MINISTRY OF FINANCE

Digital Security in the Public Sector

Public Sector ICT

Publications of the Ministry of Finance – 2020:45

Publications of the Ministry of Finance 2020:45

Digital Security in the Public Sector

Ministry of Finance, Helsinki 2020

Ministry of Finance

ISBN PDF: 978-952-367-337-3

Layout: Government Administration Department, Publications

Helsinki 2020

Description sheet

Published by	Ministry of Finance		1 June 2020
Authors			
Title of publication	Digital Security in the Public Sector		
Series and publication number	Publications of the Ministry of Finance 2020:45		
Register number	VN/1465/2020	**Subject**	Public Sector ICT
ISBN PDF	978-952-367-337-3	**ISSN (PDF)**	1797-9714
Website address (URN)	http://urn.fi/URN:ISBN:978-952-367-337-3		
Pages	44	**Language**	English
Keywords	public administration ICT, information policy, risk management, cybersecurity, preparedness, information and communications technologies		

Abstract

The Government Resolution on digital security in public sector defines the principles of development 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. Citizens, businesses and communities must be able to rely on ethically sustainable public services that support open and transparent activities and are secure. Finland is known as a leader both in terms of the prerequisites for the digitalisation of society and in providing digital services for citizens and communities. A balanced approach to digitalisation and ensuring the security of digital activities and services is therefore needed.

The Government Resolution and the implementation plan to advance its policies were prepared by an intersectoral coordination group set up by the Ministry of Finance. In line with these, measures are being taken to strengthen coordination and cooperation on the development of digital security and improve economic impact assessment practices. A further objective is to promote the skills of citizens and staff and the security of services. This supports the implementation of the cybersecurity strategy for 2019 in public administration.

Tuija Kuusisto
Senior Ministerial Adviser
Chair of the preparation group

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

Kuvailulehti

Julkaisija	Valtiovarainministeriö		1.6.2020
Tekijät			
Julkaisun nimi	Julkisen hallinnon digitaalinen turvallisuus		
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisuja 2020:45		
Diaari/hankenumero	VN/1465/2020	**Teema**	Julkisen hallinnon ICT
ISBN PDF	978-952-367-337-3	**ISSN PDF**	1797-9714
URN-osoite	http://urn.fi/URN:ISBN:978-952-367-337-3		
Sivumäärä	44	**Kieli**	englanti
Asiasanat	julkisen hallinnon ICT, tietopolitiikka, riskienhallinta, kyberturvallisuus, varautuminen, tieto- ja viestintätekniikka		

Tiivistelmä

Julkisen hallinnon digitaalisen turvallisuuden periaatepäätöksessä 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. Kansalaisten, yritysten ja yhteisöjen tulee voida luottaa eettisesti kestäviin, avointa ja läpinäkyvää toimintaa tukeviin ja turvallisiin julkisen hallinnon palveluihin. Suomi tunnetaan edelläkävijänä sekä yhteiskunnan digitalisoitumisen edellytysten osalta että kansalaisten ja yhteisöjen digitaalisten palveluiden tarjoajana. Digitalisoitumiseen sekä digitaalisen toiminnan ja palveluiden turvaamiseen on siten panostettava tasapainoisesti.

Periaatepäätös ja sen linjauksia edistävä toimeenpanosuunnitelma valmisteltiin valtiovarainministeriön asettamassa poikkihallinnollinesa koordinaatioryhmässä. Digitaalisen turvallisuuden kehittämisen koordinaatiota ja yhteistyötä sekä taloudellisen vaikuttavuuden arviointia vahvistetaan. Kansalaisten ja henkilöstön osaamista sekä palveluiden turvallisuutta edistetään. Tämä tukee kyberturvallisuusstrategian 2019 toteuttamista julkisessa hallinnossa.

Tietohallintoneuvos Tuija Kuusisto
Valmisteluryhmän puheenjohtaja

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

Presentationsblad

Utgivare	Finansministeriet		1.6.2020
Författare			
Publikationens titel	Digital säkerhet inom den offentliga förvaltningen		
Publikationsseriens namn och nummer	Finansministeriets publikationer 2020:45		
Diarie-/ projektnummer	VN/1465/2020	**Tema**	Offentliga förvaltningens ICT
ISBN PDF	978-952-367-337-3	**ISSN PDF**	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-367-337-3		
Sidantal	44	**Språk**	engelska
Nyckelord	offentliga förvaltningens IKT, informationspolitik, riskhantering, cybersäkerhet, beredskap, informations- och kommunikationsteknik		

Referat

I ett principbeslut om digital säkerhet inom den offentliga förvaltningen fastställer statsrådet principer för utvecklingsarbetet och de centrala tjänsterna för att främja säkerhet i en digital miljö. Målet är att inom ramen 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. Medborgare, företag och sammanslutningar ska kunna lita på att den offentliga förvaltningens tjänster är etiskt hållbara, stöder en öppen och transparent verksamhet och är säkra. Finland känt som en föregångare både när det gäller förutsättningarna för digitaliseringen i samhället och som tillhandahållare av digitala tjänster för medborgare och sammanslutningar. Vi måste på ett välbalanserat sätt satsa på digitalisering och på att den digitala verksamheten och tjänsterna är säkra.

Principbeslutet och genomförandeplanen, som ska stödja riktlinjerna i det, bereddes i en förvaltningsövergripande samordningsgrupp tillsatt av finansministeriet. Samordningen och samarbetet för att utveckla den digitala säkerheten och bedömningen av de ekonomiska effekterna ska förbättras. Medborgarnas och personalens kompetens samt tjänsternas säkerhet ska stärkas. Detta arbete stöder genomförandet av strategin för cybersäkerhet (2019) i den offentliga förvaltningen.

Tuija Kuusisto
informationsförvaltningsråd
beredningsgruppens ordförande

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

Contents

Summary

Citizens, enterprises and other entities must be able to have trust and confidence in ethically sustainable public services that support open and transparent activities and are secure. The rapidly evolving digitalisation and the threats related to both the illegal use of information and the influencing by disinformation, as well as the increased national and international mutual dependences set novel requirements for digital security and its steering across the public sector. Therefore, there is a justified need to decide about the digital security policy of the public sector, as well as plan and implement development items that meet the aims set in the policy. The policy gives a more detailed public sector view on Finland's Cyber Security Strategy 2019 as well. It will support the preparation and implementation of the development programme of the strategy.

Digital security aims, within the framework of comprehensive security, to protect citizens, communities and society in the digital environment from risks and threats that may affect personal data and citizens' services, as well as society's and authorities' processes, services and data. The principles for the improving of digital security in the public sector are as follows:

- We lead the security of the digital society jointly based on situation awareness and risk assessments.
- We manage and measure the impacts and costs of digital security in the public sector.
- We improve citizens' and staff understanding about the impacts of digital security risks and responsibilities.
- We improve digital security through public-private-people collaboration.
- We have an influence on EU and international digital security and utilise the outcomes of the collaboration.
- We require technologies and service provision to be secure.

The key digital security services that support authorities' processes and services are: a national and international collaboration model and risk management for digital security in the public sector; shared digital security services for municipalities; digital identity management; competence development for citizens and staff; digital security consultancy services for the public sector; assessment of digital security of services and service provision; digital infrastructure protection; and secure development of autonomous and adaptive systems and services.

Society's functioning and services as well as information sharing are based on mutual trust and confidence in security governance. Security problems in the public sector digital services may erode citizens' as well as business and non-governmental organizations' trust and confidence in the authorities. Society must therefore invest in digitalisation and in the securing of digital activities and services in a balanced way. The objectives of digital security development programs must benefit society, and the benefits must be measurable.

Principles and key services for digital security improvement in the public sector

Citizens, enterprises and non-governmental organizations must be able to have trust and confidence in ethically sustainable public sector services that support open and transparent activities and are secure. According to international digitalisation evaluations, Finland is known as one of the best countries to meet the prerequisites for the digitalisation of society[1] and as a provider of digital services for citizens, business and non-governmental organizations[2]. Finland has been ranked as near to the top countries in global evaluations of cyber security and preparedness[3].

Finland's Cyber Security Strategy 2019 sets out the key national objectives for the improving of the cyber security environment and the securing of society's vital functions in the cyber environment. Security in the digital environment, or digital security, often means the same as cyber security. The digital security framework covers aspects relating to cyber security as well as to risk management, continuity management and preparedness, information security and data protection. Digital security aims, within the framework of comprehensive security, to protect citizens, communities and society in the digital environment from risks and threats that may affect personal data and citizens' services, as well as society's and authorities' processes, services and data. The digital security policies for the public sector support securing the whole of public sector and the functioning of its services without focusing only on the securing of society's vital functions.

The rapidly evolving digitalisation and the threats related to both the illegal use of information and the influencing by disinformation, as well as the increased national

1 EU (2019) The Digital Economy and Society Index (DESI)

2 United Nations (2018) E-Government Survey 2018, Gearing E-Government to Support Transformation Towards Sustainable and Resilient Societies. United Nations, Economic & Social Affairs

3 International Telecommunications Union (2019) Global Cybersecurity Index (GCI); e-Governance Academy (2019) National Cyber Security Index (NCSI)

and international mutual dependences increase society's vulnerability and set novel requirements for digital security and its steering across the public sector.

There is an increasing need for national and international collaboration and understanding as well as for taking security factors into account in the ecosystems formed by the public sector, enterprises, non-governmental organisations and citizens. Therefore, there is a justified need to decide about the digital security policy of the public sector, as well as plan and implement development items that meet the aims set in the policy. This also supports the preparation and implementation of the development programme of the Cyber Security Strategy 2019 and contributes to the implementation of the Government Decision on the Objectives of Security of Supply (1048/2018). At the target level, the functions of the public sector, as well as digital services, information and infrastructure are reliable and the confidentiality, integrity and availability of information are secured. In addition, digital security will enable the innovating and securing of novel services.

Steering, tasks, structures, risks and resources related to digital security were evaluated in an international comparison of Finland. The reference countries were Australia, Estonia, Germany, Israel, the Netherlands, Russia, Sweden and the United Kingdom[4]. These countries have sought to develop their legislation in response to the rapid changes taking place in the digital environment. Digital security governance is being centralised and agencies have been merged into larger entities. According to the recommendations based on the comparison, Finland must assess the governance structures, responsibilities and roles related to digital security and reform them in line with international development. The reference countries commonly recognise the public sector, the business community, universities and research institutions as well as citizens as active digital security actors. All these must play an active role as digital security actors in Finland, too. Improving of digital security competence and skills must be a society-wide strategic priority. The public sector, citizens and communities must be provided with support regarding digital security incidents. Finland must describe the threats related to digital security clearly in a format understood by all actors in society. In the reference countries, the digital infrastructure is considered as part of the service structures and digital security as part of the service delivery. Service providers must meet the digital security requirements and ensure the secure use of services. Finland must systematically require the applying of international digital security standards.

A review of the current state of digital security in Finland's public sector and the international comparison of Finland were applied to form the areas and principles for

4 Digitaalisen turvallisuuden kansainvälinen vertailu (International comparison of digital security), KPMG, February 2020, in Finnish

improving digital security. In addition, they were applied to identify the key digital security services supporting authorities' functions and processes. The tasks advancing digital security services in the public sector are described in the Implementation Plan for Digital Security in the Public Sector 2020–2023. Where necessary, the implementation plan will be updated in response to changes in the environment and the requirements set by the Cyber Security Strategy 2019 development programme.

The improvement areas of digital security in the public sector are: leadership and collaboration; digital society; international collaboration; economy; technology; citizens, staff and competence.

The principles for the improving of digital security in the public sector related to the improvement areas are as follows:

- We lead the security of the digital society jointly based on **situation awareness** and **risk assessments**.
- We manage and measure the impacts and costs of digital security in the public sector.
- We improve citizens' and staff **understanding** about the impacts of digital security risks and responsibilities.
- We improve digital security through public-private-people **collaboration**.

- We have an influence on **EU and international** digital security and utilise the outcomes of the collaboration.
- We require **technologies** and service provision to be secure.

The key **digital security services** to be developed to support authorities' processes and services are as follows:

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.
2. Governance 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
3. Shared digital security services for municipalities
   The roadmap for developing municipalities' digital security will be maintained and its implementation monitored.
4. Digital identity management
5. 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.
   Competence development for citizens and staff
6. Digital security skills and awareness of the public sector staff as well as business and non-governmental organizations' personnel and citizens will be improved.
   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.
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.
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.

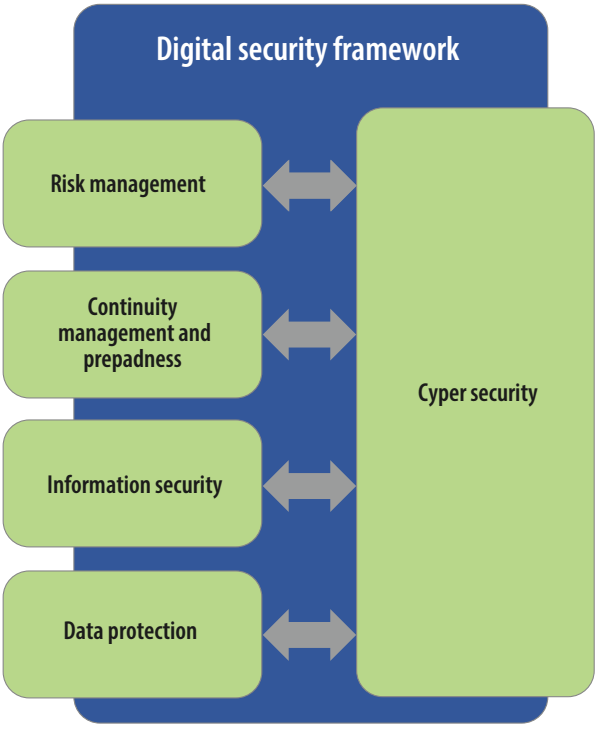
9. Secure development of autonomous and adaptive systems and services in the public sector
   The security of autonomous and adaptive systems as well as digital services will be ensured through risk management.

The change sought through implementing the principles of improving digital security is for the steering, coordination and cooperation of digital security development at the strategic and operational levels to be stronger and to cover the whole of the public sector. This is visual in the launching of new strategic-level digital security steering group for the public sector, in stronger guidance for operational-level development of digital security in the public sector, and in guiding municipalities' digital security through the roadmap.

Development will be enabled through competence-building for citizens and staff as well as through experiments and improved availability of expert services. In addition, the criticality classification and identification of critical development priorities of services, processes, infrastructure and information related to the preparation of security architecture, and the identification of critical development priorities and formulation and assessment of development plans will be conducted. To assess the state of digital security in the public sector, the management of information security assessment will be advanced through improving legislations, and capacity for analyses of the state of digital infrastructure and services in the public sector will be increased. The key actors of the Implementation Plan for Digital Security in The public sector are the Ministry of Finance, the Digital and Population Data Services Agency, the Finnish Transport and Communications Agency Traficom, and the enterprises providing procured services.

Appendix 1. Terms

Digital security The term is often used as a synonym of 'cyber security'. The digital security framework covers aspects relating to cyber security as well as to risk management, continuity management and preparedness, information security and data protection[5]. The term is new and not yet established. There is no international consensus on the term.



Digital security improving is risk management based advancing of the continuity and preparedness of processes as well as improving of information security and data protection. This improves cyber security as well.

Particularly in international contexts, cyber security includes aspects involving broader interests than those typically arising from digital security. Examples of these include cyber diplomacy, cyber operations, cyber resilience and hybrid operations.

5 Glimpses of the future – Data policy, artificial intelligence and robotisation as enablers of wellbeing and economic success in Finland, Publications of the Ministry of Finance – 2019:39, in Finnish

The OECD uses the term 'digital security'[6] as it is more consistent than 'cyber security' with the terms 'digitalisation', 'digital transformation' and 'digital economy'. Digital security and cyber security both also affect security in the physical world in the same way as digital security is affected through the physical world.

Cyber security A desired state where there is trust and confidence in the cyber environment and where its functioning is safeguarded. Cyber security means the security of a digital and networked society or organisation and its impacts on their functions.[7] The term 'digital environment' can be used synonymously with 'cyber environment'.

Information security
Arrangements to ensure the confidentiality, integrity and availability of information[8].

Data protection Protection of people's privacy and information relating to an individual against unlawful use when processing personal data[9].

Risk management
Systematic activity including risk analysis and the planning, implementation and monitoring of measures required, and corrective measures[10].

Residual risk The risk remaining after risk treatment, the removal of which is not possible or desirable. Residual risks may include unidentified risks.[11]

Continuity management
An organisational process employed to identify potential threats to operations and evaluate their impacts on the organisation and its network of actors as well as to create a policy for incident management and operational continuity in all circumstances[12].

Preparedness Activities for ensuring as incident-free performance of duties as possible, and any possibly needed measures deviating from the ordinary in incidents and emergency conditions[13].

---

6 Digital Security Risk Management for Economic and Social Prosperity, OECD Recommendation and Companion Document, 2015

7 Finnish Terminology Centre TSK TEPA term bank, Vocabulary of Cyber Security (TSK 52, 2018), in Finnish

8 Finnish Terminology Centre TSK TEPA term bank, Vocabulary of Cyber Security (TSK 52, 2018), in Finnish

9 Finnish Terminology Centre TSK TEPA term bank, Helsinki Term Bank for the Arts and Sciences, 6 August 2019, in Finnish

10 Finnish Terminology Centre TSK TEPA term bank, Vocabulary of Comprehensive Security (TSK 50, 2017), in Finnish

11 Ministry of Finance, Risk management guideline, Publications of the Ministry of Finance 22/2017, Appendix, in Finnish

12 Finnish Terminology Centre TSK TEPA term bank, Vocabulary of Cyber Security (TSK 52, 2018), in Finnish

13 Finnish Terminology Centre TSK TEPA term bank, Vocabulary of Comprehensive Security (TSK 50, 2017), in Finnish

Appendix 2. Current state of digital security

In accordance with the Programme of Prime Minister Sanna Marin's Government, strategic-level management in government will be made more effective and measures outlined concerning information, information networks and information systems critical for securing the functioning of society in a digital environment. The most recent government resolution on the development of information security in central government is from 2009. Since then, there have been significant changes in both the structures and functioning of the public sector and in strategies, statutes and guidelines, and threats faced by the digital environment have increased. Key changes include the increased cooperation and interdependencies between the various actors in society, more specific regulation of the information and communication technology sector, with the latest addition being the Act on Information Management in The Public Sector (906/2019), and the Security Strategy for Society from 2017, the Cyber Security Strategy from 2019, and centralised ICT service provision in municipalities, joint municipal authorities and central government. The Government ICT Centre Valtori was established in 2014 and the Digital and Population Data Services Agency in 2020.

The Finnish Cyber Security Strategy 2019 sets out the key national objectives for the development of the cyber environment and the safeguarding of related vital functions. It is based on the general principles outlined in Finland's Cyber Security Strategy of 2013. The three strategic guidelines are international cooperation, better coordination of cyber security management, planning and preparedness, and development of cyber security competence. Resource targeting and cooperation relating to cyber security will be improved by a National Cyber Security Development Programme extending beyond government terms. The programme aims to concretise national cyber security policies and clarify the overall picture of cyber security projects, research and development programmes. The post of National Cyber Security Director has been established at the Ministry of Transport and Communications to coordinate the national development of cyber security.

Due to changes having taken place in society and to further specify Finland's Cyber Security Strategy 2019 concerning the public sector, there is a need to assess the current state of digital security in the public sector and, on the basis of the assessment, outline the policies for the development of digital security in the public sector. The policies for digital security in the public sector seek to safeguard the functioning of the whole of the public sector and its services without this being limited to merely safeguarding the vital functions of society.

Digital society

In recent years, the digital environment and its impacts on the functioning of society and the public sector have changed significantly. With advancements made in digitalisation, information is now utilised more and more broadly and the efficiency of its use has improved thanks to new technologies such as robotic process automation and artificial intelligence. The plan is to provide citizens with people-oriented services based on life events and entities with services based on business events.

Finland has been ranked close to the top in global assessments of cybersecurity and preparedness[14]. There have been no major information leakages in Finland. The development of digital security in the public sector takes place in a decentralised manner across the various administrative organisations. In most cases, the organisations' internal responsibilities concerning digital security are clear. However, the operational management of cyber security breaches has not been determined and the formulation of the operational cyber security picture should be improved[15]. The set of digital security policies applying to the entire society is not yet complete and the division of responsibilities needs clarification in places. Shared risk management methods are not used comprehensively to support decision-making.

The key national and international digital security actors comprise the ministries, the authorities and cooperation bodies addressing digital security matters, and the public and private digital security service providers[16] (Appendix 4). The advancement of digital security through **cooperation between central government, municipalities, the private sector, non-governmental organisations and citizens** still needs to be developed further from the current situation.

International activities

Digital security and cyber security issues are increasingly issues of international policy characterised by political differences. In recent years, the international community has seen the emergence of the need to **strengthen cooperation** in security aspects relating to the digital environment. In the EU, a permanent Horizontal Working Party on Cyber Issues of the Council has been established and several other working parties within the Council deal with cyber security issues from the perspective of their mandate. The field of activity is not static. Instead, changes brought about by new technologies and artificial

14 International Telecommunications Union (2019) Global Cybersecurity Index (GCI); e-Governance Academy (2019) National Cyber Security Index (NCSI)

15 National Audit Office of Finland, Cyber protection arrangements, Audit report 16/2017, in Finnish

16 Lehto, Limnéll, Kokkomäki, Pöyhönen, Salminen. Strategic management of cyber security in Finland (abstract in English). Publications of the Government's analysis, assessment and research activities 28/2018, in Finnish

intelligence are reflected in the debate on international rules of play. Finland participates in international cyber security cooperation with a view to strengthening the rules-based international order and promoting democracy, freedom of speech and rule of law.

Management and cooperation

Cooperation within the public sector as well as between the public sector and private entities in the field of digital security is at a very good level in Finland. The public sector faces a **management** challenge of how to confidently promote the introduction of new digital services while at the same time responsibly assessing the related risks and dealing with any residual risks. The state of digital security in the public sector is not currently being assessed comprehensively. There are no clear principles concerning which digital services and digital security services should be implemented jointly.

Technical problems and incidents, natural phenomena and different types of influencing require continuous and, for critical functions, centrally steered work to enhance operational reliability. The outcomes of current sector-specific development of the public sector have not been sufficient. The development of information resources, information networks and services critical to the functioning of society has not been steered or provided with resources on a centralised basis and, the desired state for the development work has not been clearly specified.[17]

Authorities and entities do not have sufficient access to flexible and continually developed **capacities for cooperation and operating models** required in the rapidly changing operating environment. These include shared concepts and operating principles, criticality classification of information, digital service management, and responsibility and dependency descriptions.

The public sector does not have an organisation arranging **technical audits** of information security that, for example, could be responsible for continuous scanning of known vulnerabilities. Ensuring the operational capacities of all key industries also in the event of information security breaches and cyber incidents is vital for the continuity of society's functioning but currently not fully sufficient.

17 A Self-Renewing, Resilient and Sustainable Society. Contribution by the officials of the Ministry of Finance. Publications of the Ministry of Finance 2019:12, in Finnish

Citizens, staff and competence

The role of citizens and residents as providers of digital security is thinly identified and defined. Instead of customer orientation, the emphasis in digital security is often on technology solutions. Ways of reconciling the sometimes conflicting objectives of security and privacy protection are still being sought in implementation.

Competence sourcing and maintenance are major challenges in Finland, too. There are not enough people with special expertise in digital security, and recruitment is difficult for the public sector and private service providers alike. When services are outsourced, the organisations' own competence development is transferred to service providers, which undermines the development of deep competence and tacit knowledge within the organisation. There is training material available for digital security competence development among the public sector staff, but the level of systematic competence development varies.

Economy

There is no commonly used **investment cost/benefit model** determined for digital security in the public sector, and the economic impacts of digital security are not known precisely. This is partly due to it being difficult to identify the exact proportion of digital security development in the development of information and communication technology infrastructure and services. Consequently, it is difficult to estimate the current sufficiency of financial resources allocated to the development of digital security. However, information security incidents caused by insufficient resources in most cases generate multiple costs compared with being able to prevent risks in advance or counter them effectively. The costs of the loss of operational continuity of and trust and confidence in administration are difficult to measure in money terms.

The spread of digitalisation and the centralisation of ICT service provision have created cost savings and developed customer services, but at the same time new vulnerabilities have emerged in service continuity as well as the reliability, availability and integrity of information. The diversity of attackers is increasing, and attacks are becoming increasingly advanced technologically, which may have a serious adverse effect on organisations' capability to respond efficiently to growing external threats. In the digitalisation of services, the role of cost savings has gained further significance as activities are changing. **Risk management** has not been used sufficiently in **impact assessments** concerning digital security or in seeking a balance between cost savings and services and improvements in service security.

Technologies

Developing monitoring capabilities, system **surveillance** and vulnerability management, and implementing joint development between the public sector and enterprises on the basis of observations made in monitoring increase the need for resources. They also create the requirement to allocate staff working hours increasingly to digital security tasks. **Proactive information security** and **automation** of routine tasks are not utilised extensively to reduce the need for labour input.

Cloud services are an opportunity as well as a threat from the digital security perspective. The use of cloud services may increase the operational reliability of some services of the public sector. Cloud service use may also efficiently prevent impacts of denial of service attacks. There is a lack of policies on the information-secure use of cloud services and management of operational continuity, which makes it difficult to utilise the services in the public sector. Digitalisation is continuously increasing the demand for open and structured information, and this development is not supported by local and closed information systems. There is insufficient access to information-secure information processing environments, such as secure public and private cloud services or local solutions where data, algorithms and refined data can be placed. Differences in legislation between countries often pose a challenge concerning cloud services. This creates risks and uncertainties for service users if a service is provided outside Finland in compliance with that country's legislation.

Artificial intelligence (AI) and quantum technology are new technologies not used very extensively at the moment. Debate is taking place in conjunction with AI development as to how the data used when teaching systems affects AI functioning and what kinds of ethical principles should be taken into account. It is difficult to estimate the speed of development in **quantum technology** and the realisation of risks involved in its use in contexts such as the decryption of encryption algorithms.

Threat assessments

In 2019, the Public Sector Digital Security Management Board VAHTI published a report on security in the digital environment. According to the report, the key changes that have taken place in security challenges show that the activities of organisations are currently affected most by various incidents – minor ones and those with extensive impacts alike – relating to **ICT service provision**. In such situations, service functioning is typically prevented, which at the same time impacts the availability of services and the information processed in them. Consequently, disruptions in service provision are often also digital security incidents.

Efforts have been made to ensure security in shared, **centralised digital services** and related service provision through legislation. It is not possible to achieve fully watertight digital security, which highlights the significance of risk management as part of the management of the activities. The operating models of organisations for digital security are challenged by the pursuit of continuous round-the-clock service provision, which would call for the harmonisation of cultures and the clarification of approaches such as incident management. Private individuals and entities also often expect 24/7 operational reliability from digital services, but there is no centralised and continuous security operations centre (SOC) or service management system required for this in Finland's central government.

Ensuring the security of ICT services provided by external **service providers** is challenging for organisations. Efforts are made to manage this challenge through agreements, but the problem lies in including the necessary terms and conditions in agreements concluded with multinational providers. Challenges faced by **production chains** both outside and within the public sector include risk levels, information security, competences and production capacity. In shared systems, the threats are shared but there are differences in substance and risk profiles. In municipalities and joint municipal authorities, digital security operating models have not been improved sufficiently with ICT providers identified as playing a key role.

Repeated successful information security breaches affecting the public sector organisations and incidents where personal devices of private individuals have been harnessed to carry out these breaches show that the minimum requirements set for digital safety are not fully met in all respects. In addition to data trespasses, difficulties in user identification or use of **identity management** erode confidence in the public sector's digital services and jeopardise the security and privacy of users. The public sector must not pass its risks on for service users to manage, and security requirements must not prevent the intention of service users to be realised[18].

The built-in information security of various **internet of things (IoT) devices** is often weak as cost minimisation is sought in their manufacture. Such devices are, however, increasingly connected to industrial and other automation solutions. The National Cyber Security Centre's Cybersecurity label, which shows that a device complies with at least the basic requirements for informational security, is a significant improvement in this respect.

18 One of the challenges from the service user perspective is access-related incidents in situations that require users to comply with specific time limits. For example, submitting income information, changing one's tax withholding rate or registering with an employment office by the deadline set may turn out to be challenging if the digital service provided for the purpose is not available due to a technical or other incident. Clear policies are needed on how customers are to be provided with guidelines for any persistent incidents.

Old basic information systems often have insufficient **architecture** and their technological solutions fail to meet current requirements. In the purchaser-provider model, problems are difficult to pinpoint due to challenges often emerging in the management and oversight of the whole process. International standards are not always utilised sufficiently when developing the components of digital security. For example, there are not sufficient policies on the objective to utilise certifications and certified products when putting procurements to tender. The international compatibility of Finnish frameworks is not ensured in contexts such as the criteria for information security requirements/audits formulated in Finland.

When developing new innovations and technology solutions, responsibility and the creation of ethical rules are often not taken sufficiently into account. Secure operating models have not always been integrated into DevOps processes combining software development, testing and maintenance release automation.

Summary and conclusions

Society must decide what the delivery of security means in the digital environment. Which aspects of digital **security** management are the responsibility of private individuals, which are the responsibility of entities such as commercial providers of technical infrastructure or services, and which are the responsibility of municipalities and joint municipal authorities or central government authorities? The responsibilities should be clear and understood in the same way by all actors.

The phenomena and features of the digital environment differ from those of the physical operating environment. **Duties and responsibilities** should therefore be made clearer to better reflect the rapid change in the operating environment caused by digitalisation. Citizens, enterprises and various other entities must be able to connect securely to the ordinary digital services provided by the public sector. The various parties must also be able to have trust and confidence in the functioning of services and ultimately in assistance being provided by the authorities in case of incidents. In the same way, municipal actors must be able to rely upon central government actors in the event of large-scale incidents.

The focus in the public debate on the security of the digital environment and on ways to combat threats occurring in it has been on operational-level development so that the threats and incidents that have already been identified can be managed. There has been a particular emphasis on the development of monitoring and incident management capabilities as well as on data protection and information security aspects. Research and guidance of administration must be targeted more strongly at issues that are **strategically** most effective over the long term. Policies guiding development are needed

concerning the utilisation of new service solutions, cooperation between administration and enterprises, and international cooperation. The policies must provide clearer guidance on to what extent the services are provided and the infrastructure built through national measures and resources, to what extent the work is based on EU-wide or other international cooperation and (especially in the public sector) to what extent new service models and technological opportunities could and should be used in the provision of public digital services.[19]

Measuring the productivity of investments is necessary to be able to allocate limited resources as efficiently as possible. The objectives of digital security development projects must benefit society and the benefits must be measurable. Both measurement results and risk analyses must be applied when planning future investment programmes.

Security of supply in telecommunications and electricity supply are basic prerequisites for the digital environment. Information network security and the supply security of electricity are currently at a good level in Finland. The development of the digital environment calls for continuous improvement of security, management and control by telecommunications operators and power grid operators. **Citizens** must have access to a secure digital environment where security equals their experience of the safety and security of the physical operating environment. Among other things, this means attacks being guarded against already in the information network, malware being filtered, and denial of service attacks being prevented. The powers of the authorities as well as the division of supervision-related responsibilities and obligations in relation to digital infrastructure service providers must be evaluated.

Digitalisation aims for the essential development of operational processes and, in the same way, the approach to our digital future must be **innovative**, creative thinking. Digitalisation does not as such change the principles of security, but old security measures may tend to be discarded if they are regarded as features restricting activities. Security objectives must, however, be achieved in the new operating model too, regardless of any changes in implementation.

19 A Self-Renewing, Resilient and Sustainable Society. Contribution by the officials of the Ministry of Finance. Publications of the Ministry of Finance 2019:12, in Finnish

Appendix 3. International comparison of digital security

An international comparison of digital security examined the steering, duties, structures, risks and resources of digital security in eight reference countries[20]: Australia, Estonia, Germany, Israel, the Netherlands, Russia, Sweden and the United Kingdom. Comparative information was collected from the reference countries' public documents through information searches on legislation, strategic policies, organisation of activities, and resources.

There are disparities in the digital security **terminology** used in the reference countries. The concepts of 'digital security', 'cyber security' and 'information security' are not fully established in Finland, either, and the differences between the concepts appear in part to be artificial. In this comparison, 'digital security' consists of issues falling under information security, cyber security, operational continuity and preparedness, risk management and data protection. The background material used in the comparison was collected from each reference country for all of the components whenever such material was available. The differences between the concepts and definitions can also be seen in the report's background material: the reference countries' digital security was mainly addressed in a cyber security strategy. In Sweden, the policies are stated in the National Cyber Security Strategy as well as in the Digital Strategy. In the Netherlands, there is a separate Dutch Digitalisation Strategy in addition to the Dutch National Cyber Security Strategy. Germany and the United Kingdom both also have a separate government digitalisation strategy. Whenever available, national risk assessments and documents relating to the protection of critical infrastructure, data protection and other digital security were also used as background material in the comparison.

There is variation in **legislation** concerning digital security, but practices are harmonised by the EU's General Data Protection Regulation (GDPR) and the Network and Information Security (NIS) Directive. The new Regulation (EU) on ENISA, the EU Cybersecurity Agency, repealing Regulation (EU) 526/2013 and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") strengthens ENISA's coordinator and advisory role in cyber security and sets up a certification system for processes, services and products. Israel requires the personal **certification** of those who work in cyber defence, penetration testing, security breach investigations, cyber security methodologies or cyber security technologies. In the United Kingdom, a Cyber Essentials certificate can be obtained not only by enterprises and professionals but also by by private individuals. The

20 Digitaalisen turvallisuuden kansainvälinen vertailu (International comparison of digital security), KPMG, February 2020, in Finnish

Finnish Cybersecurity label is an example of a model for product and service certification than could be implemented EU-wide.

The **digital infrastructure** is not addressed in the reference countries as a separate entity. Instead, the digital infrastructure is seen as being included in the structures, functions, services and products of the physical world and, corresponding, its safeguarding is regarded as part of general preparedness and continuity management. Energy supply and the functioning of telecommunications are regarded as key prerequisites for the digitalising society.

The trend in digital security guidance appears to be towards **centralised models** where a competent authority placed under a single ministry steers and coordinates but also provides guidelines and training as well as supervision and response. In a strongly decentralised model, communication between actors and issues related to powers may pose a challenge. In EU Member States, there is a data protection authority under the GDPR responsible data protection, but there are major differences in the authority's resourcing: the Office of the Data Protection Ombudsman in Finland has a permanent staff of three, while the staff number of the authority in Estonia is 19, in Sweden 75 and in the German Federal Government 190. Israel and Australia also have a data protection authority whose duties are similar to those of the authorities of the EU Member States.

The digital security risks of the reference countries are addressed in national risk assessments or cyber security strategies. Almost without any exceptions, these identify **hostile influencing** by foreign states or groups supported by them as a strategic risk. Cyberattacks are regarded as significant threats for reasons including that they are regarded as being able to undermine the stability of society through, for example, hybrid operations or fake news. Technology required for attacks is also easily available and the risk of getting caught is low. To improve security in the digital environment, concrete measures covering the various spheres of society are required, with their implementation monitored regularly on the basis of a guideline such as the United Kingdom's National Cyber Security Strategy.

The reference countries commonly recognise the public sector, the business community, universities and research institutions as well as citizens as active national digital security actors. **Cooperation** of all actors provides a more comprehensive digital security situational picture. The development of new digital products and services generates growth in the entire cyber industry and offers new export opportunities. Israel and the Netherlands are examples of countries seeking economic benefits by developing the industry and related research.

Unlike the reference countries, Finland has not specified the role and responsibilities of **citizens** as active contributors to security in society. The reference countries have set society-wide competence development as a strategic priority and developing digital security skills and competences as a key strategic objective.

Changes in the rapidly evolving digital environment require rapid and internationally efficient **monitoring and response capacity**. The cyber environment and threats against it, such as cyber espionage, cyberterrorism or other cybercrime, do not respect national borders. This is why new kinds of special competences, exchange of information and cooperation between security authorities are necessary both nationally and internationally.

Conclusions from the international comparison

The digital infrastructure must be **part of service structures** and digital security must be part of the service entity. Service providers must respond to digital security requirements and ensure the secure use of services. Finland must systematically require the application of international digital security **standards** and criteria. National requirements set for the components of digital security must be used to supplement international standards, not to replace them.

The significance of digital security has been recognised broadly, and many countries (including Sweden, the Netherlands, Germany and Estonia) have sought to develop **legislation** to reflect the rapid changes in the digital environment. As noted above, society's digitalisation is usually typically addressed under national cyber security strategies. In Germany, data protection in government systems and networks is governed directly by the constitution. As the digital environment transcends national borders, legislation relating to digital security must be international, which requires Finland's active participation in the drafting of EU legislation: the need for regulation in society must be monitored and there must be speedy response to any need for amendments. For example, Finland must be involved in the formulation of ethical principles and practical control guidelines for learning systems and take these into use.

In the reference countries, digital security management is **centralised**, and agencies are merged to form larger entities, with Sweden currently preparing to establish a new, centralised cyber safety authority. International cooperation calls for clear responsibilities and roles. Finland should assess the **management structures, responsibilities and roles** relating to digital security and reform them in line with international development. Coordination and implementation responsibilities can be divided into smaller components, but the responsibility areas must be specified clearly to ensure well-functioning national and international cooperation. Power division issues must not

hamper the work to develop digital security. Finland must increase cooperation between all digital security actors to ensure a secure digital society.

It is not possible to evaluate the reference countries' investments in digital security on the basis of the information collected. The objectives of development projects concerning the digital environment must benefit society and the benefits must be measurable. Measurement results and risk analyses should be applied when planning future investment programmes. Minimum digital security requirements must be set for technologies used in society's services, and compliance with them must be monitored. Minimum requirements for the staff's digital security competences must be specified for the most critical tasks as regards security.

Competence development relating to digital security is included in the strategy of almost all of the reference countries. Authorities of reference countries (such as the Swedish Civil Contingencies Agency, the United Kingdom's National Cyber Security Centre and the Dutch Data Protection Agency) each provide the public sector, businesses and private individuals with guidelines and training. All of the actors in the Finnish society – the public sector, businesses, universities and research institutions as well as citizens – must play an active role as creators of digital security. Development of digital security skills should be a society-wide strategic priority. For example, shortages in citizens' security skills and solutions in the digital environment expose digital service provision broadly to attacks. Sweden, the Netherlands and Estonia aim to increase digital skills (including media literacy and cyber security) starting from primary and secondary education to strengthen the capacities of pupils and students. Israel has already progressed further in implementation and has included cyber security also in training provided during military service. In the United Kingdom, there are various cyber security courses aimed at teenagers that aim at not only increasing their capacities but also at attracting young people to careers in cyber security.

The threat analyses of the reference countries are, as a rule, similar to each other, but the big picture is not particularly clear in any of the countries examined. Finland must describe the **threats** related to digital security clearly in a format understood by all actors in society. Strategic policies to reduce the impacts of threats must be spelled out in the action plan as concrete operational tasks. Close cooperation between the authorities and businesses is emphasised in almost all of the reference countries. Administration, citizens and entities should be **provided with support** in identified digital security incidents. For example, the United Kingdom has established a unit specialised in cybercrime in all local police departments.

Appendix 4. Digital security actors and duties in the public sector

The public sector is highly digitalised in Finland, so all the public sector actors need digital security. Currently, the following are the key digital security actors in the public sector:

Parliament of Finland

The duty of the Parliamentary Office is to establish the necessary conditions for Parliament to carry out the duties belonging to it as a state organ. Services provided by the Office also support legislative work, decision-making and international cooperation relating to digital security. Parliament promotes openness, access to information and democracy.

Parliament's digital security objective is to safeguard the continuity of Parliament's activities and to prevent external interference. As Parliament is the highest state organ, the continuity of its activities must be ensured in all circumstances. The reliability and timeliness of communications are an important part of digital security delivery in Parliament.

National Audit Office of Finland

The National Audit Office of Finland (NAOF) audits central government finances and management of assets, evaluates fiscal policy and monitors political party and election campaign funding. By conducting audits, the NAOF ensures that state funds are used in accordance with Parliament's decisions and the law and in a reasonable manner and oversees that the fiscal policy is on a sustainable basis. The NAOF contributes to ensuring that the principles of the rule of law, democracy and sustainable economy are also adhered to in the management of the finances of the European Union as well as in other forms of international cooperation.

From the digital security perspective, reasonable use of funds means that the services of digitally operating administration are easily available, easy and safe to use and, in addition, provided in an economically sustainable manner. This means also ensuring the continuity of the services. The NAOF aims to reinforce trust and confidence in a high level of openness, performance and sustainability in Finnish central government, including in the digital environment.

Social Insurance Institution of Finland (Kela)

The Social Insurance Institution of Finland (Kela) is an independent institution under public law whose administration and operations are supervised by Parliamentary Trustees nominated by Parliament. Kela provides social security coverage for Finnish residents and for many Finns living abroad through the different stages in their lives. In addition to its independent status, Kela is a significant provider of national information system services. Kela IT Services employ more than 700 IT professionals, such as application designers, security architects, and network and server specialists. The information and cyber security of the information systems provided by Kela is highly important to safeguard the data content of national information systems and access to services provided by Kela. In the desired state, the operational continuity of national information system services provided by Kela is safeguarded in all circumstances.

Bank of Finland

The Bank of Finland is responsible for the introduction and general oversight of principles supporting the cyber security of financial sector infrastructures that are critical for society, such as payment and settlement systems.

Finnish Financial Supervisory Authority (FIN-FSA)

The Finnish Financial Supervisory Authority (FIN-FSA) plays a key role as a supervisor of digital security in the financial sector. FIN-FSA is responsible for supervising and auditing the operational risks, cyber security and payment systems of the entities it supervises. In addition, FIN-FSA issues regulations and guidelines on related matters. FIN-FSA also participates in emergency supply work as a member of pools operating under the Finance Sector. In addition, FIN-FSA has a strong role in the creation of the digital security and cyber security situational picture of the finance sector for normal as well as emergency conditions by monitoring incident reports submitted by its supervised entities.

Prime Minister's Office

The Prime Minister's Office is responsible for the monitoring of the implementation of the Government Programme and assists the Prime Minister in the general management of Government functions. The Prime Minister’s Office safeguards the operational capacities of the Prime Minister and Government in all circumstances. The responsibilities of the Prime Minister’s Office include Government-wide situation awareness, preparedness and security services, general coordination of incident management and the shared information management and document management of the Government and its ministries.

Suomen Erillisverkot Oy

Suomen Erillisverkot Oy is a special-purpose company wholly owned by the State of Finland. It secures the critical leadership and information society services in all circumstances. The company provides secure and reliable ICT services for public authorities and other critical operators of national security. The company develops overall security and safety in society and its operations affect nearly everyone in Finland.

Ministry for Foreign Affairs

The cyber environment and cyber security have become an important aspect of Finland's foreign and security policy. Cyber threats do not respect national borders. The strengthening of cyber security calls for deeper international cooperation. The Ministry for Foreign Affairs coordinates this international activity. The Ministry also serves as the National Security Authority (NSA) in Finland. Under the Act on International Information Security Obligations (588/2004), the NSA is responsible for steering and monitoring activities to ensure that international classified information sent to Finland is protected and processed appropriately. The NSA steers national activities and is responsible for duties including the preparation of international information security agreements.

Office of the Data Protection Ombudsman

The Data Protection Ombudsman is a national supervisory authority that supervises compliance with data protection legislation. The Data Protection Ombudsman and Deputy Data Protection Ombudsmen are autonomous and independent in their roles. It is the duty of the Data Protection Ombudsman to promote the realisation of data-related and other fundamental rights in the processing of personal data and building trust and confidence. For example, the Ombudsman reviews reports on personal data breaches, accredits certification bodies and conducts information system inspections. If necessary, the Ombudsman may impose administrative sanctions and exercise its other powers. The Data Protection Ombudsman represents Finland on the European Data Protection Board.

Ministry of the Interior

The Ministry of the Interior prepares legislation concerning the police, rescue services, emergency response centre operations, border management, maritime search and rescue and migration.

Police

The duty of the police is to prevent and investigate crimes and submit cases to prosecutors for the consideration of charges. Cybercrimes are investigated by police departments in accordance with the territorial principle.

Finnish Security and Intelligence Service (Supo)

The duties of the Finnish Security Intelligence Service (Supo) include preventing and countering the most serious threats to national security, such as terrorism and unlawful intelligence by foreign states targeted at Finland. Supo performs these duties also in the digital environment. In addition, Supo provides proactive and analysed intelligence concerning phenomena posing a threat to national security to substantiate policymaking by the state leadership and other authorities.

National Bureau of Investigation, Cybercrime Centre

The main anti-cybercrime duties of the Cybercrime Centre operating under the National Bureau of Investigation are investigating the most serious cybercrimes, maintaining situation awareness concerning cybercrime, intelligence gathering on the internet and information networks, and expert services relating to pre-trial investigations for the police and other authorities.

Ministry of Defence

As a Government ministry and a leading authority in the area of national defence, the Ministry of Defence is in charge of the national defence policy and national security as well as international cooperation in defence policy matters. The Ministry of Defence is in charge of resources for military defence and operational preconditions of the Finnish Defence Forces. To ensure national interests, the Ministry bears the responsibility for taking part in international crisis management and European security structures. The Ministry is also responsible for coordinating the comprehensive defence approach and the will to defend the country. On request, it provides executive assistance to other authorities.

Security Committee

The Security Committee assists the Government and ministries in broad matters pertaining to comprehensive security. The Committee monitors the development of Finnish society and its security environment and coordinates proactive preparedness related to comprehensive security. Finland's Cyber Security Strategy 2019 is based on the general principles of Finland’s Cyber Security Strategy 2013. As outlined in the 2013 strategy, the Security Committee monitors and coordinates the implementation of the strategy. The

goals of cyber security coordination include avoiding unnecessary duplication, identifying possible shortcomings and determining the competent entities. The competent authorities will make the actual decisions in accordance with the relevant provisions.

Finnish Defence Forces

The Finnish Defence Forces are creating a comprehensive cyber defence capability for their statutory duties as part of measures to safeguard society's vital functions. 'Military cyber defence' means intelligence as well as cyberattack and cyber defence capabilities. Military cyber defence capabilities provide intelligence information to support decisions by the state leadership and the leadership of the Defence Forces and support the operations of the Defence Forces by safeguarding the capacities for its own decision-making.

Cyber threats have become more dangerous to society in terms of their impacts. Cyberattacks can be used as tools in political and economic pressure and, in a serious crisis, pressure can be exerted as an instrument of influence alongside traditional means of military force. The defence system is dependent on the availability of the cyber environment and the environment should also be regarded as an opportunity and a resource from the perspective of military activity.

Ministry of Finance

As one of the ministries of the Finnish Government, the Ministry of Finance is responsible for economic policy that strengthens the preconditions of stable and sustainable growth, good management of central government finances, operational capacities for sustainable local government finances, and efficient public sector. The Ministry of Finance is responsible for the general principles of information policy, information management and e-services in the public sector. The Ministry of Finance prepares the general principles and requirements for digital security of the authorities ICT infrastructure, digital services and information. It prepares and directs the implementation of digital security policies, provisions and development programmes, and sets up the necessary governance groups and collaboration networks. The Ministry of Finance has set up a strategic management group for digital security in the public sector for the balanced improving of digitalisation and digital security.

Government Financial Controller's Function

The duties of the Government Financial Controller's Function include monitoring, assessing and developing internal control and the related risk management concerning central government finances. The function may submit reports on its observations to the Government and the Ministry of Finance as well as central government agencies,

institutions, unincorporated state enterprises and funds and, in that context, provide its possible proposals for measures to be taken.

The Government Financial Controller's Function heads the Advisory Council on Internal Control and Risk Management, which is appointed by the Government and which monitors and assesses internal control and risk assessment methods and general development, the functioning of internal control and utilisation of procedures in steering and management of finances and activities, and makes proposals for the development of internal control and related risk management.

Information Management Board

One of the duties of the Information Management Board is to promote the implementation of information management and information security procedures and ensure that associated requirements are met. The Board may appoint temporary divisions, publish recommendations and organise seminars and other events.

Digital and Population Data Services Agency

The Digital and Population Data Services Agency promotes the digitalisation of society, safeguards the availability of information, and provides services related to customers' life events. The Agency is responsible for many sets of services whose incident-free, secure and smooth functioning is important for society's functioning. High-quality population data, certification services and support services for electronic transactions in turn create capacities on the basis of which digitalisation can be built. The Agency is tasked with ensuring the reliability and security of these services. The Agency is responsible for digital security consultancy services and prepares recommendations and guidelines. The Agency is also responsible for the activities of the Public Sector Digital Security Management Board (VAHTI). The Agency has set up a development programme for digital security in the public sector for 2019–2021.

Government ICT Centre Valtori

The Government ICT Centre Valtori provides sector-independent ICT services for central government as well as information and data communications technology services and integration services that comply with the criteria for high preparedness and security. Valtori is tasked with ensuring that the information security and cyber security as well as continuity and preparedness management of the services it is responsible for meet the requirements set in a rapidly changing operating environment. For the requirements to be met, Valtori creates and further develops a comprehensive situational picture and monitoring capability for cyber security. These enable rapid response to information

security incidents and disruptions. Monitoring capability is implemented in cooperation with authorities under the Cyber Security Operations Centre (CSOC) covering both of Valtori's business environments. Further regarding information and digital security, there is a fixed-format information security management model in use to ensure shared operational processes and enable business-centred risk and incident management.

Ministry of Education and Culture

The Ministry of Education and Culture is responsible for development of education, science, cultural, sport and youth policies, and for international cooperation in these fields. The Ministry's duties relating to digital security include maintaining the education, training and research system as well as competences, safeguarding the prerequisites for the maintenance of library and other cultural services, and the protection of cultural assets.

The Ministry steers many digital services and registers relating to education. The Ministry's branch is responsible for ensuring sufficient access to skilled labour and the development of citizens' skills and competences required in digital environments, such as the development of media literacy skills at all levels of education. Competence development strengthens citizen's trust and confidence as well as inclusion in a digitalising society. Actors in the sector of the Ministry of Education and Culture are also responsible for the development of special competences and research relating to digital security. In addition, the duties of the Ministry's administrative branch include maintaining on a long-term basis or permanently and in an intelligible form the digital datasets created in central government and the key cultural heritage that is in a digital format. The Ministry steers other the public sector actors in the matter.

Ministry of Transport and Communications

The Ministry of Transport and Communications is responsible for the development of the information security of electronic communications services and networks. This means, for example, the development of regulation concerning information security in electronic communications services or electronic communications networks, strategy work or other general steering. The Finnish Transport and Communications Agency Traficom, established in 2019, operates under the Ministry. The internationally recognised National Cyber Security Centre operates as part of Traficom.

Finnish Transport and Communications Agency Traficom, National Cyber Security Centre

The National Cyber Security Centre of the Finnish Transport and Communications Agency Traficom plays a key role in the preparedness of the digital society. Through its activities, the Agency ensures society's functioning in case of incidents during normal

conditions as well as during emergency conditions by, for example, ensuring the functioning and information security of public communications networks and services and other communications networks and services connected to them, as well as access to frequencies and cryptographic material for purposes such as the needs of security authorities. In addition, the Agency is responsible for Finland's national top-level domain .fi and maintains the fi root name servers and supervises domain name brokers.

The Agency promotes confidentiality in communications and statutorily supervises the protection of privacy in telecommunications. The Computer Emergency Response Team (CERT) of the National Cyber Security Centre of the Agency attends to the Agency's security breach prevention, investigation and information duties as well as the maintenance and sharing of the cyber security situation awareness. CERT produces and maintains the cyber security situational picture together with trusted Finnish and foreign cooperation partners and counterparts. The National Cyber Security Centre's CERT is a known and trusted partner in several international networks built over the 19 years since the establishment of CERT.

Ministry of Social Affairs and Health

The Ministry of Social Affairs and Health steers several duties that are significant for society. Among the Ministry's areas of expertise, income security is responsible for all social allowances as well as systems including insurance and pensions, while social and health services are responsible for social welfare and healthcare services, with environmental health care also included in their scope. Alongside its main activities, the Ministry also steers security issues related to these. It should be noted that actors in these areas do not merely represent the public sector but include numerous private actors and also third-sector organisations. Security criteria may be related to patient safety, in which availability and correctness of information play a major role; to the Medical Device Regulation (MDR), which ensures the safe and secure functioning of medical devices, which these days are often computers connected to a network; or to the General Data Protection Regulation (GDPR), as the sector processes a lot of sensitive personal data. In addition to these requirements, there is a set of security requirements relating to systems connected to national electronic services, and such systems must be certified. The Ministry steers the activities and is responsible for legislation, while agencies operating under the Ministry (especially the Finnish Institute for Health and Welfare, the Finnish Medicines Agency and the National Supervisory Authority for Welfare and Health) are responsible for implementation.

Data Permit Authority Findata

Findata is a service for the secondary use of social and health data. It issues permits for the secondary use of social and health data in cases where the data is gathered and combined from multiple data controllers, the data originates from private organisers of health and social services or the data is filed in the digital services for the health care and social welfare sector (Kanta Services). Findata operates in conjunction with the Finnish Institute for Health and Welfare but separately from the Institute's other activities.

Ministry of Agriculture and Forestry

The Ministry of Agriculture and Forestry steers, promotes and monitors digital security in its sector. Its key duties concerning digital security include maintaining the Land Information System and the Topographic Data System and safeguarding continuity in all security situations, securing availability of statistical data and performing paying agency duties in accordance with ISO 27001 certification. The Network and Information Security (NIS) Directive obliges entities providing a service which is essential for the maintenance of critical societal and/or economic activities as well as key digital service providers to report information security incidents to their sector's supervisory authority. In the Ministry's sector, the NIS reporting obligation applies to water utilities with a daily capacity for a minimum of 5,000 cubic metres of water supply or wastewater reception.

National Land Survey of Finland

The National Land Survey of Finland (NLS) performs activities relating to the management of register units relating to properties and housing company shares and other units, activities relating to registers required to safeguard the credit system and positioning, promoting the interoperability and use of spatial data, and spatial data and real property research. In addition, the NLS sees to the foundation for positioning and the production of basic spatial data and provides expert services for society.

Finnish Food Authority

The Finnish Food Authority is responsible for Finnish paying agency duties in accordance with the Commission's requirements. These comprise the paying agency's ISO/IEC 27001 certified management system and, with regard to the paying agency's delegated duties, ensuring information security in compliance with the ISO/IEC 27001 and 27002 standards corresponding to paying agency duties.

Ministry of Economic Affairs and Employment

The Ministry of Economic Affairs and Employment is responsible for contributing to information security in functions and information resources in its administrative branch as well as legislation governing the duties and functions. Agencies and institutes of the administrative branch are responsible for service delivery. Key functions to be safeguarded include basic registers relating to companies and entities and their functioning (correctness and availability), the employment functions entity (data protection and availability), safeguarding energy supply, and enterprise financing services containing business secret information for businesses (process security).

National Emergency Supply Agency

The National Emergency Supply Agency (NESA) is an organisation working under the Ministry of Economic Affairs and Employment. It is tasked with planning and measures related to developing and maintaining security of supply. Together with other authorities and the business community, NESA is charged with ensuring the continuity of national critical infrastructure and services under all circumstances. NESA leads and provides resources for the Digital Security 2030 programme improving information security in cyber and digital infrastructure targeted at the needs of businesses that are critical for security of supply.

VTT Technical Research Centre of Finland Ltd

VTT Technical Research Centre of Finland Ltd is a non-profit special assignment company wholly owned by the State of Finland. VTT provides digital security services for enterprises and the public sectors.

Ministry of the Environment

The Ministry of the Environment's vision is "A better environment for future generations". The Ministry has three strategic impact objectives, each of which go beyond administrative boundaries: 1. a good environment and diverse nature, 2. a carbon neutral circular economy society, 3. sustainable urban development. Together with the Finnish Environment Institute, the Ministry is responsible for the digital security and usability of environmental information systems and steers and promotes the functioning of digital security of information systems of the built environment. Led by the Ministry, work in cooperation with other ministries was launched in autumn 2019 to develop an information platform for the built environment containing extensive information entities as regards cyber security and data protection issues alike. The Ministry of the Environment for its part takes into account the digital security requirements in the production and use of the information platform.

Municipalities and joint municipal authorities

The municipalities organise services for their residents. Most of these services are defined by law as being duties of local government. Joint municipal authorities carry out duties under their charter on behalf of their member municipalities. Municipalities operate in multiple sectors, which poses challenges relating to digital security. The municipal executive is tasked with arranging risk management. According to a report by the Association of Finnish Municipalities, basic information technology, data protection, information technology procurement and competitive tendering, development and maintenance are largely carried out in-house by municipalities and joint municipal authorities. There are differences between municipalities and joint municipal authorities, and the size of municipality affects the way in which these are arranged. Around one in three manage information security through an enterprise owned by the municipality or joint municipal authority, while outsourced services are used by around one in five.[21] Municipalities are obliged to implement the minimum information security requirement under the Act on Information Management in The public sector (906/2019) by the end of 2023.

Association of Finnish Municipalities

The duties of the Association of Finnish Municipalities include applying digital security and interoperability methods and practices in the local government sector in cooperation with municipal actors. Digital security specifications must be adapted to the activities of municipal actors, and the key purpose of interoperability is to ensure well-functioning service entities. Digital security practices must contribute towards the realisation of interoperability. With the significance of electronic transactions increasing in service entities, the delivery of secure and high-quality services is part of the everyday lives of municipal residents and part of their everyday safety and security. When implementing specifications and practices, there must be capacity to provide the necessary support to those applying them, taking the size category of municipal actors into account.

Non-governmental organisations

The role of non-governmental organisations in the development of digital security competences and in preparation for various incidents and in accident management is significant. Non-governmental organisations have experience in organising volunteering with citizens and residents.

21 Hyvärinen & Parviainen, Kuntien tietotekniikkakartoitus 2018 (Survey of information technology in municipalities), Association of Finnish Municipalities, in Finnish

Appendix 5. Preparation group

The members of the preparation group appointed for the coordination of the preparation of the principles and implementation plan for the development of digital security in the public sector for 2020–2023 during the period from 1 September 2019 to 28 February 2020 were:

- *Tuija Kuusisto*, Senior Ministerial Adviser, Ministry of Finance, Chair
- *Mika Tuikkanen*, Senior Specialist, Ministry of Finance, Vice-Chair, on leave from 1 September 2019
- *Jaakko Poikonen*, Senior Specialist, Ministry of Finance, until 31 December 2019
- *Petri Puhakainen*, Ministerial Adviser, Prime Minister's Office
- *Ari Uusikartano*, Chief Information Officer, deputy Antti Savolainen, Director, Information Security, Ministry for Foreign Affairs
- *Ismo Parviainen*, Chief Specialist, deputy Kari Santalahti, Chief Security Officer, Ministry of the Interior
- *Harri Mäntylä*, Chief Information Security Officer, Ministry of Defence
- *Liisi Hakalisto*, Senior Specialist, Ministry of Education and Culture
- *Ari Huvinen*, Director, National Land Survey of Finland, deputy Jaana Merta, Chief Information Management Specialist, Ministry of Agriculture and Forestry
- *Olli Lehtilä*, Ministerial Adviser, deputy Maija Rekola, Senior Specialist, Ministry of Transport and Communications
- *Teemupekka Virtanen*, Senior Specialist, Ministry of Social Affairs and Health
- *Kari Klemm*, Senior Government Adviser, deputy *Jaakko Jokela*, Head of Development; *Petteri Ohvo*, Head of Development until 31 January 2020, deputy *Sirpa Alitalo*, Senior Industrial Adviser, Ministry of Economic Affairs and Employment

- *Roni Kiviharju*, Senior Officer Tomi Marjamäki, Senior Specialist, Ministry of the Environment
- *Outi Juntura*, Chief Information Security Officer, Parliament of Finland
- *Antti Sillanpää*, Senior Researcher, Security Committee, from 21 January 2020
- *Mika Susi*, Chief Policy Adviser, Confederation of Finnish Industries until 31 October 2019
- *Mika Susi*, Executive Director, Finnish Information Security Cluster (FISC) from 1 November 2019
- *Markku Raitio*, Chief Information Officer until 17 December 2019, deputy *Aaro Hallikainen*, Information Security Specialist, City of Helsinki
- *Kari Perälä*, Chief Information Officer, deputy Petri Hiirsalmi, Head of Information Management and Information Security Officer, City of Imatra
- *Kalle Luukkainen*, Business Continuity Manager, from 1 January 2020 *Jarna Hartikainen*, Business Continuity Manager, National Emergency Supply Agency
- *Jari Ylikoski*, Senior Advisor, Association of Finnish Municipalities
- *Henri Burtsov*, Head of Information Security Unit, deputy *Jonna Ylikauppila*, Information Security Specialist, Social Insurance Institution of Finland (Kela)
- *Kari Nykänen*, Head of Information Security, City of Oulu
- *Juha Tallinen*, Director, Information Security, deputy *Pasi Koljonen*, Head of Information Management, deputy *Pertti Pyysing*, Head of Information Management, Finnish Defence Forces
- *Pasi Hänninen*, Head of Data Protection, Bank of Finland
- *Sami Niinikorpi*, Head of Data Protection, deputy *Otto Kolsi*, Finnish Security Intelligence Service
- *Rauli Paananen*, Head of Department, Finnish Transport and Communications Agency Traficom

– *Mika Kuronen*, Chief Security Officer, deputy Pyry Heikkinen, IT Security Manager, deputy *Antti Mielonen*, Senior Customs Officer, Finnish Customs

– *Olli Joronen*, Head of Unit, from 17 December 2019 Hannu Naumanen, Chief Security Officer, deputy Virpi Mäkinen, Head of Unit, deputy *Sonja Marjamäki-Ruuskanen*, Government ICT Centre Valtori

– *Samuli Bergström*, Director, deputy *Mikko Hakuli*, Chief Information Security Officer, Finnish Tax Administration

– *Kimmo Rousku*, Chief Senior Specialist, deputy *Kirsi Janhunen*, Chief Specialist, until 14 September 2019, deputy *Erja Kinnunen*, Chief Specialist; *Pekka Ristimäki*, Chief Information Security Officer, deputy *Jarmo Pietikäinen*, Chief Specialist, from 21 January 2020 *Antti Ahokas*, Chief Specialist, Population Register Centre, from 1 January 2020 Digital and Population Data Services Agency.

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 978-952-367-337-3 (pdf)

June 2020