Cyber Survey of Finnish Sectors 2022

National summary report

Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency

Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency

www.huoltovarmuuskeskus.fi

Security of supply refers to society's ability to maintain the basic economic functions required for ensuring people's livelihood, the overall functioning and safety of society, and the material preconditions for military defence in the event of serious disruptions and emergencies.

The National Emergency Supply Agency (NESA) is an organisation operating under the Ministry of Economic Affairs and Employment of Finland. It is tasked with planning and measures related to developing and maintaining security of supply.

The National Emergency Supply Organisation (NESO) is a network that works together for the good of Finland's operating capability and the security of supply necessitated by it. It includes the National Emergency Supply Agency and its Board of Directors, the National Emergency Supply Council and the sectors and pools of different industries. The NESO also engages in cooperation with regional actors, such as Regional State Administrative Agencies, municipalities, cities and regional committees.

Publisher: The National Emergency Supply Agency
Prepared by: The National Emergency Supply Organisation's Digital Pool and Accenture Oy
Images: GettyImages
Layout: LM Someco Oy
Year of publication: 2023
ISBN: 978-952-7470-25-1

Sisältö

1 Introduction

The Cyber Survey of Finnish Sectors was a follow-up to a previous survey carried out in 2019–20. Both surveys were part of the National Emergency Supply Agency's Digital Security 2030 programme (DT2030). The objective was to provide essential basic information for allocating the programme's investments.

The survey was carried out by assessing the cyber maturity of a total of 121 actors. The actors included in the survey were selected with the aim of producing a broad sample of different sectors and different organisations within sectors. The total number of sectors represented in the survey was 12. The participants were selected with the help of the National Emergency Supply Organisation's (NESO) sector-specific pools and comprised a comprehensive sample of security of supply chain actors with different profiles, organisational sizes, operating areas and business models.

The core finding of the survey was that the maturity of the companies and organisations assessed was at a good basic level (3.00), but there was a great deal of variation between sectors and individual companies. In addition to this, it was found that the threat and risk landscape was changing dramatically, with nearly all participating organisations having noticed an increase in cyber activities.

This report summarises the key areas for improvement and main observations of the sector-specific reports, which were prepared based on the results of the survey during 2022. The actors participating in the survey were also provided with their own and sector-specific results. In addition to this, the sector-specific results were also distributed to parties responsible for the development of operations, such as the NESO's pools.

The survey was commissioned by the Digital Pool and carried out by Accenture's information security consultants during 2022. The work was also supported by a large number of sector experts.

The cyber maturity of the different sectors and companies of the National Emergency Supply Organisation has been examined in several different ways over the years. This particular survey was the second of its kind. These types of surveys will be carried out at regular intervals in future to monitor the development of cyber maturity and provide information that promotes development to Finnish organisations.

[1]https://www.huoltovarmuuskeskus.fi/en/organisation/the-national-emergency-supply-agency/programmes/digital-security-2030

2 Management summary

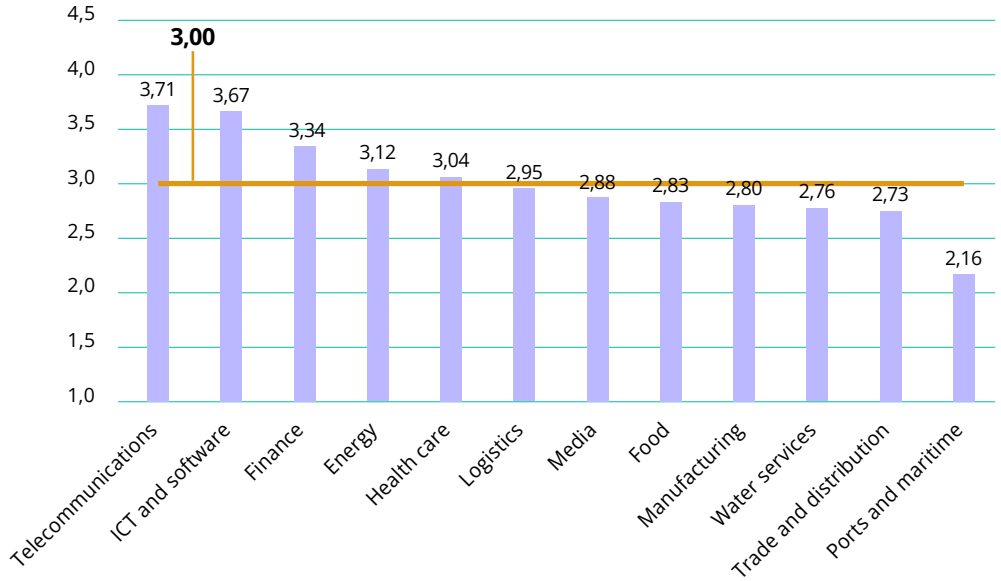
The Cyber Survey of Finnish Sectors 2022 report includes the results of cyber security maturity assessments, analysis-based recommendations and conclusions for 12 sectors. The main observations were:

- Changes in the threat and risk landscape in 2022 have added cyber security to the agendas of management groups that have not examined cyber security situational awareness on a regular basis in the past.
- Factors that were identified as increasing the maturity of an organisation included business and risk-based development of cyber security, management systems based on standards and smooth communication between those responsible for cyber security and the executive management of the organisation.
- Factors that were identified as reducing the maturity of an organisation included lack of strategic planning, a reactive approach to threats and risks that have become critical and lack of risk management practices.
- The identification of partner networks, whole supply chains and dependencies requires development in all sectors.
- The cyber preparedness of organisations is affected by the impression of how attractive the organisation is in the eyes of cyber criminals.
- Events that have a significant impact on the security environment, such as geopolitical changes in neighbouring areas, or cyber attacks that garner a great deal of public attention, such as the Psychotherapy Centre Vastaamo data breach, raise the cyber security awareness of organisations temporarily, but long-term development requires regular management reporting practices.
- The talent shortage plaguing the cyber security industry is affecting several organisations. Addressing the issue requires measures at many levels.
- Active engagement with stakeholders and the sharing of threat information are not directly reflected in organisations' maturity levels. Organisations have grown better at recognising threats and risks, but often fall short of fully utilising information obtained due to a lack of expertise, personnel or time.

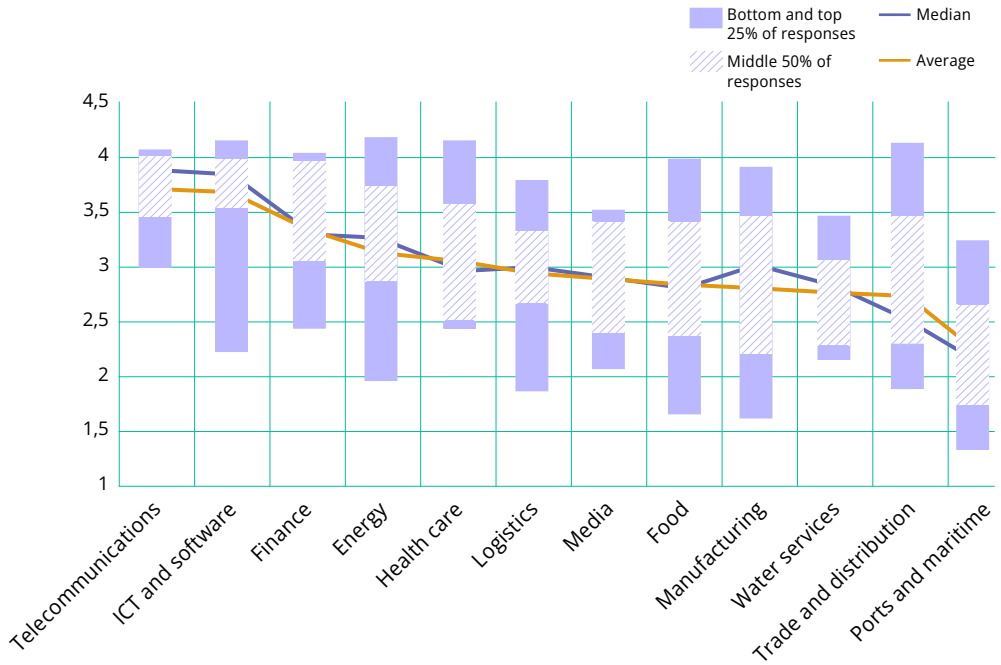
SECTORS

The average maturity level across all sectors was 3.00, which can be considered a **good basic level of maturity**

COMPANIES



In the majority of the sectors examined in the survey, the level of cyber security was at least moderate.



Variation was highest in the telecommunications sector and lowest in the food sector.

3 Recommendations

This section presents recommendations for improving cyber security that were drawn up on the basis of the results of the survey. The recommendations presented are the most frequently repeated development recommendations from the sector-specific reports. The original sector-specific recommendations were prioritised based on the results of the maturity assessments and sectors-specific threat and risk landscapes. For this national report, the most critical recommendations were divided into three categories: recommendations that promote national preparedness, recommendations that promote business activities and recommendations aimed at cyber specialists.

The observations and recommendations of the survey are divided into three levels:

- The recommendations of the national report, which answer the question: What measures should be promoted at the national level based on the survey results?
- The recommendations of the sector-specific reports, which answer the question: What kind of things should be promoted in the sector in general, based on the current situation in the sector?
- The recommendations of the company-specific reports, which answer the question: What should individual companies take into account in the development of their own maturity?

3.1 Recommendations that promote national preparedness

Development of third-party risk management
Identifying and continuously assessing the cyber risks associated with supply chains is critically important for all sectors in today's increasingly complex operating environment, where attackers often attempt to strike at the weakest links in the chain. The transparency of supply chain networks can be increased through joint risk reviews and the mutual setting of requirements and the monitoring of their implementation. When carrying out procurements, the probability of the threats associated with supply chain networks can be reduced by including minimum requirements for information and cyber security in contracts and managing these requirements throughout the lifecycle of the partnership.

Increasing cyber security awareness and competence
In today's rapidly changing environment, developing the cyber security awareness and competence of employees in general and cyber security specialists in particular requires continuous effort on the part of companies. Maintaining this competence and awareness requires the creation of models that support continuous development throughout the employment relationship. From a national perspective, the talent shortage can be addressed by continuing to invest in cyber security or technical study paths and by increasing student intake. Increasing cooperation between the public and private sectors, especially when it comes to education and training for career changers, can also contribute to addressing the talent shortage. As part of NESO's pool activities, it is advisable to identify measures and implement training that enable companies to increase the cyber security awareness of professionals in their sector and potentially develop cyber security experts with deep knowledge of the sector.

Active development of national cooperation
Some threats, such as hybrid influencing or state-level cyber influencing, require national level cooperation to address. In addition to existing good continuity exercise and information exchange models, we must find ways of exercising individual organisations or encouraging them to exercise independently. Various national level cyber exercises are effective for increasing the competence of cyber security specialists, but in future we must also find ways of increasing the cyber awareness and resilience of entire organisations.

Information exchange activity varies between sectors. For example, organisations in the telecommunications sector actively exchange threat information with each other despite the fierce competition in the sector. The NESO's pool activities or the operations of the National Cyber Security Centre Finland's (NCSC-FI) ISAC information sharing groups should be expanded in sectors where cyber security situational awareness and threat information are not yet comprehensively shared.

Development of shared situational awareness
At national level, it is advisable to continue to develop shared situational awareness. The Cyber Weather reports produced by the Finnish Transport and Communications Agency Traficom and their continued development provide a good foundation for shared national-level situational awareness. Promoting a technical perspective as part of the identification, analysis and reporting of incidents would increase the usefulness of situational awareness. The possibility of sharing nationally relevant threat information, for example, would support the visibility currently provided by the HAVARO service.

3.2 Recommendations that promote business activities

Business-driven long-term planning and development of cyber security
The long-term strategic planning of cyber security that takes into account business risks and objectives and steers decisions and investments related to cyber security provides a solid foundation for a company's cyber security management and helps keep operations under control. Business-driven cyber security is about identifying risks that threaten the continuity of the company's operations and challenges that, if realised, could hinder the achievement of strategic objectives. This kind of business-driven approach was found to be a major contributing factor to a high maturity level across all sectors.

Integrating cyber risks into companies' overall risk management
Based on the survey, many organisations do not cover cyber risks in their enterprise risk management. However, any organisation hoping to understand and assess cyber security risks should integrate them into their overall risk management. The risk-based development of cyber security requires cooperation between those responsible for cyber security at the organisation and the managers responsible for risk management so that technical understanding of cyber security can be translated into measurable risks. As a result of this more structured assessment of cyber risks, the most critical cyber risks must be communicated to the organisation's management so that development measures and investments can be aligned with risks and backed by the necessary information.

Development of OT security and harmonisation of functions
The increasing connectivity of operational technology (OT), the utilisation of analytics in monitoring and steering, and modernisation increase the need to manage cyber security. Based on the survey, companies' cyber security management and management of OT environments have diverged. While differentiated management is not a problem per se, when it comes to overall situational awareness, it is important to be able to take both environments into consideration. This requires defining and engaging in cooperation and efficient information exchange between the parties responsible. Achieving these is important for ensuring the overall cyber security of the organisation.

Development of cyber security programme management and management commitment
Management commitment ensures that budgets and planning horizons are sufficient relative to risks. One of the challenges identified in the survey was the reactivity of development planning and budgets and the lack of long-term vision to guide them. This results in organisations implementing cyber security investment decisions as individual solutions, which often also need to be provided with budgets on a project-specific basis. This often shortens the horizon of development planning and steers operations in a more reactive direction.

The key is to find common indicators for communicating cyber security situational awareness to management in an easily understandable manner so that management can actively participate in the planning of necessary measures. Communicating cyber issues and effectively describing their impacts on business operations is one of the most important elements of management commitment.

3.3 Recommendations aimed at cyber specialists

More comprehensive integration of security operations centres into other activities
The use of security operations centres (SOCs) has become increasingly common, especially in high maturity level sectors. SOCs have been implemented as both internal functions and purchased services. One of the challenges identified in the utilisation of SOC services was that they are sometimes limited to only carrying out monitoring, meaning that the SOC is only tasked with highlighting detected incidents, which the rest of the organisation is then expected to process. This kind of approach ensures compliance with SOC requirements, but provides little added value. A more effective approach is to integrate the SOC more comprehensively in the organisation's other operations, such as asset, vulnerability and threat management, enabling it to serve as a central hub for daily, operative cyber security management while also supporting the investigation of cyber security incidents.

Development of software security
Today's digital operating environment emphasises the importance of software security, regardless of sector. With different types of development being carried out by both organisations themselves and their partners, it is important to manage the information security of development models and ensure the information security of outputs. Approaches such as DevSecOps or the assignment of Security Champion roles play an important role in supporting developers and ensuring information security as part of modern software development models.

Development of the identification of liabilities
As supplier networks become more and more complex, it is important to expand their visibility to also cover the subcontractors of direct suppliers and other liabilities (e.g. dependency on software components). Partner management should also be developed to cover the entire lifecycle of services and partnerships. Based on the results of the survey, at present many organisations define initial cyber security requirements for their procurements, but do not always carry out continuous monitoring and communication or implement controls to ensure continued compliance.

Development of proactive threat identification
The development of the threat and risk landscape requires organisations to adopt an increasingly active approach to cyber security. Effective threat identification is dependent on understanding gained through asset and vulnerability management, which provides the basis for how monitoring and the resources available for responding to incidents can be effectively targeted. The development of capabilities and the implementation of protective measures must be a continuous process that also includes the monitoring and assessment of the developing threat landscape. In terms of preparedness, it is important to network and utilise information sources in different ways. For example, the ISAC information sharing groups facilitated by the NCSC-FI support the preparedness of various sectors by facilitating the confidential sharing of experiences.

4 Conclusions

This section highlights the main conclusions of the survey and presents the observations behind them. The conclusions were drawn by collecting the most frequent observations from the sector-specific reports and identifying common factors affecting cyber security across sectors based on them.

4.1 Factors affecting maturity

The survey revealed several underlying factors that have positive and negative impacts on maturity. The assessment of the impacts of these factors was based on observed correlation, as the determination of causality would require further investigation. Based on the survey data, the following factors were identified as being common to high and low maturity level organisations regardless of sector.

Factors that have a positive impact on maturity:

- business and risk-based development of cyber security
- management systems based on standards or other reference frameworks
- effective communication between the persons responsible for cyber security and the organisation's executive management.

Factors that have a negative impact on maturity:

- lack of strategic planning in the development and management of cyber security
- a reactive rather than proactive approach to critical threats and risks
- lack of risk management practices.

4.2 Changes in the threat and risk landscape

The two most significant factors in the development of the threat and risk landscape in recent years have been the COVID-19 pandemic and the change in the geopolitical situation. These issues have had extensive impacts on both business operations and the state of cyber security in all sectors. Global trends have also affected the ways in which threat actors operate. According to the organisations participating in the survey, it was clear that various types of attacks were increasing. This impression was facilitated by increased awareness of the threat situation and improved capability to detect unusual or harmful activity, among other factors.

Based on workshop discussions about changes in the threat and risk landscape, it was clear that the development of cyber security is a constant race against threat actors. Threat actors are constantly developing their tools, tactics and procedures (TTP) to support their own goals, as a result of which the threats that organisations face are also constantly developing and changing.

One threat that hardly came up in the workshops of the survey was industrial espionage. It is possible that the ways in which the world has changed and the threat situation has developed during the last two years have reduced it to a minor concern, with companies focusing on the management of more important issues. However, industrial espionage has been highlighted in the communications of public authorities in recent years, in clear contrast the threat and risks discussions carried out in the survey workshops. As such, it would be advisable to keep the threat of industrial espionage and intelligence operations in mind in the context of risk identification and assessment in future.

4.3 Third-party management

Based on the survey workshops, the partner management controls of the organisations included in the survey focus on direct partners, which are managed through both contract-level requirements and continuous cooperation and monitoring. On the other hand, several of the organisations included in the survey reported that when it comes to third-party management and monitoring, they trusted their partners and thus did not carry out any actual monitoring besides having their partners supply reports. However, neglecting monitoring can present a significant risk, which should be recognised.

In terms of identifying and managing partner networks, whole supply chains and dependencies, the organisations included in the survey still have room for improvement. Organisations manage their partner networks primarily by assigning responsibility for subcontractors to direct partners. From the perspective of overall management, it is important to also identify dependencies, as in practice having many different partners increases overall risk. Through various integrations, partners and their subcontractors can even expand a company's network, and if these kinds of dependencies have not been identified, they can end up posing a significant potential threat.

4.4 Management guided by reference frameworks has increased

The companies that were assessed to be the most mature in this survey were found to use various reference frameworks or management models steered by them. In the organisations of the most mature sectors, such as telecommunications and the ICT and software sectors, a management model implemented in accordance with standards had a positive correlation with a systematic approach to cyber security, as did certification in many organisations. Individual organisations in other sectors also found the common language provided by reference frameworks or certification schemes to be useful for communicating with stakeholders, even when certification was not actually required by customers, for example. In many sectors, operating in accordance with reference frameworks is also useful for ensuring compliance with legislative requirements and due to audits. For example, the fact that operating in the financial sector requires authorisation means that organisations need to implement certain measures related to information security and prepare documentation to demonstrate to supervisory authorities that their operations meet relevant minimum requirements.

4.5 Cyber security on the management agenda

As a result of changes in the threat and risk landscape, more and more organisations had started to add cyber security issues to their management agendas. This change was noted especially in lower maturity level organisations that did not previously have operating models for having management report on cyber risks or cyber security situational awareness, for example. In higher maturity level organisations, cyber security had been on the management agenda for a long time. These organisations had ensured management support for a cyber security development programme and the achievement of its objectives was consistently monitored.

The survey showed that events that have a significant impact on the security environment, such as geopolitical changes in neighbouring areas, or cyber attacks that garner a great deal of public attention, such as the Psychotherapy Centre Vastaamo data breach, raise the cyber security awareness of organisations temporarily. Although cyber security was on the management agendas of many organisations during the survey, it would appear that the processing of incidents and technical matters does not hold managers' interest over the long term. Because of this, the parties responsible for cyber security should focus on identifying issues that it is relevant to process and monitor at management level. The key is to find indicators and situational awareness elements that are suitable for the target audience. Successful actors had found a so-called 'common language' with which to communicate cyber security situational awareness to management in a business-oriented manner.

4.6 Business-driven cyber security is a competitive advantage

Business-driven cyber security seemed to clearly facilitate the development of maturity across domains. Even in sectors where strong regulation has created a foundation for a basic level of cyber security, it was evident that integrating the long-term development of cyber security into an organisation's business strategy and needs had a positive impact on maturity. A business-driven approach was found to help steer long-term development in particular, allowing an organisation to define cyber security objectives based on the organisation's needs and making their development easier to monitor. In addition to this, a business-driven approach was also found to benefit the planning of internal communications, providing a common language for discussing cyber security with business representatives.

Business and risk-orientation seemed to go hand in hand. Organisations that developed their cyber security management to support their business also ended up adopting a risk-based approach. This also seemed to help break down boundaries between departments in terms of risk management, in relation to which it was also found that cyber risks were not managed as part of overall risk management, with responsibility for them having been assigned to different parties. Positioning cyber security as a business facilitator thus clearly benefited both business operations and cyber security itself.

4.7 Shortage of cyber security talent

The widely reported shortage of talent affecting the entire IT industry was reflected in the survey in the availability of cyber security talent. The companies included in the survey had a clear need to develop several aspects of their cyber security management, but one of the bottlenecks was the availability of skilled employees. This shortage was particularly notable in sectors and organisations that were not among the most attractive employers, such as companies and organisations responsible for basic infrastructure. The availability of skilled employees was found to be influenced by the public image of the company and sector, the level of pay and the company's capacity to develop cyber security management and thus offer career advancement opportunities. However, it should be noted that the competition for existing talent is a competition for scarce resources between many different sectors. Because of this, one of the ways in which the talent shortage should be addressed at national, sector and organisation level alike is through the training of new professionals.

4.8 Differentiated management of production environments

OT environments have traditionally developed as part of production activities, with responsibility for maintaining them being assigned to the relevant business unit. This responsibility was undoubtedly still justified, as these units have been accumulating relevant know-how and expertise for years. However, one of the challenges that organisations faced was integrations between environments, such as the implementation of analytics and similar services, and the building of comprehensive situational awareness.

As regards the management of production environments, it was found in the survey that awareness and information exchange between the parties responsible for managing IT and OT environments was lacking at many organisations. Maintaining comprehensive cyber security situational awareness also requires an understanding of the state and management of OT environments. The management of OT systems should also be integrated into organisations' general processes, such as asset, vulnerability and threat management. Based on the survey, the OT environments of some organisations had issues such as outdated operating systems, which require vulnerability management expertise to address.

Unlike in the previous survey carried out in 2019–20, in this survey the management of operational technology (OT) environments was not examined separately. More specific observations related to OT environments were highlighted in the sector-specific reports.

4.9 Variation

The survey showed many sectors to be fairly or very divided in terms of maturity levels. The difference between the lowest and highest maturity levels in a sector, i.e. the range of variation, was greatest in the food sector at 2.25. The sector with the lowest range of variation was the telecommunications sector at 1.06. The sector with the smallest interquartile range, meaning the range that the middle 50% of results fell in, was the ICT and software sector. Variation is described in greater detail and presented visually in section 5.1.3.

In this survey, a high degree of caution was exercised in the drawing of conclusions based on variation due to some specific variables. Although the organisations included in the survey were selected with the aim of providing as comprehensive a sample as possible, it is possible that actors whose maturity levels differ significantly from the average maturity levels were excluded from the survey. Secondly, the sample sizes of individual sectors ranged from eight to sixteen organisations, which meant that the impact of individual deviating results on a sector's average varied between sectors.

Variation seemed to be smaller in sectors where cyber security management was subject to some common requirement or legislation and where actors were in some way similar to one another. For example, telecommunications companies operate in largely similar business areas and are largely subject to the same statutory obligations. At the other end of the maturity scale, the water supply sector also had a fairly low range of variation. In other words, while the maturity level of the water supply sector was not high, its organisations were similar regardless of their operating areas. In addition to this, almost all of them were owned by cities, which were also often their most notable IT service providers. Due to these circumstances, the water supply actors faced similar challenges and were fairly even in terms of their maturity. The survey also included two other sectors that, like the telecommunications sector, are subject to extensive legislative requirements, namely healthcare and finance. In spite of this, these two sectors were slightly more divided in terms of maturity, with the most likely reasons being differences between banks and insurance companies and the healthcare sector sample, which included many different types of actors.

The sectors with the greatest variation were the food and manufacturing sectors, the samples of which included notably different companies with different operating environments. In practice, it would have been possible for any sector to have more low or high maturity level actors, as the samples of this survey were limited. In a networked society, this could potentially cause risk concentrations with significant cascading effects.

5 Cyber security situational picture in 2022

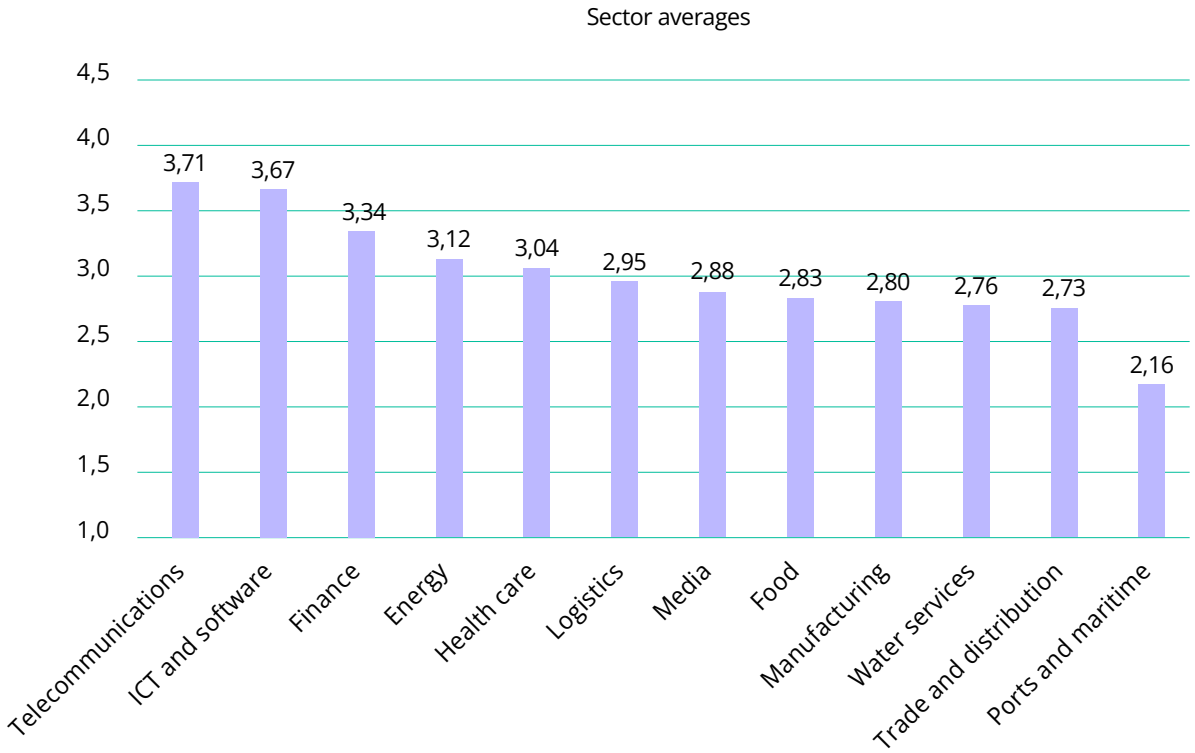


Figure 1: Sector comparison

5.1 Sector analysis

Based on maturity levels, the level of cyber security was at least acceptable in the majority of the sectors examined in the survey. If a maturity level of three is considered to indicate a good basic level of maturity, then 11 out of the 12 sectors included in the survey either exceeded it or fell slightly short. The weakest of these 11 sectors fell 0.27 units short of reaching a good basic level of maturity. However, it is important to keep in mind that examining only the average level of maturity and drawing conclusions based on it may be misleading, which is why sector variation is examined below in section 5.1.3.

The telecommunications sector, the ICT and software sector and the financial sector, which are all extensively regulated and have a long history of being targeted by cyber criminals, stood out clearly in terms of maturity. All of these sectors had benefited from development required by regulation and, based on the survey, were able to develop cyber security and controls in a business and risk-based manner. The average maturity level of the energy and healthcare sectors was also over three, which was defined as corresponding to a good basic level of maturity. However, the impact of the threat and risk level was estimated to be so significant in these sectors that they will need to improve their maturity in the future in order to adapt to the challenges posed by the growing threat and risk landscape.

Six of the sectors included in the survey fell slightly short of reaching a good basic level of maturity (logistics, media, food, manufacturing, water supply, and trade and distribution). The maturity of these sectors was close to an acceptable level, but will need to be developed further to respond to the risk and threat level. That being said, the objectives and target maturity of these sectors should be assessed and defined taking into account the special characteristics of each sector. In terms of average maturity, the ports and maritime sector was clearly behind the other sectors. For this sector, it is therefore important to map out and implement measures to develop maturity without delay.

Sector	Average maturity	Impact of risk/ threat level	Assessment of ability to respond to threat/risk level
Telecommunications	**3,71**	Rising	The telecommunications sector demonstrates a strong maturity level and is able to respond to the sector's risk and threat landscape through preparedness.
ICT and software	**3,67**	Rising	The good maturity level and risk awareness of the ICT and software sector currently provides it with the capacity to respond to threats.
Finance	**3,34**	Rising	The finance sector is able to respond to the current risk/threat situation due to its strong maturity level.
Energy	**3,12**	Rising	The energy sector's level of maturity is good overall. Cyber security is promoted by a strong culture of preparedness. The threats in this sector are so significant that companies' own preparedness may not be enough.
Healthcare	**3,04**	Rising	Data protection controls and measures are duly taken care of in this sector, in part due to regulations, but there are several actors in the sector that need to adopt a more systematic approach to cyber security.
Logistics	**2,95**	Rising	The sector is constantly evolving, prone to competition and sensitive to changes in the supply chain, as a result of which special attention must be paid to the comprehensive management of cyber security.

Sector	Average maturity	Impact of risk/ threat level	Assessment of ability to respond to threat/risk level
Media	**2,88**	Neutral	The improved maturity level of the media sector supports the sector's ability to respond to threats and manage risks. The fact that the sector is a key target for both state-level influencing and criminals raises the risk level, necessitating further risk-based development.
Food	**2,83**	Neutral	The current state of the food sector calls for further development to respond to the threat and risk landscape.
Manufacturing	**2,80**	Neutral	The manufacturing sector is fragmented in terms of maturity, making preparedness difficult to assess. The sector's average maturity level falls short of a good basic level, which means that responses to threats are not comprehensive.
Water Supply	**2,76**	Rising	The overall maturity of the water supply sector falls short of a good basic level. The key role that the sector plays in the functioning of society necessitates further investments in cyber security as well.
Trade and distribution	**2,73**	Neutral	The overall maturity of the trade and distribution sector falls short of a good basic level, and the sector's preparedness for cyber threats is not comprehensive. In particular, the large variation in maturity levels can be indicative of a risk concentration.
Ports and maritime	**2,16**	Neutral	The maturity level of the ports and maritime sector is low and requires significant measures to address.

Table 1: Risk level effect on Cybermaturity in Industry sectors

When it comes to developing maturity, it should also be noted that the risk and threat landscape changes over time, with threat actors constantly developing their own capabilities and new attack methods. Because of this, cyber security needs to be continuously developed to maintain a good level of security and protection. Engaging in continuous development is important regardless of the current maturity level. In this survey, the impacts of prevailing threats and risks were assessed to be so significant that their effect on the assessment of preparedness was deemed either neutral or high for all sectors.

Based on the results of the survey, no direct conclusions could be drawn on how the size of an organisation affects its maturity level. Although in most cases being able to make investments led to an organisation having a higher level of cyber security maturity, a factor that was found to play a greater role than the organisation's size or turnover was security orientation, meaning how highly the organisation's management prioritised cyber security and was prepared to allocate resources for it. Small organisations or newer generation companies were found to benefit from being able to more easily implement administrative measures that significantly increased maturity. The maturity development of larger, multinational companies was found to be hindered by inconsistencies within the organisation and difficulties in monitoring development measures. On the other hand, large and stable companies typically had more investment capacity and resources, which allowed them to utilise technologies related to cyber security and hire cyber security personnel, for example.

5.1.1 Factors common to higher maturity level sectors

In higher maturity level sectors, cyber security management was more often business and risk-based. In these sectors, the objectives of cyber security management supported the achievement of strategic business objectives, and the planning of business activities was not too far removed from the planning of cyber security. Moreover, in these sectors, organisations managed cyber security and defined related objectives in a risk-based manner, meaning that they supported their decisions by analysing cyber risks and assessing their potential to hinder the achievement of business objectives. In some higher maturity level sectors, risk management was steered either by legislation (e.g. the financial sector) or by existing standards and frameworks (e.g. ISO 27001), which could be seen as contributing to a good basic level of maturity to some extent.

The requirements imposed by legislation and other regulations were found to have an indisputable impact on the management of cyber security in higher maturity level sectors. In these sectors, compliance with regulatory requirements guaranteed a certain basic level of cyber security, but in this survey compliance alone was not enough for an organisation to be considered mature or very mature if they did not also develop their operations in relation to prevailing risks. Similarly, the utilisation of management systems based on general cyber security standards and reference frameworks was found to be more common in higher maturity level sectors. The most commonly used standards and frameworks were ISO standards, the NIST Cybersecurity Framework and Katakri criteria.

As a result of employing a business-driven approach, higher maturity level actors had more often managed to communicate the importance of cyber security to their executive management, thereby ensuring management support for development projects. Management support was found to correlate with cyber security budgeting and investments. In more mature organisations, management support had been ensured by obtaining approval for a cyber security development programme, sharing situational awareness on a regular basis and participating in continuity exercises.

5.1.2 Factors common to lower maturity level sectors

One of the factors that lower maturity level sectors were found to have in common was shortcomings in the strategic planning and management of cyber security. Lower maturity level organisations less frequently prepared long-term risk-based plans to support the sustainable development of cyber security maturity. The development carried out by lower maturity level organisations was more often reactive in nature, meaning that it was carried out in response to threats that had become critical or risks that had already been realised. The lack of a cyber security management system was also more common in lower maturity level sectors than in higher maturity level sectors. The maturity of organisations without cyber security management systems was found to be further decreased by the resulting dependence on individual employees, shortcomings in documentation and challenges regarding repeatability, among other factors.

In lower maturity level sectors, challenges in the development of proactive cyber security management were also evidenced by weaker cyber risk management. In these sectors, few organisations had defined risk management practices or identified the cyber risks that posed a threat to operations. Although in some sectors the management of business risks was more active than that of cyber risks, in most cases risk culture was poor overall. In lower maturity level sectors, it was more common for organisations' management to be unaware of the most critical cyber risks, for example.

In low maturity level sectors, the collection of threat information and the prevention of threats were more mature than risk management. Organisations were typically very active in collecting threat information and sharing it with parties such as stakeholders, but did not utilise this information in the assessment of cyber risks or the building of situational awareness. In other words, organisations were unable to recognise how relevant threat information was in terms of their own activities.

5.1.3 Sector variation

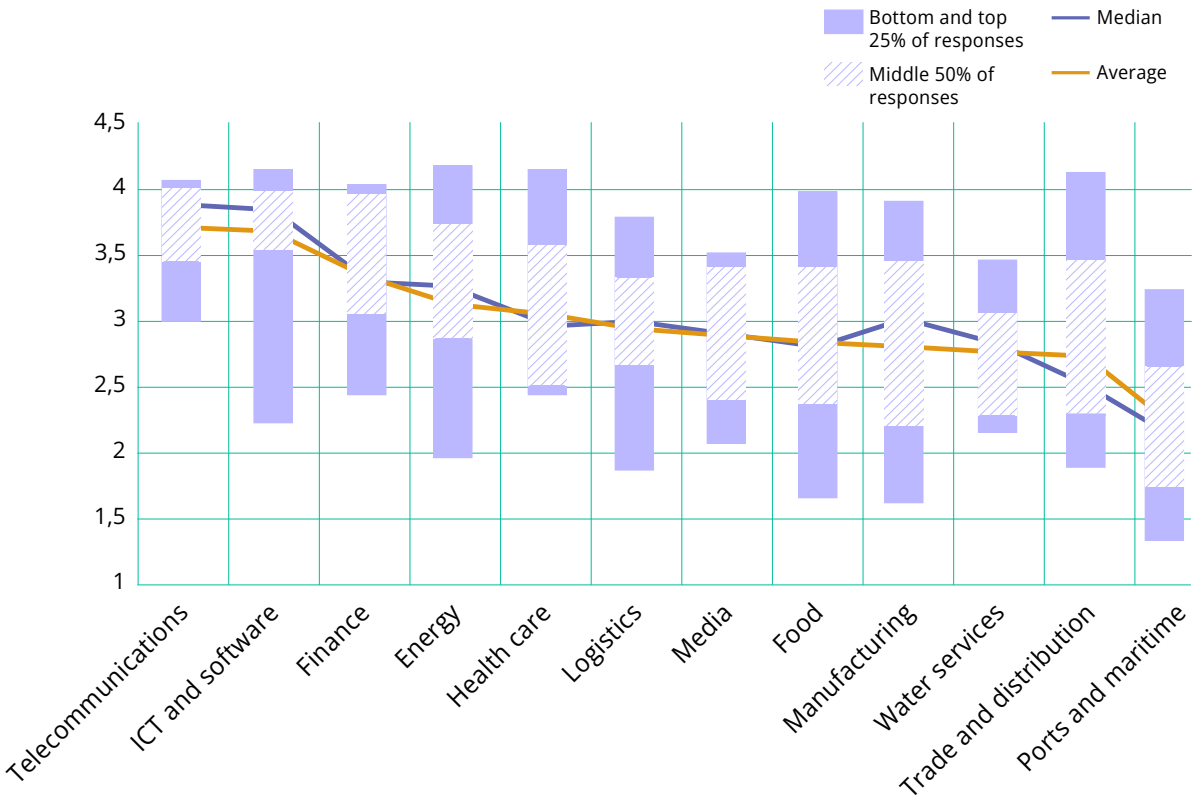


Figure 2: Variation between companies in each sector[2]

[2]The upper and lower lines on the graph indicate the range of variation of the results. The boxes between them indicate the interquartile range, meaning the range that the middle 50% of results fall into. The top 25% of results fall within the range between the box and the upper line. The bottom 25% of results fall within the range between the box and the lower line. If the value of the top 25% is the same as the highest value inside the box, no upper line is displayed. Correspondingly, if the value of the bottom 25% is the same as the lowest value inside the box, no lower line is displayed. The blue line represents the median value, while the orange line represents the average value.

Sector variation could be examined from two perspectives, focusing on either the sector's range of variation, meaning the difference between the lowest and highest result, or the interquartile range, meaning the range that the middle 50% of results fell in. The range of variation showed that there are both low and high maturity level actors in almost every sector, whereas the interquartile range could be used to examine how consistently mature each sector was. In four sectors (telecommunications, logistics, water supply, and ICT and software), the interquartile range was smaller than a single maturity level.

The sector with the smallest range of variation was the telecommunications sector, while the sector with the smallest interquartile range was the ICT and software sector. Although the ICT and software sector had a smaller interquartile range and its top 25% result were higher, the telecommunications sector had the highest maturity level overall. This was due to the fact that the telecommunications sector's interquartile range was slightly higher and the fact that the ICT and software sectors's average was lowered by its bottom 25% of results. However, the ICT and software sector's sample size was over 1.5 times the size of the telecommunication's sector's sample, in light of which the ICT and software sector's good maturity level, the bottom 25% notwithstanding, seemed to indicate that the current state of the sector's cyber security was consistently strong.

The sector with the largest range of variation was the food sector (2.25), followed by the trade and distribution and energy sectors (2.19). Variation in these sectors was contributed to at least by significant differences in investment capability and resources for cyber security between companies. Although one of the overall findings of the survey was that smaller organisations can achieve a good level of maturity despite having smaller budgets and benefit from being more agile, for example, variation was found to be affected by organisation size, investment capacity, regionality and the number of employees. Large multinational companies were found to be generally able to invest more in cyber security development and personnel, but there were also exceptions, as a result of which company size could not be considered a clear indicator of maturity. One factor that was found to affect maturity was how likely organisations considered a cyber attack targeting them to be. For example, in the energy sector, organisations operating in larger geographical areas had invested more in cyber security than actors whose operations were more localised on account of the perceived risk of cyber attacks.

Figure 2 shows not only the variation, but also the median level of maturity of each sector, which in some sectors differed from the average level of maturity. Since the sample size varied between sectors, the maturity levels of individual organisations included in the survey had a varying effect on sectors averages. Examined by the median level of maturity, the manufacturing sector was the fifth most mature, the logistics sector was sixth and the healthcare sector was seventh. However, examined by the average level of maturity, the manufacturing sector was fourth to last, or ninth, as the sector's average was dragged down significantly by the bottom 25% of organisations. The relatively large difference between the median and average levels of maturity in the manufacturing sector was contributed to by the sector's large sample size, which was as much as twice the size of some of the smallest sectors.

In general, the variation graph and figures should be examined while keeping in mind that the sample sizes of the sectors were not the same and that it is possible that more lower or higher maturity level actors ended up being left out of the survey.

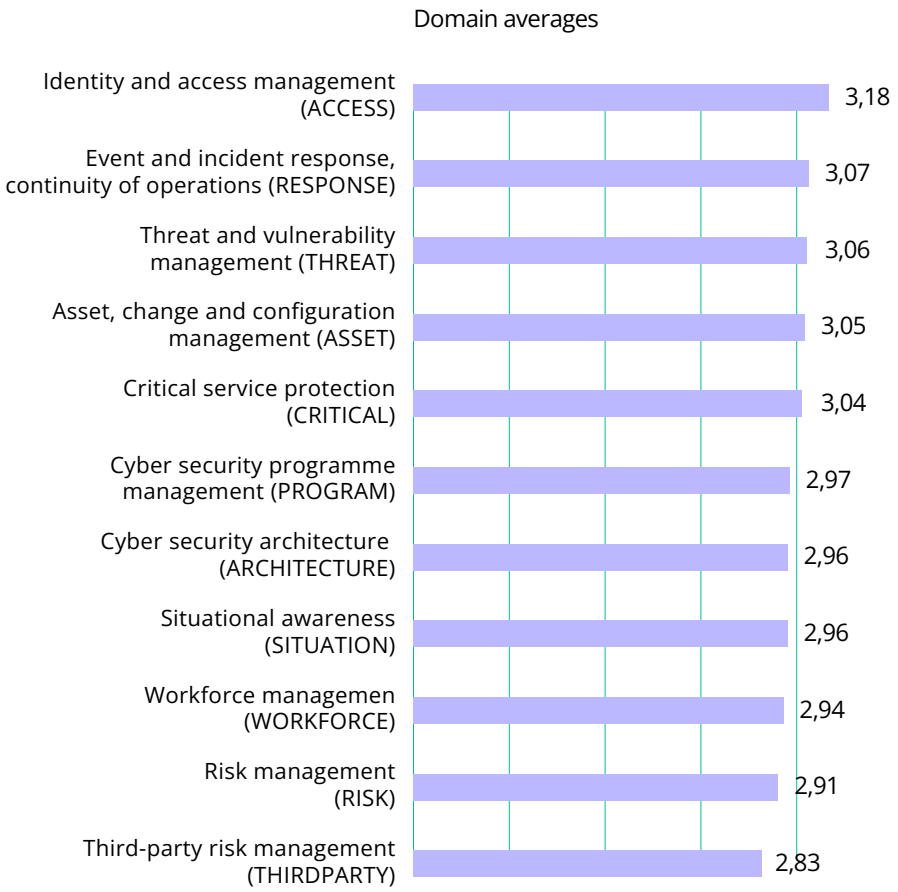


Figure 3: Domain-specific results of the survey based on the Finnish Transport and Communications Agency Traficom's Kybermittari tool

5.1.4 Results of the survey by domain

A weakness that all the sectors included in the survey could be said to have in common was third-party risk management, which is the domain where maturity was lowest overall. Depending on the sector, organisations faced challenges either managing their main partners or understanding supply chains as a whole. For example, in the water supply sector, one of the critical areas for improvement identified was challenges related to communication and the division of responsibilities with municipalities and cities, which were often the owners and among the largest IT services providers of water supply companies. In fact, lack of clarity regarding organisations' own and their suppliers' responsibilities was a challenge that came up repeatedly in all sectors. In the ICT and software sector, the management of direct partners was more often structured, but actors in the sector found the comprehensive management of complex supply chains to be challenging. Cyber threats realised through supply chains were subsequently considered one of the most critical risks in many sectors, as organisations are aware that not all dependencies and risk scenarios had been identified.

A domain where nearly all of the sectors included in the survey fared well was identity and access management (ACCESS), with 75% of sectors reaching or exceeding the good basic level of three in this domain. Within identity and access management (IAM), the most common strength was physical access management, which was well handled on average even in low maturity level sectors. Organisations have traditionally understood the dimensions of physical security earlier and better than cyber security, as a result of which related processes, controls and responsibilities were better defined. Furthermore, even small organisations that otherwise had a low maturity level fared well in identity and access management. In small organisations with a low number of employees, it was realistic to implement identity and access rights management manually, while in organisations with more resources, a centralised IAM system was often at the top of investment priorities.

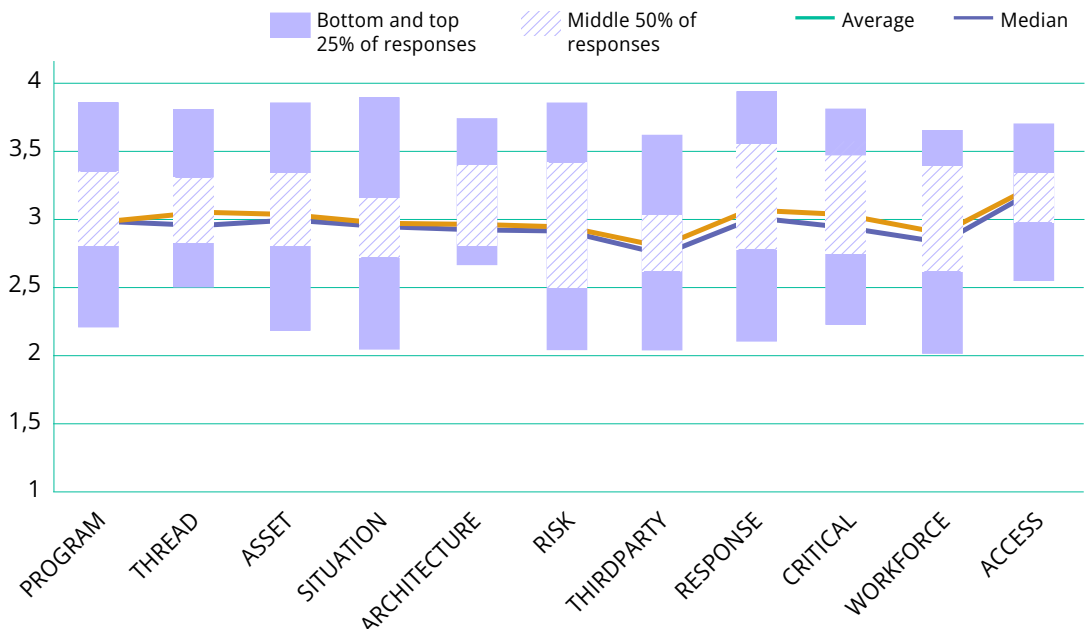


Figure 4: Variation by domain [3]

The domain with the largest range of variation was event and incident response and continuity of operations (RESPONSE). The significant variation could be partly explained by the fact that in some sectors, such as the telecommunications sector, preparedness is a statutory obligation for companies, whereas in the ICT and software sector, disruptions in services would incur significant costs for actors in the form of customer compensation, for example. At the other end of the spectrum there were sectors where continuity planning has so far focused on ensuring continuity of production, with not much thought given to cyber security. The challenges in this domain are in part linked to the previously mentioned lack of clarity in the division of responsibilities between organisations and their suppliers. For example, the survey revealed that some suppliers relied on a partner, most commonly a security operations centre (SOC) service provider, when it came to managing cyber incidents and had thus not prepared any internal continuity plans of their own. In most cases, SOC services had been outsourced, with responsibility for certain technical incident management tasks having been transferred to the partner, but other measures, such as communication with customers and stakeholders in the event of a cyber incident, had not been planned.

The survey revealed that many higher maturity level actors had either an internal or outsourced SOC and that even low maturity level actors were planning on procuring SOC services. However, not all organisations possessed a sufficient level of understanding of the importance of their own management in terms of cyber situational awareness, which is reflected in the previously mentioned uncertainty regarding the division of incident management responsibilities. Although more organisations had begun to utilise information security monitoring services, their coverage was not always sufficient from a risk-based perspective, and some organisations lacked understanding of how responsibilities had been divided between them and their supplier. Based on the survey, many organisations had an SOC

[3] The upper and lower lines on the graph indicate the range of variation of the results. The boxes between them indicate the interquartile range, meaning the range that the middle 50% of results fall into. The top 25% of results fall within the range between the box and the upper line. The bottom 25% of results fall within the range between the box and the lower line. If the value of the top 25% is the same as the highest value inside the box, no upper line is displayed. Correspondingly, if the value of the bottom 25% is the same as the lowest value inside the box, no lower line is displayed. The blue line represents the median value, while the orange line represents the average value. Individual values that deviated significantly from others in the same sample are not depicted in the graph.

that, upon detecting incidents, simply relayed information about them to the client organisation for investigation. While this kind of limited approach ensures compliance with minimum requirement for SOCs, it does not leverage all the synergies that an SOC could provide in terms of situational awareness, for example.

The domain with the largest interquartile range was risk management. This was contributed to by the factors examined under the sections on the special characteristics of higher and lower maturity level sectors, such as regulatory requirements and the criteria of management systems based on reference frameworks. In more mature sectors, enterprise risk management was often highly systematic, but cyber risks were not part of it. In less mature sectors, some organisations lacked any kind of risk culture. In all sectors, there were organisations that found it challenging to coordinate risk management methods and technical cyber security expertise. Cyber security specialists often perceived risk management as technical threat management, whereas risk management officers were used to assessing risk scenarios with the help of financial and quantitative metrics.

5.2 Comparison with the 2019–2020 survey

Compared to the survey conducted in 2019–2020, the maturity levels of Finnish sectors had remained at a good basic level or close to it (maturity level three) on average, although variation between organisations was found to be significant, as in the previous survey. In regard to comparing the surveys, it should be noted that the organisations included in the 2019–2020 survey were not the same as the ones included in the 2022 survey. Furthermore, changes in maturity levels could not be compared based on the numerical results of the maturity assessments due to changes made to Finnish Transport and Communications Agency Traficom's Kybermittari (Cybermeter) tool, which was utilised in the survey, and the assessment criteria.

The most notable common areas for improvement identified in the previous survey from the perspective of security of supply were related to the generation of shared situational awareness, secure software development and the development of personnel competence. The most notable areas for improvement identified in the previous survey from the perspective of business operations were company cyber security strategy, cyber security architecture and technical traceability. Although accelerating digitalisation, the COVID-19 pandemic and changes in the geopolitical situation have expedited the need for organisations to take cyber security into account more comprehensively than before, the most notable areas for improvement remained largely the same. As for why the situation regarding the areas for improvement has remained the same, there are multiple reasons. Since the numerical results could not be effectively compared due to changes made to the assessment scale, we decided to focus on comparing the qualitative analyses of the surveys in this text. It is worth noting that the most notable company-specific areas for improvement could differ significantly due to the variation.

In the previous survey, the results of individual sectors and companies alike highlighted the need to develop cyber security situational awareness in a consistent manner. On the other hand, investments in creating shared national and sector-specific situational awareness had already been made in the past, examples of which include the ISAC information sharing groups and the HAVARO service. Although one of the findings of this survey was that in many sectors organisations actively engaged in stakeholder activities and especially the sharing of threat information, these actions were not directly reflected in the maturity levels of organisations. Based on the survey, organisations have gotten better at recognising potential threats and risks, but often fall short of fully utilising obtained information due to a lack of expertise, personnel or time.

In the previous survey, secure software development was highlighted as one of the most important areas for improvement for all sectors. The need for common minimum requirements for the data security of software development identified in the previous survey was still there. Based on the current survey, in many sectors the maturity levels of organisations were decreased not only by lack of expertise and time, but also by shortcomings in lifecycle management. These issues were evident regardless of whether organisations carried out software development themselves or purchased software development services. Organisations in all sectors also faced challenges when it came to measures for demanding and ensuring the security of software and application development and procurements. In addition to the above, one significant reason for the shortcomings in ensuring security was trust, which seemed to be a factor that organisations relied upon heavily, especially when partnering with large and well-known service providers.

The current survey revealed lifecycle management challenges in several domains. One of theses was workforce management, where similarities to the previous study were found in the form of shortcomings in the continuous development of expertise during employment. The overall cyber security awareness of the workforce was found to have increased over the past few years, although the results of the current survey revealed ongoing challenges in carrying out workforce development throughout the employment lifecycle, with more training typically being carried out at the start of the

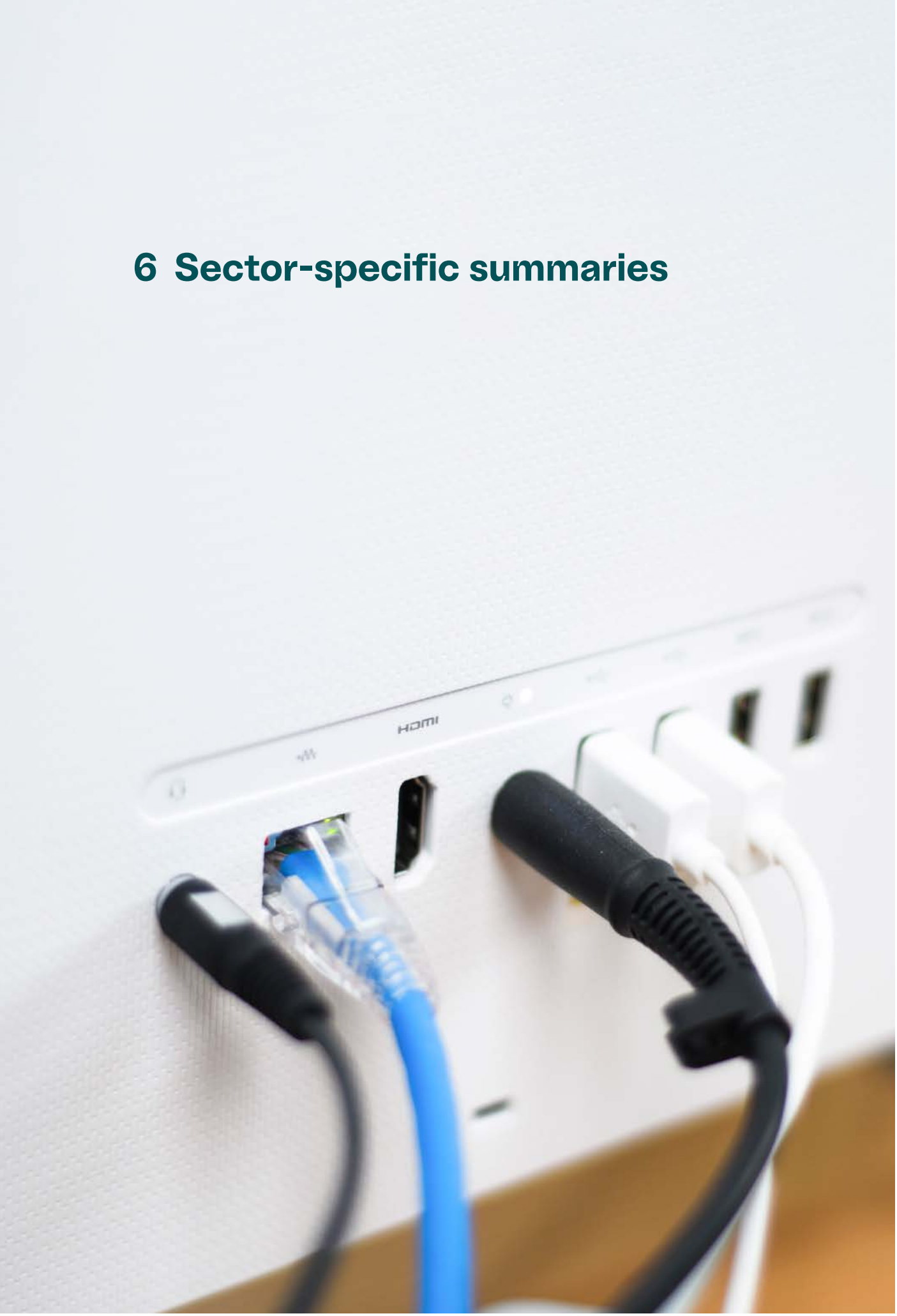
employment relationship. Challenges related to the turnover and availability of cyber security specialists continued to affect the continuity and resilience of organisations. On the other hand, looking at the big picture, it was found that the gaps between the perspectives of organisations' business management and cyber security personnel had narrowed. The number of organisations where management discussed matters related to cyber security and had adopted a more risk-based approach to management, thus taking cyber security more comprehensively into account, had also increased. In the previous survey, it was found that in a large number of organisations, executive management did not regularly discuss cyber security matters. The biggest reasons behind these changes were the geopolitical developments over the past year, as a result of which organisations have come to understand the threat of large-scale state-level cyber influencing, which all actors of supply chains critical to security of supply can become either the direct or indirect targets of.

While organisations had recognised the possibility of their activities being indirectly affected by cyber threats, the majority of actors still had plenty of room for improvement in terms of third-party risk management. In the previous survey, organisations' management of supply chains and external dependencies was deemed to be at a good level, but the management of dependency risks was found to vary between sectors, with only a quarter of the organisations included in the previous study performing well in this area. In this survey, third-party risk management was one of the most important areas for improvement identified. Based on this survey, one third of sectors could be deemed to be managing their supply chains, liabilities and dependencies in a way corresponding to a good basic level, although even in these sectors organisations found it challenging to manage complex supply chains and comprehensively identify their dependencies. As regards main partners, the current survey highlighted long-term contracts and partnerships as a significant risk vector, as organisations may not always monitor them sufficiently due to the trust built over the course of long-term cooperation. One of the common challenges identified was increasingly complex supply and subcontracting chains; in many cases, organisations had only identified and managed the first links in these chains instead of carrying out comprehensive risk management. In general, cyber risk management could be stated to be a matter that was currently not being taken sufficiently comprehensively into account as part of other enterprise risk management in several sectors. Risk management was subsequently the domain with the second lowest maturity level in this survey. However, as was the case in the previous survey, there was significant variation between organisations in this domain.

One of the findings of this survey had to do with the differentiated cyber security management of IT and OT environments, in the harmonisation which organisations have made little progress compared to the previous survey. In the previous survey, the weak or even non-existent visibility of the OT side caused a significant difference in the cyber security maturity of IT and OT environments. While the common management of business technology emerging as a result of digitalisation was already identified at the time of the previous study as being a measure with which organisations were striving to deepen the synergy and management of IT and OT environments, the current survey found no evidence of any particular progress in this area. One of the factors behind this was the partial ignorance of traditional cyber security organisation of OT environments, which is the result of IT and OT environments typically being managed by different organisations.

Based on the numerical results of the survey, the current state of the cyber security of Finnish sectors has not changed to any significant degree compared to the previous survey. However, organisations' awareness of cyber security matters was found to have developed significantly. Based on the current survey, it could be stated that several organisations were in the middle of a transformation in terms of cyber security, which will steer them to plan the continuity of their business operations with a focus on cyber security in the future. In summary, the current state of cyber security was seen as clear, and understanding of its role as a guarantor of operating reliability was already driving the development of several organisations. It is now of paramount importance to ensure that organisations are supported in different ways by authorities. The ability to invest both in the development of cyber security and in related expertise seems to have become a prerequisite for success.

6 Sector-specific summaries



6.1 Telecommunications

Sector characteristics

The telecommunications sector is an essential part of critical infrastructure and plays a key role in ensuring national cyber security. Historically, the sector has also actively promoted digitalisation and operated at the forefront of preparedness:

- limited leeway in business and risk management solutions due to strong regulation
- key role in facilitating digital operations in other sectors
- strong cooperation within the sector in the area of preparedness.

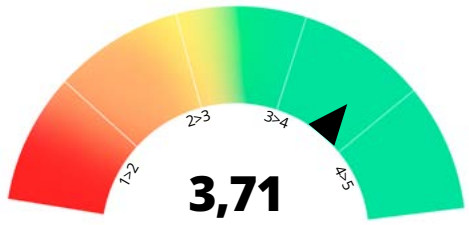
Recommendations for the sector

The telecommunications sector demonstrates a strong maturity level and is able to respond to the sector's risk and threat landscape through preparedness. The sector's role as a key provider of digital capabilities makes it an attractive target, making the continuous development and improvement of cyber security essential.

The following issues are highlighted as being important for improving maturity:

- active continuation and further deepening of cooperation with other sectors and authorities
- continued development of threat and risk-based cyber security
- management of supply chain dependencies and cyber security.

Overall maturity of the sector



Sector strengths

The strong overall maturity of the sector is particularly evident in the following areas:

- a good level of maturity across the sector is indicative of a high level of preparedness
- business and risk-based cyber security management with strong management support
- key capabilities related to operational security are strong across the board.

Risks and threats in the sector

The most notable risks and threats in the sector:

- digitalisation and technology risk, including the expanding use of cloud services
- competence risk in relation to outsourcing and the continued use of legacy infrastructure, for example
- continuous development and diversification of cyber crime and influencing.

Sector weaknesses

Even the weakest capabilities of the sector exceed a good basic level of three. The most critical areas for improvement identified were:

- third-party cyber security management
- the varying capacity of sector companies to create cyber security situational awareness.

Comparison between the 2019–2020 survey and the 2022 survey

The telecommunications sector has managed to continue improving its maturity level between the 2019–20 survey and the 2022 survey. The sector has retained the strengths identified in the previous survey and improved capabilities that were identified as weaknesses in 2019–20, showing significant progress in some areas.

Improved capabilities:

- workforce management and development, especially the development of the competence of cyber security personnel
- development of situational awareness; security operations centres widely used by sector companies
- development of asset management.

Other observations:

- The importance of the sector to national cyber security and preparedness has increased due to geopolitical events.

6.2 ICT and software

Sector characteristics

The sector plays an essential role in building national digital infrastructure and capabilities and ensuring both its own cyber security and the cyber security of customers.

- While cyber security is a trust factor in customer-facing work, in public procurements the focus on costs often results in security getting largely over-looked in quality requirements.
- Service modernisation is slowed down by customer caution and prevailing service procurement culture (e.g. cloud transformation and legacy challenges).

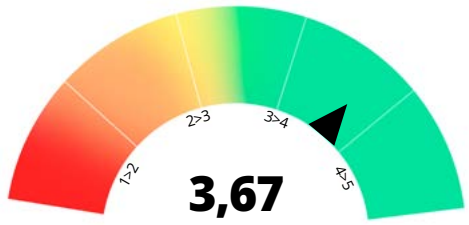
Recommendations for the sector

The good maturity level and risk awareness of the ICT and software sector currently provides it with the capacity to respond to threats. However, the sector's position in supply chains critical to security of supply and as data processor makes it an attractive target and necessitates the continuous development of capabilities.

Recommendations for improving maturity:

- identification of supply chain liabilities and comprehensive partnership risk management that goes beyond direct service providers
- internal exchange of information within the sector and joint continuity training to support the detection and prevention of cyber and hybrid threats posed by state actors.

Overall maturity of the sector



Sector strengths

The strong overall maturity of the sector is particularly evident in the following areas:

- prioritisation of the development of cyber security in business strategies, which correlates with management support and investments
- prevalence of information security management models based on the ISO 27000 information security standard.

Risks and threats in the sector

The most notable risks and threats in the sector:

- workforce-related risks, such as human errors, insider threats, employee turnover and challenges regarding the availability of skilled cyber security specialistst
- threats to supply chains
- cyber and hybrid threats posed by state actors.

Sector weaknesses

Despite the sector's good level of maturity, the following were identified as areas for improvement:

- prioritisation of customer environments and weaker focus on internal systems
- high proportion of legacy systems and slow cloud transition due to uncertainties regarding data processing regulations and customer caution.

Comparison between the 2019–2020 survey and the 2022 survey

The advanced risk management practices and continuity training of ICT and software actors have strengthened the level of preparedness of companies in the sector. On the other hand, the threat situation has developed or, more precisely, become more concrete, meaning that various monitored risks have been realised. The sector's maturity level remains high, but the development of the threat landscape will continue to pose challenges for all companies in the sector in the future as well.

Improved capabilities:

- cyber risk management
- third-party risk management
- practical continuity training.

The sector has made clear progress in cyber risk management practices and business-based cyber security management since the previous survey. Progress has also been made in that third-party management is no longer limited to direct partners, although shortcomings were noted regarding whole supply chains.

6.3 Finance

Sector characteristics

The sector is part of critical national infrastructure, which is integrated into the European-wide financial market. Its current state is characterised by rapid technological development, new technologies and the change in customer expectations caused by the COVID-19 pandemic.

Preparedness is also affected by the following:

- extensive mandatory regulation
- long history as a target of cyber crime
- strong cooperation within the sector.

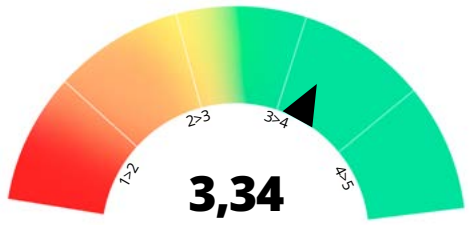
Recommendations for the sector

The financial sector demonstrates a strong maturity level across the board and is able to respond to its diverse threat and risk landscape. The sector's role as a key financier and insurer of society and as an administrator of customer data increases its attractiveness as a target, making the continuous development, protection and improvement of services in terms of cyber security crucial.

The following issues are highlighted as being important for improving maturity:

- further development of strategic guidance and business orientation and their integration into cyber security programme management
- development of the identification and management of supply chains
- continuous development of workforce competence and awareness to respond to the evolving threat environment.

Overall maturity of the sector



Sector strengths

The strong overall maturity of the sector is particularly evident in the following areas:

- strong risk management culture
- comprehensive capability for creating cyber security situational awareness
- high-level management of critical services and incidents.

Risks and threats in the sector

The most notable risks and threats in the sector:

- digitalisation and technology risk, including the expanding use of cloud services
- competence risk in relation to outsourcing and the continued use of legacy infrastructure, for example
- continuous development and diversification of cyber crime.

Sector weaknesses

Even the sector's weakest capabilities are close to maturity level three, which corresponds to a good basic level of maturity. The most critical areas for improvement identified were:

- third-party cyber security management
- comprehensive identification of liabilities with regard to complex subcontracting chains, for example.

Comparison between the 2019–2020 survey and the 2022 survey

The results of the current survey were similar to those of the 2019–2020 survey. The maturity level is stable and consistent across the sector. In both surveys, the impact of regulation is clearly reflected in the level of capabilities and preparedness.

In particular, capabilities related to the management of critical services have been and remain high.

Third-party management and the comprehensive identification and management of dependencies continue to be seen as challenges. The development of management towards ecosystem and whole supply chain thinking is still in progress.

Improved capabilities:

- internal exchange of information and development of cooperation, especially between business areas
- cyber security awareness work and related measures
- the shortage of resources related to partner management seems to have eased.

Other observations:

- Partnership management remains challenging, although progress has been made in ensuring contractual technical controls and the cyber security of critical partners.

6.4 Energy

Sector characteristics

The sector plays a key role in society's security of supply chain. Key challenges in the sector include the development of renewable energy sources and the size of the investments required.

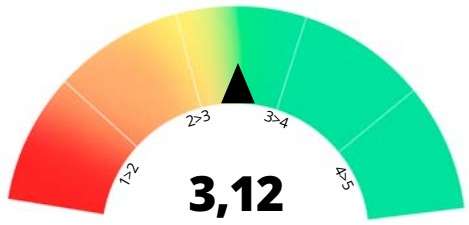
- Digitalisation and the renewal of companies' business operations is driven by the renewable energy transition.
- The Government plays an important role in creating the preconditions for business operations and managing the most notable risks.

Recommendations for the sector

The energy sector's level of maturity is good overall. Cyber security is promoted by a strong culture of preparedness. The threats in this sector are so significant that companies' own preparedness may not be enough, which increases the importance of national and higher level measures.

- integration of the cyber security management of OT environments into the management system
- more extensive assessment of the risk posed by the maturity level variation in the sector.

Overall maturity of the sector



Sector strengths

The good overall maturity of the sector is particularly evident in the following areas:

- systematic and controlled information security management guided by business and risk awareness
- strong culture of preparedness and comprehensive continuity planning supported by the exchange of information within the sector
- access control, in terms of both physical and logical rights.

Risks and threats in the sector

The most notable risks and threats in the sector:

- the sector is a key tool in interstate influencing and conflicts, not all risks can be managed by companies
- technological development opens up integration and threat vectors between IT and OT environments.

Sector weaknesses

Despite the sector's good level of maturity, the following were identified as areas for improvement:

- the sector's pronounced division into high and low maturity level actors
- varied information security culture between actors
- shortcomings related to lifecycle thinking in both partner and identity management.

Comparison between the 2019–20 survey and the 2022 survey

As noted in the previous survey, the energy sector appears to be strongly divided, with companies placed at both ends of the maturity scale in terms of their cyber security capabilities. One thing that has remained consistent between the results of the surveys is challenges in the management of OT security.

Improved capabilities:

- cyber security management
- sharing of threat information.

The sector's preparedness culture has traditionally focused on the prevention of production and distribution disruptions, with less attention paid to cyber security management, for example. Compared to the previous survey, the situation has improved, with mature companies, in particular, now taking a strategic and more comprehensive approach to cyber security development. More and more actors in the sector are collecting threat information, but, as noted in the previous survey as well, there is room for improvement regarding vulnerability management, especially in low maturity level companies.

6.5 Healthcare

Sector characteristics

The objective of healthcare is to promote and maintain the health, wellbeing, working and operating capacity and social security of the population and to reduce health inequalities. The sector's foundation consists of well-functioning preventive, corrective and rehabilitative health services available to the entire population.

- various data protection controls, quality standards and regulations
- sector actors responsible for the data protection and information security of their clients
- service providers that utilise technology for business development.

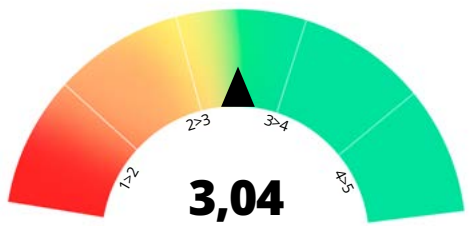
Recommendations for the sector

The healthcare sector demonstrates a good basic level of maturity, being capable of duly managing cyber security with the support of various information security controls and quality standards, for example. The sector's role as a key supporter of public health and wellbeing increases its attractiveness as a target, making the continuous development and improvement of cyber security essential.

Recommendations for improving maturity:

- Due to employee turnover, it is particularly important for actors to ensure that their employees understand their roles in the implementation of the organisation's cyber security.
- Expanding the identification of supply chains and liabilities further along supply chains.
- Comprehensive consideration of information security throughout the software development process in accordance with the DevSecOps approach.

Overall maturity of the sector



Sector strengths

The good overall maturity of the sector is particularly evident in the following areas:

- consistent, continuous development goals
- prevalence of information security management models based on the ISO 27000 information security standard
- risk management, communicating that actors are aware of their critical role in security of supply.

Risks and threats in the sector

The most notable risks and threats in the sector:

- scattered legacy systems
- labour shortage and substitutions, which create differences in competence levels, increasing risks related to ensuring high quality cyber security management and awareness
- supplier risk, the impact of which increased from minor in the previous survey to moderate in this survey.

Sector weaknesses

Despite the sector's good level of maturity, the following were identified as areas for improvement:

- supply chains, in regard to which monitoring the level of cyber security of service providers and the setting of contractual obligations are at a poor level in the healthcare sector
- critical service protection due to poor third-party risk management practices
- preparedness for hybrid threats as part of continuity planning and regular training.

Comparison between the 2019–20 survey and the 2022 survey

The variation in regional results remained similar to the previous survey. The difference in average results between the strongest and weakest domains was less than one level.

Improved capabilities:

- cyber security management
- log management and monitoring of environments.

Despite the variation between organisations, cyber security programme management is the sector's third most mature domain. In particular, the section on cyber security programme governance shows that actors in the sector have improved their cyber security programme management systems since the previous survey.

6.6 Logistics

Sector characteristics

Many other sectors depend on the smooth flow of sector-specific goods. Actors in the logistics sector operate on wheels, rails and in the air. Customers expect more streamlined and transparent service across logistical chains. A critical sector that other sectors are dependent on. There are wildly different actors operating in the sector, ranging from one-person transport companies to global logistics giants.

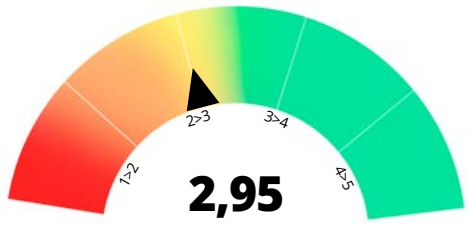
- digitalisation of supply chains
- global competition, in which investment capability is vital
- critical operations that also serve various high security level actors.

Recommendations for the sectorle

The sector is constantly evolving, prone to competition and sensitive to changes in the supply chain, as a result of which special attention must be paid to the comprehensive management of cyber security.

- need for comprehensive development of cyber security programme management
- development of situational awareness to support the creation of up-to-date situational awareness
- comprehensive consideration of information security throughout the software development process in accordance with the DevSecOps model.

Overall maturity of the sector



Sector strengths

The overall maturity of the sector is evident in the following areas:

- consideration of the impacts of cyber security in business strategies
- understanding of critical services and ensuring their continuity.

Risks and threats in the sector

The most notable risks and threats in the sector:

- various threats arising from changes in the global situation, which manifest as e.g. an increase cyber activities and hybrid influencing
- the complexity of logistics chains hinders the identification and management of the risks that they are subject to
- growth of digital supply chains, resulting in expo sure to new threat vectors in supply chains.

Sector weaknesses

The following were identified as weaknesses in the sector:

- shortcomings in the definition and implementation of log management policies
- ensuring comprehensive monitoring of the system level and OT environments
- identification of dependencies between third parties and functions.

Comparison between the 2019–20 survey and the 2022 survey

Compared to the previous survey, the sector showed significantly less variation in domain-specific capabilities. With capabilities varying primarily between individual actors and the sector's maturity levels being largely consistent across domains, no specific domains could be highlighted as strengths or weaknesses.

Improved capabilities:

- The workforce management domain has improved in terms of information security training, the implementation of which was poorer at the time of the previous survey.

6.7 Media

Sector characteristics

The sector is an integral part of information society. Key characteristics include freedom of speech, free and reliable communication and the defence of a democratic society.

- development driven by the utilisation of modern technologies (e.g. cloud services)
- an active sector in terms of corporate acquisitions, which can lead to the acquisitions of both IT and OT environments and legacy technologies
- utilisation of a wide variety of partners ranging from large companies to individual specialists in the sector causes risks.

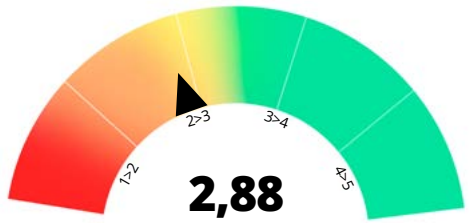
Recommendations for the sector

The improved maturity level of the media sector supports the sector's ability to respond to threats and manage risks. The fact that the sector is a key target for both state-level influencing and criminals raises the risk level, necessitating further risk-based development.

Recommendations for improving maturity:

- development of risk management and risk-based cyber security
- development of supply chain management and ensuring the cyber security of partners, including in the context of acquisitions
- development of cyber security culture in the sector.

Overall maturity of the sector



Sector strengths

The improved overall maturity of the sector is particularly evident in the following areas:

- utilisation of modern technologies and awareness of what needs to be protected improves the preconditions for developing cyber security
- ability to monitor own environments and react to incidents.

Risks and threats in the sector

The most notable risks and threats in the sector:

- the sector's role as a target of both state actors and cyber criminals
- human risks in terms of competence, human errors and influencing activities targeting individual persons
- inadequate due diligence in the context of acquisitions, particularly in relation to cyber security.

Sector weaknesses

Despite the sector's good development, the following were identified as areas for improvement:

- shortcomings in risk management culture
- lack of security thinking as part of development
- poor level of cyber security culture and workforce awareness.

Comparison between the 2019–2020 survey and the 2022 survey

The improved maturity level of the media sectors supports its preparedness for changes in the threat and risk landscape. Since the previous survey, the sector has seen investments especially in technical information security solutions driven particularly by the development of the threat landscape, cyber attacks in the sector and the development of business activities in the sector, which are reflected in maturity levels.

Improved capabilities:

- asset management
- access management
- situational awareness.

The sector has made clear progress in cyber risk management practices and business-based cyber security management since the previous survey. Progress has also been made in that third-party management is no longer limited to direct partners, although shortcomings were noted regarding whole supply chains.

6.8 Food

Sector characteristics

The food sector is an industry that produces food products and ingredients for food products. It is considered one of the cornerstones of society, playing a critical role in security of supply by ensuring the nutrition of the population and productive livestock during disruptions and emergencies.

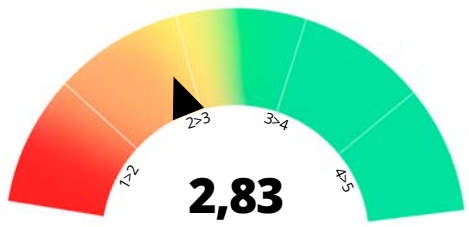
- extensive, complex field of suppliers
- continuity of operations dependent on the availability of inputs
- product safety plays a key role in operational security.

Recommendations for the sector

Food sector companies should focus on measures that improve their level of maturity over the long term. Reactive measures may temporarily increase cyber defence capabilities against specific threats, but do not help to anticipate emerging threats or increase the overall resilience of an organisation. Recommendations for improving maturity:

- outlining of long-term cyber security objectives and drawing up a development plan, thus committing executive management to shared objectives
- development of cyber risk management to support risk-based decision-making.

Overall maturity of the sector



Sector strengths

The sector's most mature practices on average can be found in the following areas:

- Identity and access management are realised in the sector's organisations primarily in accordance with an agreed-upon process.
- One of the strengths in asset management is centralised registers of IT and OT assets, which, in the best cases, also include their configurations. In addition to this, organisations in the sector have a good grasp of information asset management on average.

Risks and threats in the sector

The most notable risks and threats in the sector:

- the complex impacts on business caused by the global pandemic
- use of social manipulation in cyber attacks.

Sector weaknesses

The most critical areas for improvement identified for the sector

- shortcomings in cyber risk management processes and their impact on risk-based decision-making
- shortcomings in cyber security situational awareness as regards the utilisation of log data, for example.

Comparison between the 2019–2020 survey and the 2022 survey

In the food sector, variation between the lowest and highest maturity level organisations has increased slightly compared to the previous survey. The state of many of the areas for improvement identified in the previous survey has remained the same between the surveys. However, progress was noted in two areas.

Improved capabilities:

- asset management, particularly through the centralised system for IT and OT assets
- sharing of threat information.

The sector's preparedness culture has traditionally focused on ensuring product safety, with less attention paid to cyber security management, for example. At present, the sector is very divided, with the cyber security management of the lowest maturity level actors being almost entirely reactive or lacking any structured processes, whereas the highest maturity level actors prepare long-term strategic plans.

6.9 Manufacturing

Sector characteristics

The manufacturing sector's sample included companies from the forestry, construction, chemistry, design, engineering and defence industries. Despite the broad sample, the sector has the following things in common:

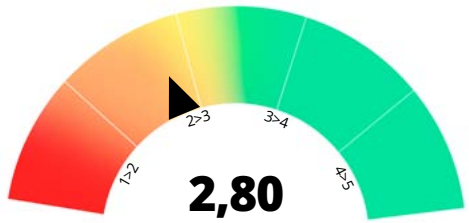
- dependence on disruption-free supply chains
- sensitivity to economic fluctuations and changes in the surrounding world
- financial risks arising from significant investments.

Recommendations for the sector

The manufacturing sector is fragmented in terms of maturity, making preparedness difficult to assess. The sector's average maturity level falls short of a good basic level, which means that responses to threats are not comprehensive. The following areas for improvement were identified in the manufacturing sector:

- expansion of the identification of supply chains and liabilities as far as possible along supply chains
- broader examination of the manufacturing sector, separation of different industries into separate entities
- integration of the management of OT and IT environments, building awareness and visibility on both sides to facilitate comprehensive situational awareness.

Overall maturity of the sector



Sector strengths

The sector demonstrates good maturity in the following areas:

- threat and vulnerability management
- identity and access management
- event and incident response, continuity of operations.

Risks and threats in the sector

The most notable risks and threats in the sector:

- digitalisation of supply chains
- impacts of changes in the geopolitical situation

the risk of grey economy, particularly in the construction industry.

Sector weaknesses

Areas for improvement identified for the sector:

- development of supplier management and identification of liabilities
- risk management, where shortcomings were identified especially in the structured cyber risk management model
- the impacts of the lack of management support and interest in the cyber security programme management domain.

Comparison between the 2019–20 survey and the 2022 survey

The sector has made progress in the three areas for improvement identified in the previous survey, as these three areas were identified in this survey as the ones where the sector's maturity was highest. However, the sector continues to face challenges regarding the isolation of the management of IT and OT environments into different departments.

Improved capabilities:

- threat and vulnerability management
- sharing of threat information
- measures related to continuity planning.

The maturity of third-party risk management remains low, especially in terms of the management of whole supply chains and the identification of liabilities.

6.10 Water Supply

Sector characteristics

The water supply sector plays a key role in maintaining everyday infrastructure and is critical to the functioning of society. Water supply are services that customers easily take for granted. Larger incidents can easily escalate into local disasters.

- focus on the maintenance and reliability of operative activities and systems
- many water supply actors depend on the services of cities or municipalities when it comes to ICT
- broad range of service providers, creating challenges in third-party management in regard to transparency.

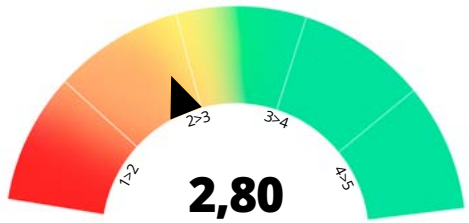
Recommendations for the sector

The overall maturity of the water supply sector falls short of a good basic level. The key role that the sector plays in the functioning of society necessitates further investments in cyber security to ensure that the sector is able to respond comprehensively to cyber threats. The critical societal role of the sector emphasises the maintenance and development of critical services.

Recommendations for improving maturity:

- development of cyber security management and related cooperation with owners and IT providers
- development of third-party risk management and ensuring the cyber security of supply chains through the identification of liabilities and transparency
- development of processes and practices to facilitate up-to-date and comprehensive situational awareness.

Overall maturity of the sector



Sector strengths

The sector's most mature practices are evident in the following areas:

- understanding of the sector's own functions that are most critical to operating reliability
- cyber security management and development based on plans or policies
- practices related to the management of assets, changes and configuration that facilitate rapid response to vulnerability information, for example.

Risks and threats in the sector

The most notable risks and threats in the sector:

- the sector's role as a target of cyber and hybrid influencing activities
- risks related to the availability of raw materials, especially in exceptional circumstances
- challenges in obtaining up-to-date or correct information to build situational awareness.

Sector weaknesses

The following were identified as the most critical areas for improvement for the sector:

- shortcomings in overall cyber security management, especially regarding IT suppliers
- poor visibility of partners' activities in development work
- high dependency on IT service providers.

Comparison between the 2019–20 survey and the 2022 survey

Regional variation in average maturity has remained largely unchanged since the previous survey. Like in the previous survey, variation was greater in organisation-specific results.

Improved capabilities:

- workforce management and development
- policies guiding the development of cyber security
- increased level of maturity of actors conducting their own secure software development.

Perhaps the most significant development between the surveys is related to the development of the threat and risk landscape, as a result of which the water supply sector has also become a potential target for cyber attacks. Many of the risks that have previously been estimated to be low are now being added to monitoring lists. This development also speaks to investments in the maturity of cyber security.

6.11 Trade and distribution

Sector characteristics

Companies in the trade and distribution sector serve as the end points of extensive material flows and operate at the customer interface of the food chain, making them very prone to disruptions.

- extremely dependent on supply chains and their reliability (food and logistics)
- automation plays an important role in the operative activities of both supply chains and e-commerce
- the exceptional impacts of the COVID-19 pandemic on trade and distribution sector actors; restrictions imposed by the authorities and long-term changes in customer behaviour.

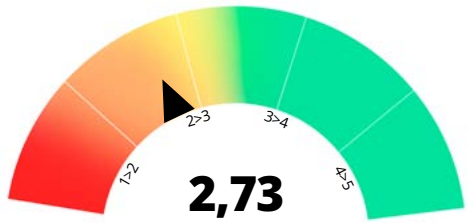
Recommendations for the sector

The overall maturity of the trade and distribution sector falls short of a good basic level, and the sector's preparedness for cyber threats is not comprehensive. The large variation in maturity levels can be indicative of a risk concentration, especially among smaller and local actors.

Recommendations for improving maturity:

- develoment of cyber risk management practices to ensure risk-based decision-making
- integration of cyber security into business and service development.

Overall maturity of the sector



Sector strengths

The sector's most mature practices are evident in the following areas:

- strong identity and access management, especially in terms of physical access management, but some actors also manage digital identities and logical access rights at a mature level
- established culture of ensuring the reliability of operative activities, the best practices of which can also be utilised to ensure cyber security.

Risks and threats in the sector

The most notable risks and threats in the sector:

- impacts of the digitalisation of the business model on protected data and data protection mechanisms and controls
- cyber threats to supply chains
- impacts of crime, including cyber crime and retail crime resulting from inflation, for example.

Sector weaknesses

The following were identified as the most critical areas for improvement for the sector:

- the cyber security perspective is not taken into account as extensively as operative continuity in the following areas, for example: event and incident response, vulnerability management, asset management and critical service protectionen
- lack of cyber risk management culture in most of the organisations assessed and resulting challenges in risk-based decision-making.

Comparison between the 2019–20 survey and the 2022 survey

Compared to the previous survey, it would appear that this time the sample of trade and distribution sector organisations included more low maturity level actors. This served to highlight how polarised the sector's actors are in terms of their maturity in different domains.

Improved capabilities:

- increased awareness of cyber threats and a slight increase in the consideration of cyber security at the management group level.

Companies in the trade and distribution sector appear more divided in terms of their maturity levels than in the previous survey. Due to the changes in sampling, it cannot be estimated with certainty whether the sector has been this divided in terms of maturity for a long time or whether the differences in maturity levels have developed during the years between the surveys.

6.12 Ports and maritime

Sector characteristicsa

A cost-effective and environment-friendly sector. An irreplaceable mode of transport, especially for large tonnage volumes.

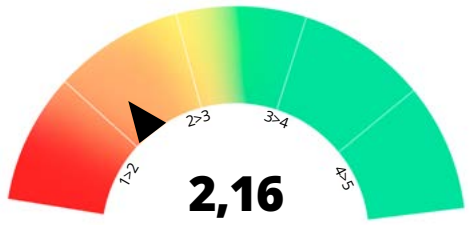
- pronounced role in maintaining national security of supply during emergencies
- tightening GDPR regulation and the impacts of the NIS2 Directive as a result of digital development
- growing environmental requirements.

Recommendations for the sector

The maturity level of the ports and maritime sector is low. In particular, the identified lack of management support prevents the effective promotion of potential development needs and investments for raising overall cyber security maturity.

- development of cyber security programme management based on a longer-term strategy, taking into account a business-based cyber security strategy
- increasing management support to ensure the achievement of cyber security objectives defined and set based on the strategy
- development of the cyber security architecture domain, taking into account especially the shortcomings related to data protection processes identified in the survey.

Overall maturity of the sector



Sector strengths

Despite the sector's low overall maturity level, there are domains where high-quality development could increase maturity to the next level:

- identity and access management
- threat and vulnerability management.

Despite low overall maturity, companies in the sector have good practices, through the further development of which overall maturity can be raised in the future.

Risks and threats in the sector

The most notable risks and threats in the sector:

- exposure to threats and risks with extensive impacts due to the low level of resources allocated to cyber security
- harassment of ships and ports as a result of the war in Ukraine.

Sector weaknesses

The sector's maturity level was identified as resulting in the following weaknesses:

- lack of management support, which hinders the addressing of development needs
- shortcomings in defining and setting a basic level of cyber security management.

Comparison between the 2019–20 survey and the 2022 survey

The state of cyber security in the ports and maritime sector has not significantly changed since the previous survey on the cyber security of Finnish sectors carried out in 2019–2020.

Improved capabilities:

- perceptible change in awareness of and attitudes towards the long-term development of information and cyber security.

The sector continues to face the same challenges, such as lack of resources, lack of management commitment and shortcomings in the communication of IT service providers. The sector's development is supported by the strong commitment of its actors to the National Emergency Supply Organisation. Because of this link, the sector has the potential to develop its cyber security maturity by increasing shared situational awareness and organising shared ways of developing capabilities.

7 Appendices

This sections details the background of the cyber security survey of Finnish sectors and the methods used. Section 7.1 explains the background of the survey and how it follows up on the previous survey carried out in 2019–2020. Section 7.2 describes the implementation of this 2022 survey. The method, tool and assessment criteria used are presented in section 7.3. The final section presents observations about the comparison between the surveys.

7.1 Background of the survey

This cyber security survey of Finnish sectors is a follow-up to a previous survey on the current state of cyber security in different sectors carried out in 2019–2020. Carried out in 2022, the survey involved assessing the current state of the cyber security of 121 Finnish companies from different sectors using a domain-based approach adapted from the Kybermittari (Cybermeter) tool. The workshops organised as part of the survey focused not only on the domains of the Kybermittari tool, but also the most typical risks identified for each sector, following up on the previous survey. The risks identified were also used as the basis for assessing the current state of companies and their preparedness to respond to the threat and risk landscapes of their respective sectors. In addition to this, the 2022 survey examined the use of cloud services and the identification of associated risks and the identification of risks associated with whole supply chains.

The results of the survey will be utilised in the definition of measures for improving the critical infrastructure and national cyber security of Finland. The survey was carried out as part of the Digital Security 2030 Programme of the National Emergency Supply Agency, the aim of which is to strengthen the ability of the Finnish private sector and society to respond to cyber threats and manage cyber security incidents.
The report of the survey carried out in 2019–2020 is available here:
The current state of cybersecurity in different sectors[1]

7.1.1 Implementation of the survey

The 2022 survey included a total of 121 Finnish companies from 12 different sectors. The results of the interviews carried out with the companies are utilised in a comprehensive national level report, which summarises the current state of cyber security across sectors. In addition to this, separate reports were prepared for each sectors. The company-specific results are anonymised; companies are referred to in the reports using company-specific codes. These codes enable companies to identify themselves and their own results from reports.

The assessment tool used in the survey was a domain-based assessment tool adapted from the Kybermittari tool – Kybermittari was not used as is, however. The assessment tool also covered the currently most notable cyber risks in each sector, based on which the current state and preparedness of companies was assessed. Furthermore, the aim was to examine the use of cloud services, attitudes towards them and the identification of the risks associated with them.

The companies included in the survey were sent an advance information package, which included instructions for finding the right parties to participate in an interview. The actual interviews were carried out in the form of discussion-based workshops. With the help of the assessment results and a risk map, each organisation was provided with an overview of their preparedness for major changes in their sector from the perspective of cyber security, their performance in the different domains of cyber security and areas for improvement. The survey thus provided the companies that participated in the workshops with information on their preparedness for cyber threats and broader, sector-specific insights. The final report also provides a cross-sectoral, national-level overview of the current state and areas for improvement of cyber security in Finland.

7.1.2 Assessment scale and criteria

The assessment scale of the maturity assessments was based on a general five-level maturity model similar to the Capability Maturity Model (CMM), for example. The general requirements of the different maturity levels are described in Table 2 below.

Maturity level	Description/general requirements of the level
1	Activities are reactive, processes have not been described or established.
2	Processes are planned, monitored and implemented in accordance with agreed upon procedures. Documentation is not comprehensive and processes are not based on a management system.
3	A management system has been defined and is used, processes are based on the organisation's common standards and policies. No continuous evaluation/auditing, shortcomings in the updating of documentation.
4	The management system implements a continuous improvement model, requirements have been set for the quality and performance of processes, which are also monitored. Activities are systematic.
5	A continuous improvement model supported by technological capabilities and their development (e.g. automation, modern solutions). Processes cover the entire organisation and are linked to the strategic level of the organisation.

Table 2: Descriptions of the maturity levels

Regarding the maturity levels, level 3 corresponds to a good basic level capability. At this level, the risks in the domain can be considered to be under control. It should be noted, however, that it is dangerous to draw conclusions on the capacity of cyber security to protect an organisation based on the maturity assessment. While the maturity assessment can serve as a basis for an assessment of how a capability is managed, determining actual capability requires the use of other testing methods as well. These include various types of information security preparedness exercises, security tests and attack simulations (such as so-called red teaming exercises).

While the assessment scale was a five-level scale similar to the one used in the previous survey, changes were made to two aspects of the assessment: the cyber security domains of the tool were updated and the assessment scale was recalibrated, as part of which the descriptions of the maturity levels were also clarified. As a result of this recalibration, the numerical results of the maturity assessment are not directly comparable to the results of the previous survey. Because of this, the comparisons between the surveys are primarily qualitative in nature, focusing on capabilities within the maturity levels and their development instead of numbers alone.

The survey was carried out utilising Traficom's Kybermittari tool[2]. Kybermittari is a concrete tool aimed at corporate managers and information security professionals for managing cyber security, sector comparisons and steering development investments.

With the help of Kybermittari, organisations can measure their maturity level in the different domains of cyber security management. Kybermittari provides both an assessment of the current maturity level and areas for improvement for reaching the next maturity level. The use of the tool is supported by the fact that the results of the measurements can also be used for benchmarking.

Kybermittari focuses on functions that are critical for business and society and covers the most common domains of cyber security risk management. The tool is based on the existing NIST and C2M2 models and best practices. The tool can also be used to report on capabilities from the perspective of the NIST CSF model. The cyber survey involved utilising only some of Kybermittari's domains instead of carrying out Kybermittari assessments in their entirety. The domains assessed in the survey are listed below in Table 3.

Domains assessed

In the workshops, the cyber security maturity of organisations was assessed in a total of 11 domains based on information provided by the participants in advance.

The domains covered in the survey were defined with the aim of ensuring that the workshops would focus on assessing the cyber security management of organisations.

Domain	Description
PROGRAM	The assessment of the **cyber security programme management** domain focuses on the organisation's ability to manage and maintain an organisation-wide cyber security programme.
ARCHITECTURE	The assessment of the **cyber security architecture** domain focuses on the organisation's ability to manage and maintain its cyber security activities.
RISK	The assessment of the **risk management** domain focuses on the organisation's capacity to identify and manage risk related to information and cyber security (cyber risks).
CRITICAL	The assessment of the **critical service protection** domain focuses on the organisation's ability to recognise its role in the provision of services critical to society and, as a result, their protection.
THREAT	The assessment of the **threat and vulnerability management** domain focuses on the organisation's ability to define and maintain plans, processes and technologies to detect, identify, analyse, manage and address cyber threats and vulnerabilities.
ASSET	The assessment of the **asset, change and configuration management** domain focuses on the organisation's ability to manage its hardware, software and information assets commensurate with the risk to the organisation and organisational objectives.
WORKFORCE	The assessment of the **workforce management** domain focuses on the cyber security awareness, skills and readiness to respond to various cyber incidents of the organisation's workforce.
THIRDPARTY	The assessment of the **third-party risk management** domain focuses on the organisation's ability to identify and manage risks related to supply chains and third parties.
SITUATION	The assessment of the **situational awareness** domain focuses on the organisation's capacity to maintain cyber security situational awareness
RESPONSE	The assessment of the **event and incident response, continuity of operations** domain focuses on the organisation's ability to manage, respond to and recover from cyber security incidents.
ACCESS	The assessment of the **identity and access management** domain focuses on the organisation's ability to manage and restrict logical and physical access rights to the company's protected assets.

Table 3: The domains assessed in the survey

Sector risk assessment

The workshops carried out as part of the survey also involved carrying out a sector risk assessment. The sector risk lists are based on the previous survey, but were expanded in this survey to include the risk of a global pandemic.

The risk scores were determined on the basis of self-assessments carried out by the participating companies. Companies assessed the probability and impact of risks both from their own perspective and as part of their sector's whole supply chain. Sector risks were assessed based on the formula of probability x impact. Probability and impact were assessed on the basis of a five-point scale, which is presented in Table 4 below.

Probability		Impact	
1	Rare	**1**	Trivial
2	Improbable	**2**	Minor
3	Possible	**3**	Moderate
4	Probable	**4**	Significant
5	Very probable	**5**	Very significant

Table 4: The risk assessment scale

7.1.3 Comparison of the results of the surveys

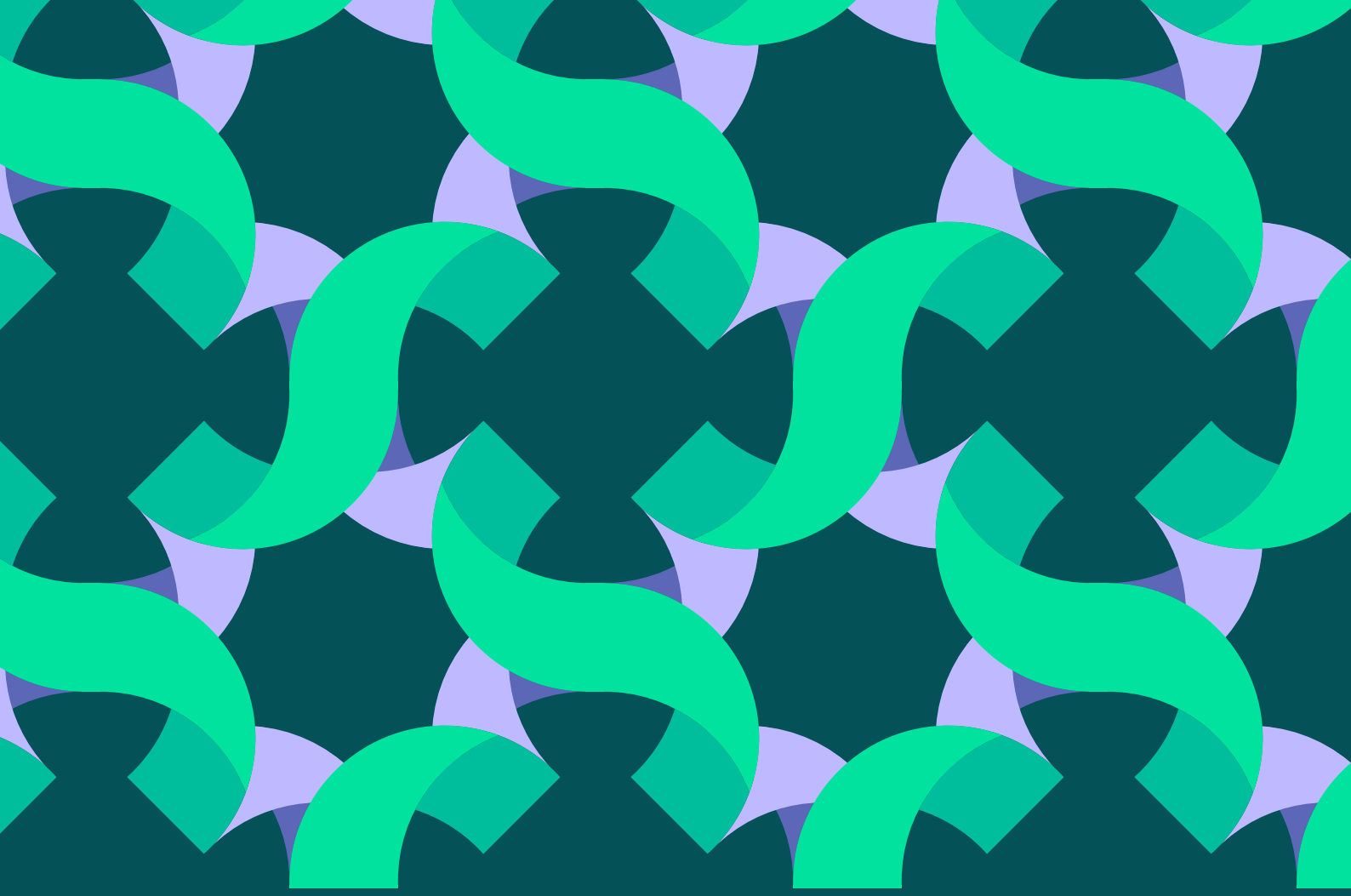
The 2019 –2020 survey and the 2022 survey are not directly comparable due to the changes made to the assessment tool and the revised assessment criteria.

Because of this, the conclusions provided in the comparison section are based on the capabilities and processes identified in the assessments instead of numerical values. The aim in the comparison was to assess development between 2020 and 2022 in general and in relation to threat and risk assessments and the sector risk assessment. It should be noted that the comparison was also further complicated by sampling issues. The exact sampling of the first survey was not used in the implementation of this survey. To ensure confidentiality, detailed sampling is also not reported for this survey. Because of this, the exact impacts of sampling on the maturity assessments could not be assessed or taken into account in the analysis. The number of sectors and companies included in this survey differed from the number of sectors and companies included in the previous survey.

Because of the aforementioned reasons, the comparison between surveys was carried out in accordance with the precautionary principle, with conclusions drawn mainly in areas where they are backed up at least by some reliable data. However, even these conclusions should be considered notably uncertain and not very reliable.

[1]https://www.digipooli.fi/sites/digipooli/files/2021-06/The-current-state-of-cybersecurity-in-different-sectors_2020.pdf

[2]https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/kybermittari-cybermeter



Huoltovarmuuskeskus
Försörjningsberedskapscentralen
National Emergency Supply Agency