkitekturen att variera. Med hjälp av centraliserad samordning kan man minska kostnaderna och förbättra planeringsresultatens enhetlighet och kvalitet liksom även säkerheten, förutsättningarna och beredskapen för tjänsterna och deras produktionsmiljö.

## 8.2 Observations-, reaktions- och analyseringsförmågan inom den offentliga förvaltningen

- Mål:** Att hantera störningar inom den digitala säkerheten snabbare och identifiera sårbarheter.
- Ansvar:** Myndigheten för digitalisering och befolkningsdata
- Kommunikation:** Tillsammans med Traficom utarbetar Myndigheten för digitalisering och befolkningsdata en kommunikationsplan och informerar organisationer inom den offentliga förvaltningen och sammanslutningar om åtgärder som knyter an till förbättring av observations- och reaktionsförmågan.
- Målgrupp:** Den offentliga förvaltningen och sammanslutningarna
- Tidsplan:** 2021, genomförande av planen 2022
- Åtgärder:** Myndigheten för digitalisering och befolkningsdata utarbetar tillsammans med Cybersäkerhetscentret anvisningar och rekommendationer för att utveckla den offentliga förvaltningens observations- och reaktionsförmåga samt förbättra modellen för hantering av VIRT-störningar. För kommunernas del görs en utredning som knyter an till åtgärden i punkt 3.1. I samband med verkställandet av den nationella cybersäkerhetsstrategin ta man fram en nationell cyberlägesbild som tar fasta på olika aktörer i samhället samt internationella samarbetspartner.
- Myndigheten för digitalisering och befolkningsdata planerar tillsammans med Cybersäkerhetscentret ett system för identifiering av kritiska informationssystem, kommunikationsnät och IoT-utrustning inom den offentliga förvaltningen. I planen behandlas genomförandet av sårbarhetstest så att innehavarna av kritiska informationssystem, kommunikationsnät och kritisk IoT-utrustning utarbetar en plan för att hitta sårbarheter. Man planerar att samla in och dela observationerna



mellan de organisationer som använder kritiska informationssystem, kommunikationsnät och kritisk IoT-utrustning. Man planerar även att kartlägga sårbarheter och hantera livscykeln i informationssystem som närmar sig slutet av sin livscykel.

Cert-fi-verksamheten ska utvecklas genom att man förbättrar observationsförmågan och sammanställer befintliga observationsdata. För observationen behövs teknisk utrustning (t.ex. Havarö), skanningstjänster och uppgifter om utvecklingen av mängden sårbarheter i kritiska system. Man planerar anskaffningar och stödtjänster för ibruktageand och en ansvarsfördelning för alla uppgifter i planen.

**Mätning:** Anvisningarna och rekommendationerna har färdigställts och stödtjänsten tagits i bruk. Sårbarhetstesterna har genomförts enligt planen.

**Kostnad/nytta:** Utredning: 60 000 euro. Genomförandet kräver uppskattningsvis två årsverken år 2021, fyra årsverken år 2020 och sex årsverken på Traficom år 2023. Genomförandet ingår inte i den uppskattade kostnaden. En snabbare reaktionsförmåga tryggar kontinuiteten och säkerheten hos de tjänster som medborgarna anlitar och minskar kostnaderna för störningssituationer och dataskyddskränkningar. Det minskar även skadorna på ryktet och förtroendet inom förvaltningen och bland sammanslutningarna och medborgarna.

### 8.3 Den offentliga förvaltningens molntjänster

**Mål:** Stöd för användningen av molntjänster inom den offentliga förvaltningen.

**Ansvar:** Myndigheten för digitalisering och befolkningsdata

**Kommunikation:** Myndigheten för digitalisering och befolkningsdata utarbetar en kommunikationsplan och informerar organisationerna inom den offentliga förvaltningen om ärenden som gäller användningen av molntjänster.

**Målgrupp:** Offentlig förvaltning

**Tidsplan:** 2021–2023

**Åtgärder:** Tillsammans med Valtori bereder Myndigheten för digitalisering och befolkningsdata avtalsklausuler, specifikationsdokument och kravspecifikationer för att byta eller avsluta en tjänst (s.k. moln-exit), varvid det också är möjligt att överföra tjänsterna till en annan molnmiljö. Man planerar hur molntjänster kan backa upp servicenät. En analys utarbetas över alternativen i olika säkerhetslägen, de risker som förknippas med

alternativen analyseras och rekommendationer ges för användningen av molntjänsterna.

**Mätning:** Krypteringsfallen och minimikraven har beskrivits.

**Kostnad/nytta:** Beredning av specifikationerna 80 000 euro. Med hjälp av enhetliga specifikationer är det möjligt att sänka kostnaderna och förbättra molntjänsternas säkerhet, förutsättningar och beredskap.

**Totalt 300 000 euro för de anskaffningar som gäller utredningsarbetet i punkt 8 och 120 000 euro för anskaffningarna för genomförandet.**

## 9 Säker utveckling av autonoma och lärande system och tjänster inom den offentliga förvaltningen

Säkerheten i de autonoma och lärande systemen samt de digitala tjänsterna säkerställs med hjälp av riskhantering.

### 9.1 Övervakning av autonoma och lärande system inom den offentliga förvaltningen

- Mål:** Att trygga övervakningen av autonoma och lärande system. Säkerhetsprinciper och en kontrollmiljö för utvecklingen och övervakningen av autonoma och lärande system ska fastställas och genomförandet övervakas.
- Ansvar:** Finansministeriet
- Kommunikation:** Finansministeriet utarbetar en kommunikationsplan och informerar organisationer inom den offentliga förvaltningen och sammanslutningar om tillämpningsanvisningarna i anslutning till autonoma och lärande system.
- Målgrupp:** Den offentliga förvaltningen och sammanslutningarna
- Tidsplan:** 2022–2023
- Åtgärder:** Finansministeriet tillsätter tillsammans med myndigheten för digitalisering och befolkningsdata en arbetsgrupp för att utreda kontrollmiljöerna i anslutning till säkerheten hos autonoma och lärande system. I gruppen skapas samförstånd kring lagstiftningen och eventuella revideringsbehov samt den gemensamma grunden för lagstiftningen och etiken. EU:s anvisningar och verktyg beaktas till fullo. Utifrån utredningen utarbetas principer för utveckling och övervakning av systemen samt en kontrollmiljö, som styr utvecklingen och underhållet av systemen samt

kommunikationen till medborgarna. Förtroendet för tjänsternas innehåll och resultat måste bibehållas i olika situationer. Kommunikationen till medborgarna om verksamheten inom tjänsten ska vara transparent.

I säkerhetsprinciperna och kontrollmiljön för de autonoma och lärande systemen ska man ta ställning till utvecklings- och övervakningskrav inom följande delområden:

- rättvisa; modellerna ska vara lagenliga och behandla data objektivt
- integritet och robusthet; modellerna ska fungera konsekvent i olika verksamhetsmiljöer och det ska finnas tillvägagångssätt för störningssituationer
- tolkningsbarhet; modellernas sätt att lära sig och fatta beslut ska kunna tolkas och förklaras

Finansministeriet främjar aktivt utvecklingen av etiska regler och kontrollmiljöer för autonoma och lärande system i det internationella samfundet.

Myndigheten för digitalisering och befolkningsdata utarbetar en standardenlig nationell anvisning om utvecklingen och ibrukttagandet av autonoma och lärande system. Myndigheten tar fram en sakkunnigtjänst för att testa och verifiera systemen.

Kontrollmiljön för autonoma och lärande system förutsätter att man fastställer nya hotbilder och risker samt lämpliga kontrollmetoder för att hantera dem. I arbetet för att utarbeta en kontrollreferensram eller ett etiskt regelverk ingår riskanalys, fastställande av kontrollmetoder samt författande av en anvisning. I projektet ingår även en pilottestning av kontrollmetodernas lämplighet för organisationer inom den offentliga sektorn.

**Mätning:** Den nationella anvisningen har beretts.

**Kostnad/nytta:** Utredning av riskanalys, fastställande av kontrollmetoder samt anvisning och pilottestning: 100 000 euro. Med hjälp av enhetliga anvisningar tryggas säkerheten och kontinuiteten hos lärande och autonoma system och kostnaderna för störningssituationer och dataskyddskränkningar minskas, liksom även skadorna på förvaltningens rykte.

## 9.2 Säker serviceutveckling inom den offentliga förvaltningen

**Mål:** Att kraven på informationssäkerheten bör uppdateras kontinuerligt beaktas i processen för serviceutvecklingen inom den offentliga förvaltningen med hjälp av riskhanteringen. Ett särskilt mål är att göra preciseringar i de lärande och autonoma systemen.

**Ansvar:** Myndigheten för digitalisering och befolkningsdata

- Kommunikation:** Myndigheten för digitalisering och befolkningsdata utarbetar en kommunikationsplan och informerar organisationerna inom den offentliga förvaltningen om tillämpningen av metoderna för serviceutvecklingen.
- Målgrupp:** Offentlig förvaltning
- Tidsplan:** 2022–2023
- Åtgärder:** Myndigheten för digitalisering och befolkningsdata specificerar hur man inom serviceutvecklingen och ska fastställa de krav på digital säkerhet som bör uppdateras kontinuerligt via riskhanteringen, särskilt beträffande autonoma och lärande system. Säkerhetskraven för serviceutvecklingen ska omfatta sådana åtgärder för att trygga säkerheten som är lämpliga för olika programutvecklingsmodeller. Myndigheten för digitalisering och befolkningsdata utarbetar även anvisningar om rekommenderade metoder, såsom DevSecOps-utvecklingsmetoden. Myndigheten producerar utbildning om säker serviceutveckling för den offentliga förvaltningen och näringslivet.
- Mätning:** Processen för att utarbeta kraven och de centrala kraven har beskrivits och tagits i bruk inom riskhanteringen i serviceutvecklingsprojekt som berör autonoma och lärande system.
- Kostnad/nytta:** Utredning av modellen för analysering av hot- och riskinformation: 40 000 euro. Fastställande av testmetod och verktyg som stöder denna: 40 000 euro. Beredning och genomförande av utbildning: 50 000 euro under ett år. Beslut om eventuella centraliserade program, såsom testverktyg, fattas separat. Med hjälp av en enhetlig modell för hot- och riskanalysdata tryggs säkerheten och kontinuiteten hos digitala tjänster och kostnaderna för störningssituationer och dataskyddskränkningar minskas, liksom även skadorna på förvaltningens anseende.

**Totalt 180 000 euro för anskaffningar som gäller utredningsarbetet i punkt 9 samt 50 000 euro för anskaffningarna för genomförandet.**

## 10 Sammanfattning av kostnaderna

Sammandrag av anskaffningarna i anslutning till utredningarna och genomförandet:

	Utredning	Genomförande
Punkt 1	80 000 €	0 €
Punkt 2	140 000 €	260 000 €
Punkt 3	160 000 €	0 €
Punkt 4	0 €	0 €
Punkt 5	40 000 €	200 000 €
Punkt 6	0 €	0 €
Punkt 7	0 €	0 €
Punkt 8	300 000 €	120 000 €
Punkt 9	180 000 €	50 000 €
<b>Sammanlagt</b>	<b>900 000 €</b>	<b>630 000 €</b>

De anskaffningar som gäller utredningsarbetet för att verkställa genomförandeplanen uppgår till uppskattningsvis 900 000 euro och anskaffningarna för genomförandet till 630 000 euro. Därtill uppskattas kostnaderna för kommunikation till 80 000 euro. Totalt 1 610 000 euro.

Kostnaderna för personarbete uppgår vid finansministeriet till 280 000 euro, vid Myndigheten för digitalisering och befolkningsdata till 990 000 euro och vid Transport- och kommunikationsverket till 780 000 euro, dvs. sammanlagt till 2 050 000 euro.

Vid finansministeriet sammanlagt 600 000 euro, vid Myndigheten för digitalisering och befolkningsdata till 2 280 000 euro och vid Transport- och kommunikationsverket 780 000 euro.

Kostnader sammanlagt 3 660 000 euro, från moment 28.70.01.

Genomförandeplanen medför ingen oundviklig bestående ökning av kostnaderna.

Följande faller utanför kostnads kalkylen:

- Kostnader för statsanställdas utanför Offentliga förvaltningens ICT, Myndigheten för digitalisering och befolkningsdata eller Traficom eller kommunanställdas eventuella medverkan i utvecklingsuppgifter i Vahti-nätverket och implementeringen av resultaten.
- Till detta hör bland annat kostnaderna för bedömning av den digitala säkerhetens risker och ekonomiska effekter som ska göras hos staten och i kommunerna.
- Kostnader för att införa och använda tjänster som förbättrar observations- och reaktionsförmågan i kommunerna.
- Kostnader för övervakningsfunktionen för cyberstörningar i kommunerna.
- Kostnader för anlita av sakkunnigtjänster inom digital säkerhet i den offentliga förvaltningen.
- Kostnader för genomförandet av informations- och kommunikationstekniska drifts- och produktionsmiljöer som motsvarar de tekniska riktlinjerna.
- Kostnader för bedömning av säkerhetsläget hos den offentliga förvaltningens infrastruktur och tjänster.









VALTIOVARAINMINISTERIÖ  
FINANSMINISTERIET

**FINANSMINISTERIET**

Snellmansgatan 1 A  
PB 28, 00023 STATSRÅDET  
Telefon 0295 160 01  
[finansministeriet.fi](http://finansministeriet.fi)

ISSN 1797-9714 (pdf)  
ISBN 978-952-367-284-0 (pdf)

Juni 2020