MINISTRY OF FINANCE

Implementation plan for digital security in the public sector

Public Sector ICT

Publications of the Ministry of Finance – 2020:47

Publications of the Ministry of Finance 2020:47

Implementation plan for digital security in the public sector

Tuija Kuusisto (Ed)

Ministry of Finance, Helsinki 2020

Ministry of Finance

ISBN PDF: 978-952-367-286-4

Layout: Government Administration Department, Publications

Helsinki 2020

Description sheet

Published by	Ministry of Finance		5 June 2020
Authors	Tuija Kuusisto (Ed)		
Title of publication	Implementation plan for digital security in the public sector		
Series and publication number	Publications of the Ministry of Finance 2020:47		
Register number	VN/1465/2020	**Subject**	Public Sector ICT
ISBN PDF	978-952-367-286-4	**ISSN (PDF)**	1797-9714
Website address (URN)	http://urn.fi/URN:ISBN:978-952-367-286-4		
Pages	38	**Language**	English
Keywords	public administration ICT, information policy, risk management, cyber security, preparedness, data security, digitalisation		

Abstract

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.

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).

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.

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

Kuvailulehti

Julkaisija	Valtiovarainministeriö		5.6.2020
Tekijät	Tuija Kuusisto (toim.)		
Julkaisun nimi	Julkisen hallinnon digitaalisen turvallisuuden toimeenpanosuunnitelma 2020–2023 (Haukka)		
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisuja 2020:47		
Diaari/hankenumero	VN/1465/2020	**Teema**	Julkisen hallinnon ICT
ISBN PDF	978-952-367-286-4	**ISSN PDF**	1797-9714
URN-osoite	http://urn.fi/URN:ISBN:978-952-367-286-4		
Sivumäärä	38	**Kieli**	englanti
Asiasanat	Julkisen hallinnon ICT, tietopolitiikka, riskienhallinta, kyberturvallisuus, varautuminen, tietoturva, digitalisaatio		

Tiivistelmä

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.

Haukka-toimeenpanosuunnitelmaan on valittu 19 tehtävää, joiden avulla kehitetään keskeisiä julkisen hallinnon digitaalisen turvallisuuden palveluita. Toimeenpanosuunnitelmalla tuetaan myös käynnistymässä olevaa kyberturvallisuusstrategian 2019 kehittämisohjelman valmistelua ja toteuttamista, sekä osaltaan pannaan täytäntöön valtioneuvoston päätöstä huoltovarmuuden tavoitteista (1048/2018).

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.

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

Presentationsblad

Utgivare	Finansministeriet		5.6.2020
Författare	Tuija Kuusisto (redaktör)		
Publikationens titel	Genomförandeplanen för digital säkerhet inom den offentliga förvaltningen 2020–2023 (Haukka)		
Publikationsseriens namn och nummer	Finansministeriets publikationer 2020:47		
Diarie-/ projektnummer	VN/1465/2020	**Tema**	Offentliga förvaltningens ICT
ISBN PDF	978-952-367-286-4	**ISSN PDF**	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-367-286-4		
Sidantal	38	**Språk**	english
Nyckelord	IKT inom den offentliga förvaltningen, informationspolitik, riskhantering, cybersäkerhet, beredskap, dataskydd, digitalisering		

Referat

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.

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).

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.

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

Contents

INTRODUCTION

The Government Resolution on Digital Security in The public sector (VM 2020: 23) describes the improvement areas and improvement principles for digital security in the public sector. In addition, it describes the key digital security services to support authorities' processes and services. In this Implementation Plan (Haukka), tasks related to each service have been selected on the basis of an assessment of the current state of digital security in the public sector and an international compari-son of Finland to the reference countries. The Implementation Plan sets objectives and timelines for the tasks and describes the actions required to achieve the objectives and the indicators used to measure progress towards the objectives. Costs and benefits are also assessed. The Implementation Plan supports, and is also intended as input for, the preparation of the development programme of Finland's Cyber Security Strategy 2019. The Implementation Plan will be updated where necessary in response to changes in the environment and the requirements set by the development programme of the Cyber Security Strategy 2019.

On 29 August 2019, the Ministry of Finance appointed a coordination group to prepare policies for digital security in the public sector for the period between 1 September 2019 and 28 February 2020. The coordination group was broadly representative of the various public sector actors. It drafted the resolution and its appendices as well as this Implementation Plan for 2020–2023 (Haukka). Opin-ions on these were requested between 24 January and 19 February 2020 via a public online consul-tation service. The feedback provided in the opinions was used to finalise this Implementation Plan first in the coordination group and then at the Ministry of Finance.

The responsible parties for the Implementation Plan 2020–2023 (Haukka) are as follows:

Ministry of Finance

- Strategic Steering Group for Digital Security in the Public Sector, chaired by Päivi Nerg, Permanent Under-Secretary: Oversees the delivery of Haukka Implementation Plan and the municipalities' digital security roadmap.
- Public Sector ICT Department; Anna-Maija Karjalainen, Director General of Public Sector ICT: Guides the delivery of Haukka Implementation Plan and steers the Digi-tal and Population Data Services Agency.
- Tuija Kuusisto, Program Manager, Haukka Program: Leads the implementation of the digital security in the public sector program Haukka.

Digital and Population Data Services Agency

- Public Sector Digital Security Management Board VAHTI: Produces the situational picture and basis for risk assessment, steers the VAHTI network of experts.
- Performs the duties allocated to the Digital and Population Data Services Agency in Haukka Implementation Plan under the Development Programme for Digital Securi-ty in The public sector (JUDO program), for which the Agency has appointed a steering group.

Finnish Transport and Communications Agency Traficom/ National Cyber Security Centre

- Performs the duties designated in Haukka Implementation Plan for Traficom/the Na-tional Cyber Security Centre as part of the JUDO program of the Digital and Popula-tion Data Services Agency.

Other ministries, Association of Finnish Municipalities and municipalities

- Perform the duties described in Haukka Implementation Plan in collaboration with the Ministry of Finance.

1 A national and international collaboration model for digital security in the public sector

Through national and international collaboration, the coordination and effectiveness of digital security will be enhanced and Finland's competitiveness will be boosted. The ministries and their administrative branches, municipalities, enterprises and non-governmental organizations will contribute actively to positive development in digital security in the European Union and in key international organisations such as the UN and OECD.

1.1 Strategic Management Group for Digital Security in the Public Sector

Objective: To advance digitalisation and digital security in a balanced way.

Responsibility: Ministry of Finance

Communications:
The Ministry of Finance will formulate a communications plan and communicate about the activities of the Strategic Management Group for Digital Security in the Public Sector.

Target: The Public Sector

Timeline: 2020–2024

Actions: The Ministry of Finance will appoint a Strategic Management Group for Digital Security in the Public Sector. The group will comprise the Prime Minister's Office, the Ministry for Foreign Affairs, the Ministry of the Interior, the Ministry of Defence, the Ministry of Transport and Communications, the Ministry of Social Affairs and Health, the Ministry of Employment and the Economy, the Security Committee, the Association of Finnish Municipalities,

a representative of the municipalities, the National Emergency Supply Agency, a representative of the universities and, as an expert, the Digital and Population Data Services Agency. The Group will coordinate the strategic risk assessment concerning digital security in the public sector, create and coordinate a collaboration model for digital security, and assess the strategic digital security situation in the public sector and the key digital security services to be developed, outline policies on key digital security aspects as well as digital security objectives, and oversee the delivery of this Implementation Plan for Digital Security and the municipalities' digital security roadmap.

Indicator(s): The Strategic Management Group for Digital Security in the Public Sector will have been appointed in 2020 and is ongoing. The strategic risk assessment has been analysed and resources have been directed based on the analysis on the most effective development targets.

Cost/benefit: The work of the Strategic Management Group for Digital Security in the Public Sector will be carried out as part of the members' official duties. The participating organisations will cover the travel and other costs of their representatives. If successful, the Management Group will have a significant impact on the prevention of key strategic digital security risks in the public sector, which will reduce extensive disruptions or paralysis of the authorities' processes and functions and harm caused by them to the continuity of society's functioning. This will reduce reputation damage and erosion of trust and confidence in the authorities and among citizens. The successful work of the Management Group will also boost Finland's competitiveness and enable innovations and growth.

1.2 Collaboration and governance model for digital security in the public sector

Objective: For the Ministry of Finance, together with other ministries, municipalities and communities, to operate in accordance with the collaboration and management model enhancing digital security in the public sector.

Responsibility: Ministry of Finance

Communications:

The Ministry of Finance will formulate a communications plan and communicate about the collaboration and governance model for digital security to the public sector organisations and citizens.

Target: The public sector, citizens

Timeline: 2021–2023

Actions: The Ministry of Finance, together with other ministries, municipalities and entities, and supported by the activities of the Public Sector Digital Security Management Board (VAHTI), will create and coordinate a national strategic-level collaboration model for digital security that covers activities and finances as well as competence development. When preparing the collaboration model, the duties and responsibilities of central government, joint municipal authorities and municipalities as well as the public sector's digital security services for citizens, and research collaboration, will be covered. Operational management responsibilities and arrangements will be determined, taking the responsibilities of the authorities into account, and the national cyber security situational picture will be developed, taking the various societal actors and international partners into account. The Ministry of Finance and other ministries will communicate about the digital security objectives and include them into the public sector's general objectives.

Indicator(s): The collaboration model has been described and is implemented. Financial plans include concrete targets that improve digital security.

Cost/benefit: Collaboration model study EUR 80,000. The coordination of implementation will take place as part of other official duties. Implementation costs will be estimated in more detail as progress is made in the study. The benefit achieved will be the development of strategic- and operational-level digital security and competence development enabled by further improvements in collaboration.

1.3 Functional-level development of digital security in the public sector

Objective: For the Public Sector Digital Security Management Board VAHTI to advance and develop collaboration in and coordination of the implementation of digital security in the whole of the public sector.

Responsibility: Digital and Population Data Services Agency

Communications:

The Digital and Population Data Services Agency will formulate a communications plan and communicate about the activities of the Public Sector Digital Security Management Board VAHTI.

Target: The public sector, international collaboration

Timeline: 2020–2024

Actions: The Digital and Population Data Services Agency will appoint the Public Sector Digital Security Management Board VAHTI as a functional-level multi-actor steering group. The new Management Group is planned to consist of senior officials and management of central agencies and key entities and bodies. The Management Group will advance national and international competence development. The situational picture on digital security produced by a variety of authorities will be utilised in digital security management (VAHTI) activities.

Indicator(s): The Public Sector Digital Security Management Board VAHTI has been appointed and is ongoing.

Cost/benefit: The work of the Public Sector Digital Security Management Board VAHTI will be carried out as part of other official duties. The participating organisations will cover the travel and other costs of their representatives in the Management Board. If successful, the Management Group will have a significant impact on the prevention of key operational risks concerning digital security in the public sector, which will reduce costs arising from incidents and materialised information security breaches as well as reputation damage and erosion of trust and confidence in the authorities and among citizens.

1.4 International collaboration of the public sector in digital security

Objective: To develop technology solutions in accordance with EU legislation and fulfil sufficient requirements set for digital security in the public sector's services. This will also boost Finland's competitiveness through international collaboration.

Responsibility: Each ministry for its own area of responsibility

Communications:
Each ministry will communicate about its international collaboration in digital security to the other ministries and entities.

Target: International collaboration

Timeline: 2021–2023

Actions: Coordinated by the Prime Minister's Office in EU matters and by the Ministry for Foreign Affairs in other international matters, each ministry will, for its own area of responsibility, advance together with the other ministries the delivery of technology solutions in accordance with EU

legislation and the fulfilment of sufficient digital security requirements in the public sector's services.

In collaboration with other ministries and actors, the Ministry of Finance will launch a study on the centralisation of reporting on international matters so that there would be a single actor in Finland compiling and reporting on Finland's data for international assessments of digital security and to various international entities.

The Ministry of Finance, together with the Public Sector Digital Security Management Board VAHTI activities of the Digital and Population Data Services Agency, will strengthen collaboration with the Baltic states and Nordic countries in the field of digital security in the public sector. The collaboration will be coordinated with actions taken by the Ministry for Foreign Affairs and the Prime Minister's Office in the field of digital security.

Indicator(s): Objectives have been set for international collaboration of the public sector and are monitored. The centralisation of reporting to international entities has been planned and is taking place. Digital security collaboration between the Ministry of Finance and the Baltic states and Nordic countries provides new information to support decision-making.

Cost/benefit: International collaboration and planning of the centralisation of reporting will be carried out alongside other official duties. The participating organisations will cover their representatives' travel and other costs. If successful, the work will have a significant impact on procurement opportunities and production models as well as the continuous improvement of services, infrastructure and information security concerning digital services of the public sector, as it is not currently possible to develop these through actions taken only in Finland.

Total procurement under section 1 relating to the study EUR 80,000.

2 Management of digital security risks in the public sector

Development priorities will be selected and resources will be directed based on risk analyses and impact assessments that have been induced from an assessment of the current state of digital security and the situation understanding.

2.1 Strategic-level risk analysis of digital security in the public sector

Objective: To make available a risk analysis based on an assessment of the current state of digital security and the strategic-level situation understanding.

Responsibility: Ministry of Finance, Digital and Population Data Services Agency

Communications:

The Ministry of Finance will communicate about the strategic risk assessment. The Digital and Population Data Services Agency will formulate a communications plan and communicate about services related to digital security risk management to the public sector organisations.

Target: The public sector

Timeline: 2020–2021

Actions: The Digital and Population Data Services Agency will identify and deliver the process and services through which it will compile, in a centralised manner, information about organisations' digital security threats, risks and maturity level, and disseminate information required for the development of digital security. Collaboration will take place between the Government Financial Controller's Function (Ministry of Finance) and the other public sector.

The Ministry of Finance will identify and deliver the process together with the Digital and Population Data Services Agency, with the help of which it will maintain the long-term strategic risk assessment on digital security

and formulate long-term policies for development activities. The Ministry of Finance will coordinate the Implementation Plan for Digital Security in The Public Sector under which the policies will be delivered and regularly assess the realisation of the policies.

Indicator(s): A risk assessment based on the overall situation understanding has been created, and is available.

Cost/benefit: Study concerning risk identification and maintenance processes EUR 80,000 and the first risk analysis concerning strategic digital security risks an estimated EUR 60,000. Risk maintenance in conjunction with the overall situation understanding service an estimated EUR 100,000. More specific delivery costs will be estimated in conjunction with the study. Organisations' internal risk management will take place alongside other official duties. Benefits are described under subsection 1.1.

2.2 Cost/benefit model for digital security in the public sector

Objective: To advance cost and impact assessment models and procedures for digital security in the public sector.

Responsibility: Ministry of Finance

Communications:

The Ministry of Finance will formulate a communications plan and communicate to the public sector about the development and utilisation of the model in the public sector. The Digital and Population Data Services Agency will communicate about the use of the model as part of the overall situation understanding service.

Target: The public sector organisations

Timeline: 2020–2021

Actions: The Ministry of Finance together with the Digital and Population Data Services Agency will formulate an effectiveness/cost model and process for digital security. Assessment of effectiveness and costs of digital security management and development in central government and municipalities will be planned. The objective is for the public sector appropriations for digital security to equal 5% of ICT expenditure. The model will be piloted, and the model will be updated on the basis of the experiences gained through the pilot. The model will be rolled out as part of the overall situation understanding service of the Digital and Population Data Services Agency in 2021.

Indicator(s): The model has been created and delivered. The effectiveness assessment is available.

Cost/benefit: The study concerning the preparation of the model and the process EUR 60,000. In delivery as part of the overall situation understanding service, data transmission interfaces for central government actors EUR 50,000 and provision of a user interface for municipalities EUR 50,000. This estimate excludes production environment maintenance costs. Delivery costs including costs from work carried out in municipalities will be specified in more detail in conjunction with the formulation of the model and the process. The model and the process will be required to enable knowledge-based strategic management of digital security. The benefits of strategic management of digital security are discussed in subsection 1.1.

Total procurement under section 2 relating to studies EUR 140,000 and to delivery and maintenance EUR 260,000.

3 Shared services advancing digital security intended for municipalities

The roadmap for developing municipalities' digital security will be maintained and its delivery monitored.

3.1 Security of information networks used by municipalities

Objective: To increase municipalities' monitoring and response capacity.

Responsibility: Digital and Population Data Services Agency, Association of Finnish Municipalities, municipalities

Communications:
The Digital and Population Data Services Agency will formulate a communications plan and communicate to the municipalities about actions for increasing monitoring and response capacity.

Target: Municipalities

Timeline: 2020–2022

Actions: Steered by the Ministry of Finance, the Digital and Population Data Services Agency, together with the Finnish Transport and Communications Agency Traficom, the Association of Finnish Municipalities and the municipalities, will set up a group to study and coordinate action to increase municipalities' monitoring and response capacity. One of the potential services is the preparation of the national monitoring and early warning system (HAVARO) for the local government sector. The action is related to subsection 8.2.

Indicator(s): Services increasing monitoring and response capacity are available to the municipalities.

Cost/benefit: Study EUR 60,000, and delivery described in conjunction with subsection 8.2. During the study, the municipalities to be using the services as well as the services will be selected and delivery costs in municipalities will

be specified. The service users will cover the costs relating to launch and service use and any licence fees required. A speedier response will help secure the continuity and security of citizens' services and reduce costs arising from incidents and materialised information security breaches. Reputation damage and erosion of trust and confidence in the authorities and among citizens will be reduced.

3.2 Municipalities' shared digital security services

Objective: To maintain the municipalities' shared roadmap for digital security development and to monitor its delivery.

Responsibility: Digital and Population Data Services Agency, Association of Finnish Municipalities, municipalities

Communications:
The Digital and Population Data Services Agency together with the Association of Finnish Municipalities will formulate a communications plan and communicate to the municipalities about the delivery of the roadmap for digital security development and the municipalities' duties for the development of digital security.

Target: Municipalities

Timeline: 2021–2023

Actions: Steered by the Ministry of Finance, the Digital and Population Data Services Agency, together with the Association of Finnish Municipalities and the municipalities, will set up a working group to study the need for and implementation of municipalities' joint digital security development projects. The study will be based on this Implementation Plan, which sets out the basis for the roadmap for the development of the municipalities' digital security. In addition, the study will cover a control room facility for digital environments (municipalities' shared cyber and information security control room). The control room facility could be delivered as a control room service available to all municipalities, with access to the alert data provided to municipal leadership to support their decision-making.

Indicator(s): The working group has been set up and the studies completed. The roadmap for municipalities' digital security is maintained.

Cost/benefit: Study EUR 100,000. During the study, the criteria that a service must meet for inclusion in the service will be identified, and the delivery costs will be specified further. The services selected must be such for which all or many

municipalities have a similar service need. Public resources are wasted if municipalities produce and study services separately.

Total procurement under section 3 relating to studies EUR 160,000.

4 Digital identity management

Access to electronic identification for all Finnish citizens and everyone residing in Finland will be improved. The development of effective electronic identification solutions enabling the use of various devices will be improved.

Objective: For the public sector to guarantee a reliable, usable electronic identity for every citizen and resident. For central government to enable in a comprehensive and non-discriminatory manner a digital identification solution for citizens and residents and to guarantee access to identity verification in a digital world.

Responsibility: Ministry of Finance

Communications:
The Ministry of Finance will formulate a communications plan and communicate to citizens about the status of digital identity management.

Target: Citizens

Timeline: 2020–2023

Actions: The Ministry of Finance together with other ministries will coordinate the necessary legislative amendments and the duties necessary at the Digital and Population Data Services Agency.

Indicator(s): The legislative amendments have been made and the necessary duties defined. Increase in the use of electronic transactions, incl. transactions on behalf of others and authorisations (i.e. the trend in the number of those with access to electronic transactions).

Cost/benefit: The service package will be delivered as a separate project in which costs and benefits will be assessed and that is also responsible for arranging funding for the service package.

5 Development of competences of citizens and staff

Digital security skills and awareness of the public sector staff as well as business and non-governmental organizations' personnel and citizens will be improved.

5.1 Digital security training services for citizens and staff

Objective: To build competences relating to digital security.

Responsibility: Digital and Population Data Services Agency

Communications:
The Digital and Population Data Services Agency will formulate a communications plan and communicate to the public sector organisations and citizens about available digital security training.

Target: Citizens, staff and management

Timeline: 2022–2023

Actions: The Digital and Population Data Services Agency together will the Ministry of Education and Culture will productise digital security training for citizens and for central government and municipal staff and management. Competence development planned for 2019–2021 under the Development Programme for Digital Security in The public sector (JUDO project) will be continued. Exercises as a component of competence development, and service attitude development, will be taken into account. The Ministry of Education and Culture will develop citizens' digital security competences comprehensively as part of the Finnish education system.

Indicator(s): The training packages have been produced and the distribution channel is in use.

Cost/benefit: Estimated annual costs EUR 80,000. Current platforms can be used as training distribution channels, so costs arising from licences and launch

will be moderate. Costs will consist of costs relating to the production and maintenance of new material, training material licences and service fees, and website and service platform licence costs (e.g. annual costs for cloud service platform). Competence development helps secure the security and reliability of the public sector's services and access among citizens and residents to the services.

5.2 Digital security driving licence for citizens and staff

Objective: To develop a citizen and staff competence identification procedure in order to increase trust and confidence and to identify competences.

Responsibility: Digital and Population Data Services Agency

Communications:
The Digital and Population Data Services Agency will formulate a communications plan and communicate to citizens and the public sector staff about the competence identification procedure.

Target: The public sector

Timeline: 2021–2022

Actions: The Digital and Population Data Services Agency will study procedures developed for citizens to demonstrate their digital security competences, such as the citizens' cyber security driving licence, and procedures developed for staff to demonstrate their basic digital security skills. The study will present the possible ways forward to deliver/expand the procedures.

Indicator(s): The study on the procedures for demonstrating digital security competences has been completed. Based on the study, delivery models, having been piloted if necessary, have been proposed. The promotion of the delivery of the procedures has been planned.

Cost/benefit: Study EUR 40,000, delivery an estimated EUR 40,000. Citizens and the public sector staff will be able to demonstrate that they comply with secure practices in the digital environment. The benefit achieved will be increased awareness of digital security among citizens and the public sector staff.

Total procurement under section 5 relating to the study EUR 40,000 and to delivery EUR 40,000 as well as EUR 80,000 per year for two years, i.e. a total of EUR 240,000.

6 Digital security consultancy services for the public sector

Centralised digital security services for the public sector will be developed and offered broadly across the public sector.

6.1 Organising digital security expert services

Objective: To have shared digital security consultancy services organised for the public sector.

Responsibility: Digital and Population Data Services Agency

Communications:
The Digital and Population Data Services Agency will formulate a communications plan and communicate to the public sector organisations about the use of digital security consultancy services.

Target: The public sector

Timeline: Preparation 2020–2021, services available 2022–2023

Actions: The Digital and Population Data Services Agency together with the central procurement unit Hansel will study and further develop the public sector's digital security consultancy and auditing services and associated procurement procedures. The study will cover service providers' uniform opportunities for service supply, the public sector's need for digital security consultancy and auditing, and alternative models relating to expert service sourcing.

Based on the study, the Digital and Population Data Services Agency will build a digital security expert service for the public sector and tools supporting the service.

Indicator(s): The consultancy service and tools are in use.

Cost/benefit: Organising the services will take place alongside other official duties. The service users will cover the costs of service use. The benefit achieved will be access to the services throughout the whole of the public sector.

7 Assessment of digital security of services and service provision in the public sector

Assessment and verification of digital services and service providers based on norms and standards will be advanced.

7.1 Legislation concerning information security evaluations

Objective: To assess any needs to reform the Act on the Evaluation of the Information Security of the Authorities' Information Systems and Telecommunications Arrangements (1046/2011) and the Act on Information Security Inspection Bodies (1045/2011), and to conduct any legislative drafting required on the basis of the conclusions.

Responsibility: Ministry of Finance

Communications: The Ministry of Finance will communicate about the legislative drafting in compliance with the communications principles applied to legislative drafting.

Target: The public sector

Timeline: 2021–2022

Actions: The Ministry of Finance, together with the Ministry of Transport and Communications as well as the Finnish Transport and Communications Agency Traficom and other ministries and possibly the municipalities, will study the current status and reform needs during 2021. Legislative drafting based on the conclusions in 2021–2022. Possible new bills to Parliament in early autumn 2022.

Indicator(s): The studies have been completed. Any follow-on measures arising from the studies have been completed.

Cost/benefit: The studies and any legislative drafting will take place alongside other official duties. Drafting will include assessments of effectiveness and economic impact assessments. The cost estimate excludes Traficom's work.

7.2 Legislation concerning evaluation of digital service preparedness and contingency planning

Objective: To assess any need for legislation concerning digital services and infrastructure contingency and preparedness planning and their assessment procedure and to conduct any legislative drafting required.

Responsibility: Ministry of Finance

Communications:
The Ministry of Finance will communicate about the legislative drafting in compliance with the communications principles applied to legislative drafting.

Target: The public sector

Timeline: 2021–2022

Actions: The Ministry of Finance, together with the Ministry of Transport and Communications as well as the Finnish Transport and Communications Agency Traficom and other ministries and possibly the municipalities, will study the current status and reform needs during 2021. Legislative drafting based on the conclusions in 2021–2022. Possible new bills to Parliament in early autumn 2022.

Indicator(s): The studies have been completed. Any follow-on measures arising from the studies have been completed.

Cost/benefit: The studies and any legislative drafting will take place alongside other official duties. Drafting will include assessments of effectiveness and economic impact assessments. The cost estimate excludes Traficom's work.

.

8 Protection of digital infrastructure needed for the authorities' processes and services

The security of key shared technologies and services will be advanced to secure information and the continuity of the functions, processes and digital services of the public sector.

8.1 The public sector's security architecture

Objective: For the public sector's security architecture to guide the development of digital infrastructure.

Responsibility: Digital and Population Data Services Agency

Communications:
The Ministry of Finance together with the Digital and Population Data Services Agency will formulate a communications plan and communicate to the public sector organisations about the development and utilisation of security architecture.

Target: The public sector

Timeline: Study 2020–2021, implementation 2021–2023

Actions: Steered by the Ministry of Finance, the Digital and Population Data Services Agency, together with the Finnish Transport and Communications Agency Traficom, Social Insurance Institution of Finland (Kela), other government agencies and institutions as well as the municipalities, will create security architecture for the public sector. The work will take place utilising information management maps and models created in conjunction with the implementation of the Act on Information Management in The public sector (906/2019) and the interoperability steering of the Ministry of Finance. The work will take place in collaboration with programmes for critical infrastructure development focusing on key elements of critical

infrastructure, such as Digital Security 2030 of the National Emergency Supply Agency (NESA).

a. A description will be provided of the level on which national capabilities will be built and what will be included in the critical digital services, information and infrastructure that involve special requirements for national control and safeguarding. Publicly available information may as such pose a risk or a risk may be created through individual pieces of public information being combined (cumulativeness of information). Examples of such information include power grid diagrams or structural drawings of bridges. It is not justifiable to allow digital access to all public information. Policies will be formulated as regards to what extent services will be provided and infrastructure built through national measures and resources, to what extent the work will be based on common development within the EU or on other international collaboration and, especially in the public sector, how new service models and technological opportunities could and should be used in the provision of public digital services.
b. A criticality classification system will be drawn up and introduced for the public sector's services and information systems, the need for an information system register will be assessed, and the current compliance situation of critical services, information systems and telecommunications solutions will be evaluated.
c. A list of technologies recommended for use in the public sector's digital services will be prepared. A list of technologies to be avoided and any use of which must be assessed from the risk management perspective, such as obsolete technology, will also be prepared.
d. Relating to section 7, a plan will be drawn up to develop security checks of services and service networks.

Actions for compliance with architecture:

e. A knowledge base on the long-term development needs of society's critical information systems, information resources and information networks will be compiled, and a plan for the launch of a development programme carried out with centralised funding will be drawn up. In this context, mapping and life-cycle planning of critical old information systems in particular will be examined.
e. A long-term development plan will be drawn up to improve the compliance of critical services, information systems and data communications solutions and to deal with the existing maintenance backlog.

Indicator(s): Actions a–d have been completed. Actions e–f have been completed as regards the public sector's services or shared central government services.

Cost/benefit: Study of current situation and mapping of shortcomings EUR 60,000. Description/study of security architecture development needs including matters in accordance with actions a–d EUR 100,000. Formulation of technology policies EUR 120,000. Each authority will be responsible for delivering the technology policies and building the environments in accordance with the policies as regards actions e–f, and these costs will be estimated project-specifically. The level of security architecture will vary if each authority separately prepares matters related to security architecture. Centralised coordination can help reduce costs and improve the consistency and quality of the outcomes of planning as well as the security, preparedness and contingency of the services provided and their provision environments.

8.2 Monitoring, response and analyses required by the public sector

Objective: To speed up the handling of digital security incidents and to identify vulnerabilities.

Responsibility: Digital and Population Data Services Agency

Communications:

The Digital and Population Data Services Agency together with the Finnish Transport and Communications Agency Traficom will formulate a communications plan and communicate to the public sector organisations and entities about measures to boost monitoring and response capacity.

Target: The public sector and entities

Timeline: 2021, implementation of plan 2022

Actions: The Digital and Population Data Services Agency together with the National Cyber Security Centre will produce guidelines and recommendations for the development of monitoring and response capacity relating to the public sector's services and to improve the Virtual Incident Response Team (VIRT) model for incident management. As regards municipalities, the action description is provided under 3.1. Together with the implementation of Finland's Cyber Security Strategy, the national cyber security situational picture will be developed, taking into account the various societal actors and international partners.

The Digital and Population Data Services Agency, together with the National Cyber Security Centre, will plan the identification of the public sector's critical information systems, telecommunications networks and IoT devices. The plan will cover the implementation of vulnerability testing in the manner whereby the owners of information systems, telecommunications networks and IoT devices identified as critical will formulate a plan to detect vulnerabilities. Plans will be made for compiling monitoring observations so that they can be shared with the organisations using the critical information systems, telecommunications networks and IoT devices. In addition, the mapping of vulnerabilities in and life-cycle management of information systems nearing the end of their life cycle will be planned.

CERT-FI activities will be developed further by increasing monitoring capacity and compiling current monitoring data. Monitoring will require technical tools (e.g. the National Monitoring and Early Warning System, HAVARO), scanning services and information about quantitative developments in vulnerabilities in critical systems. Procurements, launch support services and implementation responsibilities will be planned for all duties included in the plan.

Indicator(s): The guidelines and recommendations have been produced and the support service is in use. Implementation of vulnerability testing as planned.

Cost/benefit: Study EUR 60,000. Delivery will require an estimated two full-time equivalents (FTEs) of human resources in 2021, four FTEs in 2022 and six FTEs 2023 in Traficom. Delivery is not included in the cost estimate. Speedier response will safeguard the continuity and security of citizens' services and reduce costs arising from incidents and materialised information security breaches. This will reduce reputation damage and erosion of trust and confidence in administration, entities and among citizens.

8.3 The public sector's cloud services

Objective: To support the use of the public sector's cloud services.

Responsibility: Digital and Population Data Services Agency

Communications:

The Digital and Population Data Services Agency will formulate a communications plan and communicate to the public sector organisations about matters relating to the use of cloud services.

Target: The public sector

Timeline: 2021–2023

Actions: The Digital and Population Data Services Agency together with the Government ICT Centre Valtori will prepare contractual clauses, specifications documents and requirements definitions for switching or exiting cloud services (cloud exit strategy), also enabling the migration of services to another cloud environment. The use of cloud services in service network assurance will be planned. An analysis of the options in various security situations, a related risk analysis and recommendations relating to the use of cloud services will be provided.

Indicator(s): Use cases and minimum requirements have been described.

Cost/benefit: Preparation of specifications EUR 80,000. Uniform specifications can help reduce costs and improve the security, preparedness and contingency of cloud services.

Total procurements under section 8 relating to studies EUR 300,000 and to delivery EUR 120,000.

9 Secure development of autonomous and adaptive systems and services in the public sector

The security of autonomous and adaptive systems as well as digital services will be ensured through risk management.

9.1 Surveillance of autonomous and adaptive systems in the public sector

Objective: To ensure the surveillance of autonomous and adaptive systems. To have determined the security principles and control environment related to the development and surveillance of autonomous and adaptive systems and to supervise delivery.

Responsibility: Ministry of Finance

Communications: The Ministry of Finance will formulate a communications plan and communicate to the public sector organisations and entities about application guidelines relating to the use of autonomous and adaptive systems.

Target: The public sector and entities

Timeline: 2022–2023

Actions: The Ministry of Finance together with the Digital and Population Data Services Agency will appoint a working group to study the control environments relating to the security of autonomous and adaptive systems. The working group will create a common understanding of legislation and any need to develop it and of the common foundation of legislation and ethics. EU guidelines and tools will be taken fully into account. Based

on the study, the principles and control environment relating to system development and surveillance will be created to steer system development and maintenance as well as communications, including to citizens. Trust and confidence must be included in service contents and outcomes in the various situations. Service functioning must be communicated transparently to citizens.

The security principles and control environment for autonomous and adaptive systems must address development and surveillance requirements in the following areas:

- Fairness – The models must be compliant with legislation and process information in an unbiased manner.
- Integrity and robustness – The models function consistently in different operating environments and their functioning during incidents has been specified.
- Explainability – The way the models learn and make decisions can be interpreted and explained.

The Ministry of Finance will actively advance the development of ethical codes and the control environment for autonomous and adaptive systems in international collaboration.

The Digital and Population Data Services Agency will draw up national application guidelines for the development and introduction of autonomous and adaptive systems in accordance with the standard. The Agency will develop an expert service for systems testing and assurance.

The control environment for autonomous and adaptive systems will require the specification of controls suitable for new threat scenarios and risks and their management. The formulation of the control framework or ethical codes and the control environment will consist of risk analysis, control specification work and writing of the application guidelines. In addition, the project must include a pilot phase during which the suitability of the controls for a public sector organisation will be tested.

Indicator(s): The national application guidelines have been prepared.

Cost/benefit: Study concerning the risk analysis, control specifications and guidelines and their piloting EUR 100,000. Uniform guidelines will ensure the security and continuity of adaptive and autonomous systems and reduce costs arising from incidents and materialised information security breaches as well as reputation damage.

9.2 Secure service development in the public sector

Objective: For the public sector's service development process to take continuously updated information security requirements into account through risk management, with a specific objective being more detailed specifications relating to adaptive and autonomous systems.

Responsibility: Digital and Population Data Services Agency

Communications:
The Digital and Population Data Services Agency will formulate a communications plan and communicate to the public sector organisations about the use of secure service development methods.

Target: The public sector

Timeline: 2022–2023

Actions: The Digital and Population Data Services Agency will determine how continuously updated digital security requirements will be set in service development through risk assessment, in particular as regards autonomous and adaptive systems. Security requirements relating to service development must cover measures relating to security assurance suitable for the various application development models. In addition, the Digital and Population Data Services Agency will draw up guidelines on recommended methods, such as the DevSecOps development method. The Digital and Population Data Services Agency will productise secure service development training for the public sector and businesses.

Indicator(s): The requirement formation process and key requirements have been described and are used though risk management in service development projects relating to autonomous and adaptive systems.

Cost/benefit: Study concerning the model required for analyses of threat and risk analysis information EUR 40,000. Determination of the testing method and tools supporting it EUR 40,000. Preparation and delivery of training EUR 50,000 during one year. Decisions on any centralised software such as testing tools will be made separately. The uniform threat and risk analysis information model will safeguard the security and continuity of digital services and reduce costs arising from incidents and materialised information security breaches as well as reputation damage.

Total procurement under section 9 relating to studies EUR 180,000 and to delivery EUR 50,000.

10 Summary of costs

Summary of procurements relating to studies and delivery:

	Study	Delivery
Section 1	EUR 80,000	EUR 0
Section 2	EUR 140,000	EUR 260,000
Section 3	EUR 160,000	EUR 0
Section 4	EUR 0	EUR 0
Section 5	EUR 40,000	EUR 200,000
Section 6	EUR 0	EUR 0
Section 7	EUR 0	EUR 0
Section 8	EUR 300,000	EUR 120,000
Section 9	EUR 180,000	EUR 50,000
Total	**EUR 900,000**	**EUR 630,000**

Procurements relating to studies required for the delivery of the Implementation Plan amount to an estimated EUR 900,000 and those relating to delivery an estimated EUR 630,00, in addition to which an estimated EUR 80,000 for communications. Total EUR 1,610,000.

As regards the use of human resources, the Ministry of Finance has allocated an estimated EUR 280,000, the Digital and Population Data Services Agency an estimated EUR 990,000 and the Finnish Transport and Communications Agency Traficom an estimated EUR 780,000, i.e. a total of EUR 2,050,000.

The Ministry of Finance a total of EUR 600,000, the Digital and Population Data Services Agency EUR 2,280,000 and the Finnish Transport and Communications Agency Traficom EUR 780,000.

Total costs amount to EUR 3,660,000, from Budget item 28.70.01.

The delivery of the Implementation Plan will not result in any necessary permanent increase in costs.

The following have been excluded from the cost estimate:

- The possible participation of central government or municipal staff outside of the Ministry of Finance's Public Sector ICT department, the Digital and Population Data Services Agency and the Finnish Transport and Communications Agency Traficom in development duties in the Public Sector Digital Security Management Board VAHTI network and taking the outcomes into use.
- This includes costs such as those arising from assessments of digital security risks and economic impacts conducted in central government and municipalities.
- Costs of the launch and use of services boosting central government's and municipalities' monitoring and response capacity.
- Costs of municipalities' control room facility for cyber incidents.
- Costs of digital security consultancy service use in the public sector.
- Costs of delivering usage and production environments of information and communications technology compliant with the technology policies.
- Costs of assessing the state of security in the infrastructure and services of the public sector.

MINISTRY
OF FINANCE

MINISTRY OF FINANCE
Snellmaninkatu 1 A
PO BOX 28, 00023 GOVERNMENT
Tel. +358 295 160 01
financeministry.fi

ISSN 1797-9714 (pdf)
ISBN 978-952-367-286-4 (pdf)

June 2020