Digital Security Overview Service: Digital security resources

Best practices

DIGI- JA VÄESTÖTIETO-VIRASTO

Contents

- Background
- Documentation of digital security resources in the organisation
- Reporting on digital security resources in the overview service
- Using the results of the service
- Example: Municipality of Tyrskylä

Background

DIGI- JA VÄESTÖTIETO-VIRASTO

What is the Digital Security Overview Service?

The Digital Security Overview Service is a free tool that organisations can use to assess and develop their digital security. With the service, organisations are able to cost-effectively:

- Assess and report on the situational awareness of digital security to their management
- Identify areas for development and plan measures to develop digital security
- Compare the state of their digital security to that of other similar organisations
- Implement legal requirements

Effective use of the service promotes the ongoing strategic monitoring and reporting of an organisation’s digital security. The service has been technically audited, requires strong identification, and your detailed answers are visible only to the limited main user team at DVV.

The Overview Service also plays a key role in the implementation of Finland's Cyber Security Strategy. With the data produced in the service, an organisation is included in a group of similar organisations that can be compared, monitored and reported as a set. This also allows for the monitoring of state of digital security and the allocation of measures and resources to key development areas.

The overview service consists of the following areas:

- **Background information**
- **Observation**
- **Management**
- **Risk management**
- **Continuity of operations and preparedness**
- **Information security**
- **Data protection**
- **Cybersecurity**

Introduction

The Implementation Plan for Finland's Cyber Security Strategy plans and monitors the cybersecurity resources of public administration in the long term, applying the Digital Security Overview Service of the Digital and Population Data Services Agency and other assets. The state of public administration cybersecurity resources must be sufficiently known to ensure their appropriate resourcing and efficient application.

The Digital Security Overview Service monitors the digital security resources used by organisations. This support material has been prepared for public administration organisations for the identification of cybersecurity and digital security resources and reporting in the Digital Security Overview Service.

In the overview service and this material, digital security resources are considered to be divided into three sections: resources related to the development and maintenance of digital security, and human resources related to digital security.

To help identify the above-mentioned aspects in practice, a workshop was also carried out within the VAHTI network where participants identified resources and divided them into each category.

Documentation of digital security resources in the organisation

DIGI- JA VÄESTÖTIETO-VIRASTO

Resource documentation within the organisation

Kategoria	Kuvaus	Riskienhal (Htv)	Jatkuvuus ja varautumi (Htv)	Tietoturvalli (Htv)	Tietos (Htv)	Kyberturvalli (Htv)	Ulkoinen asiantu (Htv)	Ulkoinen pal (€)	Oma henkil (€)	Kehittäm (€)	Yli	Lisähuomio
Henkilöstöresurssit	Tietoturvapäällikkö	0,2	0,2	0,4		0,2			100000		100000	
Henkilöstöresurssit	Tietosuojavastaava				1				100000		100000	
Henkilöstöresurssit	Riskienhallintapäällikkö	0,5	0,5						120000		120000	
Henkilöstöresurssit	Turvallisuusjohtaja		0,5						150000		150000	
Henkilöstöresurssit	Ulkoinen konsultti			0,3		0,2	0,5	50000		20000	30000	
Koulutukset	Henkilöstön koulutus (2h/hlö - 5000 hengen organisaatio - osallistumisprosentti 50% (Koku kysymys nro 21)								200000		200000	Henkilöstön koulutus on ylläpitoa. 5000h = n. 2,5 Htv - keskimäärin 1 h / henkilö (Koku kysymys nro 20)
Koulutukset	Asiantuntijoiden koulutus Spv/hlö työaika+koulutus (Tietoturvapäällikkö)									3000		Asiantuntijoiden koulutus on kehittämistä (Shtp/vuosi)!
Koulutukset	Asiantuntijoiden koulutus Spv/hlö työaika+koulutus (Tietosuojavastaava)									3000		Asiantuntijoiden koulutus on kehittämistä (Shtp/vuosi)!
Koulutukset	Asiantuntijoiden koulutus Spv/hlö työaika+koulutus (Riskienhallintapäällikkö)									4000		Asiantuntijoiden koulutus on kehittämistä (Shtp/vuosi)!
Koulutukset	Asiantuntijoiden koulutus Spv/hlö työaika+koulutus (Turvallisuusjohtaja)									5000		Asiantuntijoiden koulutus on kehittämistä (Shtp/vuosi)!
Palvelut	SOC-SIEM laajennuksen käyttöönotto							20000		20000		
Palvelut	SOC-SIEM peruspalvelu toimittajalta							40000			40000	
Palvelut	Riskienhallinnan hankittu uusi ohjelmisto							10000		10000		
Palvelut	Jatkuvuuden ja varautumisen uusi suunnitelumalli							15000		15000		
Palvelut	O365 E5:n tietoturvaominaisuuksien käyttöönottoprojekti							30000		30000		
Palvelut	Tietosuojan DPIA ohjelmiston hankinta- ja käyttöönotto							10000		10000		
Palvelut	Henkilöstön yleiskoulutuksen ohjelmisto ja räätälöinti							8000		8000		
Palvelut	Keskitetyn haittaohjelmantorjunnan käyttöönotto							60000		60000		
Lisenssit	Riskienhallinnan ohjelmiston vuosilisenssi							6000			6000	
Lisenssit	O365 E5:n tietoturvaominaisuuksien lisenssiosuus							50000			50000	
Lisenssit	DPIA -ohjelmiston vuosilisenssi							6000			6000	
Lisenssit	Henkilöstön yleiskoulutuksen ohjelmistolisenssi							8000			8000	
Lisenssit	Keskitetyn haittaohjelmantorjunnan vuosilisenssi							10000			10000	
Laitteistot	YubiKey avaimet IT-osaston ylläpitohenkilöille ja käyttöönotto									1000		
Laitteistot	NAS-laitteisto salassa pidettävän tietoaineiston paikalliseen arkistointiin									2000		
Laitteistot												
Laitteistot												
Laitteistot												
Muu	Tietoturvapoliittikan päivitys (konsultti)							10000		10000		
Muu	Harjoittelun (esim. TAISTO) kustannus ja osallistujien aika rahassa								2000		2000	Harjoittelu on ylläpitoa, joka tuo esille kehityskohteita! - 5 hlöä osallistui koko päivän + harjoitusmaksu 0€
Muu												
Muu												
Muu												
Yhteensä		0,7	1,2	0,7	1	0,4	0,5	333000	672000	201000	822000	
Koku kysymys nro		12	13	14	15	16	17	18	19	7	8	

- By documenting digital security resources, you can:
  - determine how much and what kind of competencies the organisation has
  - identify potential shortcomings and areas for development
  - facilitate reporting to management, authorities and other potential parties
  - better monitor competence development and resource allocation.
- Resources are assessed in euros and/or person-years. You can use the tool or system of your choice for internal documentation. For documentation, you can also use the model of the fictional Municipality of Tyrskylä (Resource_excel.xlsx), which, as an example, compiles the answers to the resource questions in the overview service, starting from the classification:
  - Human resources
  - Training
  - Services
  - Licences
  - Equipment
  - Other

Finding information to be documented

- Information related to digital security resources can be found in various sources within the organisation. Some examples of this are:
  - Financial administration (e.g. outsourced services, personnel costs, ongoing expenses, investments)
  - Information administration/IT department (e.g. human resources, systems used, licences, service contracts, development projects and initiatives)
  - Project office/PMO (e.g. costs, resources and timetables for projects related to data security)
  - Data security team/chief information security officer (e.g. roles, data security budget, data security solutions used, human resources, competence level and training needs, outsourced services)
  - HR/personnel administration (e.g. training costs, use of personnel's time)
  - Purchased services/procurement (e.g. outsourced data security services or products and their costs)
- It is recommended that the documentation of resources is continuous and maintained regularly whenever changes occur. For example, when new persons are appointed to positions of responsibility, new projects or initiatives are launched, or there are changes to training.
- If continuous maintenance of the documentation is not possible, it should be reviewed and updated every six months or at least once a year. In connection with the review, it is a good idea to record the date of the review and the person in charge of the review and to assess the adequacy of resources and any development needs.
- Once the resources related to digital security have been documented, it is easier to report them to management and the overview service, for example.

Reporting on digital security resources in the overview service

‘Background information’ section

DIGI- JA VÄESTÖTIETO-VIRASTO

Reporting on resources in the overview service

- Questions related to digital security resources can be found in the Background Information section of the overview service.
- The questions examine the organisation’s digital security resources in the previous calendar year:
  - Costs of digital security development and maintenance
  - Person-years related to risk management, continuity and preparedness, information security, data protection and cybersecurity
  - Costs of purchasing digital security specialist services from service providers
  - Costs of the organisation’s internal digital security personnel
  - The amount of digital security training provided for the organisation’s personnel and the participation rate (%)
- The next pages present questions related to the resources, plus instructions and examples for interpretation. The aim is to help organisations interpret the statements in a commensurate manner so that the different responses can be compared to each other.

AREA: Background information

- **Question 7.** How much was the total **cost of developing** digital security in the previous calendar year? (EUR)
  - **Info text:** Please include the total costs in your estimate, including personnel costs, services, licences, equipment, training, etc. related to the development of digital security.

- **Instructions for interpretation:**

  Include **development costs** in all areas of digital security (risk management, continuity and preparedness, data security, cybersecurity, data protection), such as
  - creating and updating a planning model for risk management, continuity or preparedness
  - creating and updating policies related to digital security and preparing guidelines
  - software acquisition for annual personnel training
  - security assessments of systems (e.g. vulnerability scans, Hyöky, Havaro)
  - new digital security systems, services and their extensions with deployment costs
  - audits carried out, remedying their findings, and planning of new audits
  - change, risk and impact assessments carried out (e.g. DPIA) and risk mitigation
  - continuous training, national cooperation and peer support for digital security awareness of core persons (e.g. VAHTI)
  - reporting (e.g. year-end data statements, overview service, executive reporting). Note: may include both development and maintenance.

AREA: Background information

- **Question 8.** How much was the total **cost of maintaining** digital security in the previous calendar year? (EUR)

- **Instructions for interpretation:**

  Include **maintenance costs** in all areas of digital security (risk management, continuity and preparedness, data security, cybersecurity, data protection), such as

  - licensing costs of systems related to digital security and the related training
  - licensing costs of software used for data protection impact assessment
  - licensing costs and updates of the annual personnel training program
  - time/costs spent by personnel on training and exercises (e.g. TAISTO, webinars, lectures, seminars)
  - basic costs of system assessment, testing and monitoring services (e.g. SOC-SIEM, NOC, Hyöky, Havaro)
  - updates and repairs of existing systems and equipment
  - use of management models and standards to maintain situational awareness and instructions
  - maintenance of the application, software, hardware and technology lists (e.g. CMDB)
  - reporting (e.g. year-end data statements, overview service, executive reporting). Note: may include both development and maintenance.

AREA: Background information

Questions:

- 12. How many of the reported person-years focus on risk management?
  - **Info text:** Please estimate the total number of person-years, e.g. 1 person works on risk management for 25% of their working time = 0.25 person-years.
- 13. How many of the reported person-years focus on continuity and preparedness?
  - **Info text:** Please estimate the total number of person-years, e.g. 1 person works on continuity and preparedness for 25% of their working time = 0.25 person-years.
- 14. How many of the reported person-years focus on information security?
  - **Info text:** Please estimate the total number of person-years, e.g. 1 person works on data security for 25% of their working time = 0.25 person-years.
- 15. How many of the reported person-years focus on data protection?
  - **Info text:** Please estimate the total number of person-years, e.g. 1 person works on data protection for 25% of their working time = 0.25 person-years.
- 16. How many of the reported person-years focus on cybersecurity?
  - **Info text:** Please estimate the total number of person-years, e.g. 1 person works on cybersecurity for 25% of their working time = 0.25 person-years.

- **Instructions for interpretation:**
  Consider **all people** whose work focuses on the areas of digital security, regardless of whether they work within the organisation or as external specialists, such as:

AREA: Background information

- **Question 17.** How many person-years of digital security specialist services does the organisation purchase from a service provider?
  - **Info text**: For example, the organisation purchases the services of a data protection officer/chief information security officer from a service provider.

- **Instructions for interpretation:**

  Consider all external specialist services purchased, such as consultants, auditors, specialists and outsourced data security and data protection roles.
  - For example, person X works full-time for one year = 1 person-year; person Y works 20 days a year = approx. 0.1 person-years; person Z works 50% of the working time for six months = approx. 0.25 person-years.
  - If detailed hourly records are not available, apply the **best estimate**, if necessary.

AREA: Background information

- **Question 18.** If the organisation purchases digital security specialist services from a service provider, how much did they cost in the previous calendar year? (EUR)

- **Instructions for interpretation:**

  Include all **services purchased from external service providers** related to maintaining or developing digital security in all areas of digital security. If the service is part of a more extensive contract (e.g. an IT service contract), only estimate the proportion related to digital security. Purchased services may include:

  - consultants and specialist work
  - outsourced data security and data protection roles
  - audits, evaluations and inspections
  - monitoring services (e.g. SOC)
  - vulnerability scans and security testing
  - data protection services and legal counsel
  - facilitation of exercises, training sessions and workshops.
  - Apply the actual annual costs or **best estimates**, if necessary

AREA: Background information

- **Question 19.** How much were the costs of the organisation's own digital security personnel in the previous calendar year?
  - **Info text:** Please include the total costs in your estimate, including wages and indirect costs.
- **Instructions for interpretation:**

  Consider the total costs related to personnel in all areas of digital security, such as:
  - wages and indirect costs
  - statutory payments
  - travel expenses
  - audits carried out and their specific resources
  - training, courses and exercises (note also the following question #20).

- **Question 20.** On average, how many hours of digital security training did the organisation's personnel receive in the previous calendar year? (hours per person)
- **Instructions for interpretation:**

  Take into account training related to all areas of digital security, such as online courses, simulated phishing tests, live lectures and workshops, awareness raising campaigns, and certification training.

  ➔ Please note: This is also included in the previous question #19.

Using the results of the service

DIGI- JA VÄESTÖTIETO-VIRASTO

Using the results of the overview service

The organisation can also utilise the data it has provided in the overview service in terms of digital security resources.

For example, it can be used to:

- identify areas where resources concentrate the most and to identify areas that are already at a good level
- identify competence gaps in the weakest areas where resources should be allocated and measures planned to develop digital security
- identify any missing roles and responsibilities in digital security
- create a basis for preparing a digital security budget and planning development measures
- hold discussions between various units of the organisation (e.g. IT, HR, management).

The data in the overview service can also be used to extract information, especially for the management of the organisation, on topics such as how the organisation's resources focus on the various areas of digital security, whether the resources are sufficient, which areas should be developed in particular, and where resources should be allocated in the future.

Through the weakest areas, it is possible to bring up with management the risks related to insufficient resources, as well as concrete recommendations and proposals for measures to develop the weakest areas, such as any investment needs, reserving a budget for a specific case, or using external support.

The findings also make it possible to compare how the organisation is positioned in relation to other organisations of the same size or in the same sector. In particular, management may be interested in the level of their own organisation: whether the organisation is a pioneer, at the average level, or at the tail end of its reference group.

Example: Municipality of Tyrskylä

DIGI- JA VÄESTÖTIETO-VIRASTO

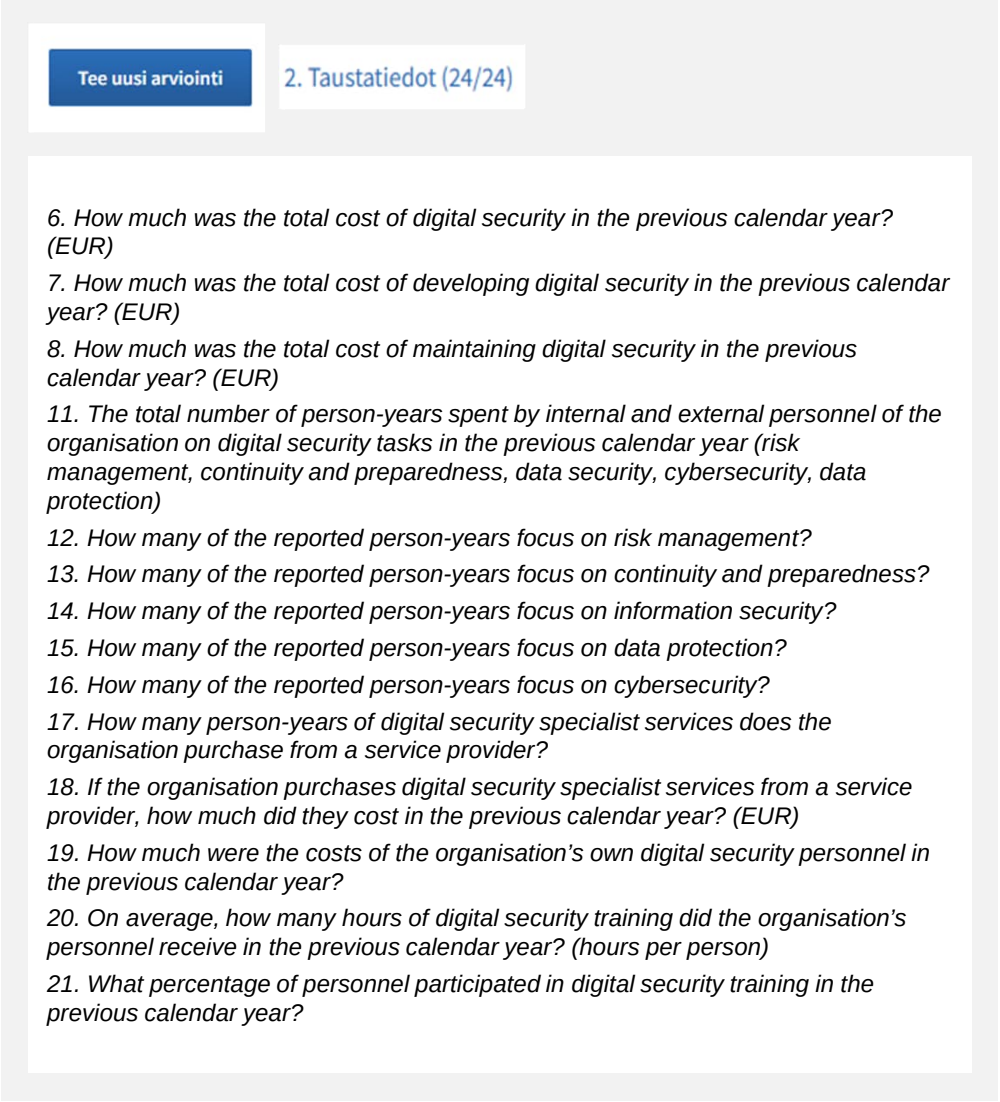
Municipality of Tyrskylä

The coastal municipality of Tyrskylä is located in Southeast Finland. This rapidly-growing municipality of 55,879 residents is home to several high-tech companies and a port for 2.42% of Finland’s maritime exports and imports. Additionally, a modern data centre of an internationally significant cloud service provider operates in the municipality. Thanks to its busy port, the municipality itself is also a significant employer with its personnel of nearly 5,000 people.

Tanja is the Chief Information Security Officer in the Municipality of Tyrskylä. Tanja wants to understand how digital security development, maintenance and human resources can be easily identified and documented in the municipality, as the municipality has a very limited budget for digital security.

Tanja reports the identified and documented digital security resources of the Municipality of Tyrskylä in the overview service provided by the Digital and Population Data Services Agency as part of the annual reporting in the service. She knows that the results of the service provide valuable information on whether the municipality's digital security resources are adequate and where the resources should focus on to develop digital security in the future.

Invitation to fill in the information in the overview service



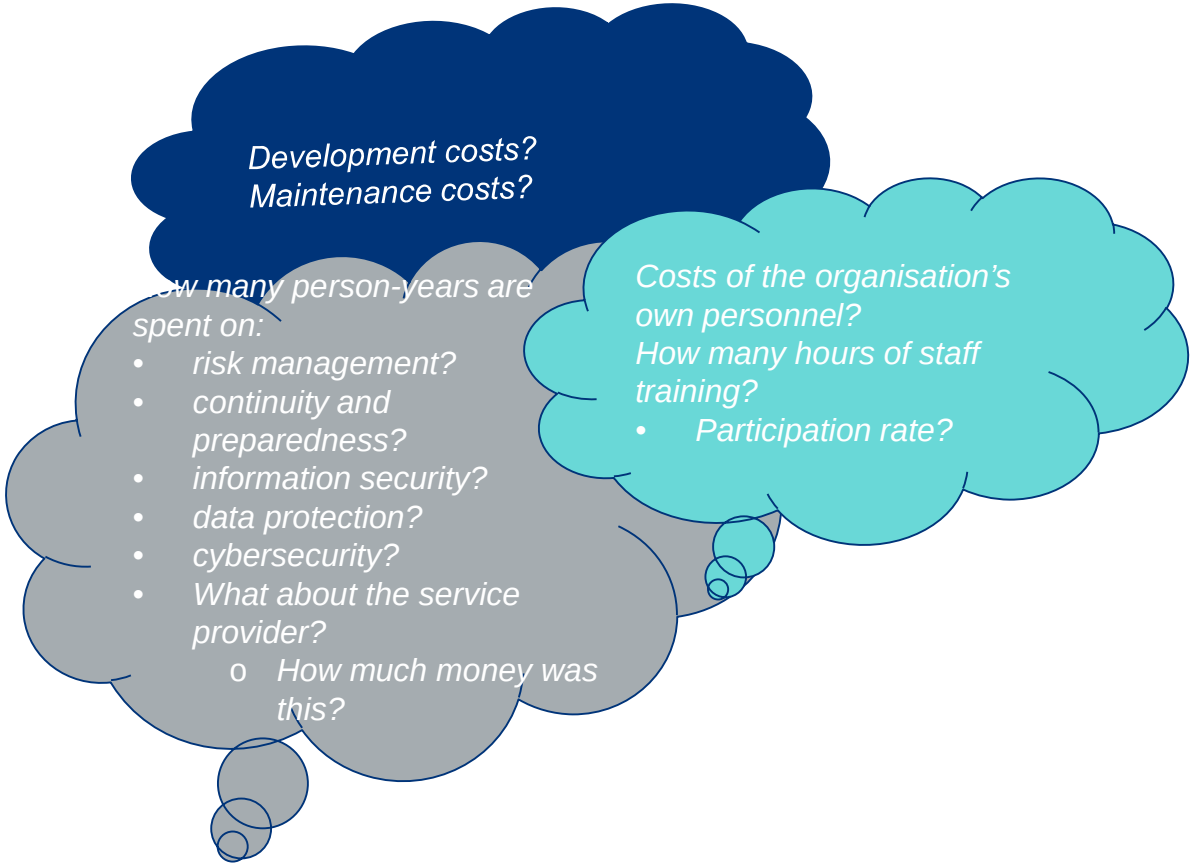
The Digital and Population Data Services Agency has again sent an invitation via the municipality's registry office for Tanja, the Chief Information Security Officer, to update the information in the overview service under the section 'Complete a new assessment'.

Reporting the resources used for digital security is a key point in the background information of the survey, the responses of which indicate the municipality's operating possibilities and investments.

To answer questions related to resources, Tanja first goes through the questions and identifies topics that should be taken into account.

- This is a matter of digital security and all its aspects
- Costs of both development and maintenance
- Resources are reported both in person-years and in euros
- Outsourced services and persons such as consultants must be included
- Basic training for personnel in digital security, special training for internal specialists and practical training should all be remembered
- In addition, the overview service gives the following alerts:
  - *"Please include the total costs in your estimate,*

What are digital security resources?



To answer the questions related to resources, Tanja stops to think about and investigate the following:

- What is included in the development costs?
- What about maintenance costs?
- For example, into which category do the training of personnel or licensing costs go?
- How do I find the requested costs?
- How do I know the correct amounts in euros and person-years?

After a while of reflection, Tanja recalls that for a few years, she has produced regular executive reporting on key digital security events, development needs and their progress, including their costs. She can pick the maintenance and implemented areas of development from these reports, and the financial department of the municipality will be sure to help if she needs it.

Resources and person-years as well as the time spent on training, for example, still need to be considered as far as possible. An estimate based on job descriptions is certainly a good starting point, as well. The time spent on training and attendance information are probably found in the systems in

Last year's maintenance and development work?

Tanja starts reviewing her reporting and HR data and picks up the following areas from the previous year that are included in the resourcing of digital security.

- Activation of the SOC-SIEM extension (24x7) and its annual basic service from the provider
- New software license acquired and activated for risk management
- New planning template and process description for continuity and preparedness
- Microsoft M365 E5 security deployment project and licence
- Procurement, activation and annual licence of the data protection impact assessment (DPIA) software
- New software, customisation and software licence for general personnel cybersecurity training
- Activation and licensing of new centralised anti-malware
- Acquisition of strong authentication keys (e.g. YubiKey) for IT administrators and deployment installation
- New storage system (NAS) for the local archiving of non-disclosable data
- Work on the data security policy update (consultant work)
- Annual TAISTO exercise: costs and time spent by participants
- Participation rate and time spent in annual digital security training for personnel
- For the development of the digital security skills of the organisation's own specialists, 5 person-days/person + the course price have been reserved.

Human resources in Tyrskylä digital security

According to the HR system of Tyrskylä, the human resources of digital security are:

- Chief information security officer (in an employment relationship)
- Data protection officer (public post)
- Head of risk management (public post)
- Safety and security manager (public post)
- External part-time data security consultant (0.5 person-years)

Tanja notices that, with human resources, you must identify which areas of digital security they focus on – some focus on more than one area:

- Chief information security officer ➔ Data security 40%, cybersecurity 20%, risk management 20%, continuity and preparedness 20%
- Data protection officer ➔ Data protection 100%
- Head of risk management ➔ Risk management 50%, continuity and preparedness 50%
- Safety and security manager ➔ Continuity and preparedness 50%
- External part-time data security consultant ➔ Data security 30%, cybersecurity 20%

In total, Tyrskylä has digital security human resources worth 4.5 person-years

- When converting into euros, the instructions were: *"Please include the total costs in your estimate, including wages and indirect costs."*

Development or maintenance?

At a few points, Tanja considers which digital security resources are part of maintenance and which are part of development:

- Training
  - ➔ Annual digital security training of personnel is maintenance
  - ➔ Training of internal specialist personnel is development
- Digital security software, hardware and services
  - ➔ Annual service charges, licences and updates are maintenance
  - ➔ New service and software procurements and their activation are development
- Training
  - ➔ is maintenance (e.g. TAISTO).
  - ➔ Working on emerging areas of development is development
- General
  - ➔ The development work is a project, after which the resource goes to maintenance once it is acquired and deployed
    - ➔ The resource becomes an established part of the organisation's normal operations

Summary and maintenance of resource-related responses

The information needed for the responses has now been found, and Tanja compiles it in the Municipality of Tyrskylä's table template (Resource_excel.xlsx), which she can then use in other reporting. If she keeps maintaining the table, she can also use it in the next assessment in the overview service.

Päivittäjä	Tanja											
Päiväys	27.10.2025											
Kategoria	Kuvaus	Riskienhallinta (Htv)	Jatkuvuus ja varautuminen (Htv)	Tietoturvallisuus (Htv)	Tietosuoja (Htv)	Kyberturvallisuus (Htv)	Ulkoinen asiantuntija (Htv)	Ulkoinen palvelu (€)	Oma henkilöstö (€)	Kehittäminen (€)	Ylläpito (€)	Lisähuomio
Henkilöstöresurssit	Tietoturvapäällikkö	0,2	0,2	0,4		0,2			100000		100000	
Henkilöstöresurssit	Tietosuojavastaava				1				100000		100000	
Henkilöstöresurssit	Riskienhallintapäällikkö	0,5	0,5						120000		120000	
Henkilöstöresurssit	Turvallisuusjohtaja		0,5						150000		150000	
Henkilöstöresurssit	Ulkoinen konsultti			0,3		0,2	0,5	50000		20000	30000	
Koulutukset	Henkilöstön koulutus (2h/hlö - 5000 hengen organisaatio - osallistumisprosentti 50% (Koku kysymys nro 21)								200000		200000	Henkilöstön koulutus on ylläpitoa. 5000h = n. 2,5 Htv - keskimäärin 1 h / henkilö (Koku kysymys nro 20)
Koulutukset	Asiantuntijoiden koulutus 5pv/hlö työaika+koulutus (Tietoturvapäällikkö)									3000		Asiantuntijoiden koulutus on kehittämistä (5htp/vuosi)!
Koulutukset	Asiantuntijoiden koulutus 5pv/hlö työaika+koulutus (Tietosuojavastaava)									3000		Asiantuntijoiden koulutus on kehittämistä (5htp/vuosi)!
Koulutukset	Asiantuntijoiden koulutus 5pv/hlö työaika+koulutus (Riskienhallintapäällikkö)									4000		Asiantuntijoiden koulutus on kehittämistä (5htp/vuosi)!
Koulutukset	Asiantuntijoiden koulutus 5pv/hlö työaika+koulutus (Turvallisuusjohtaja)									5000		Asiantuntijoiden koulutus on kehittämistä (5htp/vuosi)!
Palvelut	SOC-SIEM laajennuksen käyttöönotto							20000		20000		
Palvelut	SOC-SIEM peruspalvelu toimittajalta							40000			40000	
Palvelut	Riskienhallinnan hankittu uusi ohjelmisto							10000		10000		
Palvelut	Jatkuvuuden ja varautumisen uusi suunnittelumalli							15000		15000		
Palvelut	O365 E5:n tietoturvaominaisuuksien käyttöönottoprojekti							30000		30000		
Palvelut	Tietosuojan DPIA ohjelmiston hankinta- ja käyttöönotto							10000		10000		
Palvelut	Henkilöstön yleiskoulutuksen ohjelmisto ja räätälöinti							8000		8000		
Palvelut	Keskitetyn haittaohjelmantorjunnan käyttöönotto							60000		60000		
Lisenssit	Riskienhallinnan ohjelmiston vuosilisenssi							6000			6000	
Lisenssit	O365 E5:n tietoturvaominaisuuksien lisenssiosuus							50000			50000	
Lisenssit	DPIA -ohjelmiston vuosilisenssi							6000			6000	
Lisenssit	Henkilöstön yleiskoulutuksen ohjelmistolisenssi							8000			8000	
Lisenssit	Keskitetyn haittaohjelmantorjunnan vuosilisenssi							10000			10000	
Laitteistot	YubiKey avaimet IT-osaston ylläpitohenkilöille ja käytttöönotto									1000		
Laitteistot	NAS-laitteisto salassa pidettävän tietoaineiston paikalliseen arkistointiin									2000		
Laitteistot												
Laitteistot												
Laitteistot												
Muu	Tietoturvapolitiikan päivitys (konsultti)							10000		10000		
Muu	Harjoittelun (esim. TAISTO) kustannus ja osallistujien aika rahassa								2000		2000	Harjoittelu on ylläpitoa, joka tuo esille kehityskohteita! - 5 hlöä osallistui koko päivän + harjoitusmaksu 0€
Muu												
Muu												
Muu												
Yhteensä		0,7	1,2	0,7	1	0,4	0,5	333000	672000	201000	822000	
Koku kysymys nro		12	13	14	15	16	17	18	19	7	8	

Responses in the overview service

Next, Tanja picks the responses and enters them in the overview service for the Municipality of Tyrskylä as follows:

7. How much was the total cost of developing digital security in the previous calendar year? (EUR)

➔ *EUR 201,000*

8. How much was the total cost of maintaining digital security in the previous calendar year? (EUR)

➔ *EUR 822,000*

12. How many of the reported person-years focus on risk management?

➔ *0.7 person-years*

13. How many of the reported person-years focus on continuity and preparedness?

➔ *1.2 person-years*

14. How many of the reported person-years focus on information security?

➔ *0.7 person-years*

15. How many of the reported person-years focus on data protection?

➔ *1 person-years*

16. How many of the reported person-years focus on cybersecurity?

➔ *0.4 person-years*

17. How many person-years of digital security specialist services does the organisation purchase from a service provider?

➔ *0.5 person-years*

18. If the organisation purchases digital security specialist services from a service provider, how much did they cost in the previous calendar year? (EUR)

➔ *EUR 333,000*

19. How much were the costs of the organisation's own digital security personnel in the previous calendar year?

➔ *EUR 672,000*

20. On average, how many hours of digital security training did the organisation's personnel receive in the previous calendar year? (hours per person)

➔ *5,000 h*

21. What percentage of personnel participated in digital security training in the previous calendar year?

➔ 50%

Responses in the overview service

Tanja double-checks that the responses are correct and in line with the information she has collected.

6. Kuinka paljon ovat olleet digitaalisen turvallisuuden kokonaiskustannukset edellisen kalenterivuoden aikana? (euroa)

Huom! Tämä vastaus täytetään automaattisesti muiden vastausten perusteella.

1023000

+ Lisää muistiinpano

7. Kuinka paljon ovat olleet digitaalisen turvallisuuden kehittämiskustannukset edellisen kalenterivuoden aikana? (euroa)

201000

+ Lisää muistiinpano

8. Kuinka paljon ovat olleet digitaalisen turvallisuuden ylläpitokustannukset edellisen kalenterivuoden aikana? (euroa)

822000

+ Lisää muistiinpano

18. Jos organisaatio ostaa digiturvan asiantuntijapalveluita palveluntuottajalta, kuinka paljon kustannukset olivat edellisen kalenterivuoden aikana? (euroa)

333000

+ Lisää muistiinpano

19. Kuinka paljon olivat organisaation oman digiturvaan liittyvän henkilöstön kustannukset edellisen kalenterivuoden aikana?

672000

+ Lisää muistiinpano

20. Kuinka monta tuntia digitaalisen turvallisuuden koulutusta organisaation henkilöstö on keskimäärin saanut edellisen kalenterivuoden aikana? (tuntia / henkilö)

5000

+ Lisää muistiinpano

21. Kuinka monta prosenttia henkilöstöstä osallistui digitaalisen turvallisuuden koulutukseen edellisen kalenterivuoden aikana?

- ○ noin 25 %
- ◉ noin 50 %
- ○ noin 75%
- ○ noin 100%

+ Lisää muistiinpano

11. Organisaation oman ja ulkoisten henkilöiden digiturvatehtäviin yhteensä käyttämä henkilötyövuosimäärä organisaatiossa edellisen kalenterivuoden aikana (riskienhallinta, jatkuvuus ja valmius, tietoturva, kyberturva, tietosuoja)

Huom! Tämä vastaus täytetään automaattisesti muiden vastausten perusteella.

4

+ Lisää muistiinpano

12. Kuinka monta ilmoitetuista henkilötyövuosista kohdistuu riskienhallintaan?

0,7

+ Lisää muistiinpano

13. Kuinka monta ilmoitetuista henkilötyövuosista kohdistuu jatkuvuuteen ja varautumiseen?

1,2

+ Lisää muistiinpano

14. Kuinka monta ilmoitetuista henkilötyövuosista kohdistuu tietoturvallisuuteen?

0,7

+ Lisää muistiinpano

15. Kuinka monta ilmoitetuista henkilötyövuosista kohdistuu tietosuojaan?

1

+ Lisää muistiinpano

16. Kuinka monta ilmoitetuista henkilötyövuosista kohdistuu kyberturvallisuuteen?

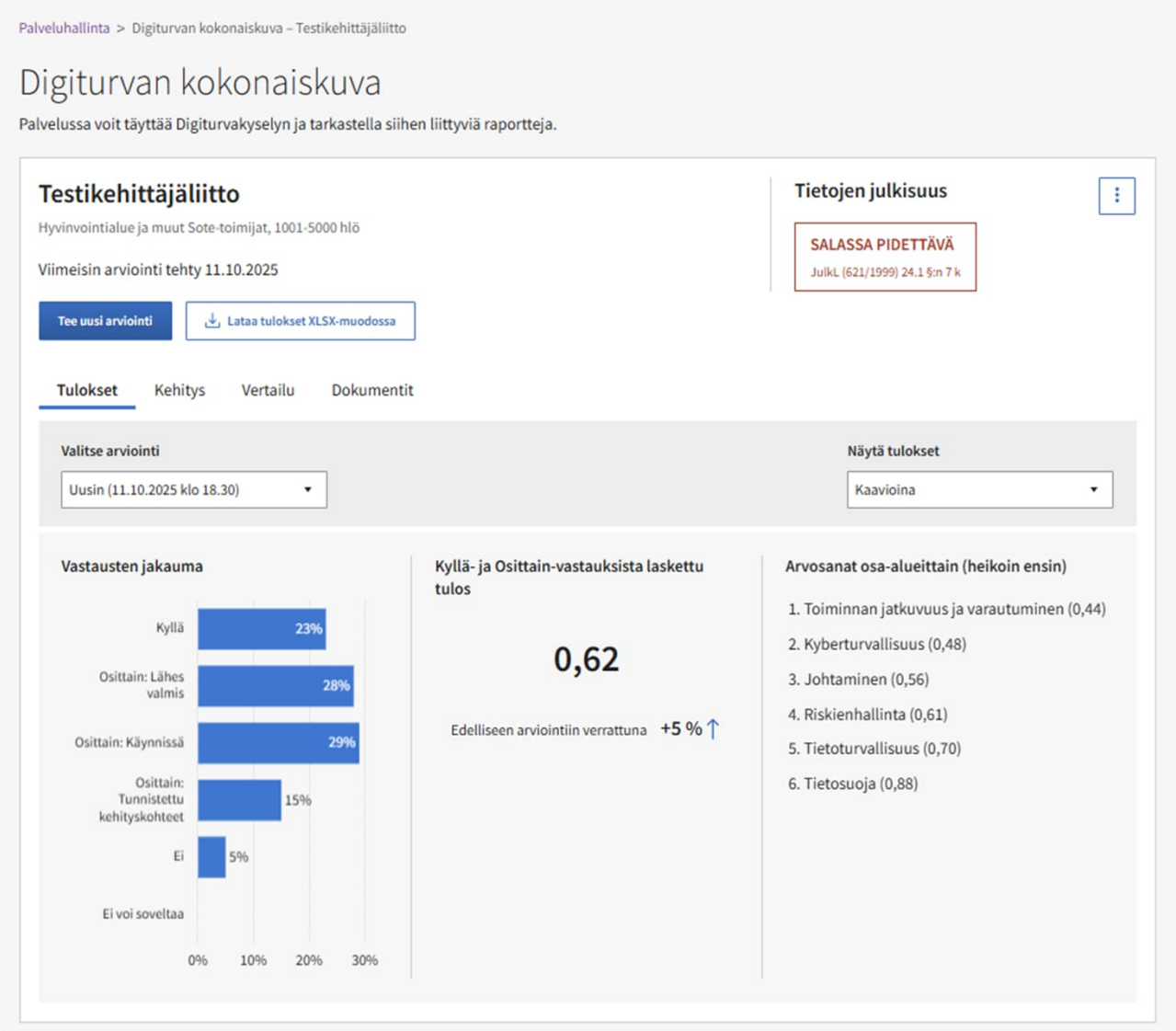
0,4

+ Lisää muistiinpano

17. Kuinka monta henkilötyövuotta organisaatio ostaa digiturvan asiantuntijapalveluita palveluntuottajalta?

0,5

Use of the results



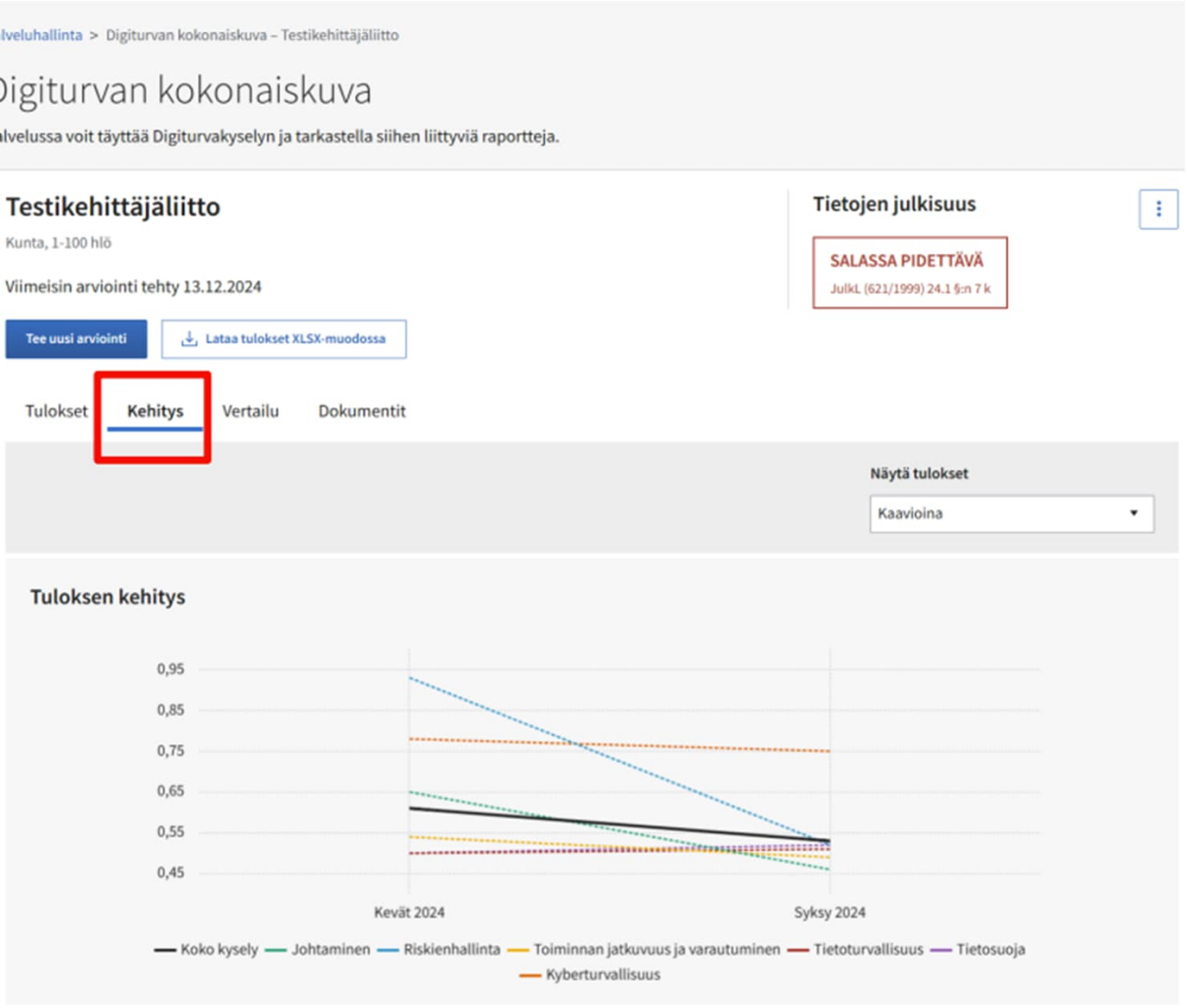
Finally, Tanja reviews the results of the responses she has entered in the service. From the results, Tanja is able to assess the adequacy of digital security resources in Tyrskylä.

When looking at the results, she notices that the calculated result of the 'Yes' and 'Partially' responses is significantly better than the previous time. This indicates that the municipality has allocated more resources to digital security than in the previous year and that things have improved.

Based on the areas' ratings shown on the right, Tanja sees which areas got the weakest rating in the municipality. She is delighted to see that data protection in the municipality remains at the highest level. However, she becomes more serious when she notices that continuity and preparedness and cybersecurity are at the weakest level. She reflects on the need to pay more attention to the weakest areas and to allocate more resources to them, moving forward.

Tanja includes the results as part of the reporting to the municipality's management. The results allow her to clearly justify to the management where resources should be allocated next.

How has digital security developed in Tyrskylä in recent years?



Next, Tanja examines the results in the Development section of the service. The graph shows the situational picture of the municipality's digital security and the development trends in its various areas.

Tanja sees that the overall development of different areas of digital security has been fairly stable, except that risk management has gone in a significantly worse direction than before. Tanja reflects on the need to discuss with the head of risk management how the direction could be reversed. Similarly, for other areas, the situation must be reviewed and development targets included in the development plan prepared during the annual cycle.

Tanja includes the situational picture of digital security in her regular reporting to the municipality's management to illustrate the development trends in various areas of digital security. She wants to emphasise to management that they should turn the development trends upward and raise digital security as a whole to a better level. Starting with the additional resources required.