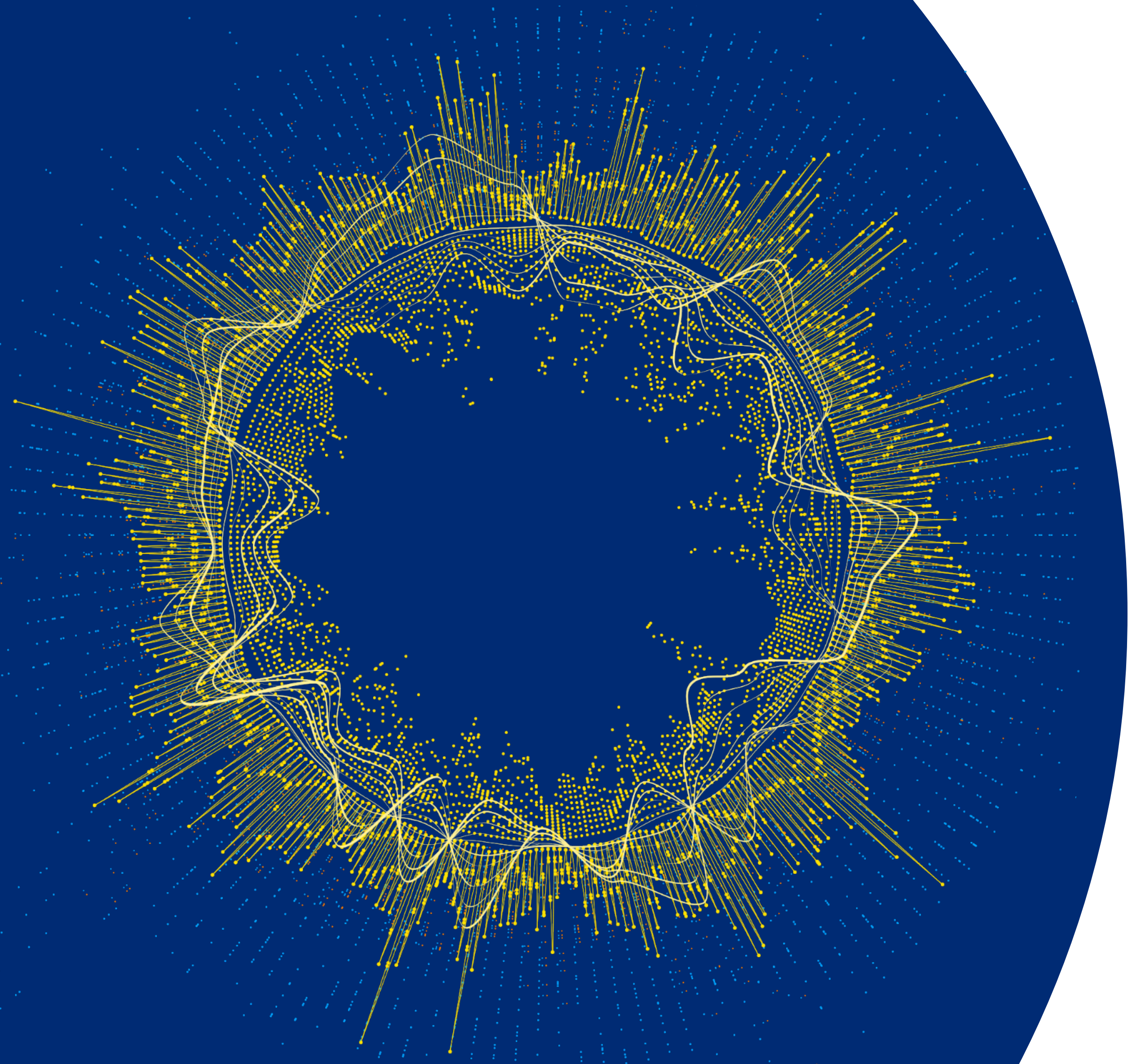


4FRONT

TRAFICOM
Finnish Transport and Communications Agency

NCC-FI
FINLAND NATIONAL COORDINATION CENTRE FOR CYBERSECURITY

Impact evaluation of the financial support provided by the National Coordination Centre Finland (NCC-FI)

Evaluation Report Summary

17th of January 2025

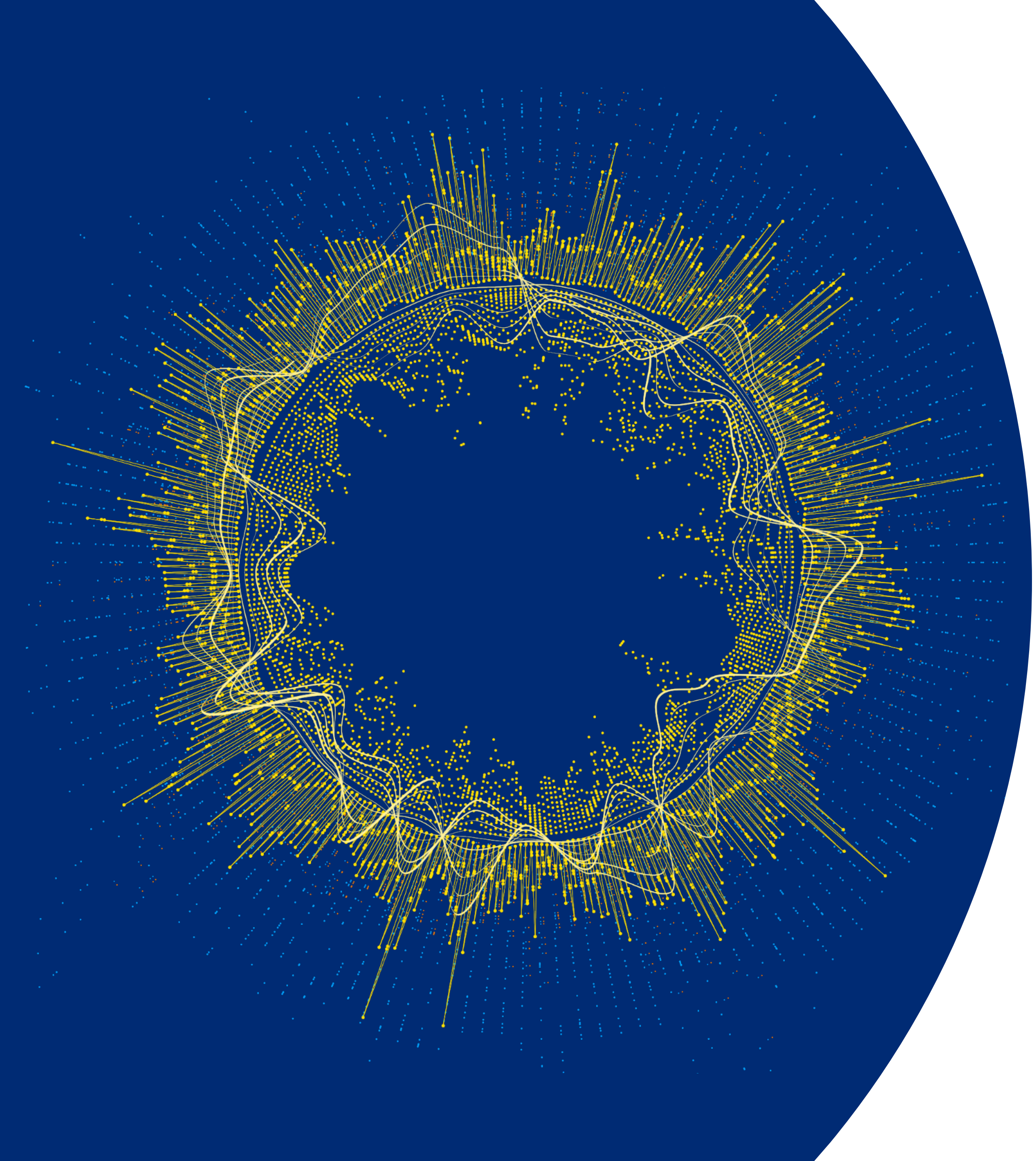
Co-funded by the European Union

Abstract

- The evaluation assessed the direct and indirect impacts of Finnish Transport and Communications Agency's National Cyber Security Centre's National Coordination Centre's (NCC-FI) financial support for SMEs to implement state-of-art information and cyber security solutions and innovations. The main methods and data sources of the evaluation were analysis of project plans, applications and data, beneficiaries survey, expert interviews, literature review and validation workshop.

- In terms of direct impacts to beneficiaries, the evaluation found that the financial support has well fulfilled its purpose and its direct impact to beneficiaries can be considered high. Almost all the projects (95 %) stated that they have successfully implemented their technology upgrading and reached the project goals. The companies were also reporting increased resilience against cyber-attacks. In terms of indirect impacts, the evaluation was looking at effects on cyber security market and overall national cyber security capacity. The financial support has generated some additional demand for the provision of IT services with the volume of around EUR 0.9 million. The services were mainly provided by Finnish companies. The purchased technological solutions were mainly those provided by international large-scale companies. In terms of proportionality and appropriateness, it seems clear that the volume (2 MEUR) is limited, when considering the national needs. Therefore, volume is appropriate either as a targeted support and incentive to address certain identified challenges. The grant size (max EUR 60 thousand) could be equally effective in a slightly smaller form (e.g. EUR 20 thousand), thus allowing for more grants to be delivered.

- The evaluation recommends that further support for companies to upgrade their cyber security should be ensured, the effectiveness could be increased by decreasing the size of individual grants, while expanding the number of given grants, the instrument should support holistic approach to cyber security and encourage companies to take actions beyond adoption of technology and that financial support should be complemented with non-financial support, such as technical guidance and sharing of good (process) practices, to enhance its effectiveness.



TRAFICOM

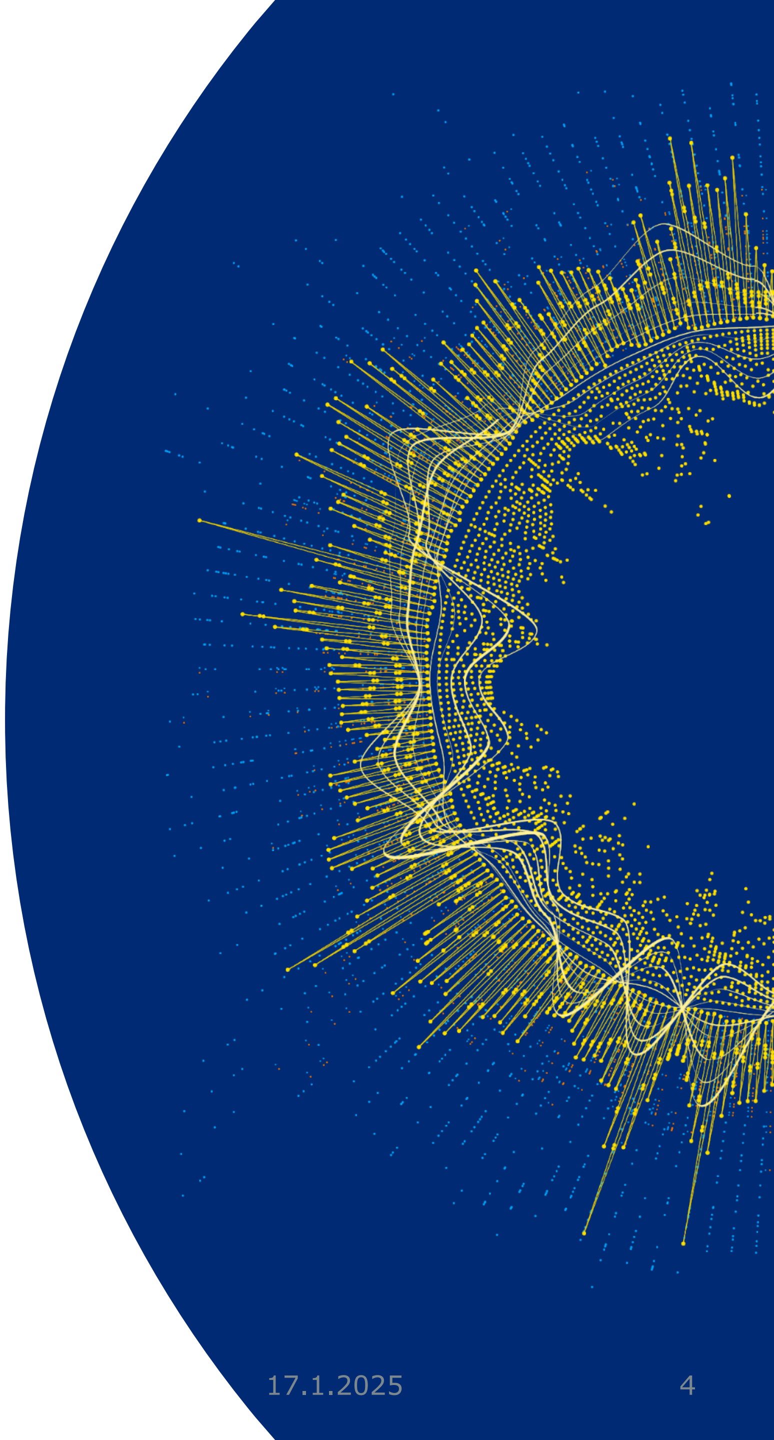
Finnish Transport and Communications Agency

4FRONT

Evaluation approach and methods

Background and objectives of the evaluation

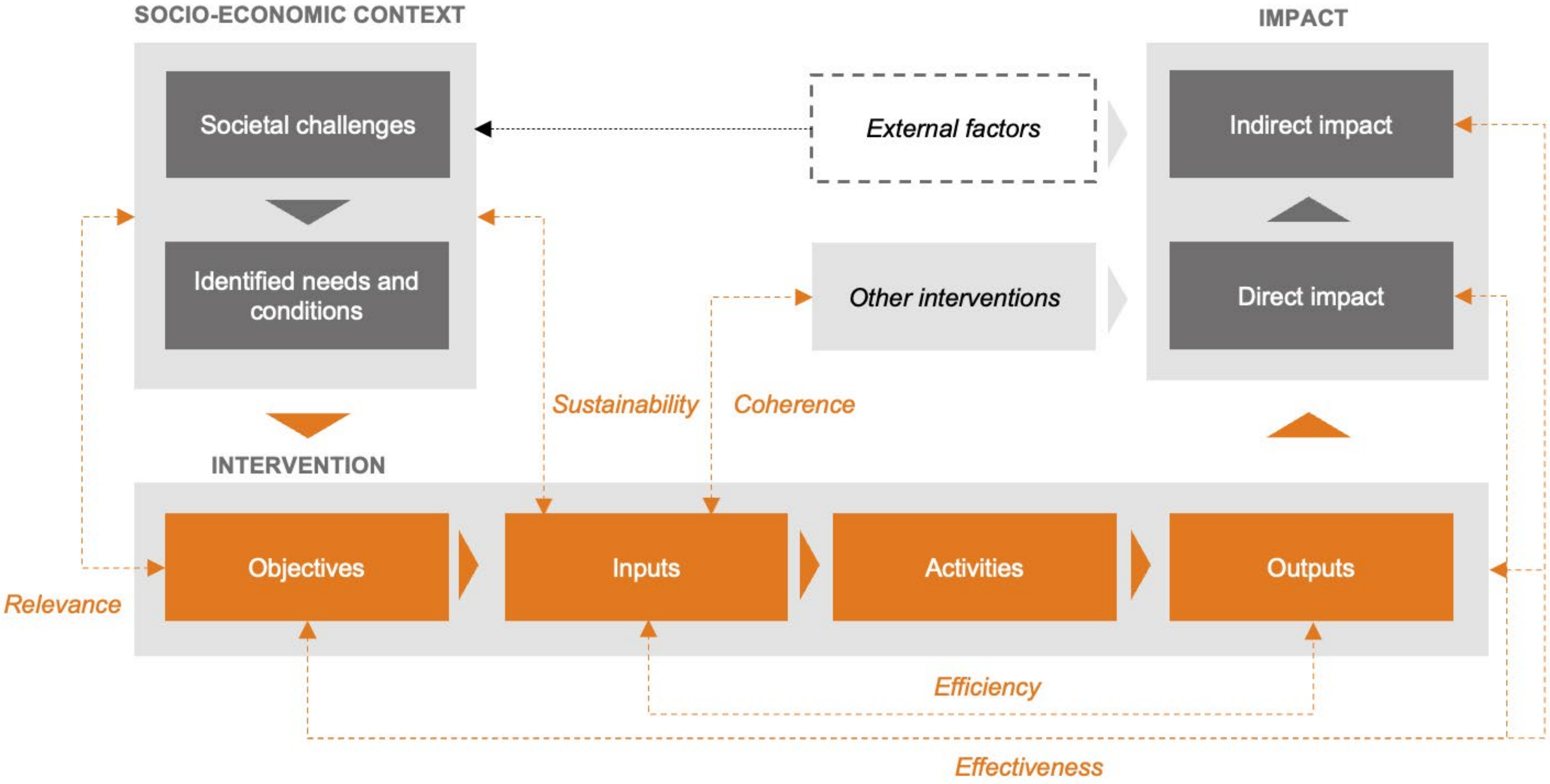
- During the years 2023-2024, the Finnish Transport and Communication Agency (Traficom) and the National Coordination Centre Finland (NCC-FI) has received financial support from the Digital Europe Programme, part of which NCC-FI has distributed to third parties.
- The financial support has been primarily aimed at strengthening the capabilities of small and medium-sized enterprises as well as enhancing Finland's national capacity and infrastructure to defend against cyberattacks.
- The NCSC-FI has commissioned an impact evaluation on the support on implementation of state-of-the-art cyber and information security solutions.
- The evaluation was conducted by 4FRONT Oy together with Timo Kotilainen (Kasin Consulting Oy).



Evaluation questions

	Sub-questions
Direct and short-term impact on beneficiaries	• How has the financial support affected the recipients' own cyber and information security? • To what extent has the financial support encouraged beneficiaries to implement measures that improve their own information security (incentive effect)? To what extent would these measures have been left unimplemented without the financial support? • To what extent has the financial support met the needs of the recipient companies? • To what extent has the financial support affected the beneficiaries to competitiveness/competitive situation (competitive effects)? • To what extent has the financial support had the expected effects? • How has the financial support affected the different recipients of the support, the company's size, location and activities by industry?
Short and long-term indirect impact	• How has the financial support affected Finnish cyber security companies and to their business? • How has the financial support affected other companies? • How has the financial support affected society's cyber security capacity? • How has the financial support affected Finland and the European Union strategic autonomy on cyber security and competitiveness?
Proportionality and appropriateness	• To what extent has the financial support been proportionate to the problems to be solved? • To what extent could the same effect have been achieved with less financial support or with a different form of support? • To what extent could the same effect have been achieved with other measures? • To what extent was the chosen financial support instrument the most effective, and could alternative instruments have been more suitable or effective?

Analytical framework for the impact evaluation (Theory-of-Change)



SOCIO-ECONOMIC CONTEXT

Societal challenges

Identified needs and conditions

External factors

Other interventions

IMPACT

Indirect impact

Direct impact

Sustainability

Coherence

INTERVENTION

Objectives

Inputs

Activities

Outputs

Relevance

Efficiency

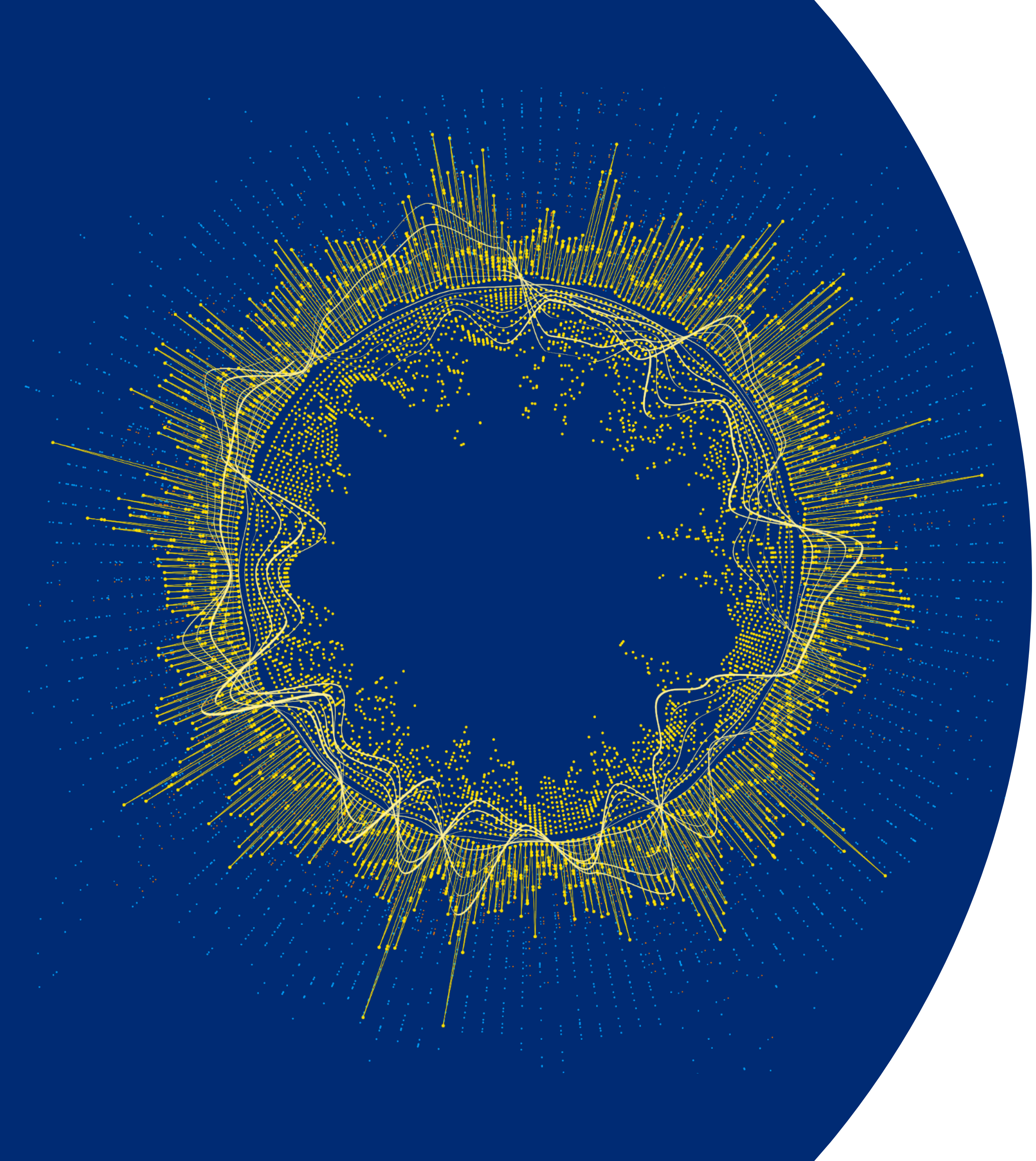
Effectiveness

Methods and data sources

Method	Description
Document analysis	Project plans, final reports, and other documentation were analysed in the evaluation. Reports were used to draft the survey questions.
Literature review	A literature review was conducted to get an in-depth understanding of the operating environment and the needs of SMEs.
Expert interviews	Expert interviews were used to deepen the understanding of the operating environment and the needs of SMEs. A total of 7 external experts were interviewed and a total of 5 experts from NCC-FI.
Data analysis	Financial support data was analysed to get an understanding of the distribution of the financial support.
Beneficiaries survey	A survey was sent to beneficiaries of the financial support programme to assess the direct impacts. The survey was also quantifying the findings of the project reports. Additionally, Eurostat data was used to compare the baseline security level of beneficiaries and companies in Finland. The survey was sent to all 50 beneficiaries and got a total of 44 responses.
Workshop	The evaluation organised a workshop for NCSC-FI staff and external experts to validate and further develop the findings of the evaluation.

Basic information on the financial support

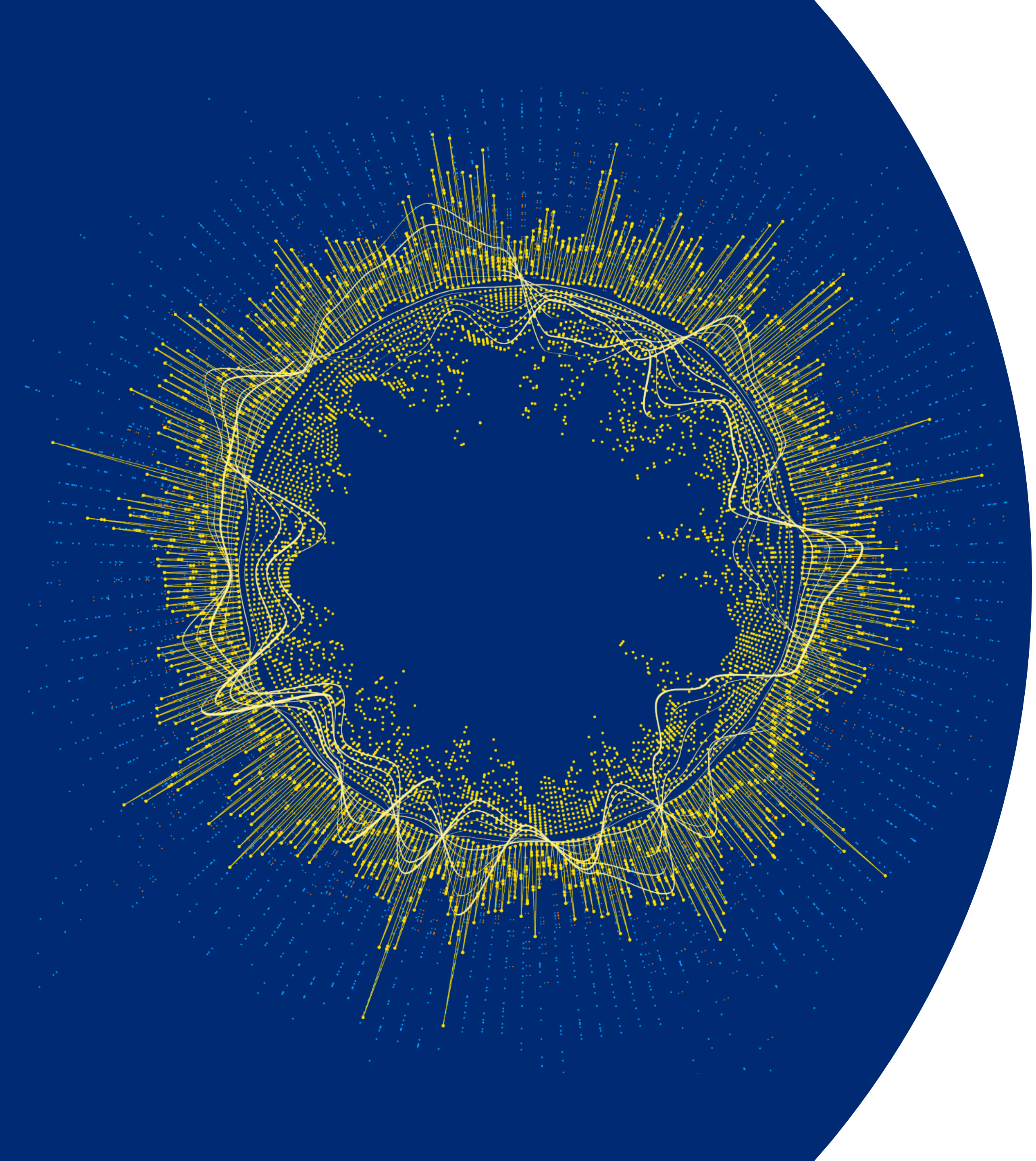
	Financial support by the National Coordination Centre
Objective	Support the adoption of state-of-the-art cyber security and information security solutions and innovations by companies.
Focus group	Micro and small- to medium-sized enterprises (SMEs) registered in Finland.
Financial support type	Grant type: De minimis aid. Maximum grant per applicant/project: EUR 60 thousand. Co-financing requirement: Minimum of 25%.
Time period	First call round open: 16.6.-18.6.2023, project implementation time: 16.5.2023-31.5.2024 Second call round open: 2.1.-1.3.2024, project implementation time: 2.1.-30.9.2024
Volume	Total financial support pool: EUR 2 million. Project support ranges from EUR 6,622 to EUR 60 thousand.
Beneficiaries	50 SMEs supported (2023 13/17 applications; 2024 37/170 applications).
Selection process	Applications that meet the eligibility criteria are scored according to relevance, implementation, and impact of the project as presented in the call for proposals document.
Monitoring and evaluation	A report on the use and impact of the support is required after project completion.



TRAFICOM
Finnish Transport and Communications Agency

4FRONT

Evaluation Findings

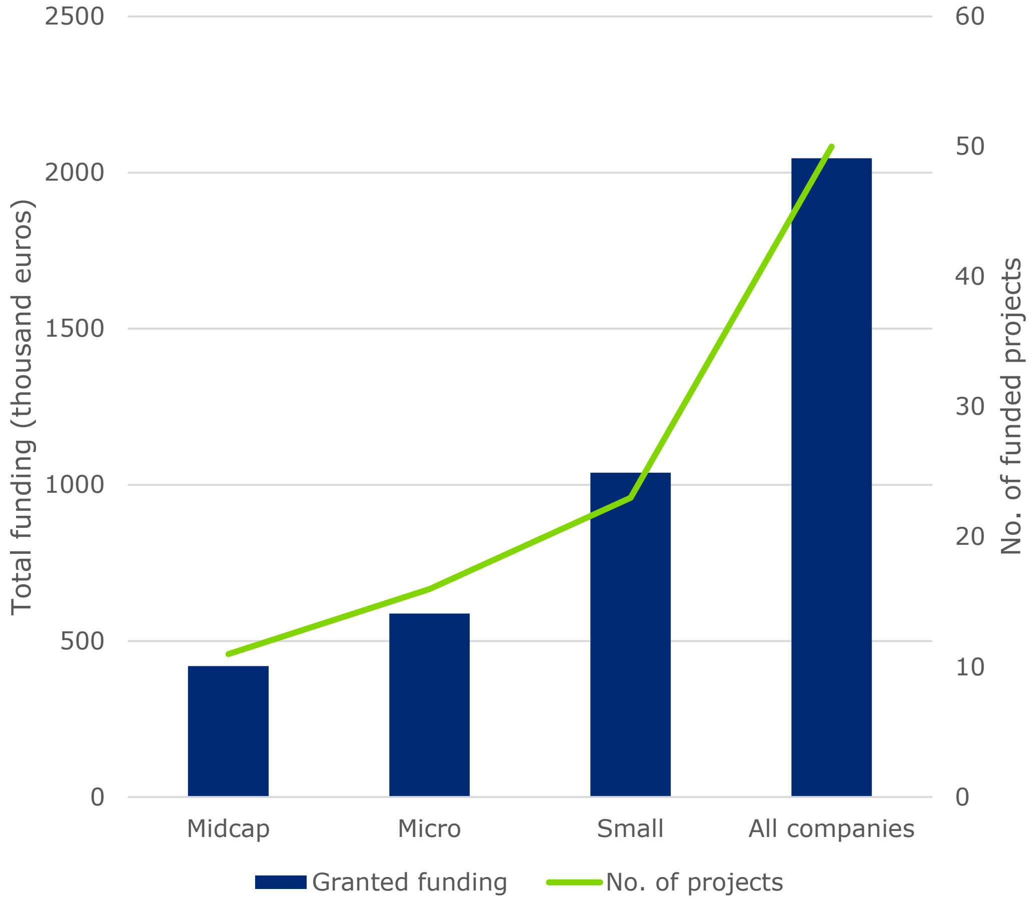


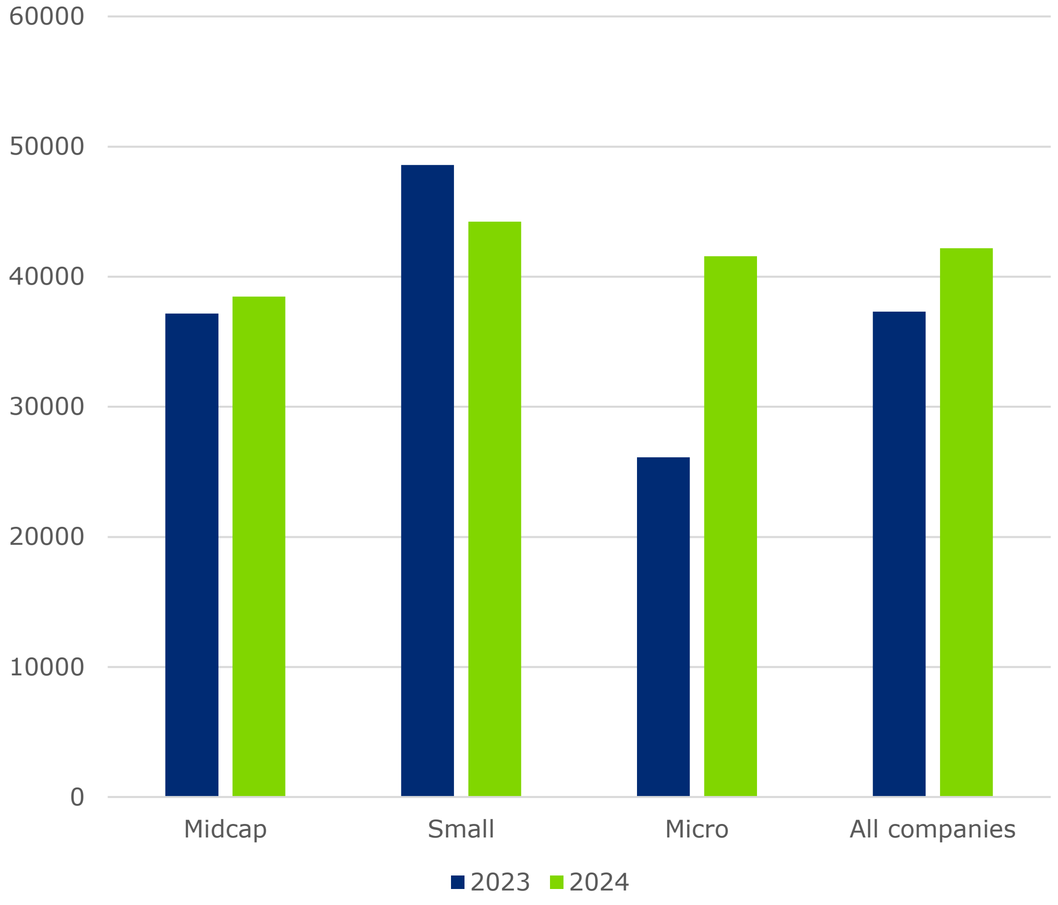
TRAFICOM
Finnish Transport and Communications Agency

4FRONT

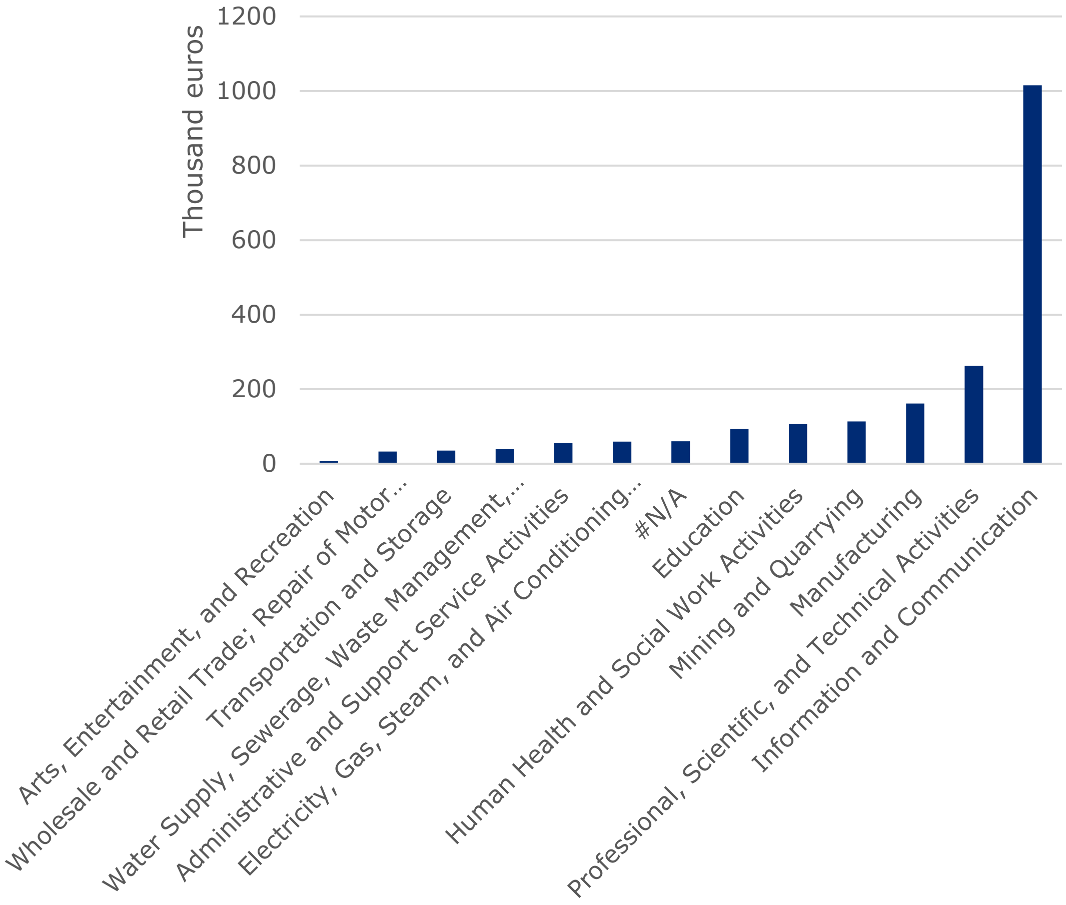
Distribution of financial support

Distribution of financial support

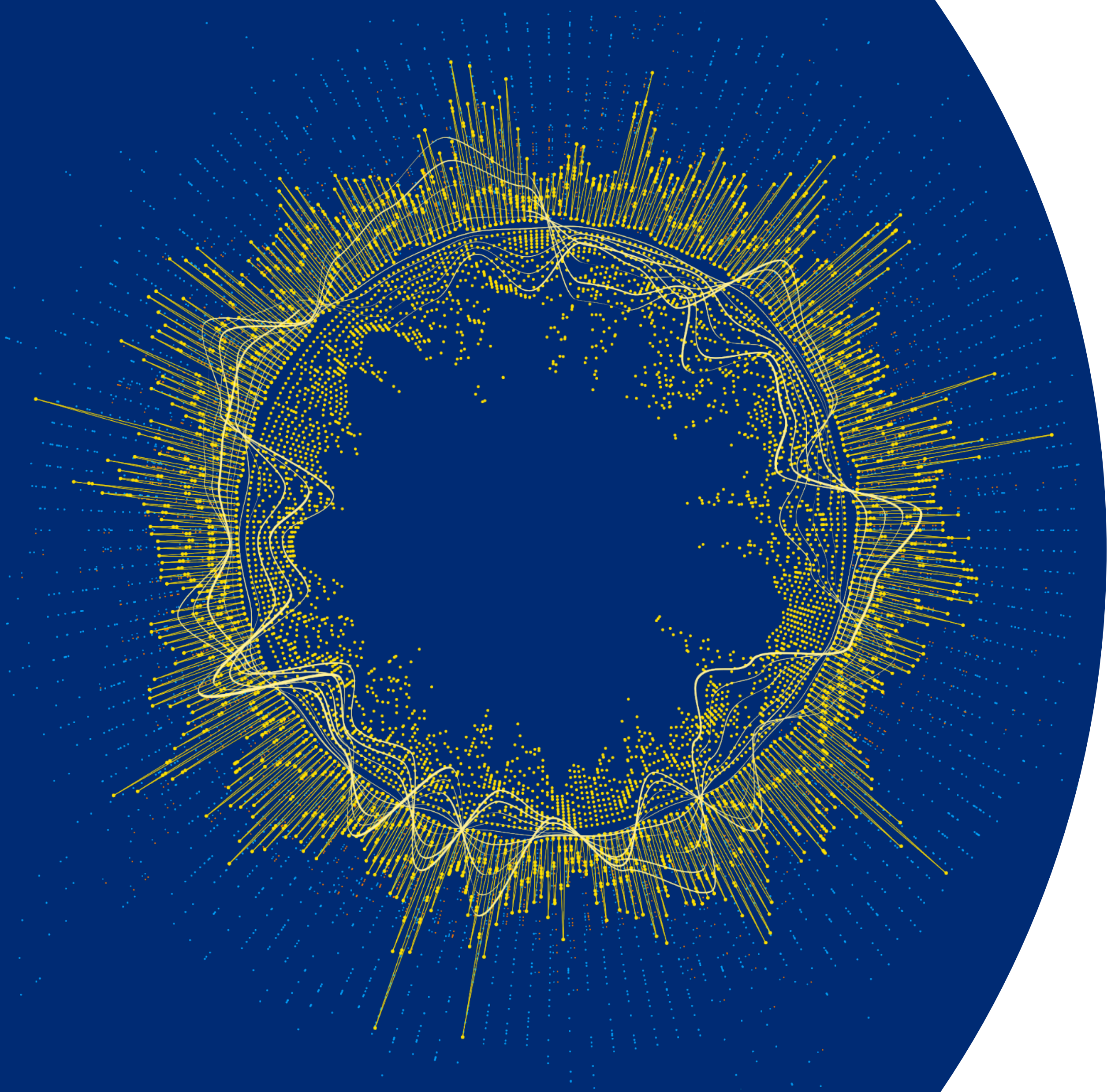




Sectoral distribution of the financial support



- Majority of the financial support was granted to companies operating in the sector of information and communications (ICT) (EUR 1 million).
- The second largest sector was professional, scientific and technical activities (PST) (EUR 0.26 million) and manufacturing (EUR 0.61 million).
- Within ICT sector, the most common subsector was software design and development and in terms of PST, the most common subsector were management consulting, mechanical and process engineering and patent offices.

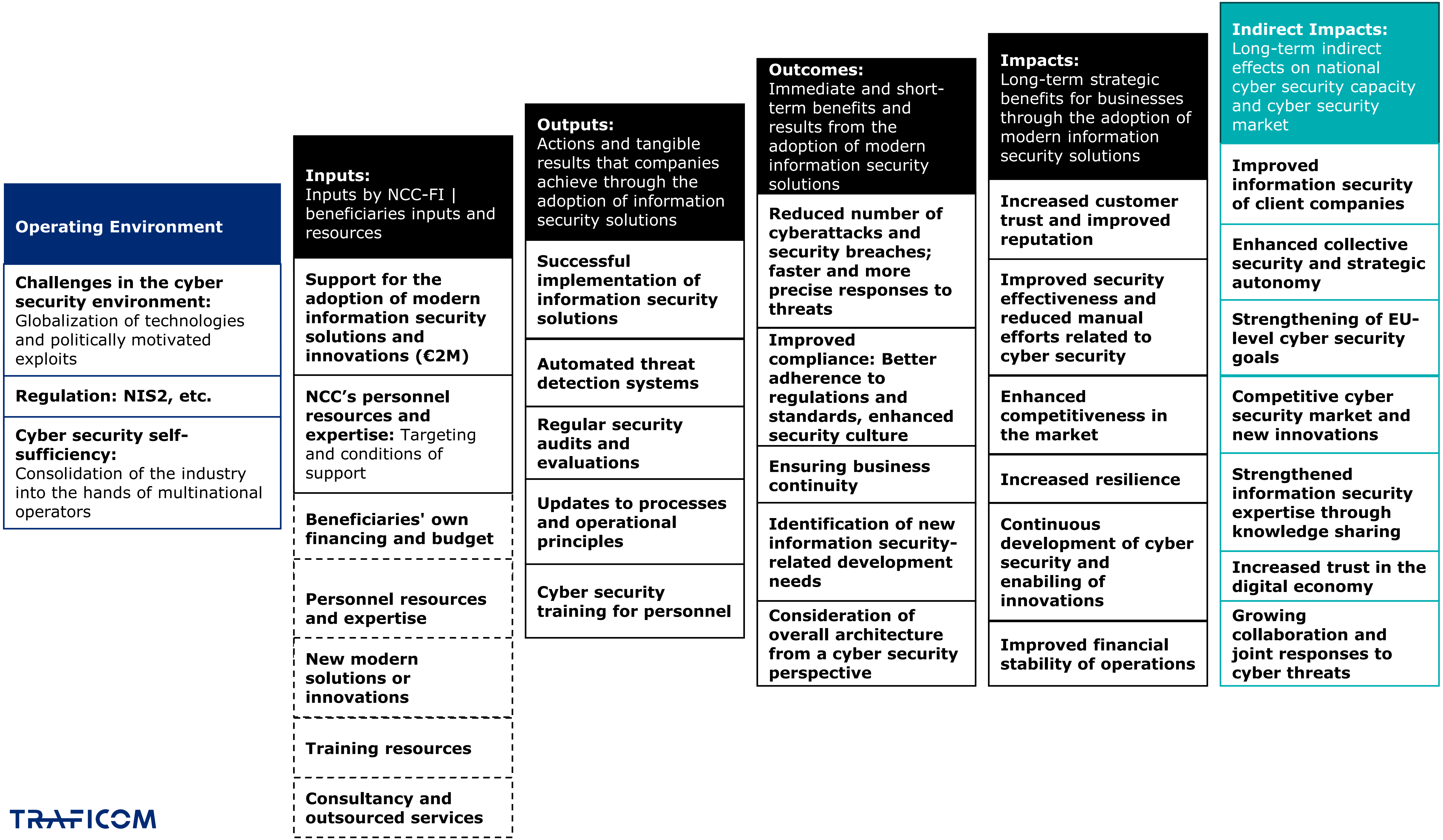


TRAFICOM

Finnish Transport and Communications Agency

4FRONT

Direct impact on beneficiaries of the financial support



Operating Environment

- **Challenges in the cyber security environment:** Globalization of technologies and politically motivated exploits
- **Regulation: NIS2, etc.**
- **Cyber security self-sufficiency:** Consolidation of the industry into the hands of multinational operators

Inputs: Inputs by NCC-FI | beneficiaries inputs and resources

- **Support for the adoption of modern information security solutions and innovations (€2M)**
- **NCC’s personnel resources and expertise:** Targeting and conditions of support
- **Beneficiaries' own financing and budget**
- **Personnel resources and expertise**
- **New modern solutions or innovations**
- **Training resources**
- **Consultancy and outsourced services**

Outputs: Actions and tangible results that companies achieve through the adoption of information security solutions

- **Successful implementation of information security solutions**
- **Automated threat detection systems**
- **Regular security audits and evaluations**
- **Updates to processes and operational principles**
- **Cyber security training for personnel**

Outcomes: Immediate and short-term benefits and results from the adoption of modern information security solutions

- **Reduced number of cyberattacks and security breaches; faster and more precise responses to threats**
- **Improved compliance: Better adherence to regulations and standards, enhanced security culture**
- **Ensuring business continuity**
- **Identification of new information security-related development needs**
- **Consideration of overall architecture from a cyber security perspective**

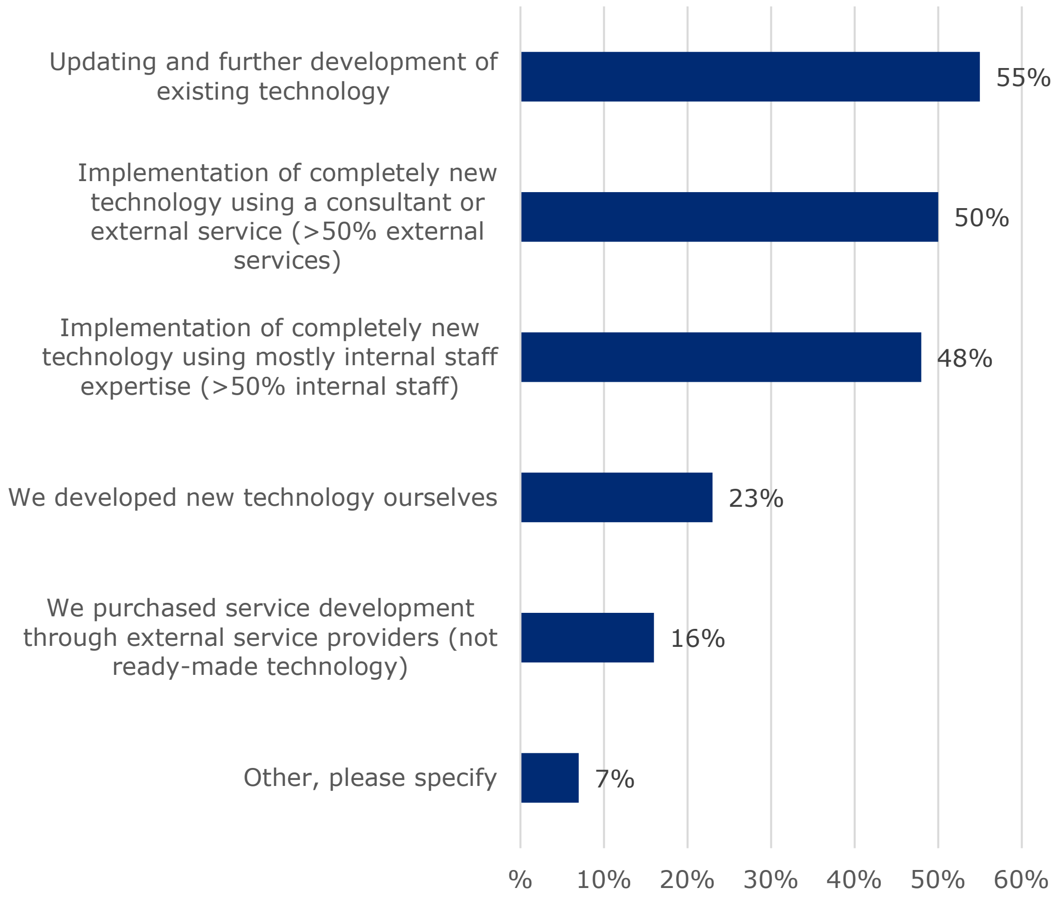
Impacts: Long-term strategic benefits for businesses through the adoption of modern information security solutions

- **Increased customer trust and improved reputation**
- **Improved security effectiveness and reduced manual efforts related to cyber security**
- **Enhanced competitiveness in the market**
- **Increased resilience**
- **Continuous development of cyber security and enabiling of innovations**
- **Improved financial stability of operations**

Indirect Impacts: Long-term indirect effects on national cyber security capacity and cyber security market

- **Improved information security of client companies**
- **Enhanced collective security and strategic autonomy**
- **Strengthening of EU-level cyber security goals**
- **Competitive cyber security market and new innovations**
- **Strengthened information security expertise through knowledge sharing**
- **Increased trust in the digital economy**
- **Growing collaboration and joint responses to cyber threats**

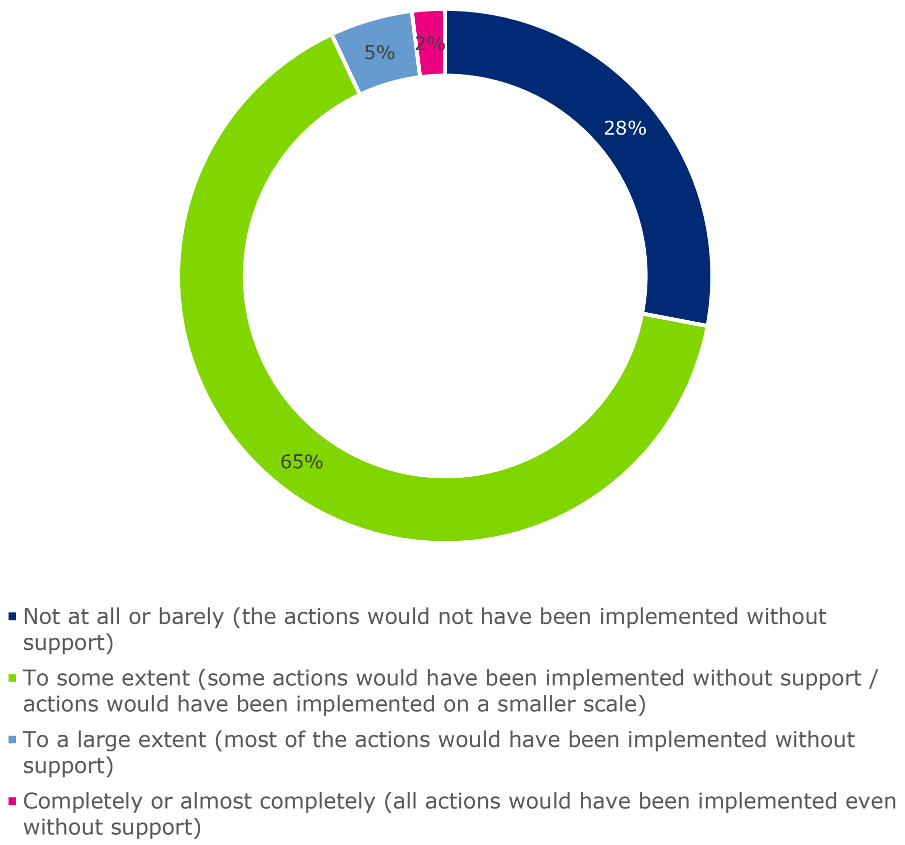
Activities and input



- The main aim for the financial support is to support micro, small and medium-sized enterprises to uptake state-of-the-art cyber and information security solutions and improve their capacity.
- A typical supported project allocated part of its financial support into purchasing services from specialised companies to assist in integration of the solution/innovation into their IT system. Most of the service firms were Finnish.
- The purchased solutions/innovations were typically provided by large multinational companies.

Question: How was the project implemented? (you can select multiple options). n=44 (N=50).

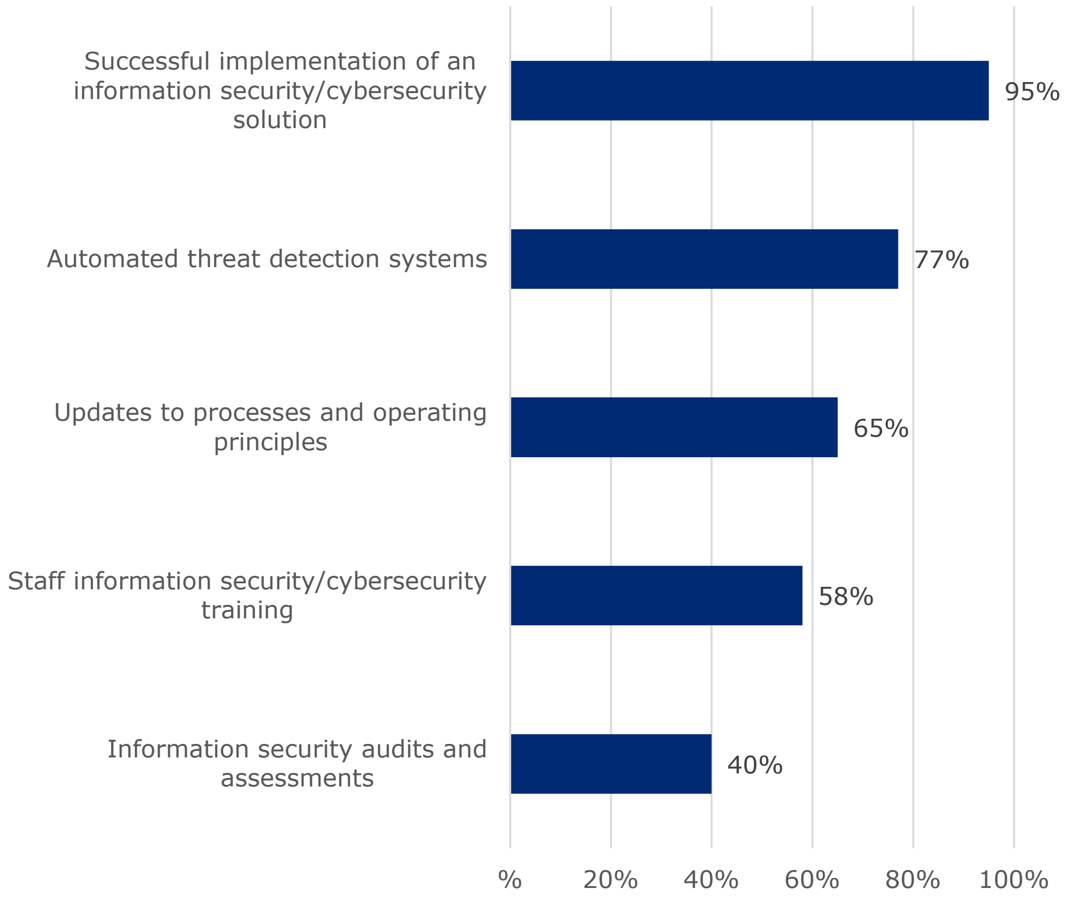
Additionality of the financial support



- According to the beneficiaries’ survey, the financial support was critical for the implementation of measures. 93 % stated that the measures would not have been implemented at all or only partially without the support.
- The support also significantly accelerated the implementation of the measures (73 %). 27 % reported that the financial support accelerated the uptake of technologies to some extent.

Question: To what extent would the actions implemented in the project have been carried out without support? n=44 (N=50)

Outputs of the projects



- Overall, the survey companies reported that the project goals were achieved very well (61 %) or fairly well (38 %).

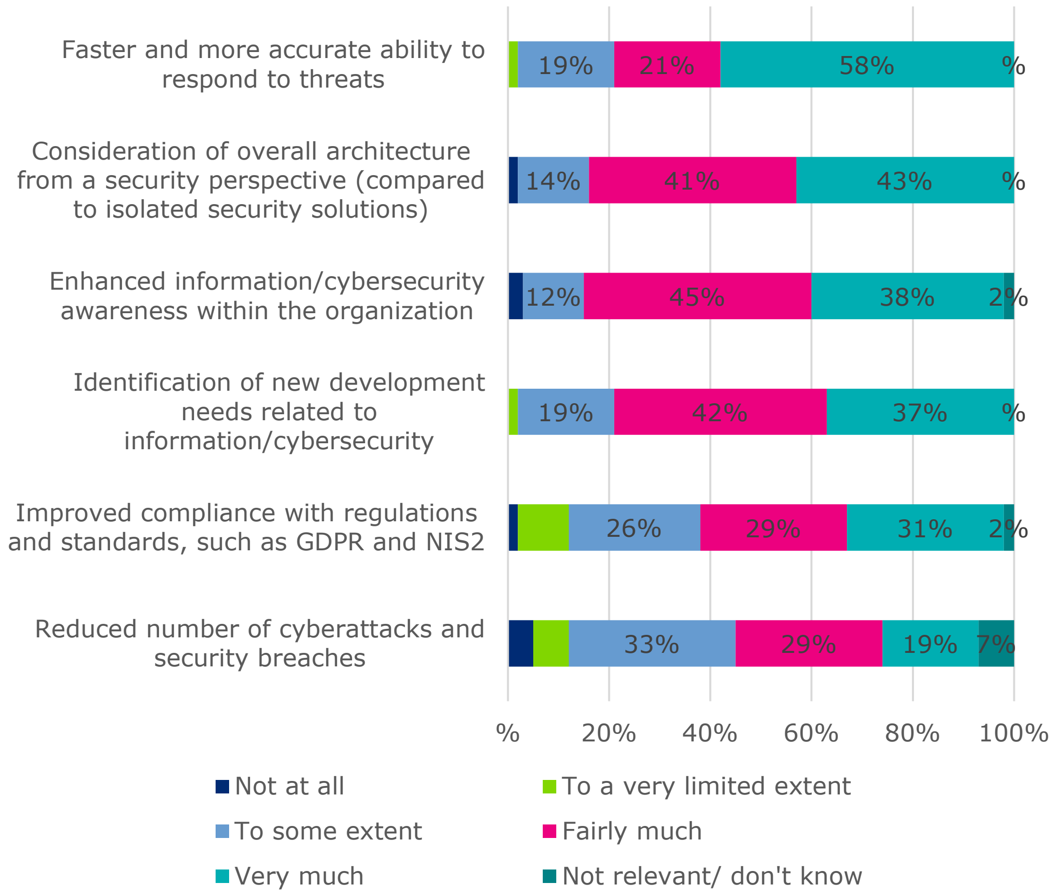
- The projects were reportedly very successful in terms of their main goal. Altogether 95 % of the respondents state that they successfully implemented and up took the technology they were planning to.

- In addition to up taking solutions and new technologies, the companies were reported to have taken actions to integrate cyber and information security holistically. This included activities on threat detection systems, updating processes and training staff.

- While the results regarding activities seem holistic and thorough, only 40 % stated that they organized information security audits and assessments during the project.

Question: What kinds of outcomes have been achieved in your company with the help of financial support? (You can choose multiple options) n=44 (N=50)

Short-term outcomes of the projects

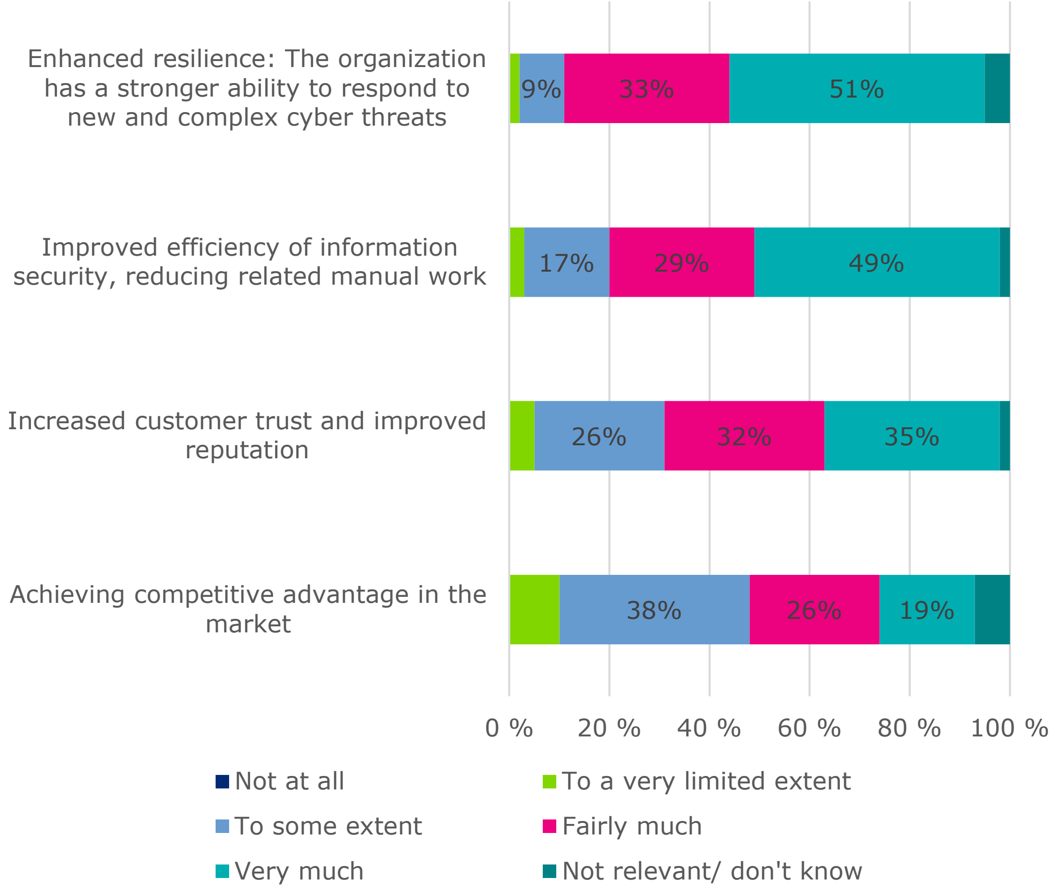


- In terms of short-term results, approximately 80 % companies are self-assessing that the project improved their ability to respond to threats, enhanced information security awareness across the organisation and allowed them to implement their security via overall architecture instead of isolated security solutions.

- 82 % reported that the project helped to identify new security related development needs, which is a good predictor of financial support’s long-term impact, and a mindset change within the beneficiaries. Approximately 60 % mentioned also, that they are better equipped to comply with regulations and standards (such as NIS2 and GDPR).

Question: To what extent has the organisation experienced (or are expected to experience shortly after the project's conclusion) direct and short-term benefits and outcomes from implementing information/cyber security solutions? n=44 (N=50)

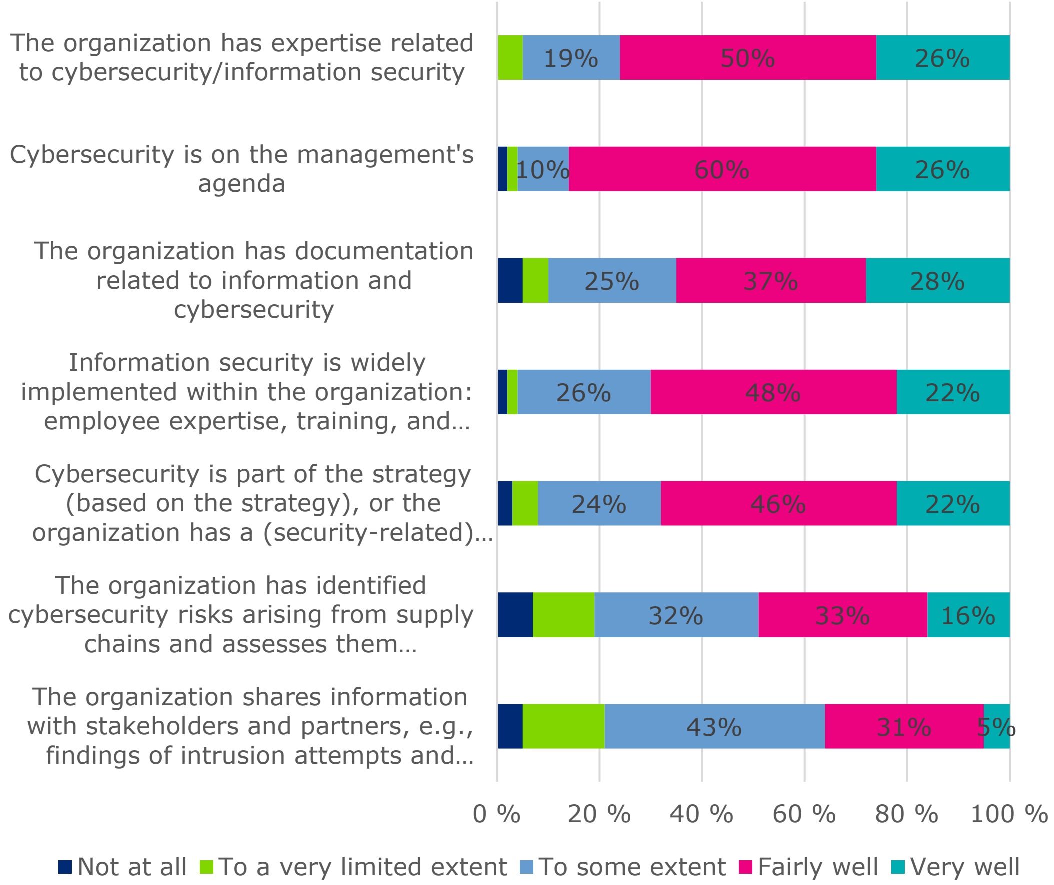
Anticipated impacts of the projects



- The main anticipated impacts were related to enhanced resilience and ability to respond to new and complex cyber threats (84 % very or fairy much) and improved efficiency of information security and reduced manual work (78 % very or fairly much).
- Many of the respondents saw also potential positive economic impacts, namely increased customer trust and improved reputation (67 % very or fairly much) and achieving competitive advantage in the market (45 % very or fairly much).

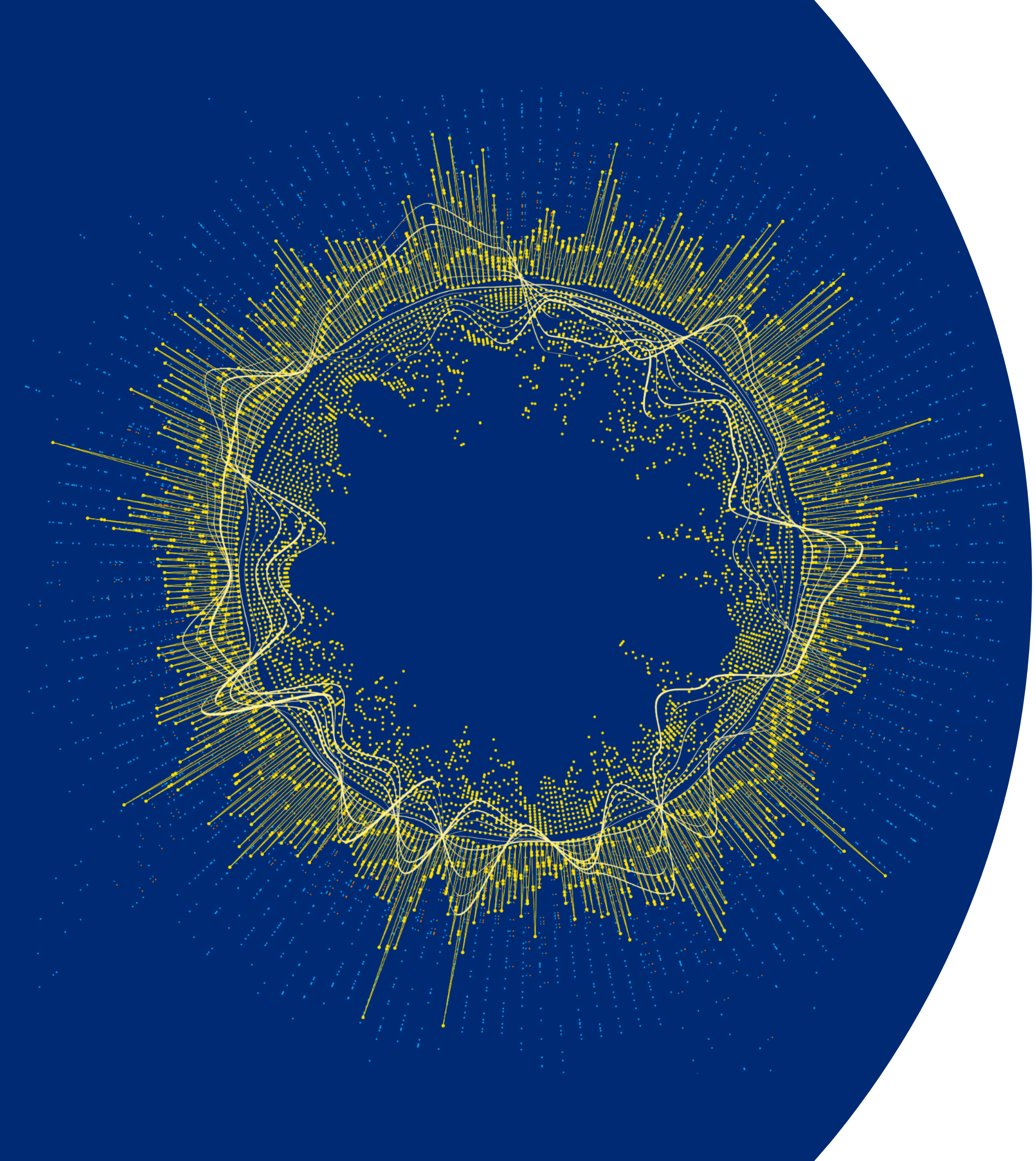
Question: To what extent has your organisation achieved or is expected to achieve the following long-term strategic benefits from the implementation of a state-of-the-art information/cyber security solution? n=44 (N=50)

Holistic approach in beneficiaries



- Raising the maturity level of cyber security requires not only implementation of solutions but also the enhancement of skills, practices, and information exchange across the entire organisation.
- As reported by the beneficiaries, the support has had positive impacts on embedding cyber security within organisations.
- For the majority, the project has advanced cyber security-related expertise (76 % very or fairly much) and elevated the topic more prominently on management agendas (86 % very or fairly much).

Question: To what extent has the project implemented with the support improved or advanced the following aspects in your organisation? n=44 (N=50)



TRAFICOM

Finnish Transport and Communications Agency

4FRONT

Indirect impact of provided financial support

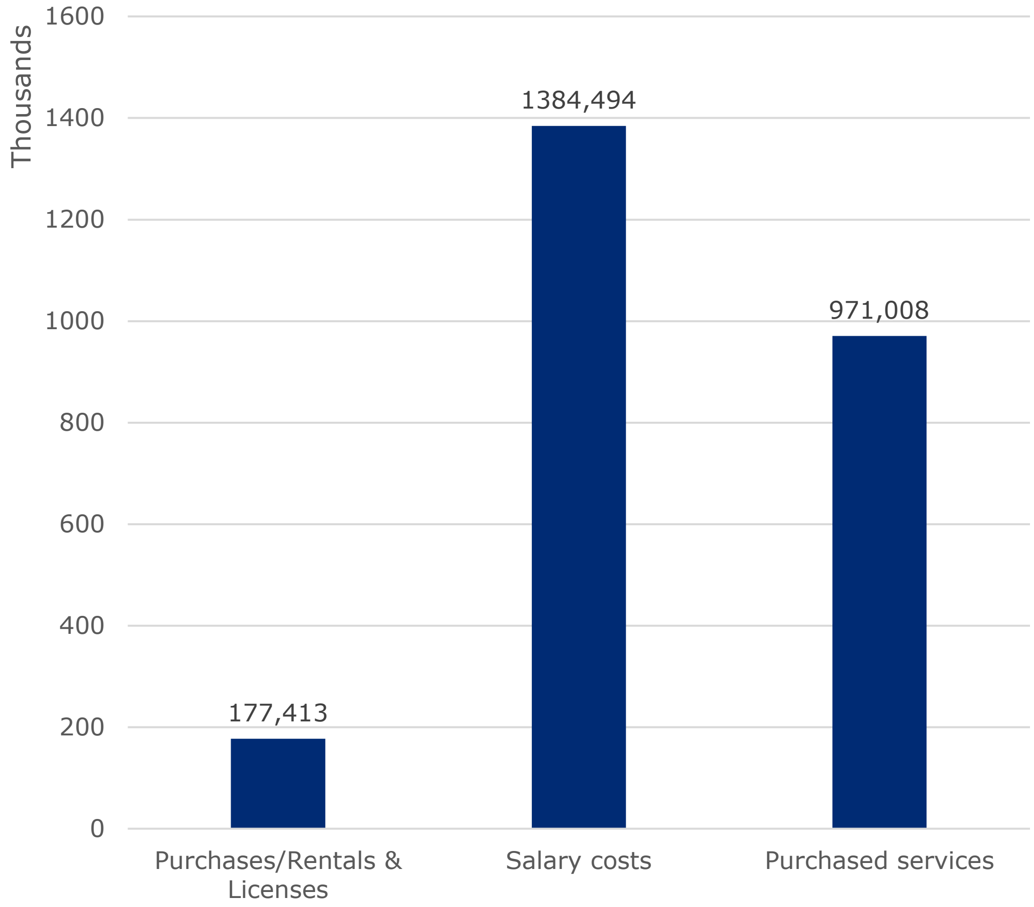
Current state and needs of Finnish cyber security environment

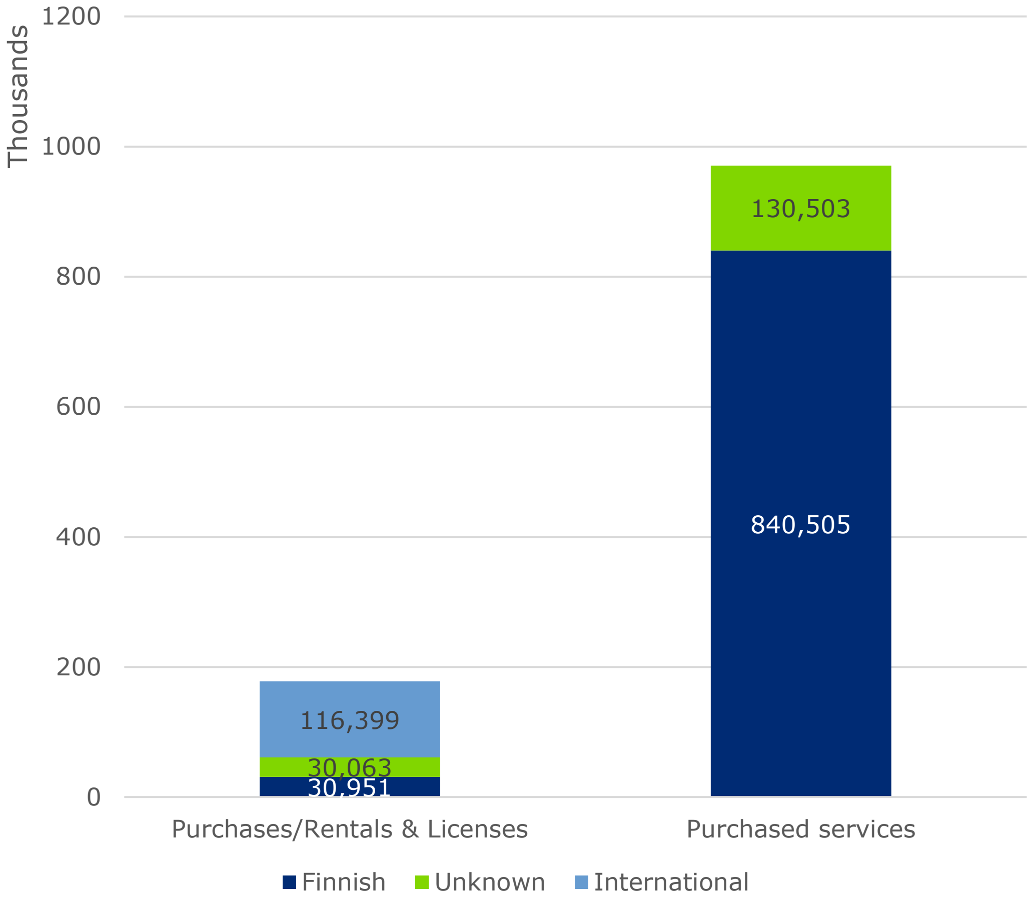
- Finland's cyber security environment has become more challenging, dynamic, and the motivation factors for attackers increasingly diverse. Severe attacks are more frequently large-scale and prolonged APT (Advanced Persistent Threat) attacks.
- Despite the challenges in the cyber security environment, Finland's corporate sector and broader society have traditionally achieved high international rankings in cyber security.
- However, this situation may be changing, and Finland's lead narrowing. The primary reason for this is the globalisation and platformisation of technologies being used.
- The growing significance of cyber threats impacts the entire society, businesses, and individuals due to digitalisation and technical advancement. Each entity's so-called attack surface is expanding and diversifying. Networked operating models increase the likelihood that successful attacks on one component will cause disruptions across the entire chain.

Systemic preparedness is increasingly important

- National risk management capacity includes production capacity (development side) and actions in other organisations (adoption of solutions and innovations).
- On the adoption side, Finland's performance is very good compared to other nations. It boasts high competence and well-organised structures. **However, the issue is that the level of cyber security across organisations is highly uneven**. Especially SMEs are experiencing bottlenecks related to financing and skills to implement up-to-date security systems.
- As the modern-day risks are often systematic, it is not sufficient for national risk management capacity that only critical players are secured.
- For the SMEs to meet the required security levels, the traditional (firewalls, antivirus etc.) solutions are no longer sufficient. While state-of-the-art technologies are important, the SMEs should adopt also state-of-the-art strategies on management models. State-of-the-art management models can be based on e.g., standards like ISO27001.

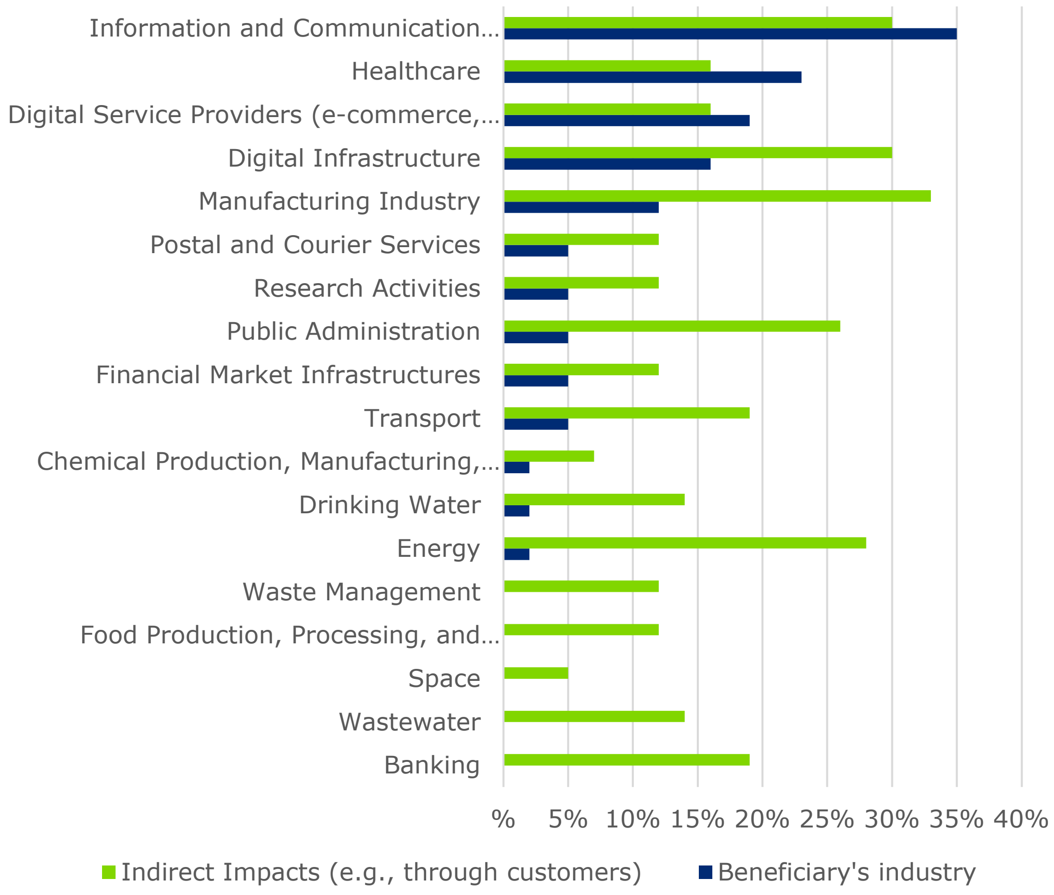
The analyzed project reports reveal that the beneficiaries were buying international solutions and national services for integration and other support activities.





Analysis is based on project reports.

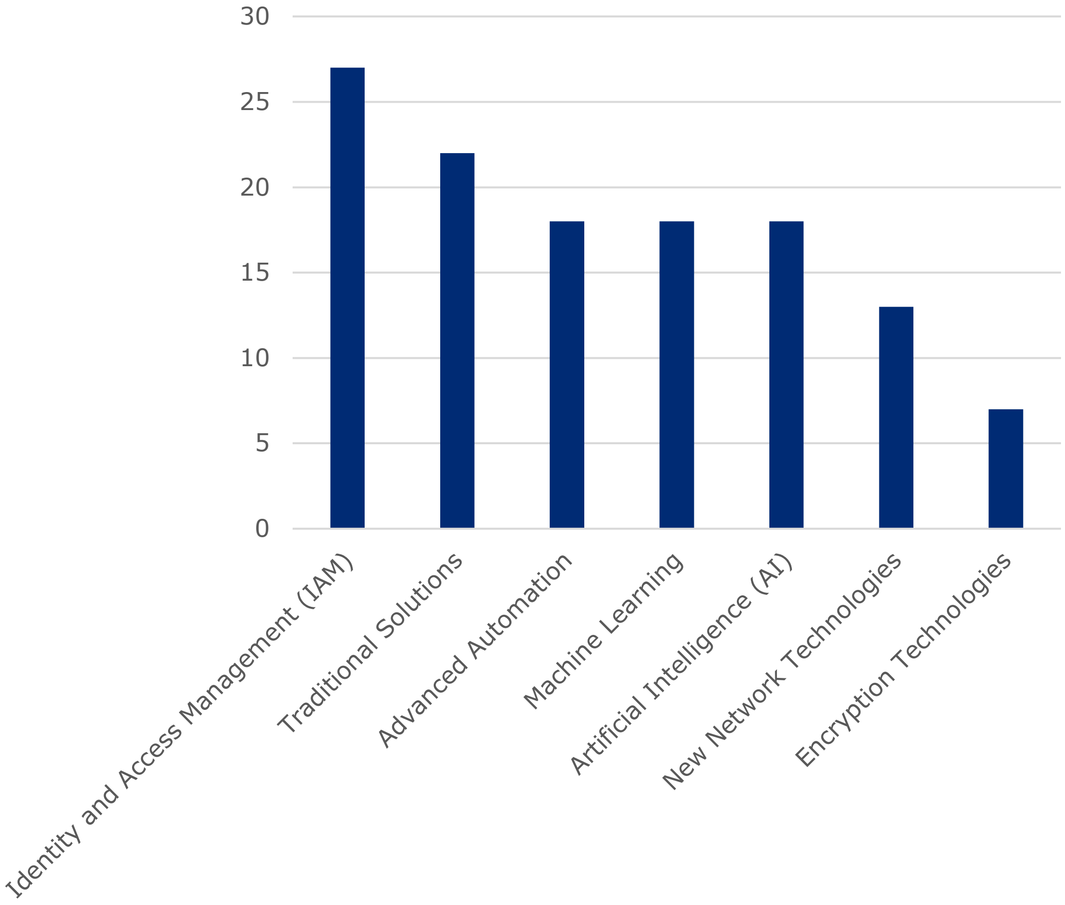
Impact on other companies



- Critical sectors form the backbone of society. The cyber security of companies operating in these sectors directly affects societal functionality, including supply chain reliability and the management of disruptions.
  - SMEs, can be linked to critical organisations though their clients or supply chains.
- The financial support does not have criteria for targeting support to critical or other sectors.
  - The financial support has been mainly utilised on the information and communication technology sector, health care, digital services and digital infrastructure.
  - The beneficiaries have linkages (e.g., via customers or supply chains) to sectors, that are considered in NIS2 regulation as highly critical, such as energy. This way, the financial support may have indirect positive spillover effects to critical sectors and impact beyond the beneficiaries themselves.

Question: Does your organisation 1) operate in any of the following industries, or 2) indirectly impact the cyber security of organisations in these industries (e.g., through a customer relationship)? n=44 (N=50). The classification is based on the categorisation of critical sectors outlined in the NIS2 Directive.

The projects have implemented various state-of-art solutions and innovations



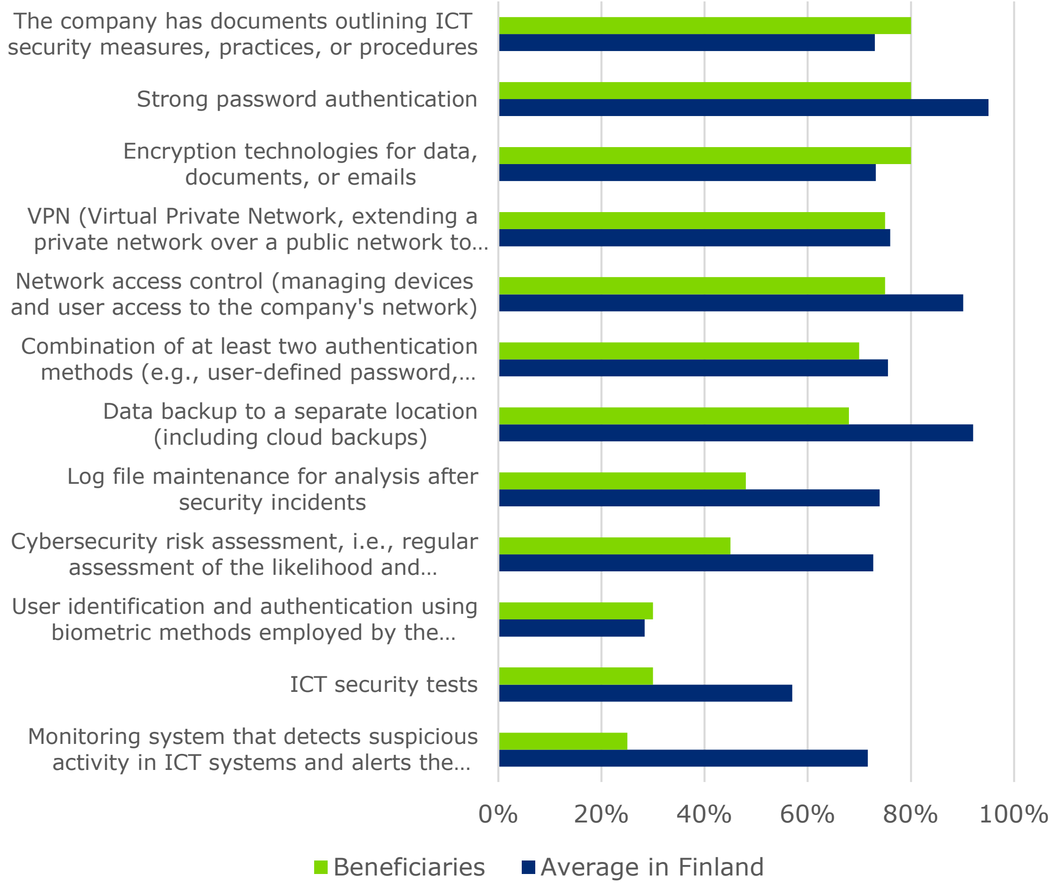
- In terms of national preparedness, it is no longer sufficient that companies acquire point solution services and technologies to specific situations that meet immediate needs but rather consider the whole architecture. For the SMEs to meet the required security levels, the traditional (firewalls, antivirus etc.) solutions are no longer sufficient.

- Acknowledging that some of the nation-wide cyber security issues stem from outdated technologies in use, the financial support was targeted to up take of state-of-the-art cyber and information security solutions and innovations.

- Majority of the technologies were indeed state-of-the-art, while there were some traditional solutions involved as well.
  - Most of the projects were up taking more than one solution and some solutions may involve more than one the following categories.

The classification is based on the technologies or solutions mentioned in project plans. One project plan may involve multiple technologies and categories. Only projects that received financial support are included in the classification.

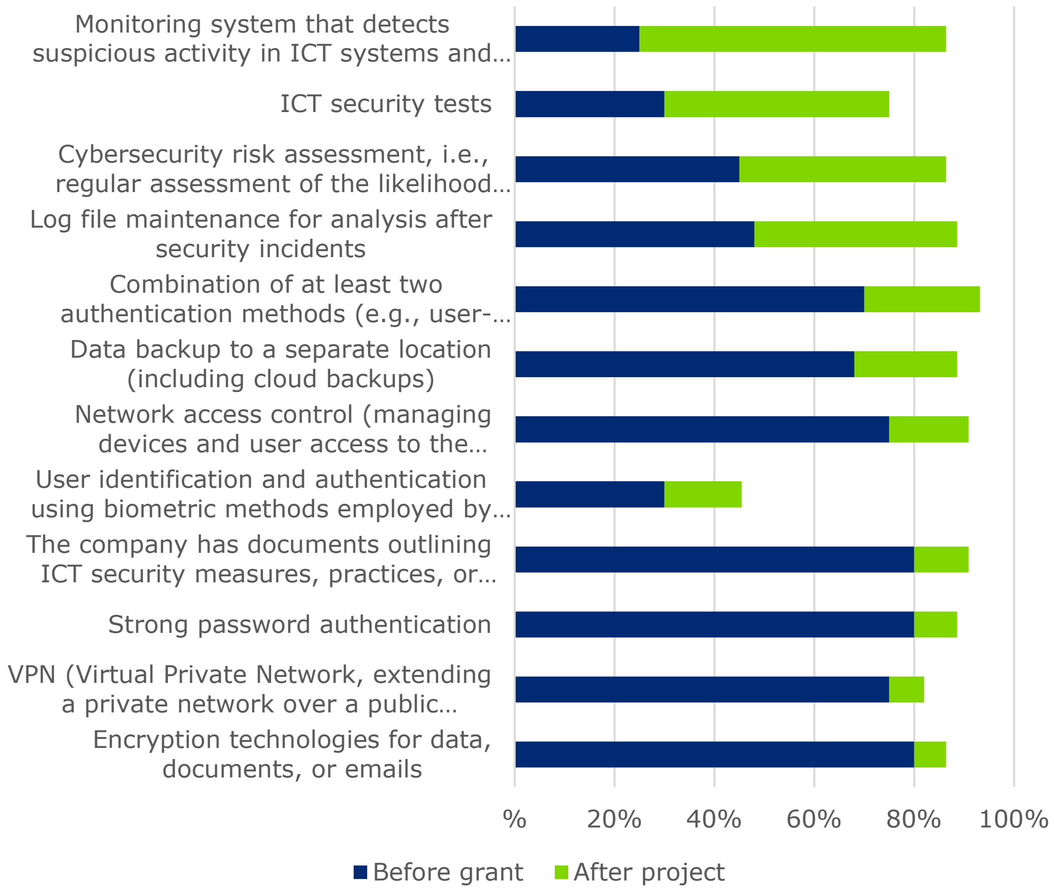
NCC-FI support has focused on companies that are in need for technological upgrade



- From the perspective of nation and EU wide cyber competence, it is crucial that improvements in cyber security are being implemented in all businesses, not only the frontrunners.
- The evaluation was comparing the beneficiaries' survey results to Eurostat's statistics on ICT security measures on Finnish companies.
- The beneficiaries were lagging in several measures, most drastically in monitoring systems, ICT security testing, and user authentication solutions.
- However, based on the survey results, the projects improved adoption of those security measures that the companies were lacking before the financial support.

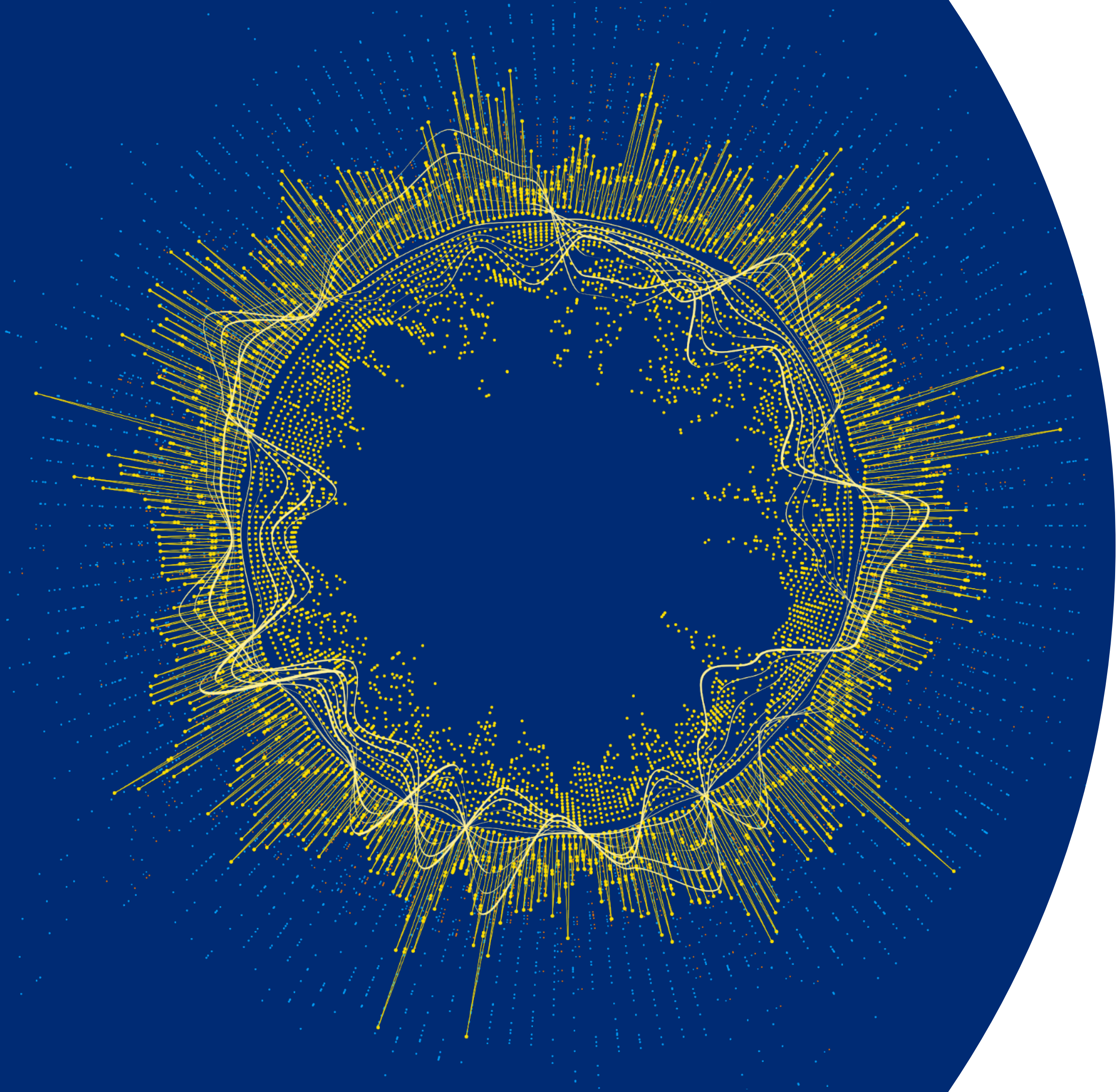
Question: Which of the following information/cyber security-enhancing measures were in use before receiving the support? n=44 (N=50); Finnish average is based on ICT, and professional, scientific, and technical activities and manufacturing sectors, which were also the most common sectors among the support recipients. Source: Eurostat, ICT security in enterprises.

The beneficiaries were improving adoption of those measures they were lagging before the funding



- Largest improvements were in adopting monitoring systems, ICT security tests and risk assessments
- After the financial support, the beneficiaries had on average more ICT security measures in use comparing to their Finnish counterparts (see previous slide).

Question: Which of the following information/cyber security-enhancing measures were in use a) before and b) after receiving the support? n=44 (N=50);



Finnish Transport and Communications Agency

Conclusions

Direct and short-term impact of the financial support

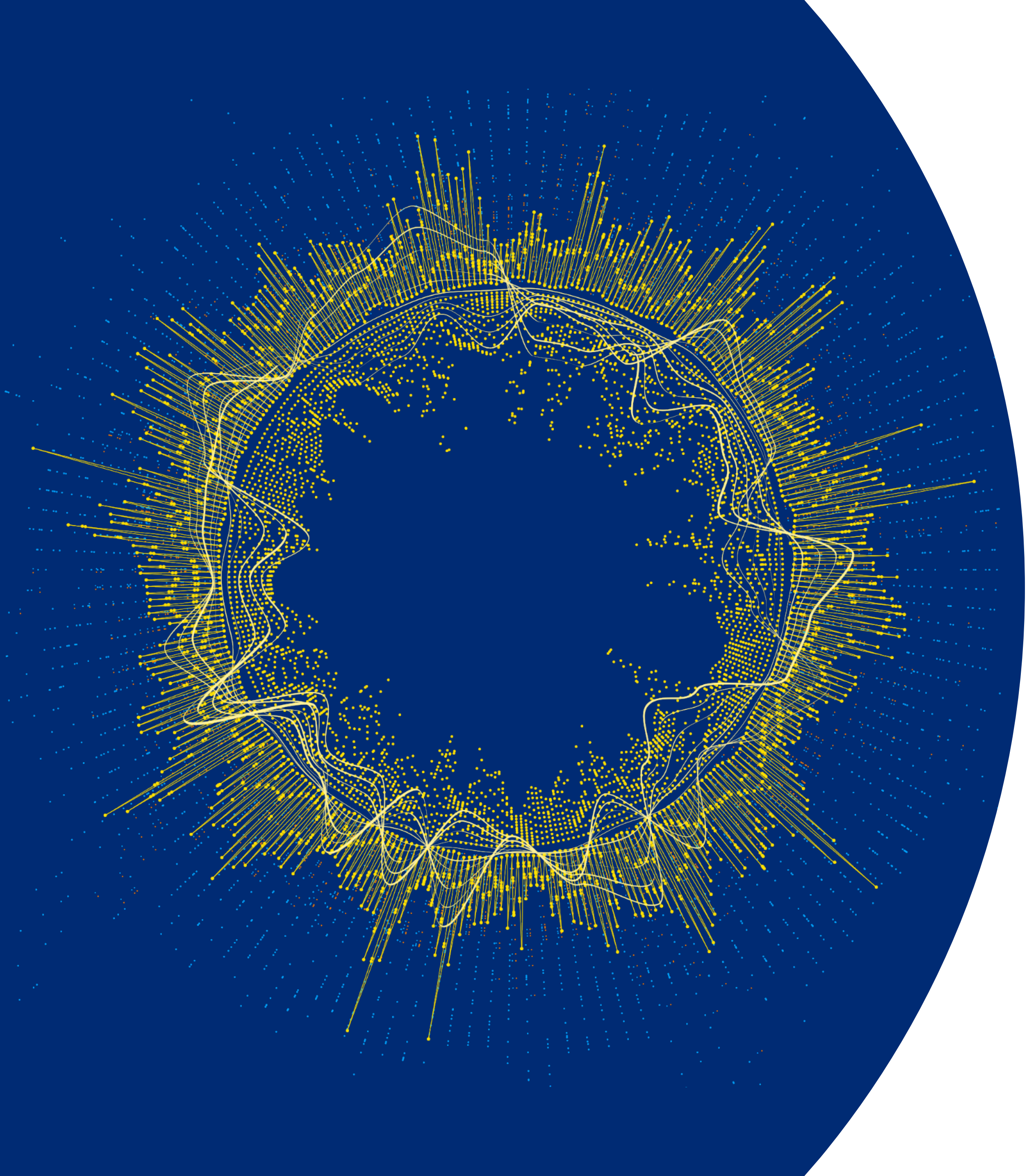
- The financial support has well fulfilled its purpose and its direct impact to beneficiaries can be considered high.
- Technically all projects (95 %) stated that they have successfully implemented their technology upgrading and reached the project goals. Besides adoption of the technology, the companies have organized training for staff and developed internal processes and documentation. The companies are also reporting increased resilience against cyber-attacks.
- Some companies reported that during the course of the project, they had also identified additional security issues to be addressed.
- Furthermore, beneficiaries were conducting also actions that were not primarily targeted in the call for proposals document, such as trainings for staff and sharing of information and experience with other companies. This is an indication that the financial support has triggered some behavioral changes and new practices with longer-term impacts. Staff training and peer-to-peer knowledge sharing are eligible costs for projects.
- There is a clear additionality of the financial support. Most beneficiary companies reported that they would have not implement the project at all, or in a similar scale without having received the financial support and that the financial support had sped up their actions to improve cyber security. In particular SMEs and micro enterprises are facing investment and skills barriers with regard to cyber security upgrades. The financial support has managed to alleviate both. The necessary expertise was usually procured from external service providers.
- All in all, it appears the support has met the needs of the beneficiaries to a great extent. The recipients reported that the amount of the financial support was sufficient and in general, the terms, conditions and application processes were appropriate. The only issue was regarding the timeline, which was considered too tight by most beneficiaries.

Short and long-term indirect impact

- It appears that the support has had, at least to some extent, positive impact on beneficiaries’ competitiveness more generally. Many companies (80 % said fairly or very much) report that the projects have made their security functions more cost-effective, had a positive impact on their reputation and customer trust (70 % said fairly or very much) and have given some competitive advantage also in the market (50 % said fairly or very much). There is however little concrete evidence on the scale of this impact.
- The financial support has also generated some additional demand for the provision of IT services with the volume of around EUR 0.9 million. Comparing this to the size of the domestic service market (~EUR 1.3 billion), this impact is quite small and rather temporary. The purchased technological solutions were mainly those provided by international large-scale companies. The demand was increased by 180 000 euros during the project time span, but as most of them are license based, the lifetime cost will be higher.
- As the state-of-the-art IT systems are strongly interconnected, also cyber security upgrades generate positive spillovers to other companies (e.g. to collaborators, subcontractors, clients). Typically, particularly smaller enterprises have lower capacity to address security issues. This network effect is both impacting other companies and improving the overall capacity to address security issues.
- Based on the survey and in reflection to Eurostat statistics, the NCC-FI financial support beneficiaries represent those industry sectors that were using overall less ICT security measures than companies on average in Finland before the financial support. This suggests that the NCC-FI support was granted to companies that are in need for technological upgrade.
- Considering national cyber capacity, there is a need for companies to share their cyber threat information and best practices with each other. Some of the beneficiaries were reporting that they started to share information during the project and many of them understood the benefits of doing so. However, more work could be done to incentivize companies to share information and collaborate in larger scale.
- From the perspective of Finnish and EU-wide cyber self-sufficiency, there is a threat that current solutions and innovations are predominantly made outside EU. The solutions that were adopted in the projects were largely international solutions. While it might be problematic to directly mandate the support to nationally produced solutions, there is room for sharing information and knowledge about native options.

Proportionality and appropriateness

- It seems clear that the limited volume (EUR 2 million) of provided financial support is not enough to address the cyber security challenges of Finnish enterprises at large. The volume is appropriate either as a targeted support and incentive to address certain identified challenges.
- The grant size (max EUR 60 thousand) could be equally effective in a slightly smaller form (e.g. EUR 20 thousand), thus allowing for more grants to be delivered. This could increase the impact and spread awareness. Overall, the companies were reporting that the individual grant sizes were sufficient for implementing the project.
- The type of financial support (grant-based co-financing) is typical and probably the most suitable form of financial support for these kinds of investments by companies. In particular, when Traficom also provides alternative voucher-type of financial support separately. Other possible forms, such as tax incentives or loan financial support would be more difficult to administer, target (tax incentives) and to apply for, and would probably better suited for larger and longer development projects with technological risks to be shared.
- Experience from other evaluation suggest that financial support is more effective when complemented with non-financial support, in particular technical assistance or professional guidance. This would appear a relevant option to consider in the case of cyber security too, where technological choices play an important role in system upgrades.



TRAFICOM

Finnish Transport and Communications Agency

4FRONT

Recommendations

Recommendations

1. There appears further need to support the upgrading of cyber security solutions of Finnish companies with financial incentives. NCC-FI should aim to continue its efforts to this end and pursue relevant financial support for it from European and national sources.

2. The effectiveness of the instrument could most likely be increased by decreasing the size of individual grants, while expanding the number of given grants. This would widen the reach of support to additional beneficiaries.

The support has been very attractive and not all applicants have received financial support. In terms of national cyber security capacity, it is important to ensure that all businesses, also the non-critical ones, have sufficient security level and are prepared to meet the necessary regulations (NIS2). Hence, there is a need to raise the awareness, competence and cyber security level of the business sector, as a whole.

3. The instrument should better support holistic approach to cyber security and encourage companies to take actions beyond adoption of technology, e.g., training staff, conduct company specific risk assessments, exchange information and collaboration with other companies regarding cyber threats and best practices.

4. The financial support should be complemented with non-financial support, such as technical guidance and sharing of good (process) practices, to enhance its effectiveness. In particular, the lesson and practices from other NCCs countries should be systematically collected and applied.

4FRONT

TRAFICOM

Finnish Transport and Communications Agency

NCC-FI

FINLAND NATIONAL COORDINATION CENTRE FOR CYBERSECURITY

The evaluation report is available on Traficom’s website traficom.fi

Contact:
ncc-fi@traficom.fi

National Coordination Centre Finland (NCC-FI)
National Cyber Security Centre Finland (NCSC-FI)
Finnish Transport and Communications Agengy Traficom