EUROPEAN UNION AGENCY
FOR CYBERSECURITY

NIS INVESTMENTS 2024

Cybersecurity Policy Assessment

NOVEMBER 2024

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services, and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building, and awareness raising, the Agency works with its key stakeholders to strengthen trust in the connected economy, increase the resilience of the Union's infrastructure, and, ultimately, keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

To contact the authors, please use resilience@enisa.europa.eu.
For media inquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Athanasios Drougkas, Ugne Komzaite, Eleni Philippou, ENISA
Patrick Abel, François Gratiolet, Edwin Maaskant, Gartner

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-676-7, ISSN 2600-4712, DOI : 10.2824/5220134, Catalogue nr. TP-01-24-001-EN-N

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report aims at providing policy makers with evidence to **assess the effectiveness of the existing EU cybersecurity framework** specifically through data on how the NIS Directive has influenced cybersecurity investments and overall maturity of organisations in scope. As 2024 is the year of the transposition of NIS 2, this report also intends to capture a **pre-implementation snapshot of the relevant metrics for new sectors and entities in scope of NIS** 2 to help future assessments of the impact of NIS 2.

This fifth iteration of the report presents data **from 1350 organisations from all 27 EU Member States covering all NIS 2 sectors of high criticality, as well as the manufacturing sector**. As the past couple of years have been characterised by a proliferation of the EU cybersecurity policy framework with the introduction of key horizontal (e.g. CRA) and sectorial (e.g. DORA, NCCS) legislation, the report provides insights into the readiness of entities to comply with these new requirements, as well as into the challenges they face. Moreover, a sectorial deep dive was conducted for entities in the Digital infrastructure and Space sectors. Key findings from the report include:

- Organisations earmark 9,0% of their IT investments for Information Security, **a significant increase of 1.9 percentage points compared to last year**.
- Organisations allocate 11,1% of their IT FTEs for information security a **decrease of 0,8% compared to last year**, despite the overall increase in cybersecurity spending and **the fourth year in a row where a decrease in this metric is observed**.
- **89% of organisations will require more cybersecurity staff to comply with NIS 2**, primarily in the cybersecurity architecture and engineering (46%) and cybersecurity operations (40%) domains.
- Organisations will also need **additional FTEs to comply with other horizontal** (CRA - 85%) **or vertical** (DORA - 84%; NCCS - 81%) **cybersecurity legislation**.
- Most organisations anticipate **a one-off or permanent increase in their cybersecurity budgets for compliance with NIS 2** though a substantial number of **entities will not be able to ask for the required additional budget**, a percentage that is especially high for SMEs (34%).
- 51% of surveyed organisations reported that their leadership participates in dedicated cybersecurity training **a 2% increase compared to last year**.
- **Sectors previously covered by NIS reported higher perceived maturity** in cyber-risk management (6.8 vs. 6.2), network and information security arrangements (7 vs. 6.3), and cyber-attack detection and response capability (7.1 vs. 6.3) compared to new sectors.
- **Sectors newly covered by the NIS 2 Directive in most cases lag behind sectors already covered by it** in areas such as participation in information-sharing initiatives (60% non-participation), participation in cybersecurity preparedness initiatives, controls to establish trust in supply chain (20% implicitly trust it).
- Only 4% of organisations have already invested in Post-Quantum Cryptography, while **68% of respondents indicated that they will not invest in QSC**.
- **90% of entities expect an increase in cyberattacks in the coming year.** Despite this, **participation in cybersecurity preparedness initiatives is predominantly internal,** with 74% of organisations engaging in such activities within their own companies.

1. INTRODUCTION

This report is the fifth edition of the NIS Investments study published by the ENISA to understand how the **Directive concerning measures for a high common level of security of network and information systems across the Union (NIS Directive**)[1] has impacted the cybersecurity investments, cybersecurity strategy and cybersecurity posture of organisations in scope, and what is the respective projected impact of the **Directive on measures for a high common level of cybersecurity across the Union** (**NIS 2 Directive**)[2] which replaced the NIS Directive as of October 2024.

The NIS 2 Directive which, during the time of this study, is being transposed across the EU (European Union), represents a significant update to the previous NIS Directive. It expands the scope of the NIS Directive to cover a wider range of organisations and imposes more stringent cybersecurity requirements. These changes are likely to have a significant impact on how entities in scope allocate their cybersecurity budgets and manage their risks.

As the implementation of the NIS 2 Directive is under progress, it will be essential to monitor its effectiveness and assess its impact on the cybersecurity posture of organisations across the EU. The insights provided in this report can serve as a valuable baseline for future analysis and inform policy decisions related to cybersecurity.

To ensure representative results, a total of **1,350 organisations were surveyed across 27 EU Member States**, hence **50 organisations per Member State**. Additional information on the demographics of the survey is available in Annex A. This report collects data from entities already in scope of the NIS Directive as well as entities that will be in scope of NIS 2. **The terms "organisations" or "entities" will be used throughout chapters 3 – 9 to refer to surveyed entities**.

For this study, entities from all sectors of high criticality (listed in Annex I of NIS 2 Directive) and the manufacturing sector (listed in Annex II of NIS 2 Directive) have been surveyed. This year's report also provides a more in-depth analysis for entities in the Digital Infrastructure and Space sectors.

The target audience of this report is EU and national policymakers. It is part of a series designed to produce historical datasets to track the development of key indicators – such as information security (IS) budgets – over time. These reports also assess how policy influences these indicators, providing insights and evidence to inform policy decisions. This work is part of ENISA's Cybersecurity Policy Observatory (CSPO) activities.

[1] European Union. (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148

[2] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555

2. INFORMATION SECURITY DYNAMICS AND OUTLOOK

This chapter provides a high-level overview of global trends and perspectives in information security, using independently gathered data and metrics to enhance and contextualise the survey's findings.

The following sections of this chapter address key areas that either enhance the understanding of the context in which the surveyed entities operate by covering topics outside the survey scope, or complement the insights it provides, specifically in the following areas:

- **Spending:** Forecasts for information security spending across domains, equipment, and services, along with year-on-year spending trends by region.
- **Priorities:** Analysis of top technology investment areas for businesses, security priorities for midsize enterprises, and the balance between third-party risk management investment and operational interruptions.
- **Workforce Challenges:** Examination of information security full-time employees as a percentage of IT FTEs by region, the cybersecurity talent gap, and its impacts.
- **Impact of AI:** Analysis of AI-related breaches and security concerns, as well as applications of AI in cybersecurity.
- **Cybersecurity Incidents and Vulnerabilities:** Key insights into security incidents and vulnerabilities.

2.1 INFORMATION SECURITY SPENDING

2.1.1 Forecast spending on information security and risk management

The following section provides forecast data for the global security market. Data is presented by region for key segments of the security industry.

By the end of 2023, the information security market reached € 146 billion, growing by 12.7% annually[3]. This growth is due to the high priority placed on information security by CIOs and tech leaders, driven by increased threats, cloud adoption, and a shortage of skilled professionals.

The market is projected to grow to €166 billion by 2024[4]. Key growth factors include the use of AI by both providers and attackers, leading to increased investment in security software for applications, data, privacy, and infrastructure protection. The ongoing adoption of cloud technology will boost demand for cloud security and enterprise networking security. The shortage of skilled professionals is also expected to drive investment in security services. However, market consolidation and economic factors may slightly slow growth in the coming years.

In contrast, consumer security software is the slowest-growing segment, with an annual growth rate of approximately 5%.

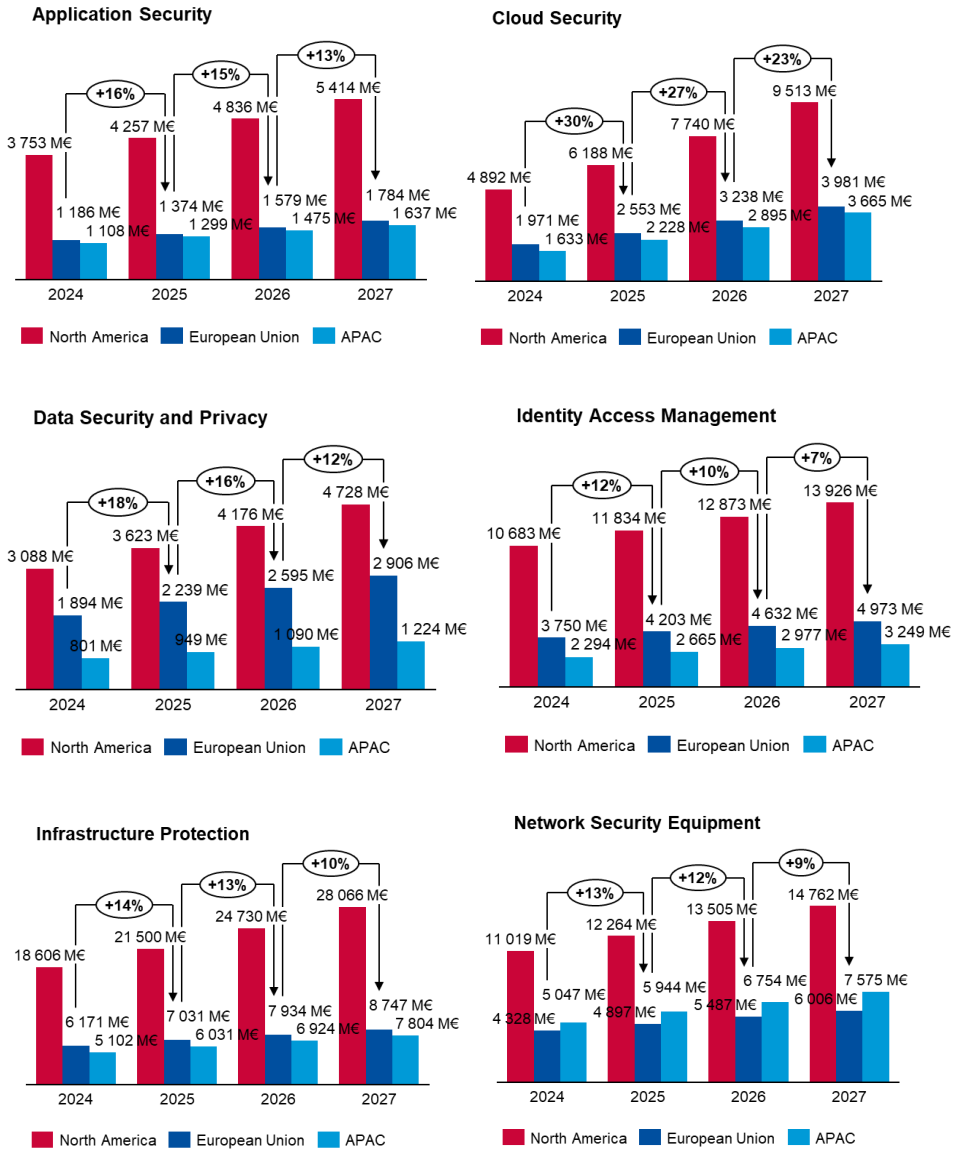
[3] Gartner. (2024). Forecast: Information Security and Risk Management, Worldwide, 2022-2028, 2Q24 Update
[4] ibid

Figure 1 depicts the forecast of information security spending per region and security segments.

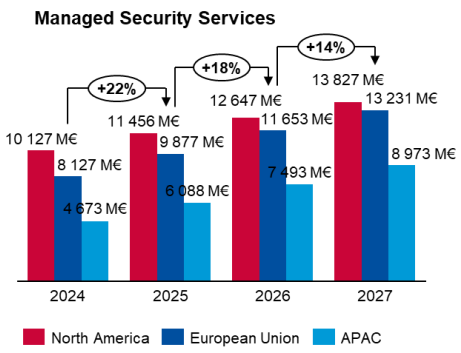
Overall, the North American market remains ahead of other regions, with continued growth in every segment over the next three years.

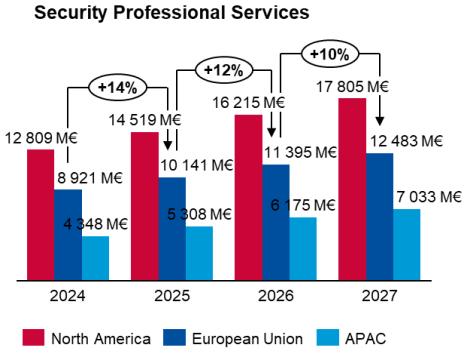
Cloud security is the fastest-growing segment in the security industry, with an annual growth rate of approximately 25% projected through 2027. In contrast, consumer security software is the slowest-growing segment, with an annual growth rate of approximately 5%.

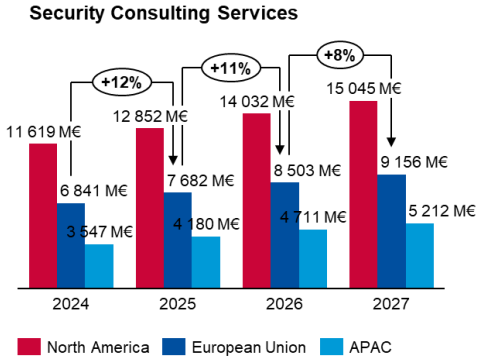
Figure 1: Breakdown of information security spending per region and security segment[5]

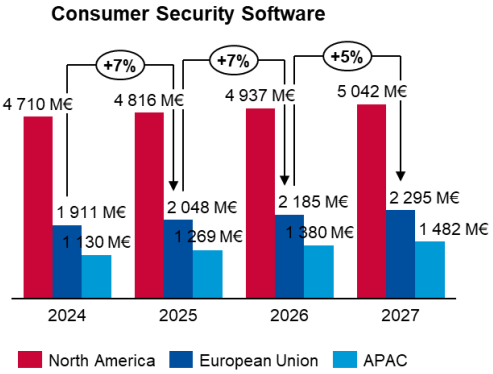


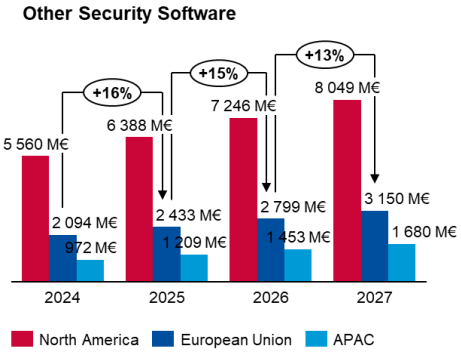
[5] ibid











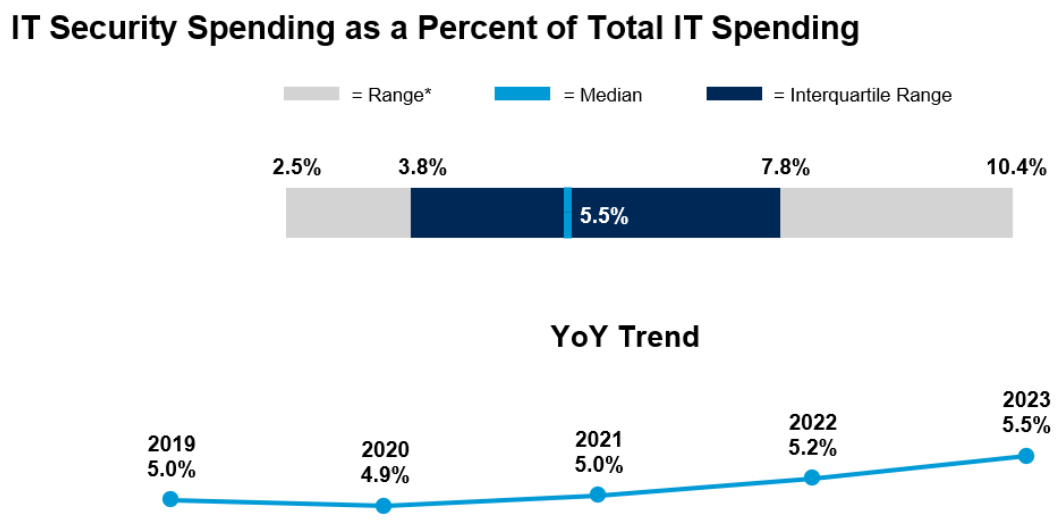
2.1.2 Information security spending

Information security spending as a percentage of Information Technology (IT) spending is a key metric used to capture an organisation's investment level in securing its total IT environment[6].

Figure 2 illustrates the global year-over-year (YoY) trend of this metric. Information security spending as a share of IT spending reached 5.5% in 2023, marking a consecutive increase of 0.3 percentage points from 2022, following a 0.2-point rise the previous year[7]. This trend indicates that organisations are increasing their IS investments relatively to their IT investments.

[6] Boston Consulting Group. (2018). Are You Spending Enough on Cybersecurity?
[7] Gartner. (2024). IT Key Metrics Data 2024: IT Security Measures — Analysis

Figure 2: Information security spending as a percentage of total IT spending globally



Source: Gartner (2023)
* Range includes the 10th to 90th percentile of the sample.
ID: 801291

Furthermore, the IS technology market is expected to experience significant growth in the coming years. By 2030, global spending on information security is projected to more than triple from 2017 levels, fuelled by the rise of digital threats, increased focus on data protection, and the adoption of advanced technologies like AI and cloud-based solutions.[8]

In addition, Table 1 provides a regional breakdown of information security spending, offering further insight into how different areas allocate budgets within the IS technology market.

Table 1: Information security spending metrics by region[9]

Region	IS spending as % of IT spending 2022 *(average)*	IS spending as % of IT spending 2023 *(average)*
North America (NA)	6.4%	6.7%
European Union*	**5.1%**	**5.6%**
Asia Pacific (APAC)	6.3%	6.1%

*The peer group does not include Cyprus

[8] Statista. Global Security Technology and Services Market Spending by Segment (2023)
[9] Gartner, Security Spend Analytics Workbench.

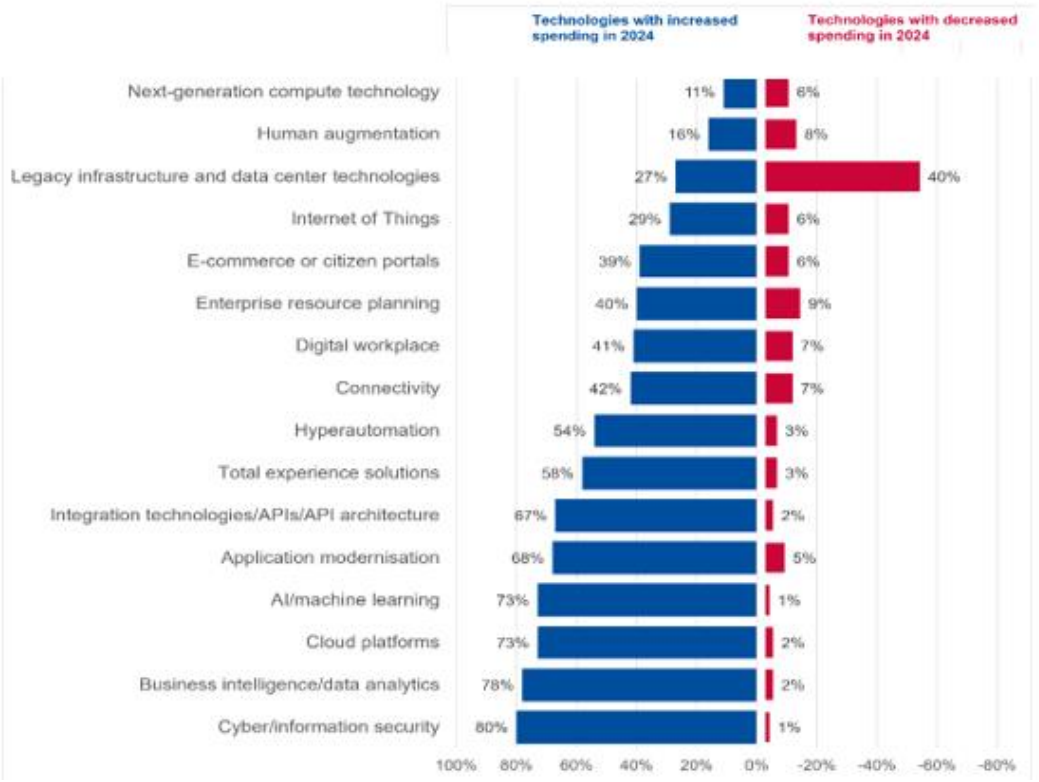
2.2 CYBERSECURITY PRIORITIES

2.2.1 Investment Priorities

This section outlines the top investment priorities among CIOs and technology executives who participated in a 2024 survey[10], representing various regions, revenue bands, and sectors (both public and private). Figure 3 highlights the technology areas where respondents plan to allocate the most significant new or additional funding in 2024 compared with the previous year, as well as areas where budgets will be reduced.

As shown in Figure 3, information security, business intelligence/data analytics (BI/DA), and cloud platforms remain top priorities for increased investment among CIOs and technology leaders, consistent with trends observed last year. Notably, 80% of respondents anticipate raising their information security budgets, underscoring its importance as a strategic focus for most organisations.

Figure 3: Top technologies for new or increased spending by CIOs in 2024 compared to 2023



In a 2024 survey[11], alongside investments in information security, data analytics, and cloud platforms, CIOs emphasise digital transformation initiatives and AI adoption. Increasingly, they focus on enhancing automation, improving decision-making through data insights, and building agile infrastructures to support business continuity. This strategic focus addresses the need for adaptive, data-centric approaches that align IT capabilities with rapidly evolving market demands.

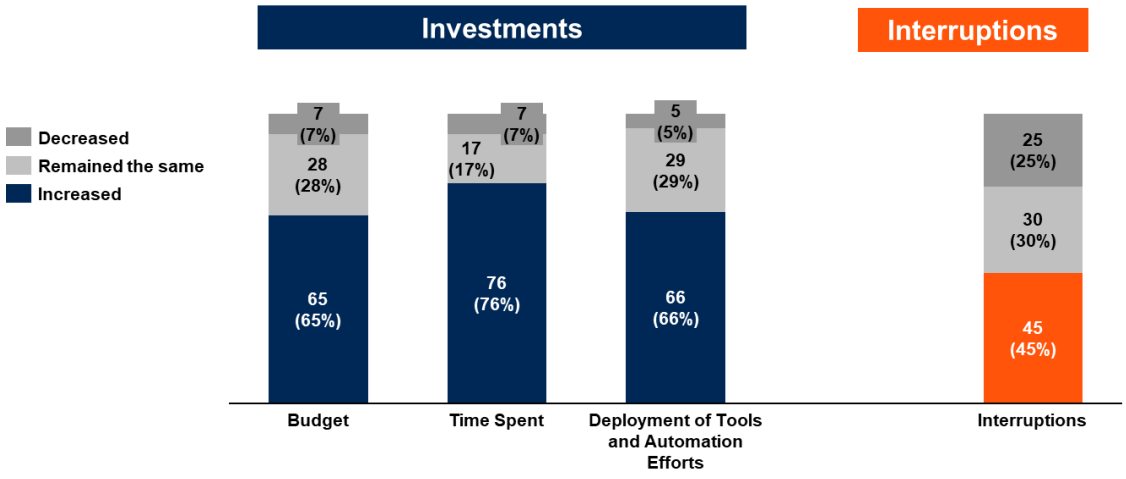
[10] Gartner. (2024). 2024 CIO and Technology Executive Survey, conducted in 2023 on 2,457 CIOs and technology executives.
[11] PwC. (2024). CIO Executive Leadership Hub.

2.2.2 Third-Party Cyber Risk Management

Over 370 organisations were surveyed in 2023 as part of a Third-Party Cybersecurity Risk Management (TPCRM) study[12], which explored key practices for cybersecurity leaders to enhance management of risks associated with third-party relationships. This study provides valuable insights into effective strategies for strengthening third-party cybersecurity risk management across various sectors.[13]

Key findings from this survey, illustrated in Figure 4, reveal that despite increased investments in TPCRM from 2021 to 2023 by 65% of organisations, an increase in time dedicated to TPCRM by 76%, and the deployment of new tools by 66%, nearly 45% of organisations still reported a rise in business disruptions due to third-party incidents. This suggests that cybersecurity teams face significant challenges in building resilience against third-party disruptions and influencing business decisions related to third-party risks.

Figure 4: 3rd party cyber-risk management evolution of investments against business interruptions between 2021 and 2023



2.3 CYBERSECURITY WORKFORCE CHALLENGES

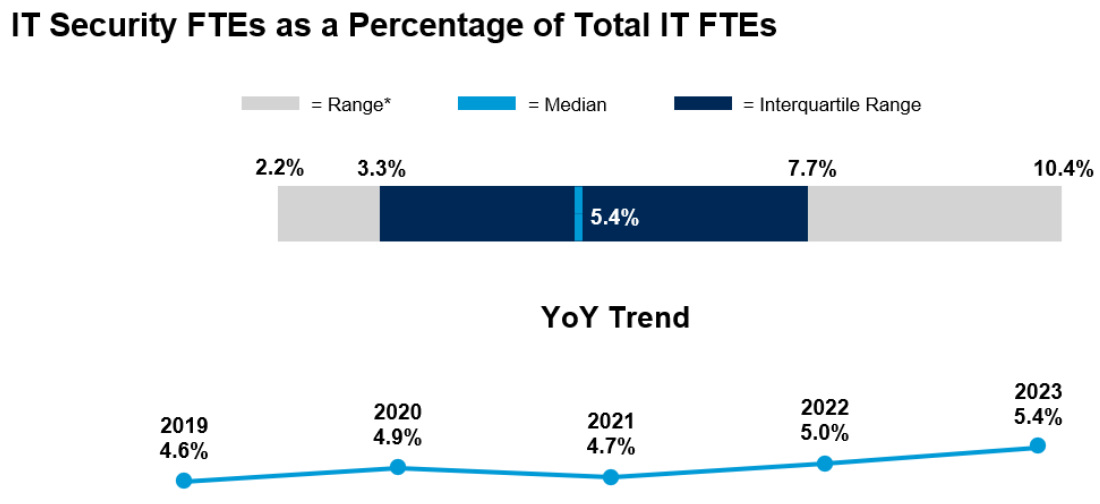
2.3.1 Information security staffing

Aligned with the approach in section 2.1.2, data was collected on a key metric related to information security staffing: IT security full-time equivalents (FTEs) as a percentage of total IT FTEs. This metric measures the intensity of IT security support from a human capital perspective, offering insights into whether the security staff size is appropriate for supporting a secure IT environment.

Figure 5 shows the year-over-year trend for this metric on a global scale. In 2023, information security staffing, which includes both internal personnel and contractors, accounted for 5.4% of total IT personnel.

[12] Gartner. (2024). Infographic: Minimise Disruption from Third-Party Cybersecurity Risks
[13] ibid

Figure 5: IT Security FTE as a Percentage of Total IT FTEs year over year evolution[14]



Source: Gartner (2023)
* Range includes the 10th to 90th percentile of the sample.
ID: 801291

In addition, Table 2 provides a regional breakdown of information security staffing, offering further insights into staffing levels across different regions.

Table 2: Information security staffing as a percentage of total IT staffing globally

Region	IS FTEs as % of IT FTEs 2022 *(average)*	IS FTEs as % of IT FTEs 2023 *(average)*
North America (NA)	6.5%	6.2%
European Union*	**4.5%**	**5.9%**
Asia Pacific (APAC)	6.3%	5.4%

*The peer group does not include Cyprus

While North America and Asia Pacific saw slight decreases in IS staff as a percentage of total IT staff from 2022 to 2023, the EU showed a notable increase, suggesting a heightened focus on cybersecurity resources within the EU.

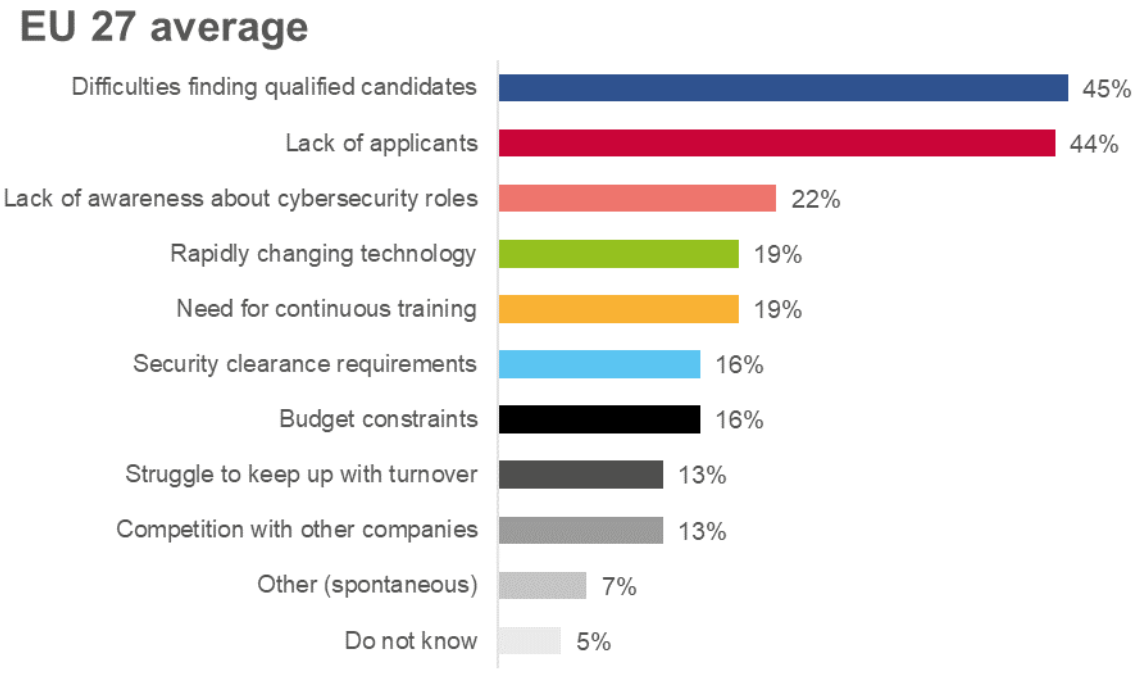
2.3.2 Talent scarcity and impacts

A recent Eurobarometer survey reveals that the cybersecurity talent gap across the EU is widening, with a significant number of organisations struggling to recruit and retain staff with essential cybersecurity skills.[15] Many companies report difficulties in recruiting cybersecurity staff, which hampers their ability to maintain a strong security posture. This shortage particularly

[14] Gartner. (2024). IT Key Metrics Data 2024: IT Security Measures — Analysis
[15] European Commission. (2024). Eurobarometer: EU faces growing cybersecurity skills gap. Available at: https://europa.eu/eurobarometer/surveys/detail/3176

affects technical roles essential for safeguarding digital infrastructure, which remain hard to source.

Figure 6: Key challenges in recruiting cybersecurity talent[16]



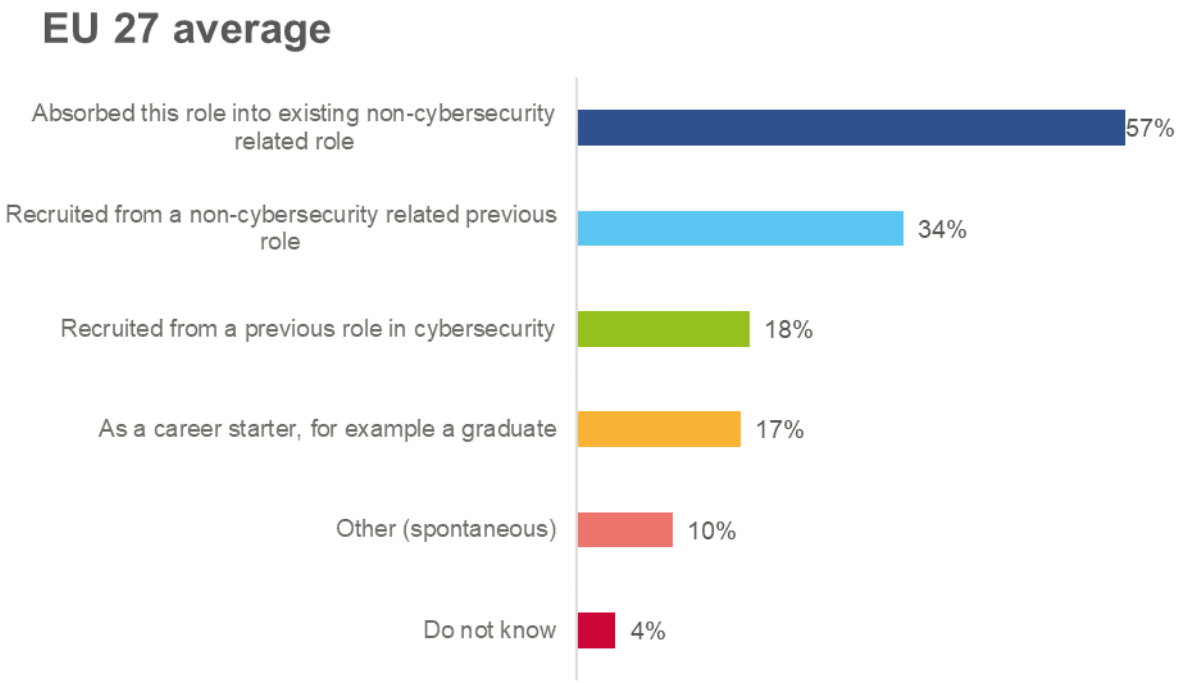
The lack of skilled professionals creates challenges for organisations in meeting their cybersecurity objectives, impacting overall security resilience. Many of them now face delays in implementing essential security measures, increasing their exposure to cyber threats. The digital skills gap poses a particularly serious challenge for small and medium-sized enterprises (SMEs), with nearly half indicating that a lack of in-house cybersecurity expertise leaves them vulnerable to cyber incidents.[17]

Recent research highlights that specific cybersecurity skill areas, such as incident response, cloud security, and application security, are among the most challenging to fill. Furthermore, the growing demand for expertise in artificial intelligence (AI) and machine learning within cybersecurity has created significant skill gaps, with many organisations unable to source qualified candidates. These shortages are compounded by rapid technological advancements and the shift toward cloud-based systems, increasing complexity for security teams.[18]

A significant 76% of employees in cybersecurity roles lack formal qualifications or certified training creating critical skill gaps in the workforce[19]. As shown in Figure 7 below, 34% have transitioned from non-cyber roles, and 57% handle cybersecurity alongside other duties. These factors highlight the need for more targeted training and certification efforts to strengthen cybersecurity resilience across organisations.

[16] European Commission. (2024). Eurobarometer: EU faces growing cybersecurity skills gap. Available at: https://europa.eu/eurobarometer/surveys/detail/3176
[17] Yaqoob, I., Salah, K., Jayaraman, R., Omar, M., & Ahmed, E. (2023). Cybersecurity Skills Gap: A Growing Problem and Steps to Bridge the Gap. Available at: https://arxiv.org/abs/2309.17186
[18] (ISC)². Cybersecurity Workforce Study, 2023. Available at: https://www.isc2.org/Research/Cybersecurity-Workforce-Study
[19] European Commission. (2024). Eurobarometer: EU faces growing cybersecurity skills gap. Available at: https://europa.eu/eurobarometer/surveys/detail/3176

Figure 7: Key challenges in recruiting cybersecurity talent[20]



This shortage in cybersecurity talent is recognised as a top risk, with implications for both the frequency and cost of cyber incidents. Skills shortages contribute to delays in detecting and responding to breaches, increasing the likelihood and financial impact of cyber incidents.

2.4 IMPACT OF ARTIFICIAL INTELLIGENCE (AI)

2.4.1 Cybersecurity of AI and AI for cybersecurity

The growing use of enterprise applications that incorporate prompts supported by commercial or proprietary Large Language Models (LLMs) expands an organisation's attack surface, creating new entry points for threat actors. This shift emphasises the importance of secure and ethical AI adoption, as LLMs introduce unique risks, such as susceptibility to prompt injections and adversarial manipulation. As organisations explore these advanced tools, establishing robust security protocols and ethical guidelines for AI integration becomes essential to mitigate potential threats and ensure safe deployment.

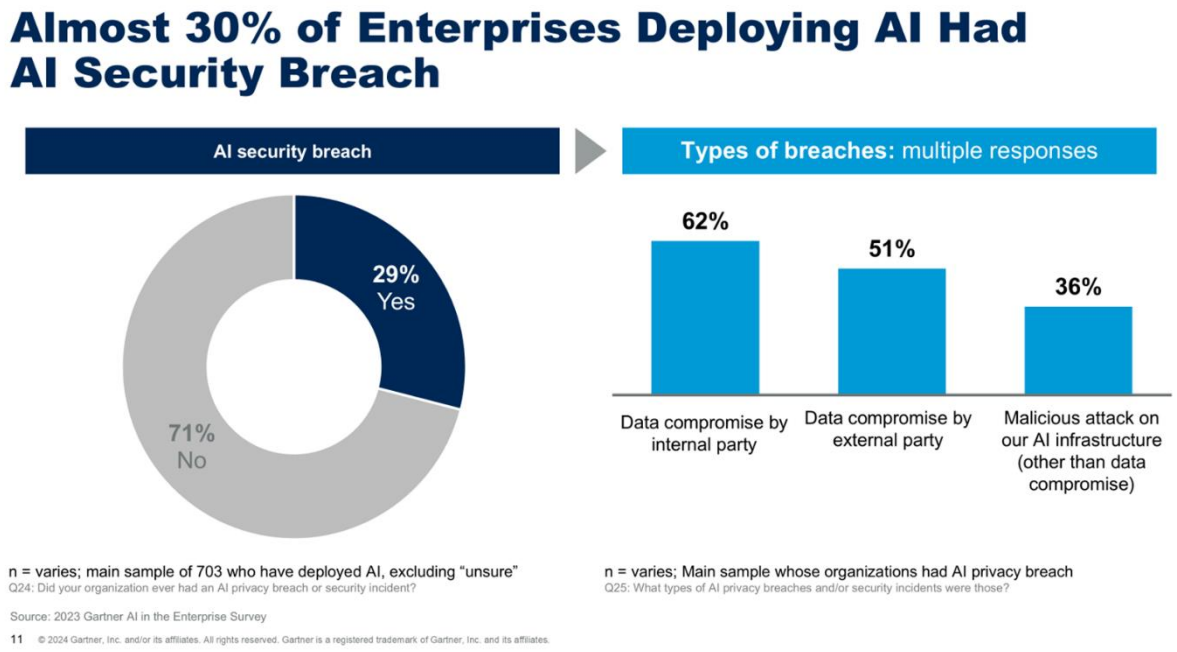
Cybersecurity of AI

A recent report highlights that while many organisations recognise the risks associated with AI, only two-thirds have implemented a documented strategy to address them. Additionally, a concerning 80% of organisations have not yet conducted audits of their third-party vendors for AI-related vulnerabilities, underscoring a critical gap in proactive risk management[21].

[20] European Commission. (2024). Eurobarometer: EU faces growing cybersecurity skills gap. Available at: https://europa.eu/eurobarometer/surveys/detail/3176
[21] Ivanti. (2024). State of Cybersecurity Report

A recent 2024 survey on AI in enterprise use[22] reveals that nearly 30% of organisations deploying AI have experienced AI-related security breaches. Figure 8 provides a detailed breakdown of these breaches by type.

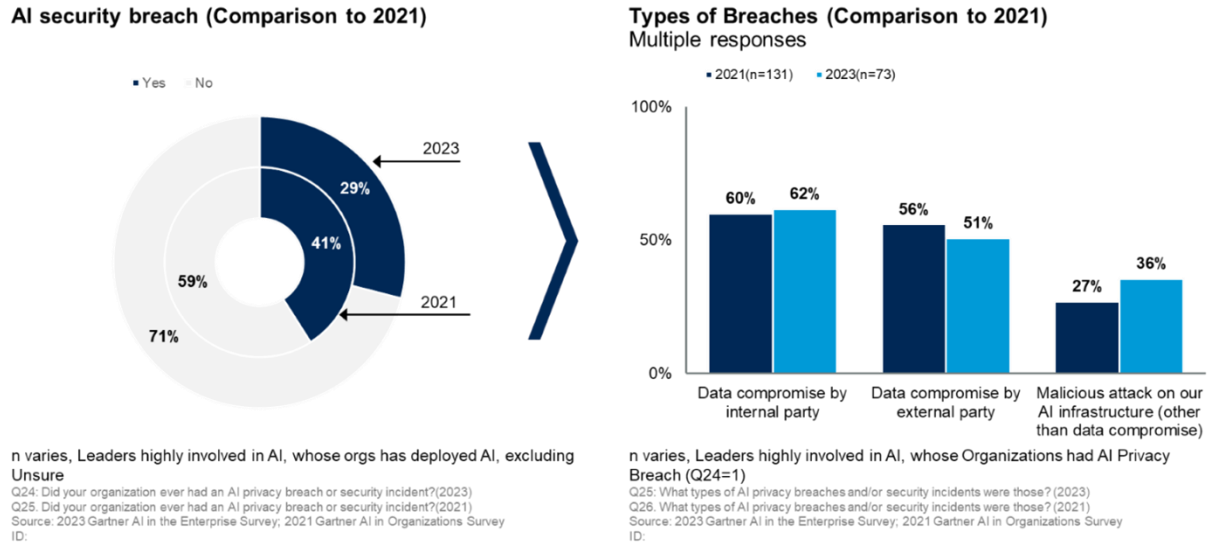
Figure 8: AI security breach and breakdown by type of breach



Encouragingly, the frequency of AI security breaches has decreased from 41% in 2021 to 29% in 2023, as shown in Figure 9. This trend suggests improvements in managing AI security risks.

[22] Gartner. (2024). AI in the Enterprise Survey

Figure 9: AI security breach in 2023 compared to 2021

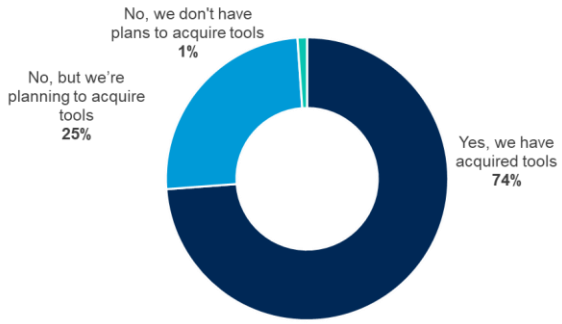


n varies, Leaders highly involved in AI, whose orgs has deployed AI, excluding Unsure
Q24: Did your organization ever had an AI privacy breach or security incident?(2023)
Q25. Did your organization ever had an AI privacy breach or security incident?(2021)
Source: 2023 Gartner AI in the Enterprise Survey; 2021 Gartner AI in Organizations Survey
ID:

n varies, Leaders highly involved in AI, whose Organizations had AI Privacy Breach (Q24=1)
Q25: What types of AI privacy breaches and/or security incidents were those? (2023)
Q26. What types of AI privacy breaches and/or security incidents were those? (2021)
Source: 2023 Gartner AI in the Enterprise Survey; 2021 Gartner AI in Organizations Survey
ID:

74% of organisations report acquiring new tools for AI privacy, security, and risk management, which may contribute to this positive trend.

Figure 10: AI privacy, security and/or risk management deployment



n = 642, Main sample; Excludes Unsure
Q26: Has your organization acquired tools for AI privacy, security and/or risk management?
Source: 2023 Gartner AI in the Enterprise Survey
ID:

AI for cybersecurity

A recent report[23] reveals that organisations are swiftly implementing Generative AI, and perceptions of its advantages are changing just as fast. Just eight months ago, only 17% of Chief Information Security Officers (CISOs) saw generative AI as beneficial to security efforts, but now nearly half (43%) believe it offers advantages for defenders.

This shift reflects vendors' increased integration of generative AI into security products, which is enhancing security workflows. As a result, more than a third of CISOs now recognise significant potential for generative AI in four key cybersecurity areas: identifying risks (39%), analysing

[23] Splunk. (2024). State of Security Report

threat intelligence (39%), detecting and prioritising threats (35%), and summarising security data (34%).

Moreover, 86% of organisations believe generative AI can help attract entry-level cybersecurity talent, with 58% expecting it to expedite the onboarding process for new hires. Additionally, 65% of experienced security professionals anticipate productivity gains from generative AI through faster synthesis of news and information, accelerated research, and optimised detection engineering[24].

2.5 CYBERSECURITY INCIDENTS AND VULNERABILITIES

2.5.1 Cybersecurity incidents

A 2024 report reveals that the average cost of a data breach has risen to €4.4 million, marking a 10% increase over the previous year. This figure includes a range of expenses, such as lost revenue, customer attrition, recovery efforts, and regulatory penalties. Sector-specific data shows that health sector remains the most impacted, with breach costs averaging around €8.4 million. Regionally, the United States leads globally with an average breach cost of approximately €8.4 million, while within the EU, Benelux records the highest average cost at €5.3 million, followed by Germany at €4.8 million, and Italy at €4.3 million[25].

One major contributor to data breaches is "shadow data" or hidden data, which accounts for nearly one-third of all breaches. This type of data, stored in unmanaged sources and often scattered across multiple systems and devices, is challenging to track and secure. Consequently, breaches involving shadow data are typically more costly and time-consuming to resolve. In addition, the report highlights that 46% of breaches involve customers' Personally Identifiable Information (PII), 43% target intellectual property (IP), and 37% involve employees' PII, underscoring the variety of sensitive data commonly at-risk during incidents[26].

Additionally, human error continues to play a significant role in data breaches, with 68% of incidents in 2024 attributed to such errors, consistent with previous years. Phishing remains a widespread threat; during simulation exercises, 20% of users reported phishing attempts, and of those, 11% still clicked on the malicious links. Notably, the median time for a user to click a malicious link is just 21 seconds after opening a phishing email, with another 28 seconds to enter their data. This rapid response highlights the need for ongoing security awareness training to mitigate the risks posed by phishing and human error, which can lead to breaches in under a minute.[27]

2.5.2 Vulnerabilities

From late 2022 to late 2023, 60% of breaches exploited known vulnerabilities for which patches were available but not applied, underscoring the need for prompt patch management. During this period, vulnerability exploitation surged, showing a 180% increase as a primary method of attack. Despite available patches, organisations still delay remediation, taking about 55 days on average to address half of critical vulnerabilities. This slow response allows attackers prolonged access to unpatched systems, raising the risk of successful breaches.[28]

Since early 2023, disclosed zero-day vulnerabilities have shifted focus from file management software to VPNs and edge devices. High-risk remote execution vulnerabilities with CVSS scores above 9.0 include notable cases like Ivanti (CVE-2023-46805, CVE-2024-21887), Fortinet (CVE-2024-21762), and Palo Alto (CVE-2024-3400). These critical vulnerabilities

[24] ibid
[25] IBM. (2024). Data Breach Report
[26] ibid
[27] Verizon. (2024). Data Breach Investigations Report
[28] ibid

highlight the persistent need for timely patching and secure network device management to safeguard against exploitation by malicious actors.[29]

Implementing risk-based vulnerability management (RBVM) is crucial to reducing patching workloads to manageable levels for IT teams. Effective prioritisation is the core of risk-based filtering, allowing teams to focus on the most critical vulnerabilities. In early 2022, the US Cybersecurity and Infrastructure Security Agency (CISA) issued a directive emphasising the importance of addressing known, exploited vulnerabilities to mitigate significant security risks.[30]

Mature, well-managed vulnerability management (VM) programs should systematically integrate with other security functions to maximise effectiveness. Following continuous threat exposure management (CTEM) principles allows the VM program to align with other security inputs, creating a holistic approach to exposure management.

[29] ibid
[30] Cybersecurity and Infrastructure Security Agency. (2022). Binding Operational Directive 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities. U.S. Department of Homeland Security

3. INFORMATION SECURITY INVESTMENTS

3.1 METHODOLOGY

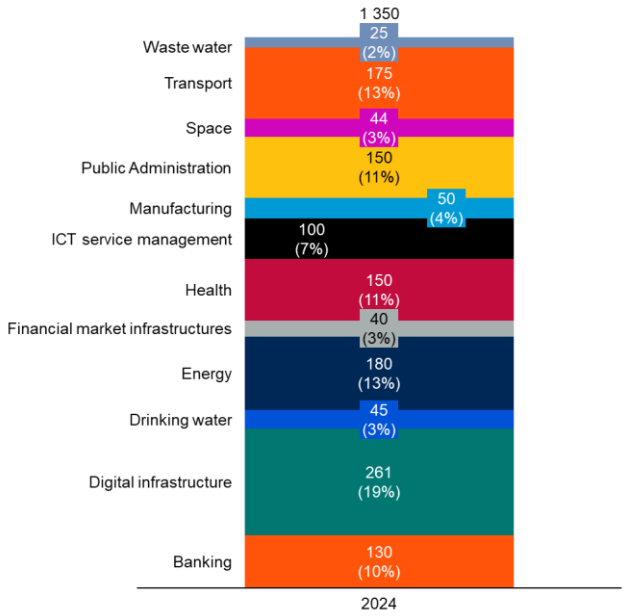
This study is based on a dedicated market survey conducted among 1350 organisations — with 50 organisations surveyed in each Member State. This survey data has been collected through dedicated phone interviews with cybersecurity experts and managers in those organisations by following a questionnaire designed specifically for the study and including both quantitative questions where ballpark figures or high-level estimates are requested and closed qualitative questions.

Some are yearly recurring questions to enable observation of NIS investment trends**. It must be noted that this study's sample is different in terms of composition and size compared to previous studies, which can influence the results and observations derived.** For more information on the design of the demographics of this year's study, please refer to the ANNEX A.

A notable difference in the sample composition is related to changes in the sector definition under the NIS2 Directive. Indeed, one of the significant changes introduced by the NIS 2 Directive is the expansion of its scope.

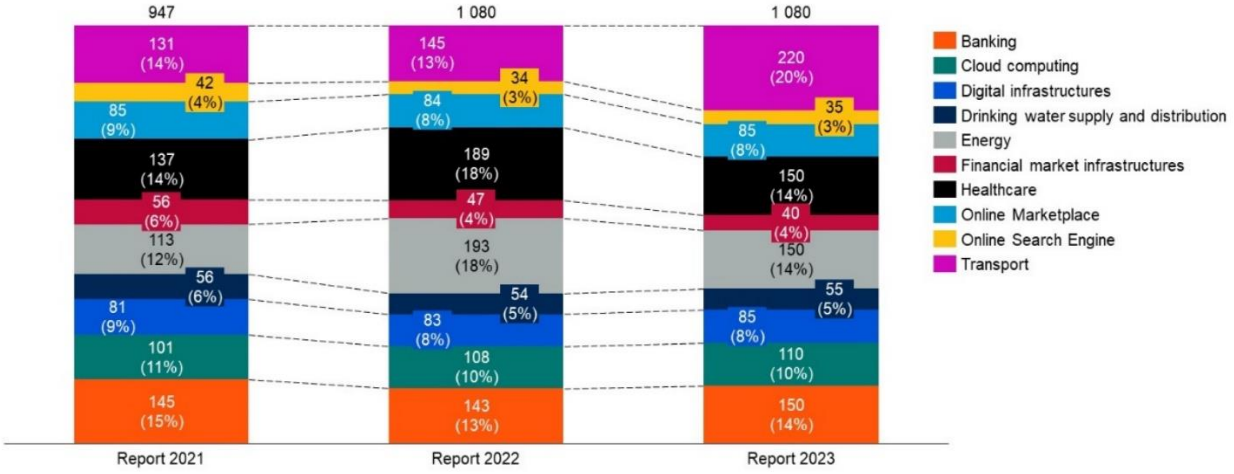
Figure 11 illustrates the distribution of sectors within this year study panel while Figure 12 provides the distribution in the previous studies from 2021 to 2023. Please note that there is a discontinuity as the sectors definition and scope has changed with the NIS2 Directive.

Figure 11: Composition of the 2024 study sample[31]



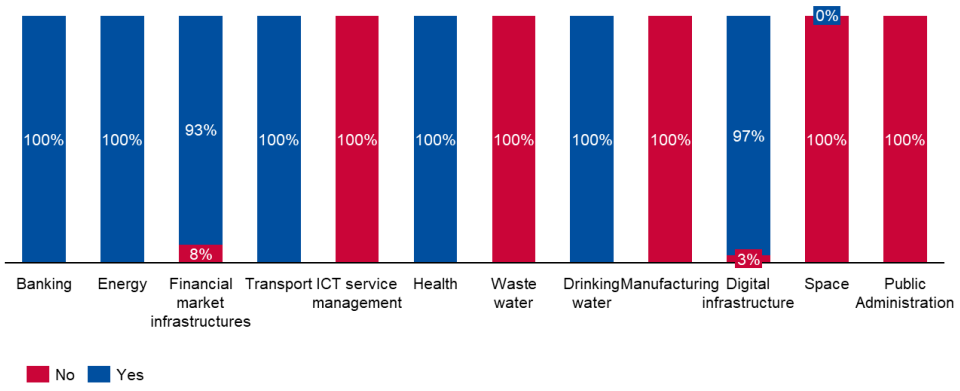
[31] For the purposes of this study and because the number of operators in Space that meet the criteria for essential entities under NIS 2 was low, additional operators from the Space sector were surveyed

Figure 12: Composition of the study sample from 2021 to 2023



Additionally, **the large majority of respondents in NIS 1 sectors were already subject to the NIS Directive while in new sectors, all respondents declare they were not subject to NIS Directive before NIS2**. The breakdown per sector is available in the below figure.

Figure 13: Was the organisation already subject to NIS Directive



The quantitative metrics collected in the survey have been analysed based on a median and average perspective so that the reader can appreciate both viewpoints.

Though not necessarily representing the "typical" value in a highly fragmented dataset, the median value should be seen as the most representative value for entities within a specific sector or country. The average value will often be higher because it is affected by large organisations that do not necessarily reflect the populated and fragmented market of most sectors and countries analysed.

For instance:

- The median value for IT spending is €15 million in 2023 (cf. Figure 14). This implies that an entity within the European Union spends yearly around €15 million in IT.
- In contrast to this median value, the average IT spending for entities in the European Union amounts to € 98.5 million. Still, this number is skewed by large organisations with significant budgets dedicated to IT.

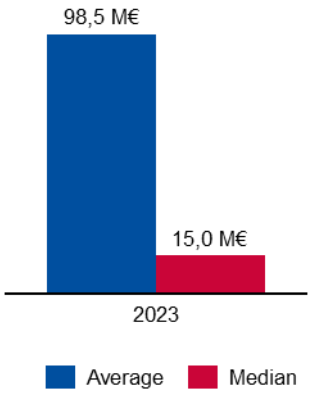
3.2 SPENDING ON INFORMATION SECURITY

Key Figures
The median IT spending of an organisations in the EU was 15,0 M€ million in 2023, while the average value of IT spending was 98,5 M€ over the same period.
The median spending for information security of organisations in the EU was 1,4 M€ 2023, while the average expenditure was 6,7 M€
Organisations in the EU earmark 9,0% of their IT investments for information security, while the average value is 9,6%. a significant increase of 1.9 points is observed compared to the median IS vs IT spending in 2022.
Only 4% of organisations have already invested in Post-Quantum Cryptography, while 22% have not yet invested but plan to do so. A significant majority (68%) of respondents indicated that they will not invest in QSC.

3.2.1 IT spending

Survey Question: What was your organisation's estimated IT budget or spending in Euros for 2023 (including CAPEX and OPEX for hardware, software, internal personnel, contractors, and outsourcing spending)?

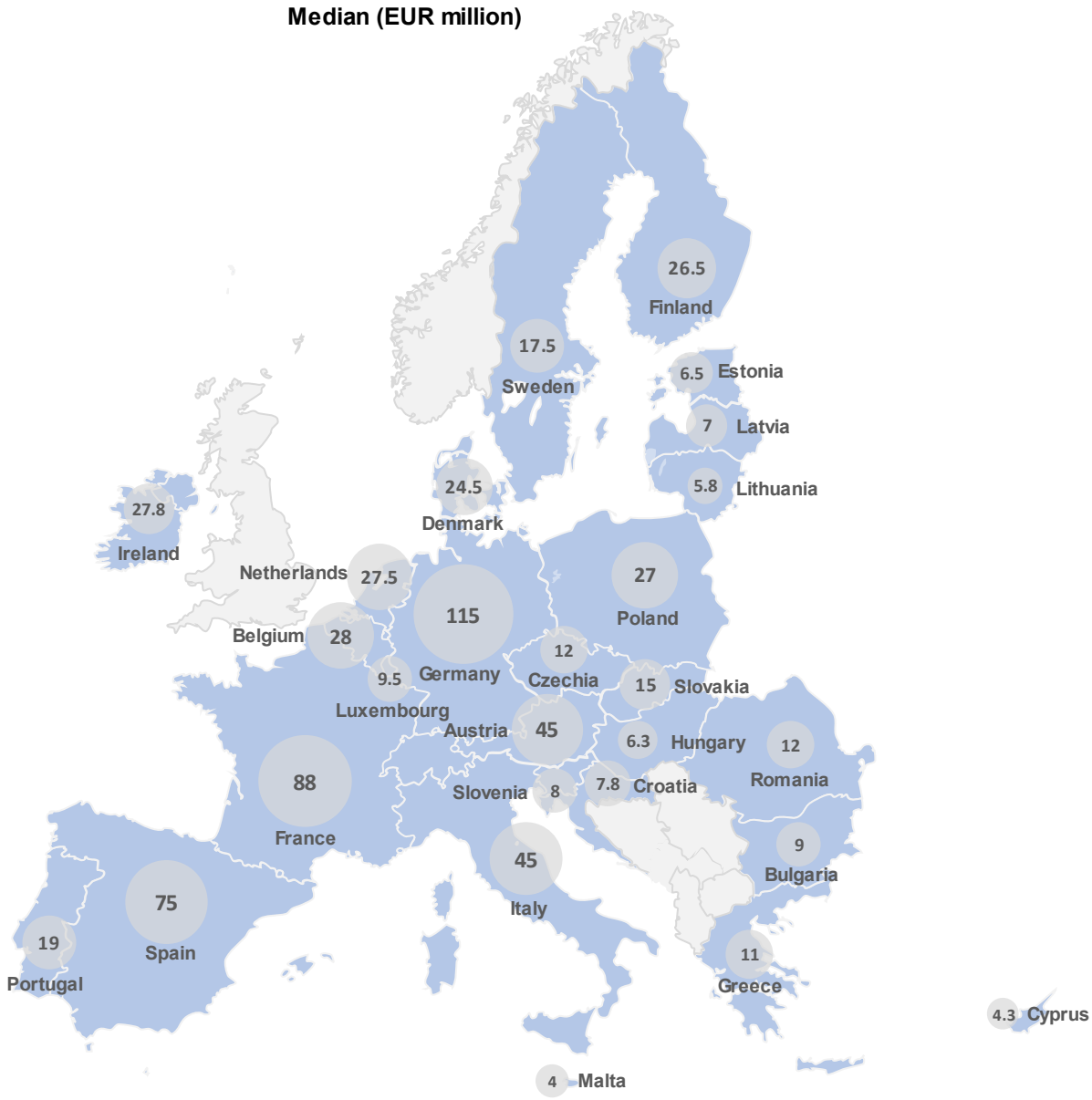
Figure 14: IT spending - all NIS2 sectors



The median IT spending of an entity in the EU was €15 million in 2023, while the average value of IT spending was €98.5 million over the same period.

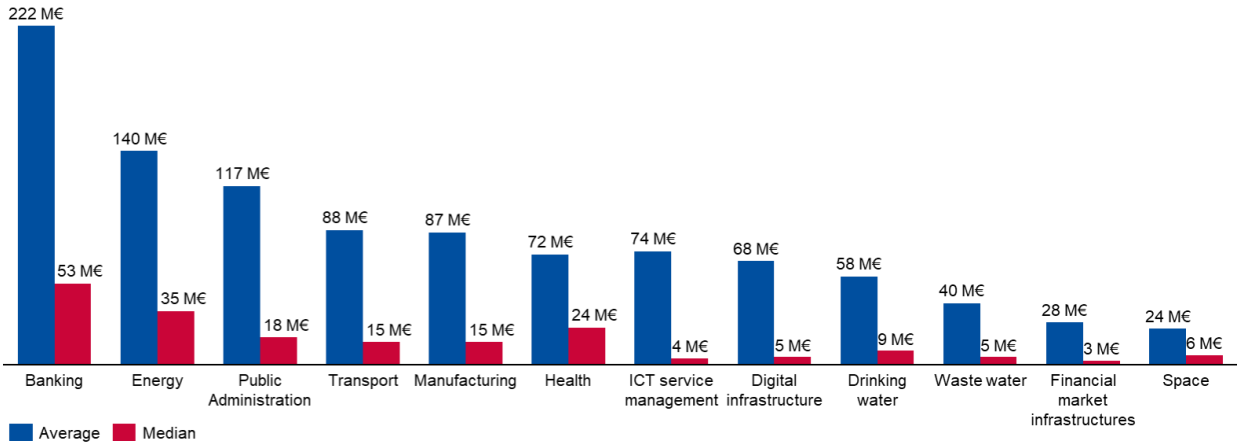
While these are absolute values that must be interpreted considering the sector's structure and organisation size, a smaller budget does not necessarily imply a lower level of cybersecurity maturity. Furthermore, as detailed in the methodology section, it must be noted that the sample in this study was different in terms of composition and size compared to previous studies, which can influence the results and observations derived.

Figure 15: IT Spending in each Member State



Note: The map visualisations throughout the report depict data collected from the organisations surveyed in each Member State. Hence, investment data refers to the median among the organisations surveyed, not the Member State's investments. In addition, when interpreting these figures, the market fragmentation or average operator size in each Member State and the specific sectors need to be factored in.

Figure 16: IT spending by NIS 2 sector

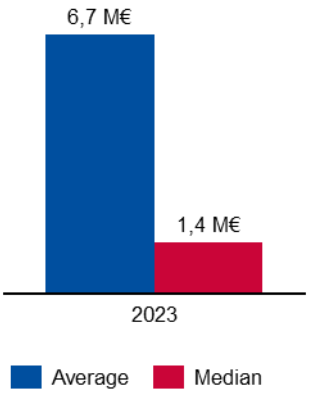


The survey data indicates that median IT spending is highest within the Banking sector (€ 53 million), followed by Energy (€ 35 million), Public administration (€18 million) and Transport sectors (€ 15 million). The IT spending in these industries significantly exceeds IT spending in other sectors, as illustrated in Figure 16. Furthermore, ICT Service management and Financial market infrastructures (FMI) have the lowest IT spending across all sectors, with a median expenditure of € 4 million and € 3 million respectively.

3.2.2 IS spending

Survey Question: What was your organisation's estimated Information Security budget or spending in Euros for 2023 (including CAPEX and OPEX for hardware, software, internal personnel, contractors, and outsourcing spending)?

Figure 17: Information security spending - all the NIS 2 sectors



The survey data indicates that the median spending for information security of an organisation in scope of the NIS2 Directive was € 1.4 million in 2023, while the average expenditure was € 6.7 million.

While these are absolute values that must be interpreted considering the sector's structure and organisation size, a smaller budget does not necessarily imply a lower level of cybersecurity maturity.

Furthermore, as detailed in the methodology section, it must be noted that the samples in this report are different in composition and size compared to previous studies, which can influence the results and observations derived.

Figure 18: IS spending in each Member State

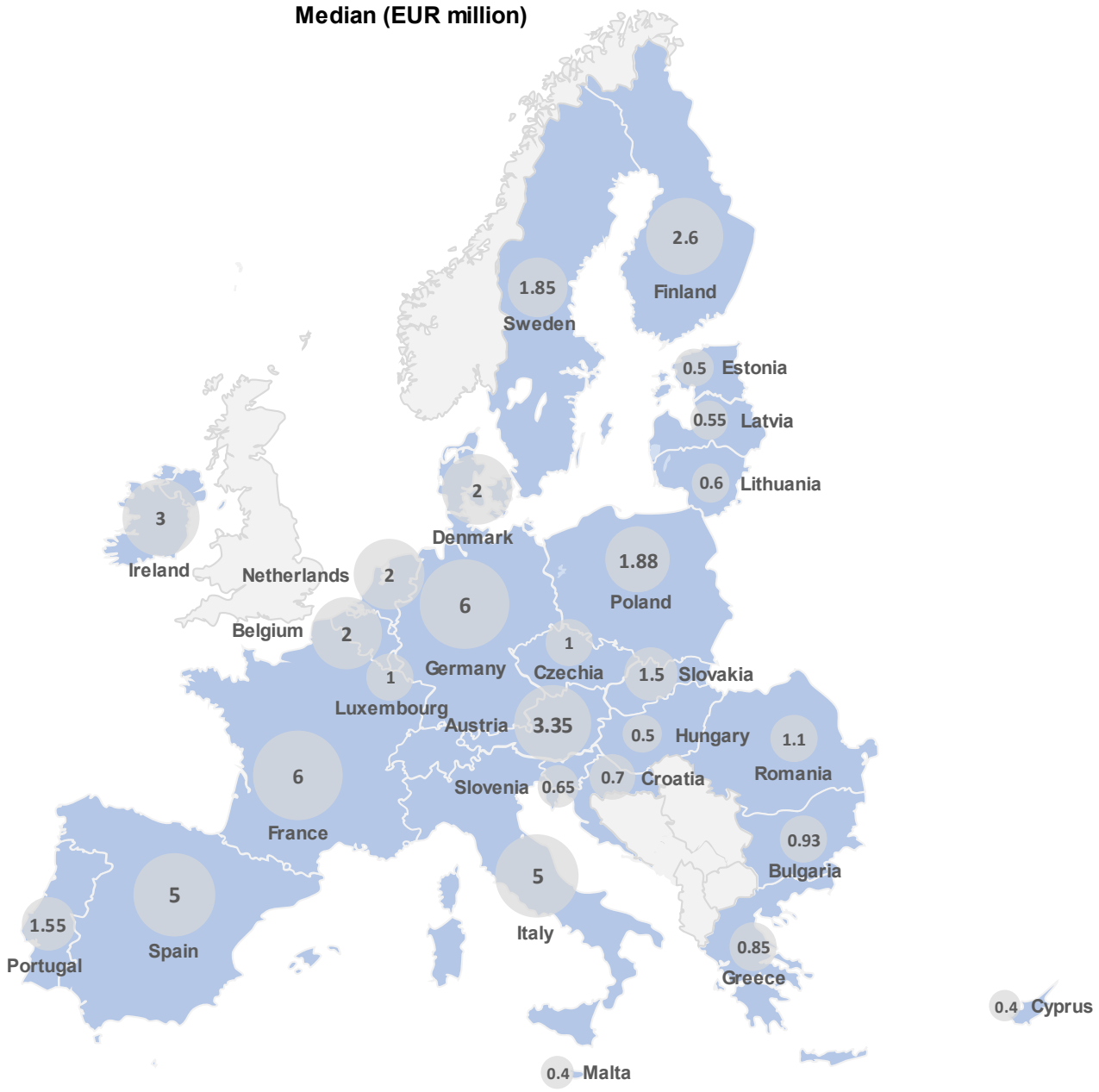
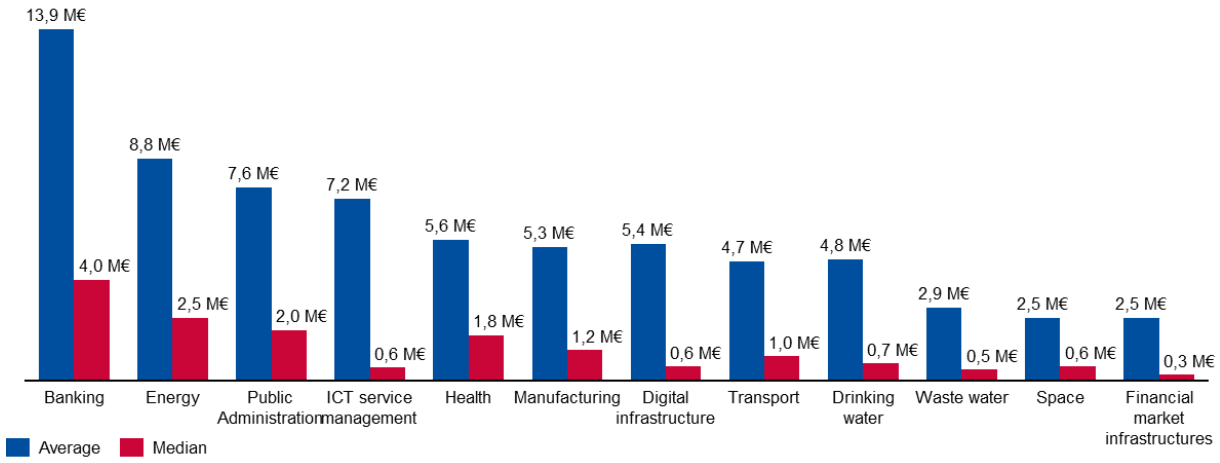


Figure 19: Information security spending by NIS 2 sector



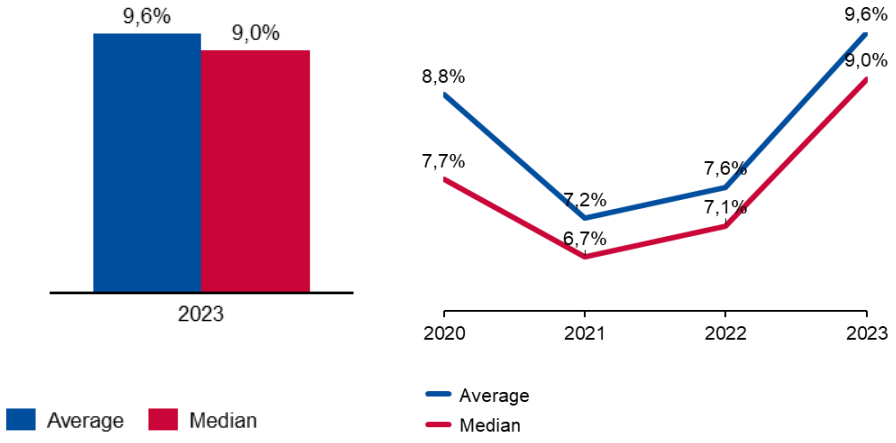
In 2023, the Banking sector leads in information security investment with an average spending of € 13.9 million and a median of € 4.0 million. Following closely, the Energy sector allocates an average of € 8.8 million and a median of € 2.5 million. Public administration ranks third, with an average spending of € 7.6 million and a median of € 2.0 million.

Conversely, the sectors with the lowest investment in information security are Space, Financial market infrastructures, and Waste water.

3.2.3 IS spending as a share of IT spending

To define the importance of IS spending for an entity, the relative share of IS spending against the overall IT spending was calculated and illustrated in the figure below.

Figure 20: Information security spending as a share of IT spending - all the NIS2 sectors



Looking at the median value, a critical entity in the EU earmarks 9.0% of its IT investments for information security, while the average value is 9.6%. When analysing this normalised data set with historically available data, a **significant increase of 1.9 points is observed** compared to the median IS vs IT spending in 2022. **This is the highest IS vs IT spending ratio observed since the introduction of this report**.

As detailed in the methodology section, the historical analysis must be done while considering the slight differences in the samples between the years of study and the potential changes in the macro environment.

For example, we can observe on the figure below that new sectors included in NIS 2 Directive (ICT service management, Manufacturing, Public administration, Space and Waste water) have a higher IS spending as a share of IT spending when compared to existing NIS sectors.

Figure 21: Information security spending as a share of IT spending for existing NIS sectors and new sectors

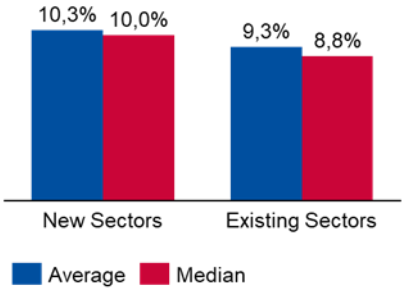


Figure 22: IS spending as a share of IT spending of entities surveyed in each Member State

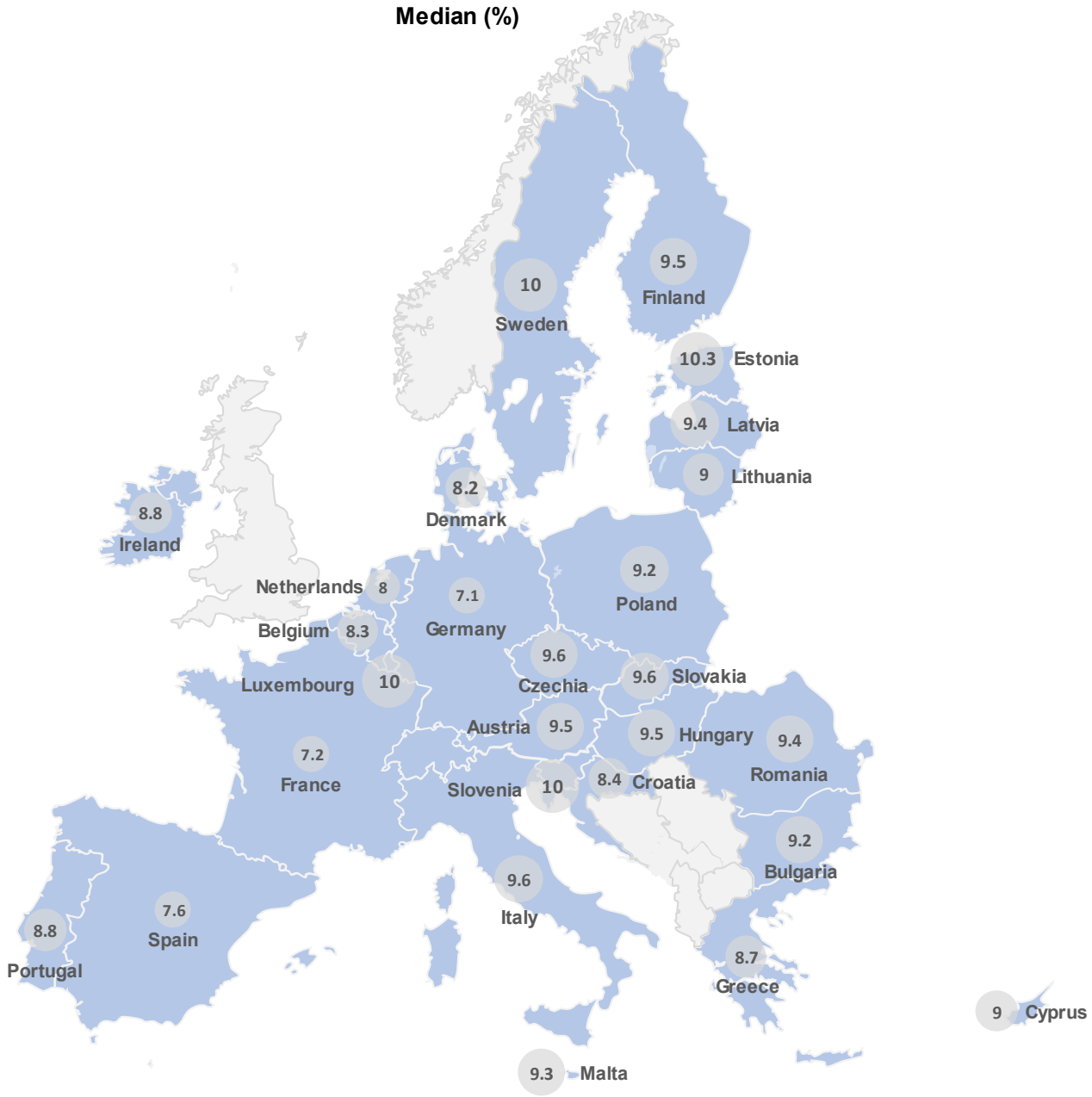
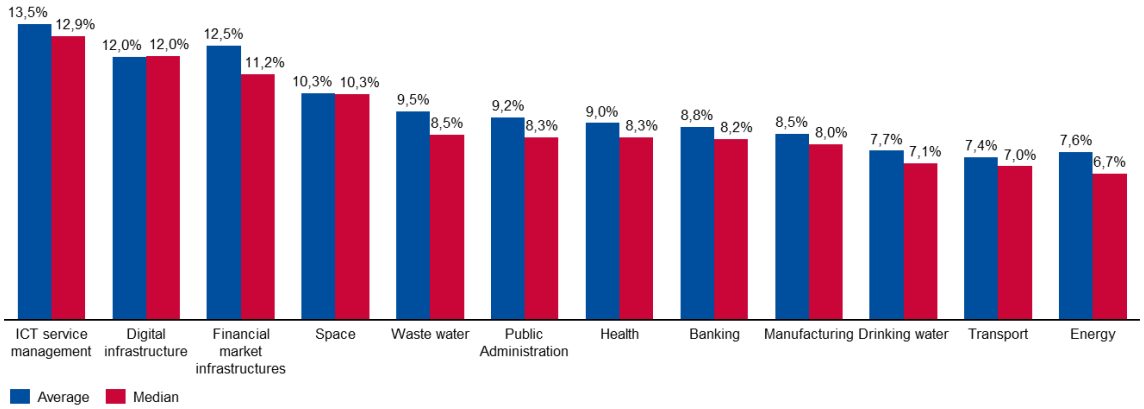


Figure 23: IS spending as a share of IT spending, per NIS2 sector



The comparison per NIS 2 sector could provide a rationale as to why the IS vs IT spending ratio is higher than previous years, as 3 out of the top 5 ratios (ICT service management, Space and Waste water) are sectors that were added in the NIS 2 Directive but out of scope of the NIS Directive.

3.2.4 Investment in post-quantum cryptography (PQC)

Figure 24 depicts the investment status of entities regarding Post-Quantum Cryptography (PQC). Overall, only a small minority (4%) have already invested in QSC, while 22% have not yet invested but plan to do so. A significant majority (68%) of respondents indicated that they will not invest in QSC.

Survey Question: Is your organisation investing in post-quantum cryptography?

Figure 24: Investment in Post-Quantum Cryptography

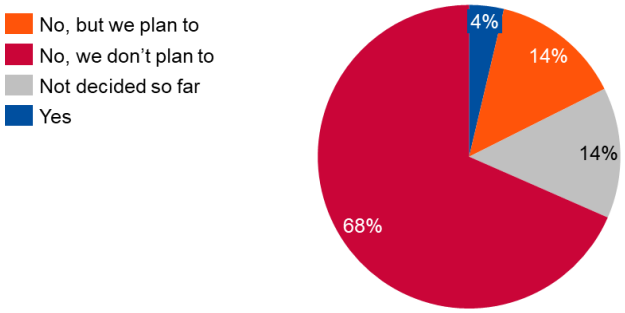


Figure 25: Investment in Post-Quantum Cryptography, per Member State

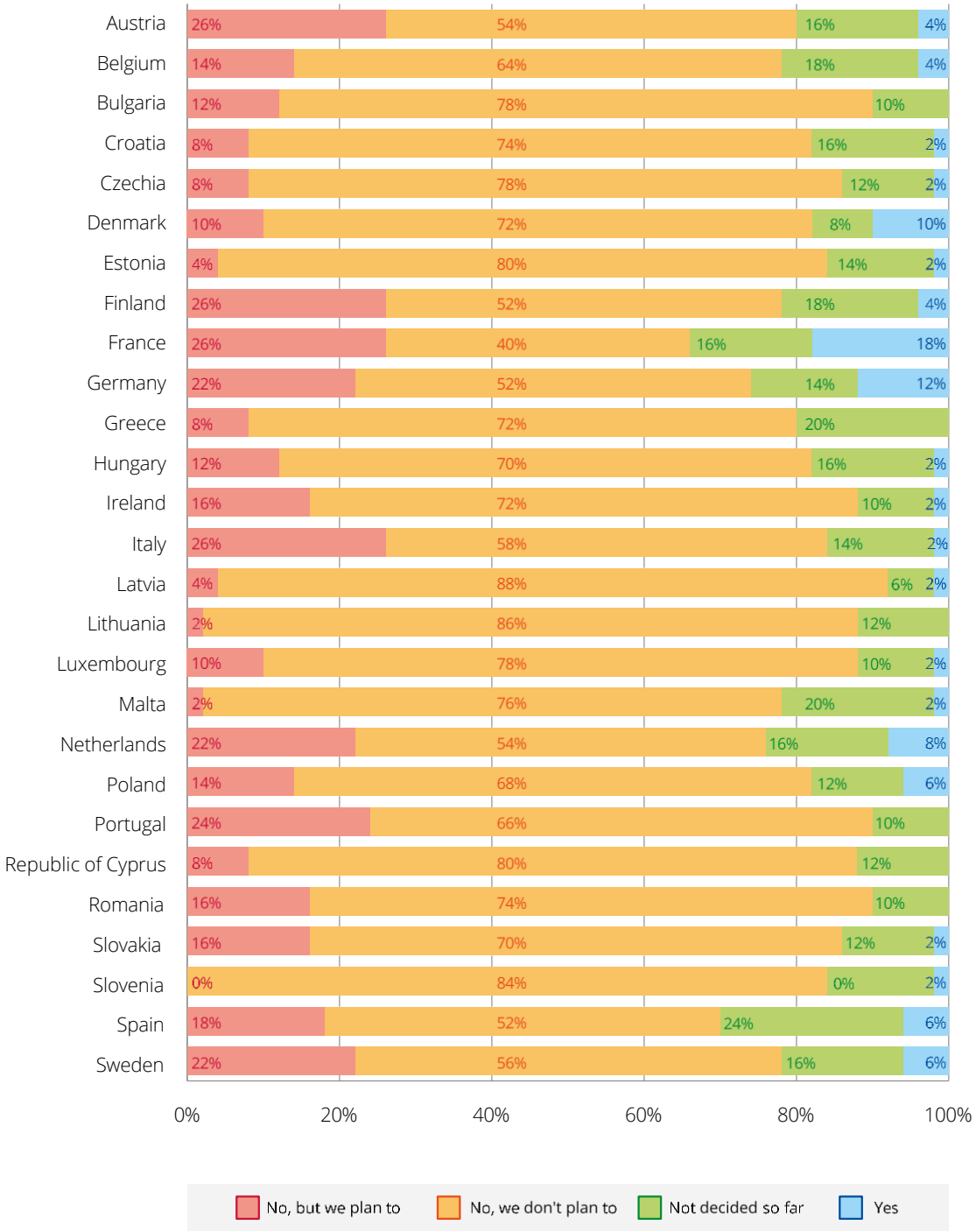
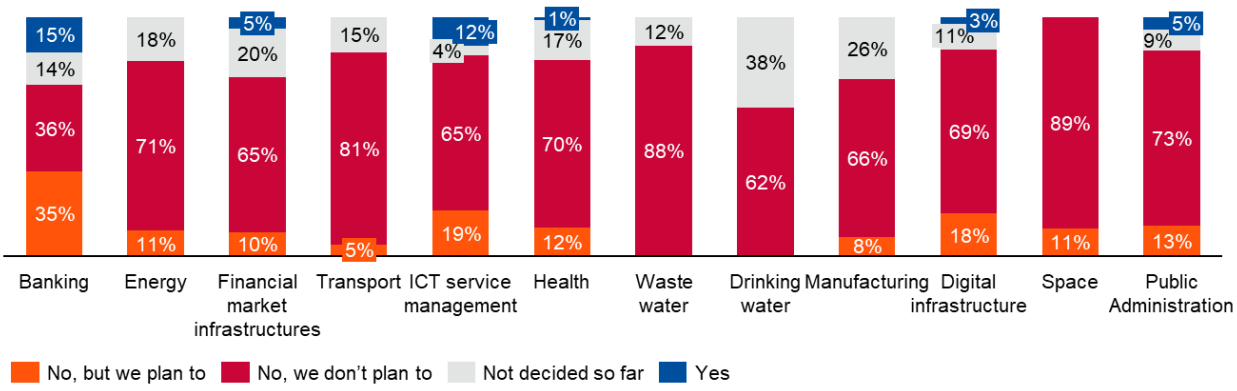


Figure 26: Investment in Post-Quantum Cryptography, per NIS2 sector



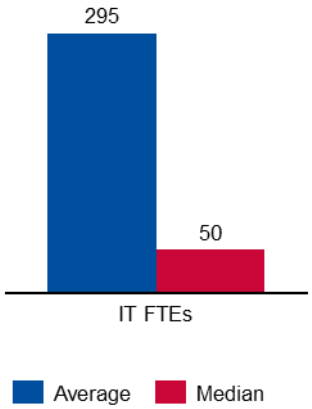
3.3 INFORMATION SECURITY AND NIS STAFFING

Key Figures
Looking at the median value, organisations in the EU allocate 11,1% of their IT FTEs for information security, while the average value is 12,8%. This metric has consistently decreased in the past four years, despite the overall increase in information security spending.
32% of organisations are facing difficulties hiring in all domains. The domain that stand out the most is Cybersecurity Architecture and Engineering with 25% of respondents having difficulty in this domain, a finding consistent with last year's data as well.
Aside from NIS2, entities report the need of additional resources to comply with other sectorial pieces of the regulatory framework, such as DORA (84% will need to hire additional IS FTEs) and the electricity network code for cybersecurity (81% will need to hire additional staff). The skills gap is most evident in the Cybersecurity Operations domain.

3.3.1 IT FTEs

Survey Question: What was your organisation's estimated number of IT FTEs for 2023 including internal staff and contractors?

Figure 27: IT FTEs - all the NIS 2 sectors



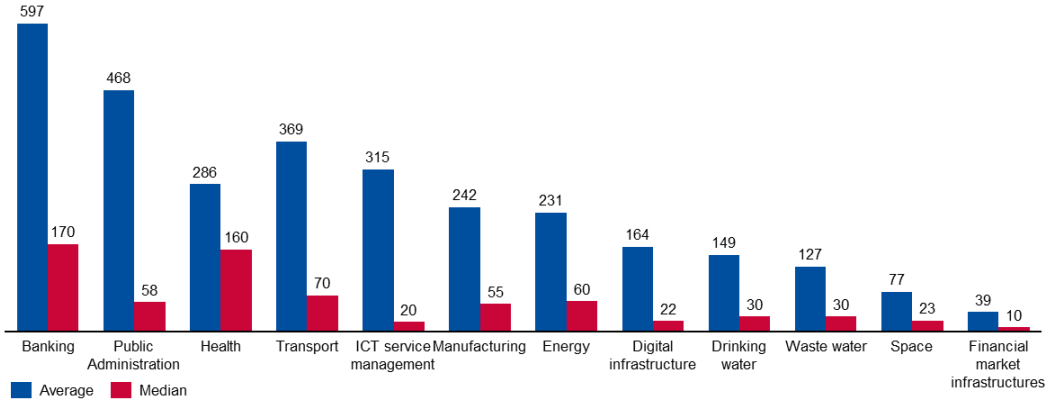
The survey data indicates that an entity in the EU employs a median of 50 IT FTEs and an average of 295 IT FTEs. The disparity between the median and average values indicates that most organisations use a low number of IT FTEs while larger organisations engage a substantial number of IT FTEs.

These figures represent absolute values, but they need to be interpreted with consideration of the sector's structure and the size of the organizations involved. For example, a smaller number of FTEs does not automatically mean a lower level of cybersecurity maturity. Additionally, as explained in the methodology section, this sample differs in composition and size from previous studies, which could impact the results and the insights derived.

Figure 28: IT FTEs for entities surveyed by Member State

Significant discrepancies exist in the total number of IT FTEs in the organisations surveyed among Member States, with median values ranging from over 360 IT FTEs in France to 13 employees in Cyprus. When interpreting these figures, the market structure and size of organisations surveyed in each Member State must be factored in.

Figure 29: IT FTEs by NIS 2 sector

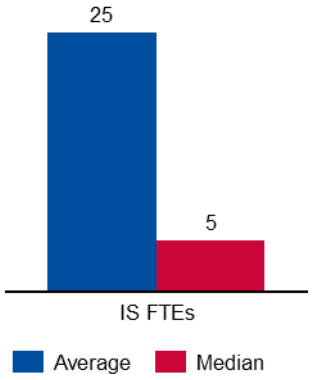


As illustrated in Figure 29 there are significant discrepancies in the number of IT FTEs across sectors. For example, the Banking sector has the highest median value of 170 IT FTEs when ICT Service management and Financial market infrastructures have the lowest median value with 20 IT FTEs and 10 IT FTEs respectively.

3.3.2 IS FTEs

Survey Question: What was your organisation's estimated number of Information Security FTEs for 2023 including internal staff and contractors?

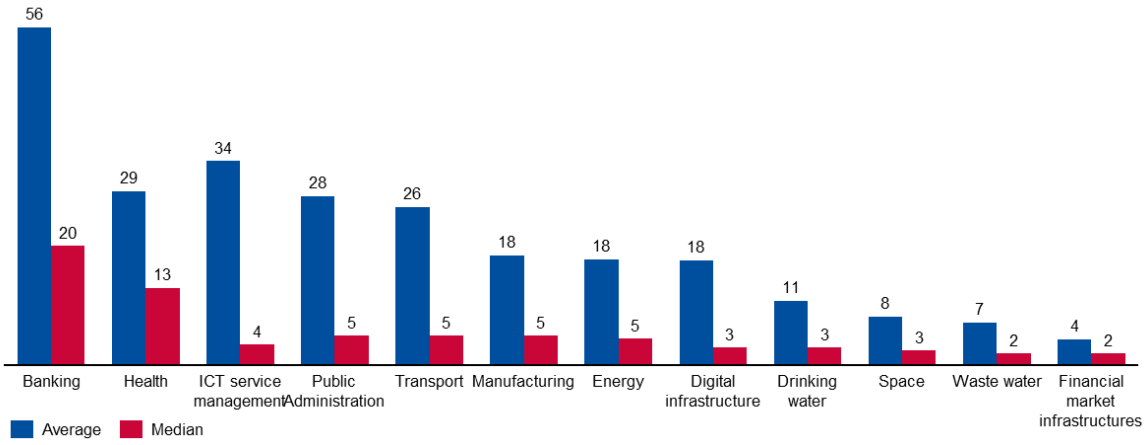
Figure 30: IS FTEs - all the NIS 2 sectors



The survey data indicates that an entity in the EU employs a median of 5 IS FTEs and an average of 25 IS FTEs. The disparity between the median and average values indicates that most organisations use fewer IS FTEs while larger organisations engage a substantial number of IS FTEs.

Figure 31: IS FTEs for entities surveyed in each Member State

Figure 32: IS FTEs by NIS 2 sector

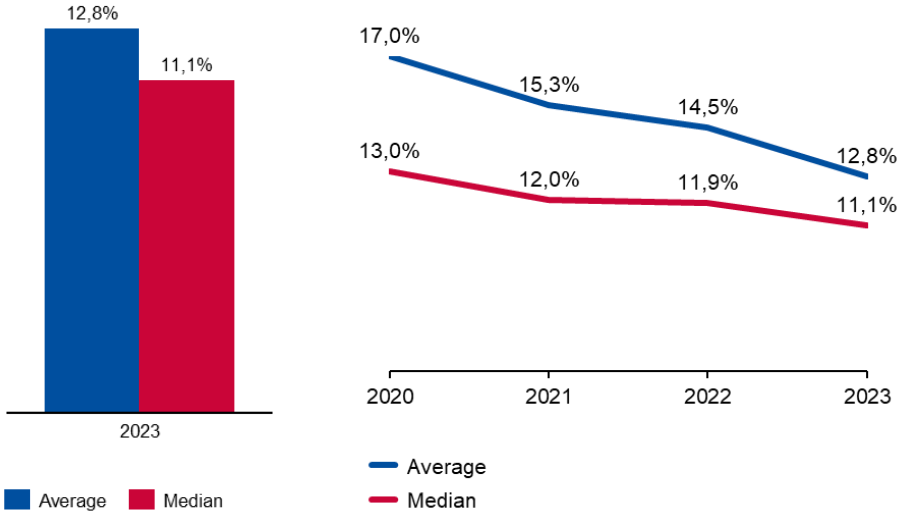


As illustrated in Figure 32, the Banking sector has the highest number of IS FTEs, with a median value of 20 FTEs in 2023, followed by the Health sector with 13 FTEs. With two FTE each, the Waste water and Financial market infrastructures sectors have the lowest median number of IS FTEs.

3.3.3 IS FTEs as a share of IT FTEs

To determine how cybersecurity is positioned in terms of resources within a given organisation, the relative share of IS FTEs against the overall IT FTEs was calculated and is depicted Figure 33.

Figure 33: IS FTEs as a share of IT FTEs - all the NIS 2 sectors



Looking at the median value, an entity in the EU allocates 11.1% of its IT FTEs for information security, while the average value is 12.8%. When analysing this normalised data set with historically available data, a decrease of 0.8% is observed compared to the median IS FTEs vs. IT FTEs ratio in 2022[32].

[32] As explained in the methodology section, the historical analysis must be done while considering the differences in the samples between the years of study and the differences in the macro environment

This decreasing ratio of IS FTE to IT FTEs, coupled with the increasing ratio of IS spending to IT spending, suggests that organisations may be facing challenges in recruiting and retaining cybersecurity experts. This may also suggest that cybersecurity investments are increasingly being directed toward software, hardware, and other expenditure categories unrelated to personnel. It could also reflect the growing use of AI and machine learning to automate tasks that were previously performed by humans especially in certain domains of cybersecurity (e.g., security operations).

Figure 34: IS FTEs as a share of IT FTEs for entities surveyed in each Member State

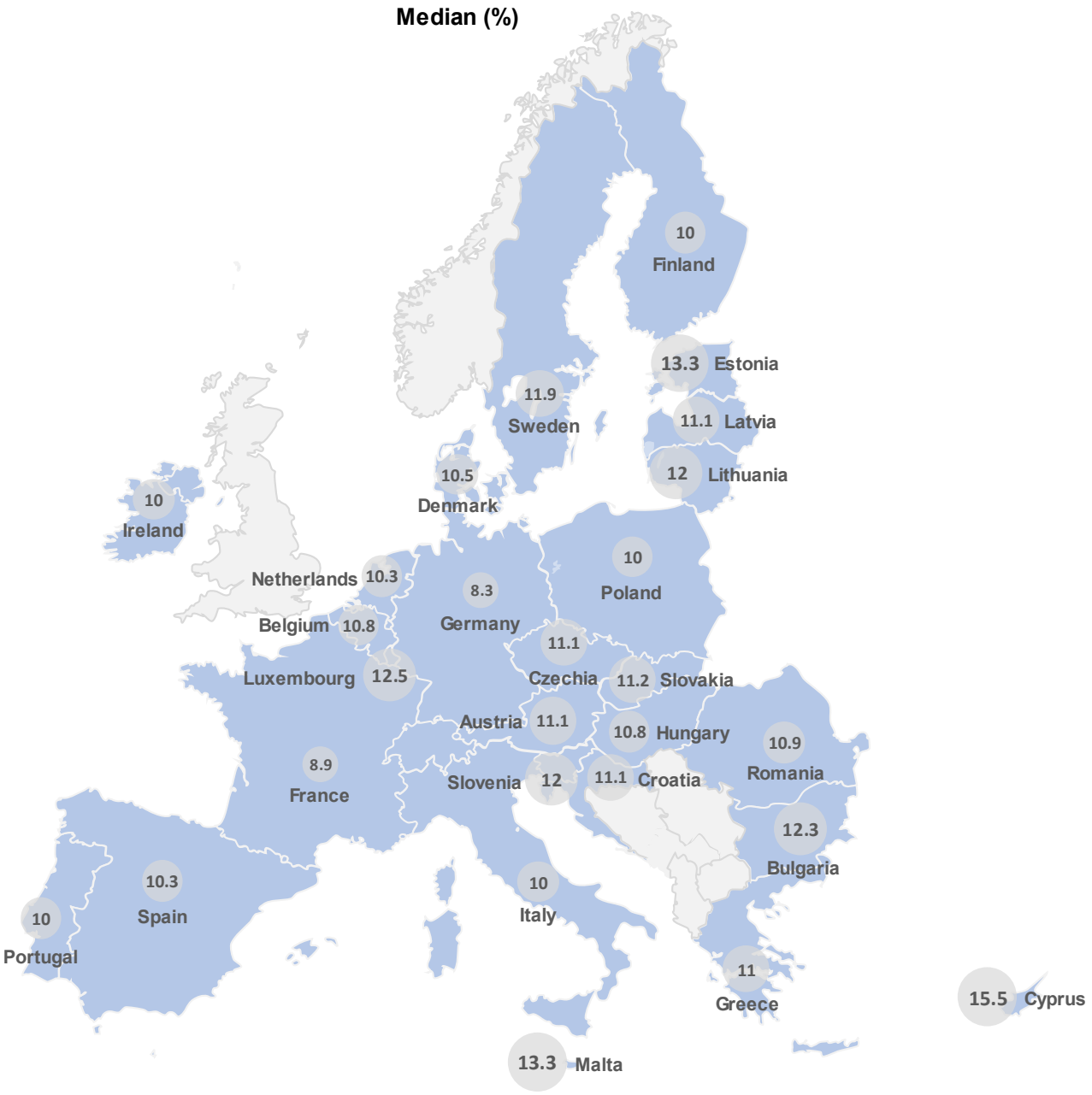


Figure 35: IS FTEs as a share of IT FTEs, per NIS 2 sector

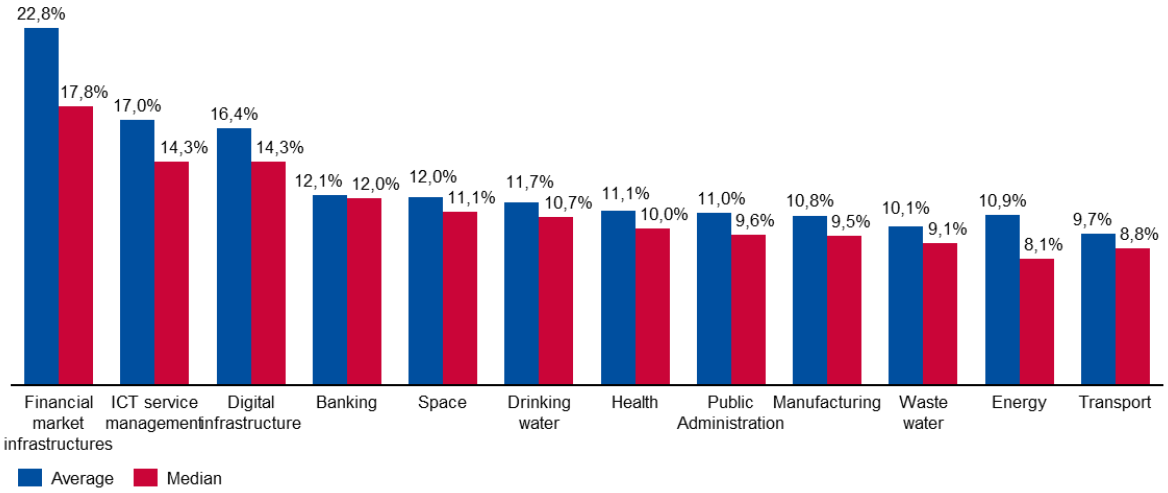
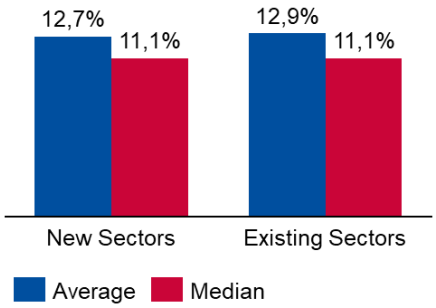


Figure 36: Information security FTEs as a share of IT FTEs for existing NIS sectors and new sectors



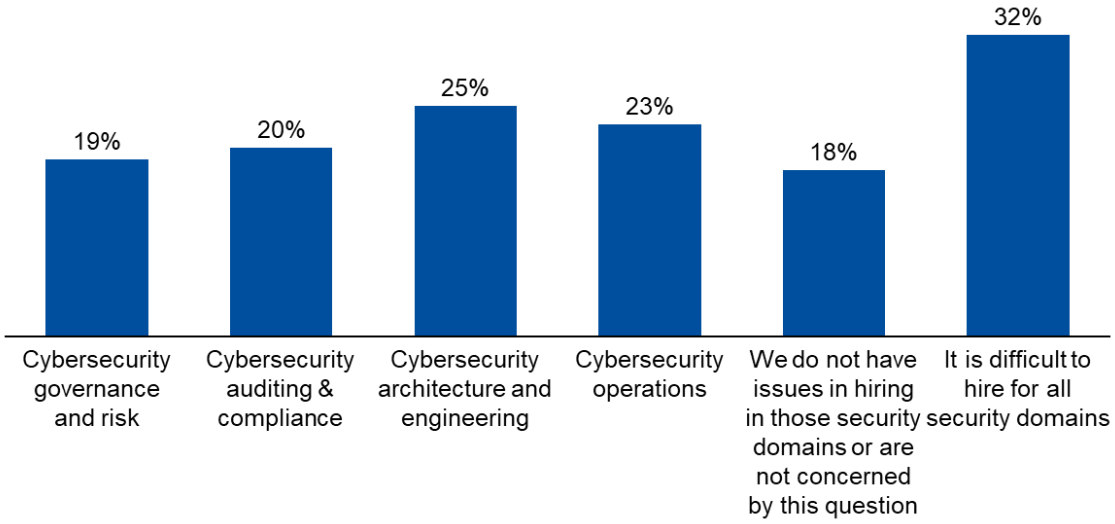
While the ratio of IS spending as a share of IT spending was higher in new NIS 2 sectors compared to existing NIS sectors, the ratio of IS FTEs as a share of IT FTEs is similar.

3.3.4 Security domains with difficulties in hiring

Survey Question: In which security domains are you facing difficulties in hiring?

When asked about security domains where organisations are facing difficulties in hiring, 32% have answered they are facing difficulties in all domains. Only 18% of entities indicate they do not have difficulty in hiring cybersecurity personnel. Otherwise, the domain that stand out the most is Cybersecurity Architecture and Engineering with 25% of respondents having difficulty in this domain. Overall, about half of respondents (48%) estimate that it is difficult to hire in more technical or hands-on domains like cybersecurity architecture and engineering or cybersecurity operations.

Figure 37: Security domains with difficulties in hiring



Staffing needs must also be considered in the context of the new compliance requirements arising from the evolving EU cybersecurity legislative framework, both sector-specific (discussed in the following two sections) and horizontal (outlined in sections 4.4 and 5.7). When asked about areas where they expect to require additional staff to meet compliance with both sectoral and horizontal regulations, entities largely echoed the same response: the need for more hands-on, technical cybersecurity profiles.

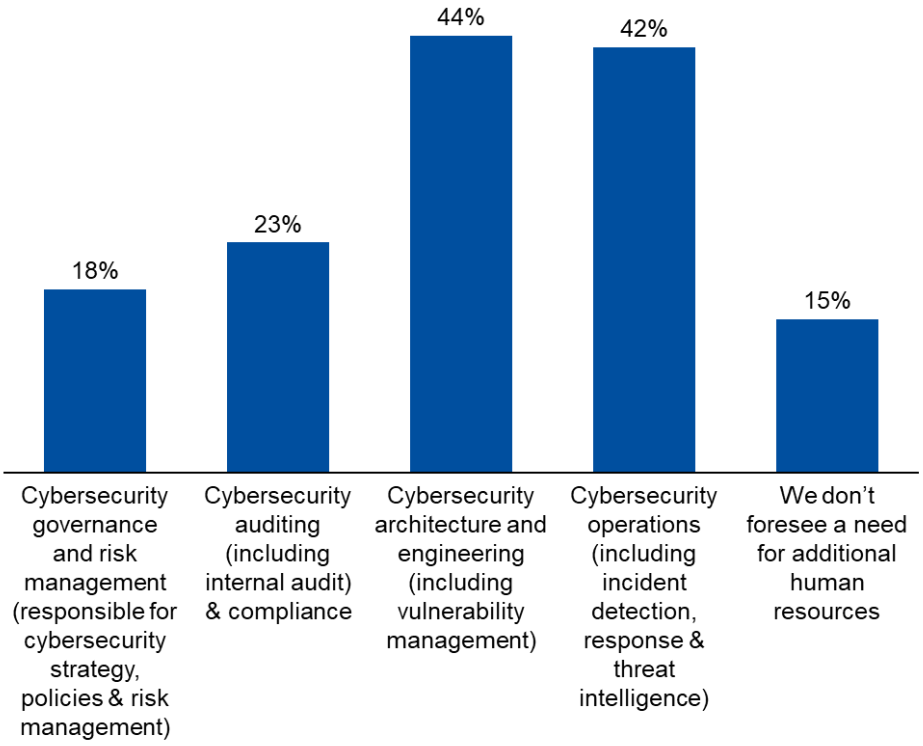
3.3.5 Staffing evolution to comply with the DORA

Survey Question: For which of the following area will you need additional human resources to comply with the DORA?

Banking and financial market infrastructure entities are expected to require more human resources to comply with the Digital Operational Resilience Act (DORA)[33], especially for cybersecurity architecture and engineering (44%) and cybersecurity operations (42%). Only 15% of the surveyed entities declare that they do not foresee a need for additional human resources to comply with the DORA.

[33] European Insurance and Occupational Pensions Authority (EIOPA). (n.d.). Digital Operational Resilience Act (DORA). Available at: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

Figure 38: Cybersecurity human resources to comply with the DORA



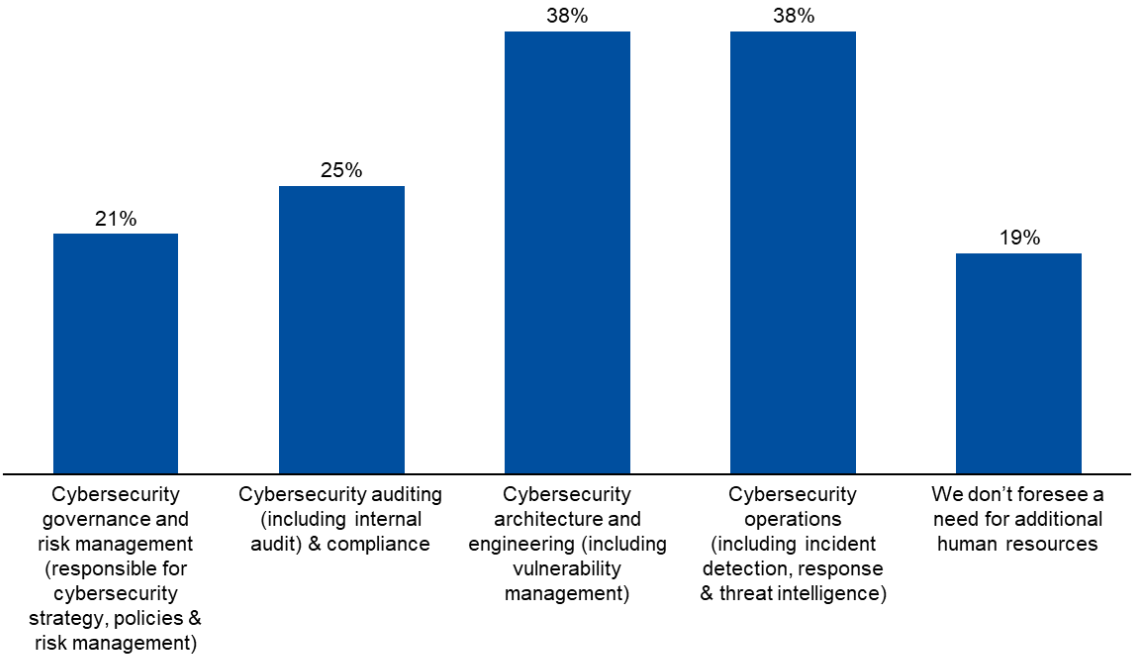
n=169. excluding 1 « I don't know »

3.3.6 Staffing evolution to comply with the cybersecurity network code for electricity

Survey Question: For which of the following area will you need additional human resources to comply with the Cybersecurity Network Code for Electricity?

38% of the entities that must comply with the Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows (NCCS)[34] declare that they will need additional human resources in cybersecurity architecture and engineering as well as in cybersecurity operations. Only 19% don't foresee a need for additional human resources.

Figure 39: Cybersecurity human resources to comply with the Cybersecurity code for electricity



n=121

[34] European Union. (2024). Commission Delegated Regulation (EU) 2024/1366 of 17 May 2024. Available at: http://data.europa.eu/eli/reg_del/2024/1366/oj

4. NIS 2 DIRECTIVE READINESS

4.1 NIS 2 AWARENESS

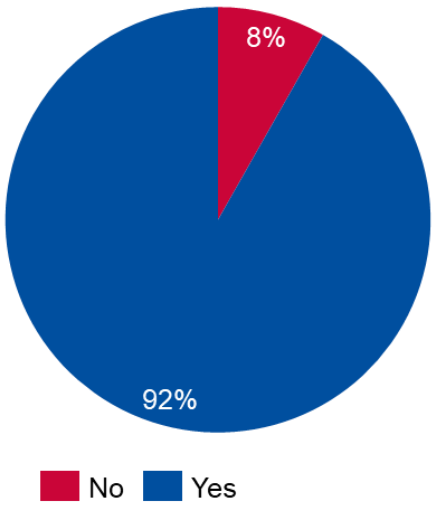
Survey Question: Are you aware of the NIS 2 Directive?

Awareness of the NIS 2 Directive is widespread, with 92% of respondents suggesting being aware of its general scope or provisions. However, awareness levels vary significantly across Member States and sectors.

As an example, France and Finland have 100% of the respondents aware of the NIS2 Directive when Malta has 80% and Bulgaria 82%.

With regards to sectors, the Space sector demonstrates the lowest awareness, with only 57% of respondents familiar with the directive, though, due to the selection of entities to be surveyed from this sector, it is expected that several of them will in fact not be in scope of NIS 2[35]. Waste water (60%), Manufacturing (62%), and Public administration (73%) also exhibit lower awareness levels, indicating a need for increased outreach and awareness raising in these sectors.

Figure 40: NIS2 Directive Awareness

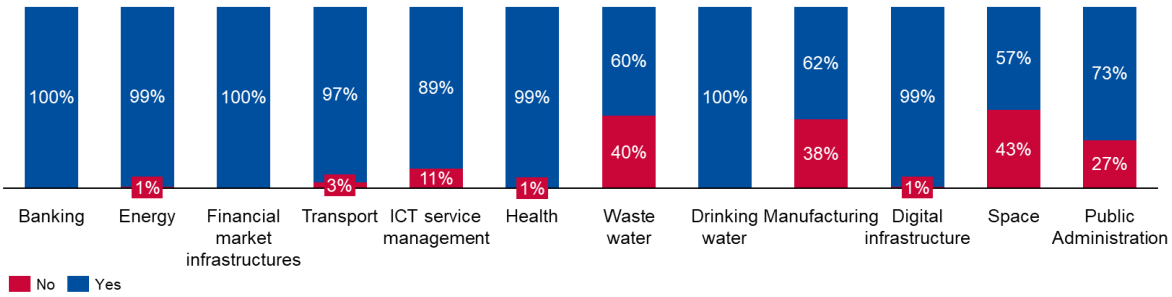


[35] For the purposes of this study and because the number of operators in Space that meet the criteria for essential entities under NIS 2 was low, additional operators from the Space sector were surveyed

Figure 41: NIS2 Directive awareness per Member State

	YES %	NO %
Austria	90%	10%
Belgium	92%	8%
Bulgaria	82%	18%
Croatia	84%	16%
Czechia	96%	4%
Denmark	96%	4%
Estonia	88%	12%
Finland	100%	0%
France	100%	0%
Germany	98%	2%
Greece	94%	6%
Hungary	92%	8%
Ireland	90%	10%
Italy	96%	4%
Latvia	90%	10%
Lithuania	86%	14%
Luxembourg	96%	4%
Malta	80%	20%
Netherlands	98%	2%
Poland	94%	6%
Portugal	88%	12%
Republic of Cyprus	92%	8%
Romania	88%	12%
Slovakia	92%	8%
Slovenia	92%	8%
Spain	94%	6%
Sweden	94%	6%

Figure 42: NIS2 Directive awareness per sector



4.2 MOST CHALLENGING NIS 2 REQUIREMENTS

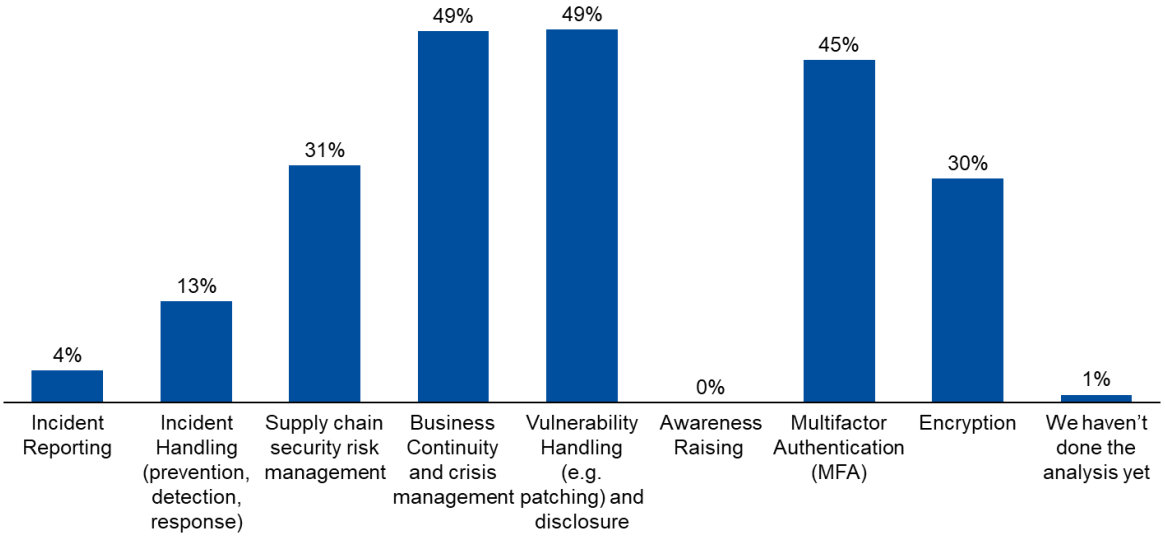
Survey Question: Which of the following NIS 2 Directive requirements do you expect to be the most difficult to implement in your organisation?

Among the various obligations for entities under NIS2, almost half of the respondents (49%) have highlighted Business Continuity and Crisis Management and Vulnerability Handling as the most challenging. Multi Factor Authentication (MFA) comes third with 45% of the responses.

Interestingly, a link seems to exist between this and key areas where entities anticipate to require more staff to comply with NIS2 requirements (see section 4.4), suggesting that compliance challenges may be linked to recruitment challenges.

On the other side of the spectrum, Incident Reporting and Incident Handling are perceived as the least challenging with respectively 4% and 13% of the answers.

Figure 43: Most challenging NIS 2 Directive requirements



n=1239. excluding 111 respondents not aware of NIS 2 Directive

4.3 NIS 2 BUDGET ARRANGEMENTS

Survey Question: Which of the following statements best represents your NIS 2 budget approach arrangement?

Overall, 38% of the organisations declare not needing additional budget to implement the NIS 2 Directive requirements and 14% will not be able to ask for more budget to implement them.

On the other hand, 34% of the entities foresee permanent increase to their security budget to maintain NIS 2 Directive compliance and 14% will only need a one-off investment.

Figure 44 NIS 2 budget arrangements overview

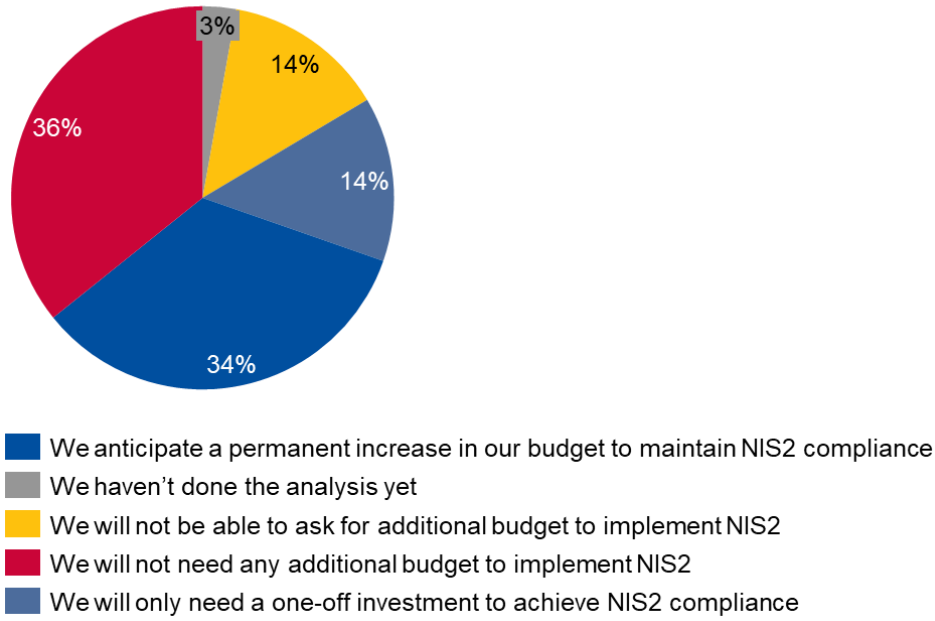


Figure 45 depicts the NIS 2 Directive anticipated impact on budget arrangements per MS, whereas Figure 46 depicts the NIS 2 Directive budget arrangement of entities in each sector.

Figure 45: NIS 2 budget arrangements, per Member State

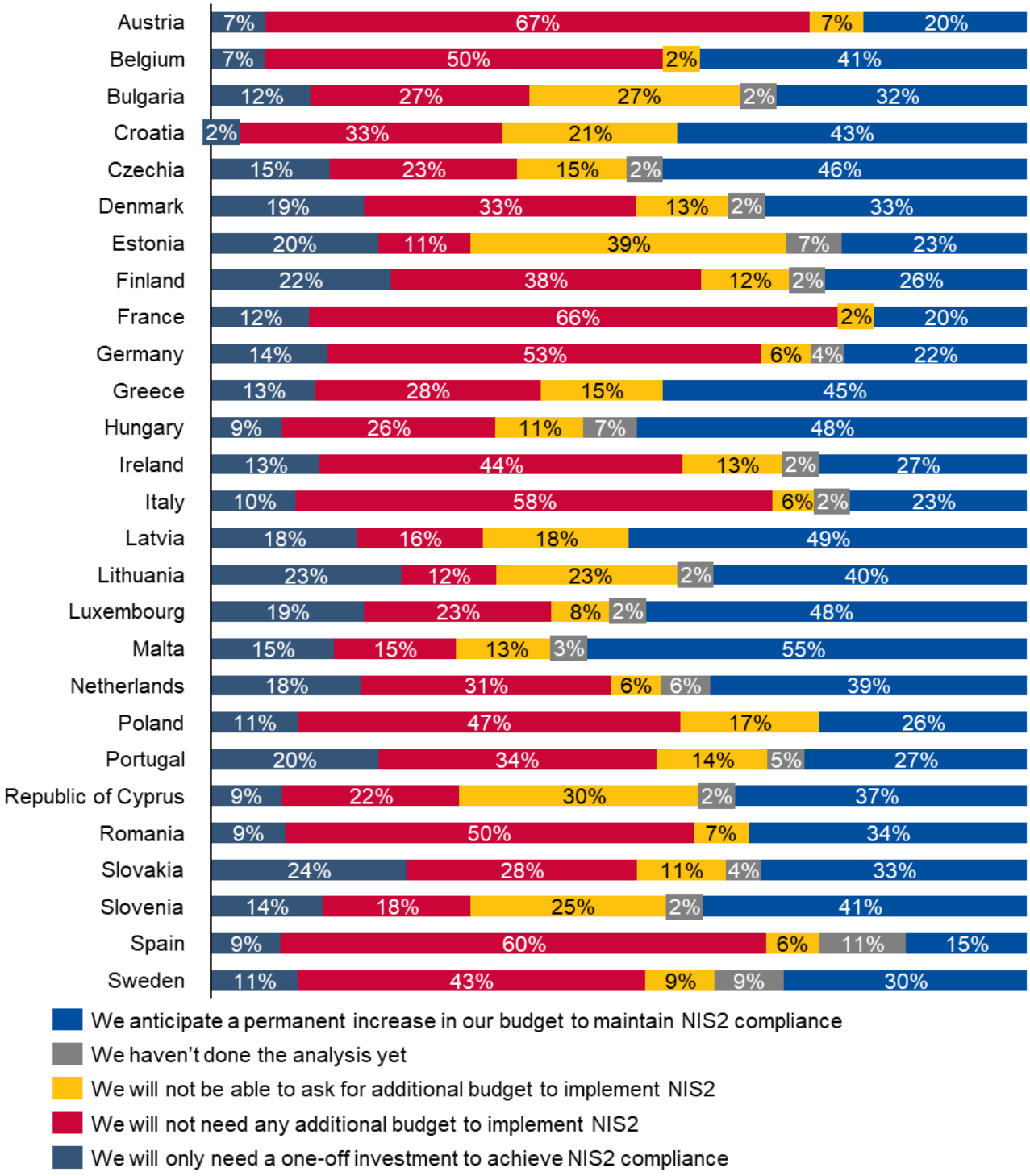
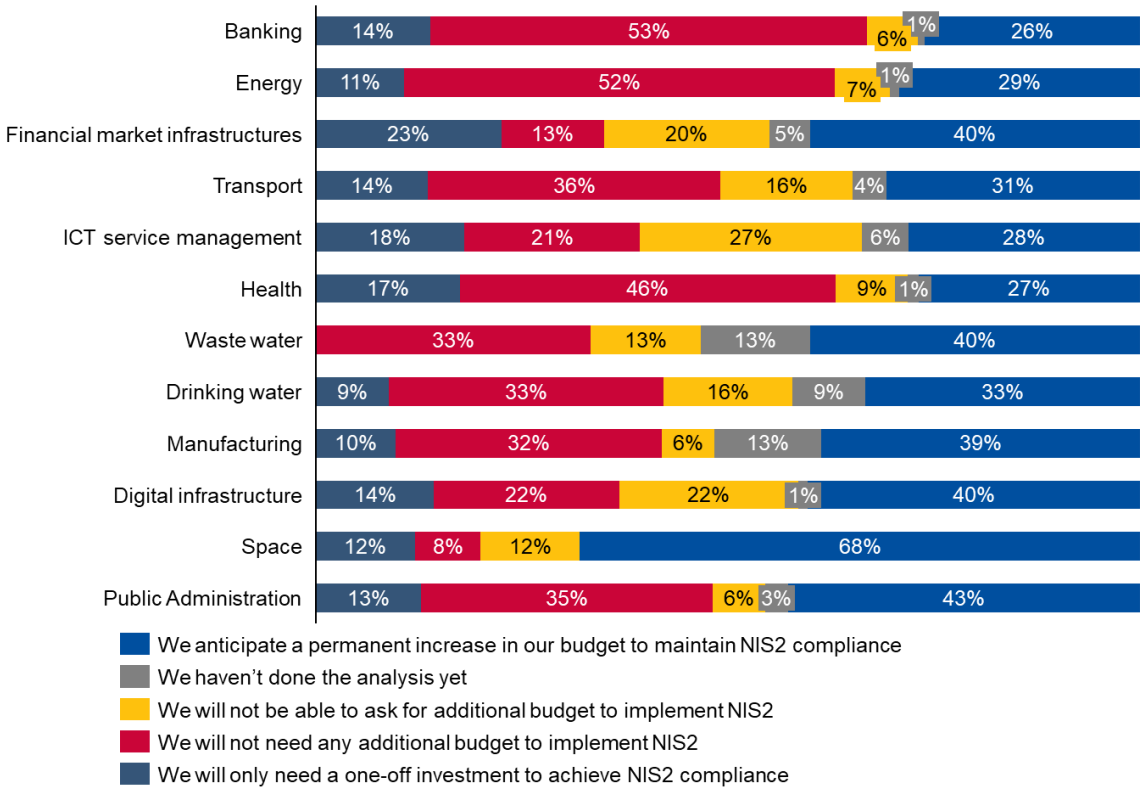


Figure 46: NIS 2 budget arrangements, per NIS 2 sector



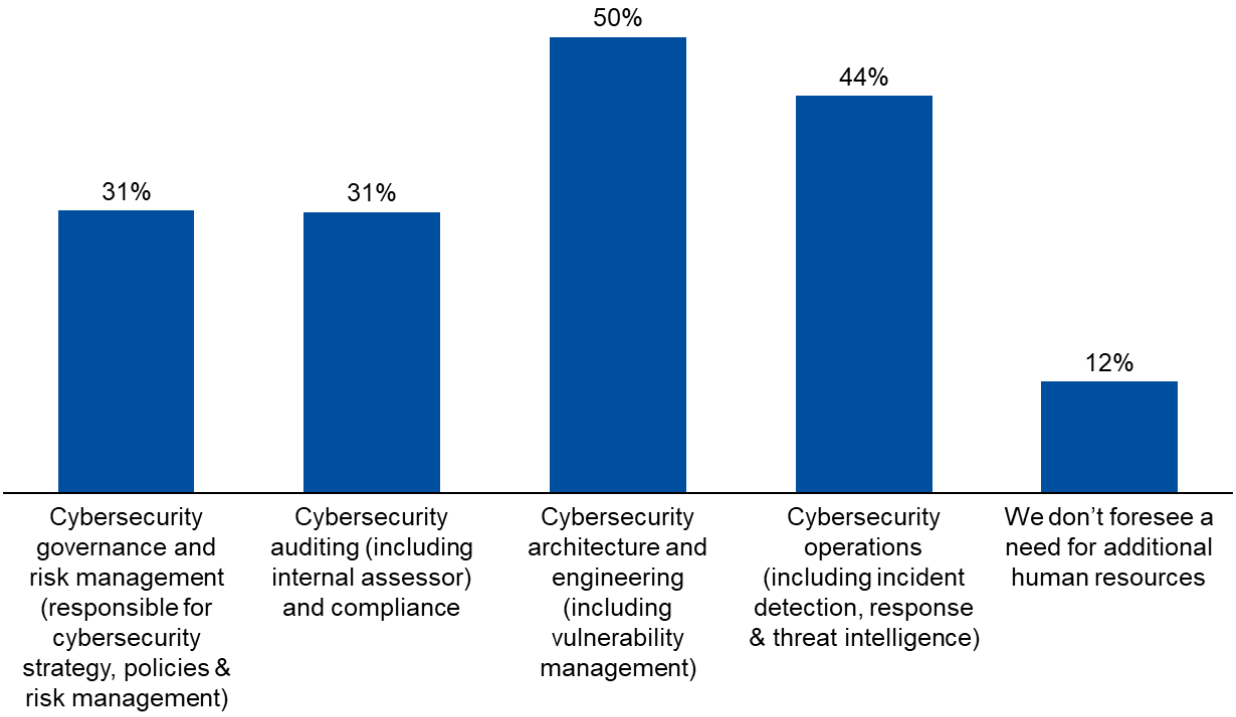
4.4 STAFFING EVOLUTION TO COMPLY WITH NIS2

Survey Question: For which of the following areas will you need additional human resources to comply with NIS2 Directive?

Cybersecurity architecture and engineering and cybersecurity operations are the two domains where organisations foresee the highest need for additional human resources to comply with the NIS 2 Directive with respectively 50% and 44% of the answers. The importance of those two domains with regards to NIS2 Directive compliance could be linked with the fact that they are deeply involved in the implementation of the most challenging NIS2 requirements highlighted in section 4.2. Part of the challenge could actually come from the difficulty in finding the expertise to do it.

12% of the organisations do not foresee a need for additional human resources.

Figure 47: Additional human resources to comply with NIS2 Directive



n=1229 excluding 111 respondents not aware of NIS2 Directive and 10 « I don't know »

5. CYBERSECURITY GOVERNANCE AND RISK MANAGEMENT

Key Figures
51% of surveyed organisations reported that their leadership participates in dedicated cybersecurity training. Several of the new sectors, not previously covered by NIS, show non-participation rates exceeding 70%.
75% of the organisations surveyed have a policy related to supply chain risk management for third parties.
When asked about how they establish trust in the IT and OT supply chain, 55% of organisations reported they rely on vendors' credentials and certifications, while 49% have strict procurement criteria focused on information security. At least 20% of entities in new sectors admit to not conducting specific assessments and trusting their supply chain implicitly.
Sectors previously covered by NIS reported higher perceived maturity in both cyber-risk management (6.8 vs. 6.2) and network and information security arrangements (7 vs. 6.3), compared to new sectors.
Sectors newly covered by the NIS Directive report over 60% non-participation in information-sharing initiatives, substantially higher than entities already under NIS.

5.1 LEADERSHIP INVOLVEMENT IN CYBERSECURITY

The NIS 2 Directive introduces specific provisions for management bodies of essential and important entities, specifically in relation to:

- **approving the cybersecurity risk-management measures** taken by those entities (Art. 20.1),
- **following training** to ensure they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity (Art. 20.2).

While NIS 2 is still under implementation during the time of the study and these measures are not necessarily mandatory in all EU MS yet, it is important to capture the current state of play concerning leadership approval of cybersecurity risk-management measures and receiving training and see how these evolve once NIS 2 comes into play.

Survey Question: Does your organisation's leadership receive dedicated cybersecurity training?

51% of the surveyed organisations suggested their leadership attends dedicated cybersecurity training, compared to 50% the previous year.

Italy (70%), Denmark (68%) and Germany (68%) are the countries with the highest share of leadership receiving dedicated cybersecurity training.

Sector wise, ICT Service management comes first with 75% of surveyed entities having declared that their leadership is receiving dedicated cybersecurity training, followed by Banking with 69%.

Figure 48: Leadership engagement in dedicated cybersecurity training

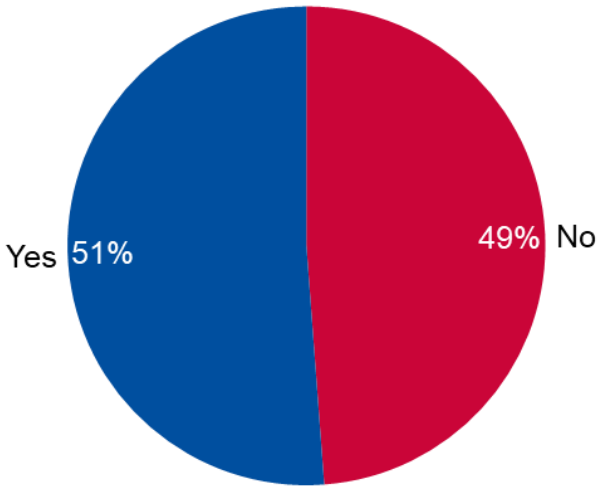
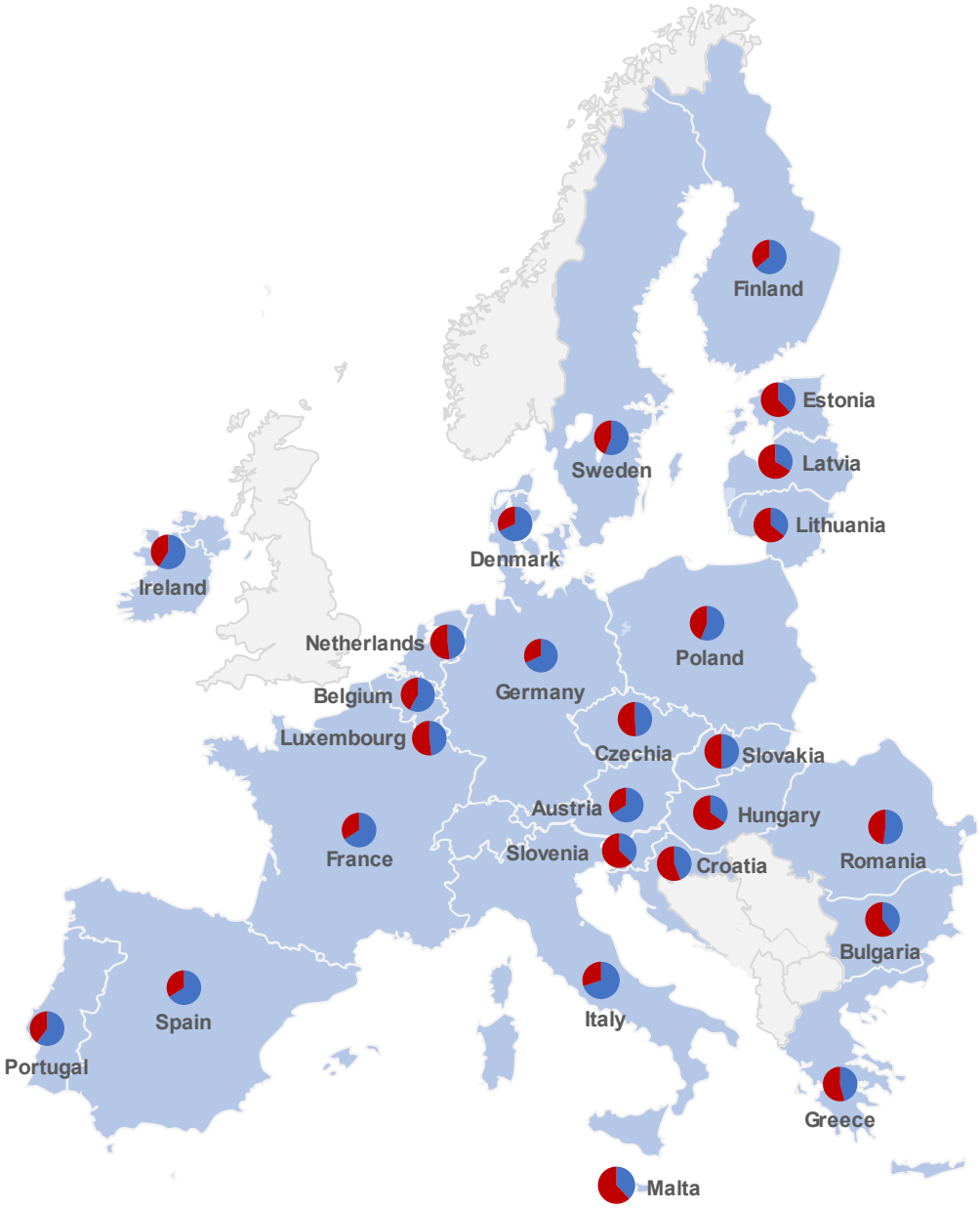
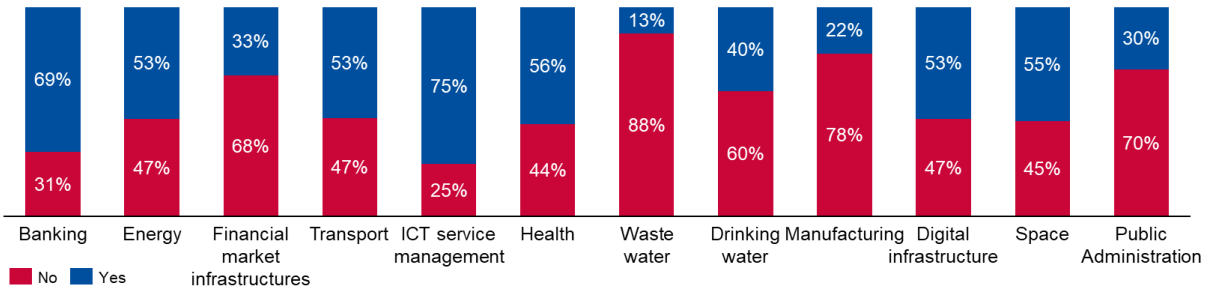


Figure 49: Leadership engagement in dedicated cybersecurity training, per Member State.



	YES %	NO %
Austria	66%	34%
Belgium	58%	42%
Bulgaria	40%	60%
Croatia	44%	56%
Czechia	49%	51%
Denmark	68%	32%
Estonia	38%	62%
Finland	64%	36%
France	66%	34%
Germany	68%	32%
Greece	46%	54%
Hungary	35%	65%
Ireland	59%	41%
Italy	70%	30%
Latvia	34%	66%
Lithuania	36%	64%
Luxembourg	48%	52%
Malta	38%	62%
Netherlands	48%	52%
Poland	56%	44%
Portugal	60%	40%
Republic of Cyprus	30%	70%
Romania	52%	48%
Slovakia	50%	50%
Slovenia	37%	63%
Spain	66%	34%
Sweden	56%	44%

Figure 50: Leadership engagement in dedicated cybersecurity training, per NIS 2 sector



Survey Question: Is your organisation's leadership responsible for approving cybersecurity risk-management measures?

Leadership is involved in approving cybersecurity risk management measures for 85% of the organisations surveyed, a 4% increase compared to last year (81%).

Germany (98%) and Belgium, France, Italy, Poland, and Spain (94%) have the highest percentage of entities declaring their leadership is responsible for approving cybersecurity risk management measures.

Sector-wise, ICT Service management leads with 96% of surveyed entities indicating that their leadership approves cybersecurity risk management measures, followed closely by Financial market infrastructures at 95%.

Figure 51: Leadership involvement in the approval of cybersecurity risk-management measures

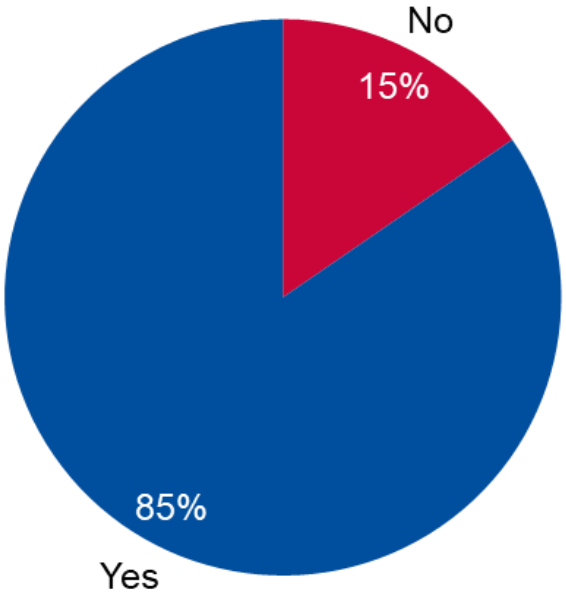
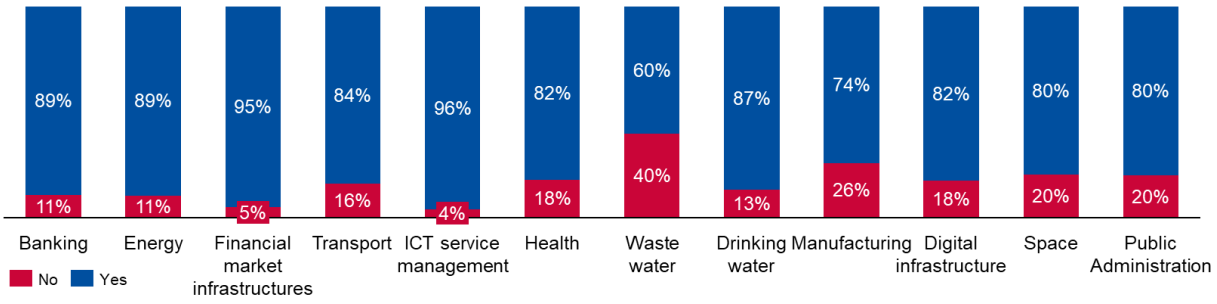


Figure 52: Leadership involvement in the approval of cybersecurity risk-management measures, per Member State

	YES %	NO %
Austria	88%	12%
Belgium	94%	6%
Bulgaria	78%	22%
Croatia	76%	24%
Czechia	86%	14%
Denmark	74%	26%
Estonia	74%	26%
Finland	88%	12%
France	94%	6%
Germany	98%	2%
Greece	82%	18%
Hungary	76%	24%
Ireland	92%	8%
Italy	94%	6%
Latvia	80%	20%
Lithuania	74%	26%
Luxembourg	88%	12%
Malta	76%	24%
Netherlands	88%	12%
Poland	94%	6%
Portugal	86%	14%
Republic of Cyprus	66%	34%
Romania	88%	12%
Slovakia	92%	8%
Slovenia	82%	18%
Spain	94%	6%
Sweden	82%	18%

Figure 53: Leadership involvement in the approval of cybersecurity risk-management measures, per NIS 2 sector



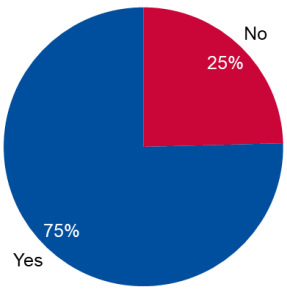
5.2 CYBERSECURITY RISK MANAGEMENT FOR THIRD PARTIES

<u>Survey Question:</u> Does your organisation have a policy related to supply chain cybersecurity risk management for third parties such as partners, vendors or suppliers?

75% of the organisations surveyed have a policy in place for managing cybersecurity risks in the supply chain related to third parties. However, the Waste water, Manufacturing, and Public administration sectors report the lowest proportions of entities with such policies.

Overall, the percentage of respondents with a third-party management policy in place for new NIS 2sectors (62%) is lower than that for existing NIS sectors (80%).

Figure 54: Cybersecurity risk management policy for third parties



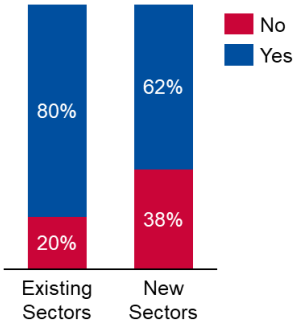
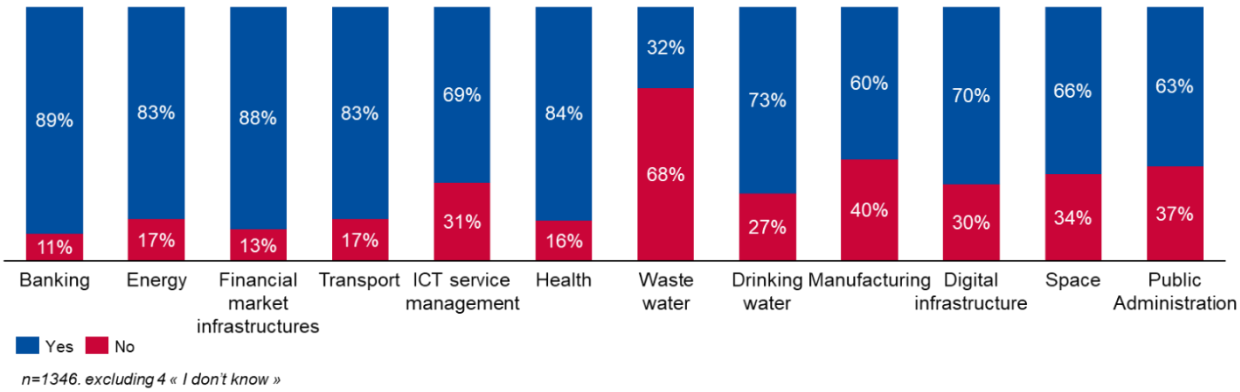


Figure 55: Cybersecurity risk management policy for third parties, per Member State

	YES %	NO %
Austria	80%	20%
Belgium	88%	12%
Bulgaria	68%	32%
Croatia	70%	30%
Czechia	82%	18%
Denmark	70%	30%
Estonia	58%	42%
Finland	80%	20%
France	88%	12%
Germany	86%	14%
Greece	68%	32%
Hungary	66%	34%
Ireland	90%	10%
Italy	90%	10%
Latvia	67%	33%
Lithuania	60%	40%
Luxembourg	74%	26%
Malta	65%	35%
Netherlands	84%	16%
Poland	84%	16%
Portugal	76%	24%
Republic of Cyprus	49%	51%
Romania	82%	18%
Slovakia	78%	22%
Slovenia	68%	32%
Spain	86%	14%
Sweden	78%	22%

Figure 56: Cybersecurity risk management policy for third parties, per NIS2 sector



5.3 IT/OT PRODUCTS SECURITY

Survey Question: How do you establish trust in your supply chain and ensure confidence in the security of IT/OT products and services you use?

When asked about their method to establish trust in the supply chain of IT and OT products, 55% of organisations indicate that they rely on vendors' credentials and certifications for products/services and 49% that they have strict procurement criteria focused on information security.

16% of the organisations across all sectors do not conduct any specific assessment, with a peak at 48% reported by entities in the Waste water sector.

Figure 57: IT/OT Products and Services Supply Chain Trust

Figure 58: IT/OT Products and Services Supply Chain Trust, per NIS2 sector

- We rely on our vendors' credentials and certifications for products/services.
- We have strict procurement criteria focused on security when selecting vendors.
- We perform regular audits.
- I We perform our own security testing of products.
- We engage in collaborative efforts with vendors to enhance security practices and address vulnerabilities.
- We do not conduct any specific assessments and trust our supply chain implicitly.

5.4 PERCEIVED CYBER-RISK MANAGEMENT MATURITY

Survey Question: On a scale from 1 to 10, please rate your organisation's cyber-risk management maturity

Survey respondents were asked to perform a self-assessment of their cyber-risk management maturity based on the following scale definitions:

- Score = 1 – Minimal Maturity: Limited understanding of cyber risks and insufficient practices.
- Score = 5 – Developing Maturity: Improving understanding of cyber risks with progressing practices.
- Score = 10 - Highly Mature: Deep understanding of cyber risks and state-of-the-art measures.

The figures that follow depict the results of this self-assessment.

Overall, the score across all sectors is at 6.7, indicating that surveyed organisations perceive having a solid understanding of cyber risks and effective management measures in place. New NIS 2 sectors seem to have a lower perceived maturity of 6.2 against 6.8 for existing NIS sectors.

Banking ranks highest in perceived cyber risk management maturity with a score of 7.8, followed by Health at 7.4. Energy and Transport both hold a perceived maturity score of 7. At the lower end, Waste water reports a perceived maturity of 4.3, while Space and Financial market infrastructure follow with scores of 5.4 and 5.5, respectively.

Figure 59: Cyber-risk management perceived maturity, all sectors

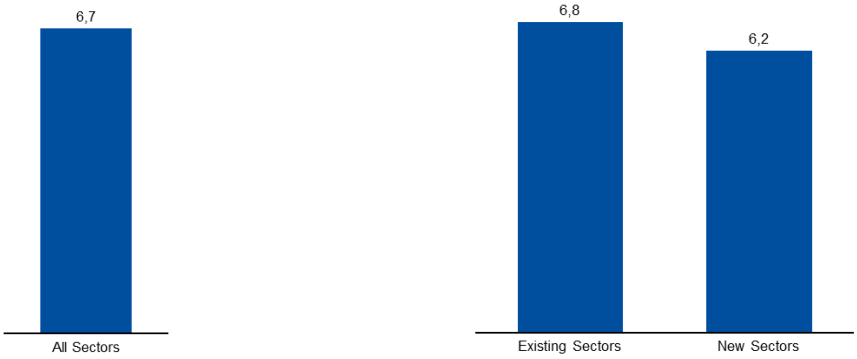
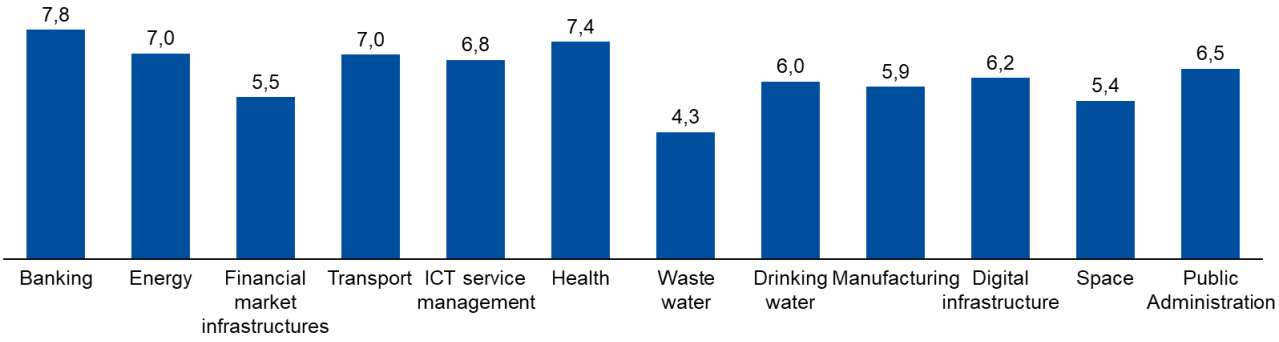


Figure 60: Cyber-risk management perceived maturity, per Member State

Figure 61: Cyber-risk management perceived maturity, per NIS 2 Sector



5.5 PERCEIVED NETWORK AND INFORMATION SECURITY MATURITY

Survey Question: On a scale from 1 to 10, please rate your organisation's network and information systems cybersecurity maturity level

Survey respondents were asked to perform a self-assessment of their network and information systems cybersecurity maturity based on the following scale definitions:

- Score = 1 – Minimal Maturity: Security measures are inadequate, frequent oversight of vulnerabilities, and significant risks from legacy technology.
- Score = 5 – Developing Maturity: Making progress in the implementation of security measures but still struggling with areas such as legacy or vulnerability management.
- Score = 10 - Advanced Maturity: Optimised security measures, effective vulnerability management, minimal risks from legacy systems.

The figures that follow reflect the results of this self-assessment.

Overall, the average perceived maturity across all sectors is 6.8, suggesting that surveyed organisations generally perceive having effective security measures, adequate vulnerability management arrangements and effective measures in place to deal with legacy systems in both IT and OT.

The perceived maturity of entities in sectors previously in scope of NIS was higher (7) than that of entities in new sectors (6.3).

The Banking sector demonstrates the highest perceived maturity, with a score of 7.9, followed by the Health sector at 7.5. The Energy and Transport sectors follow with perceived maturity levels, at 7.2 and 7.1, respectively.

In contrast, the Waste water, Space, and Financial market infrastructure sectors report the lowest perceived maturity levels, with scores of 4.3, 5.5, and 5.6, respectively.

Figure 62: Network and information security perceived maturity

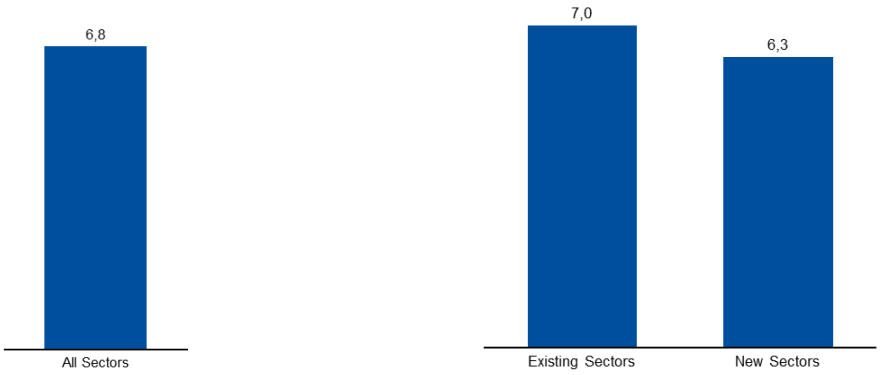


Figure 63: Network and information security perceived maturity, per Member State

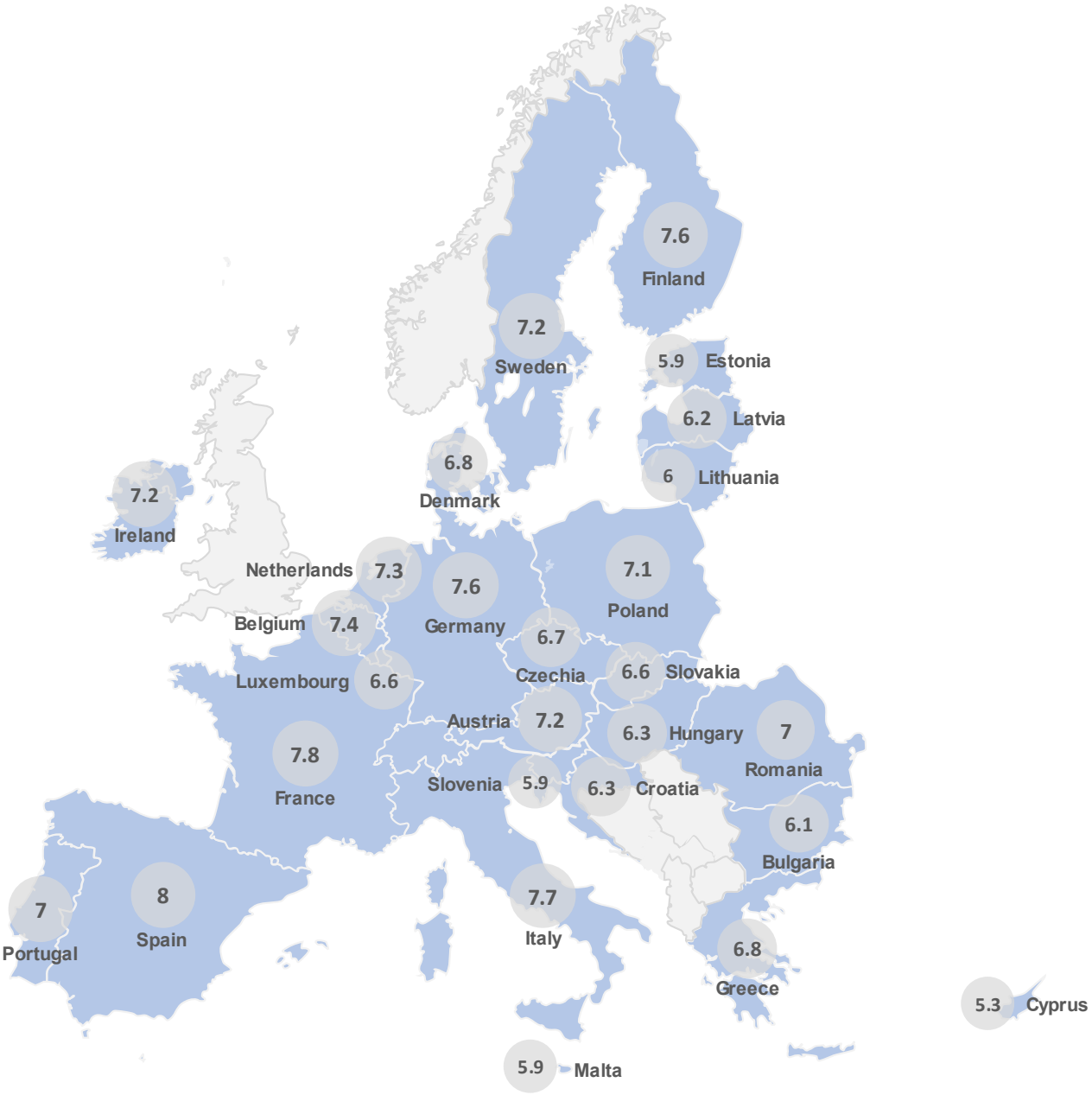
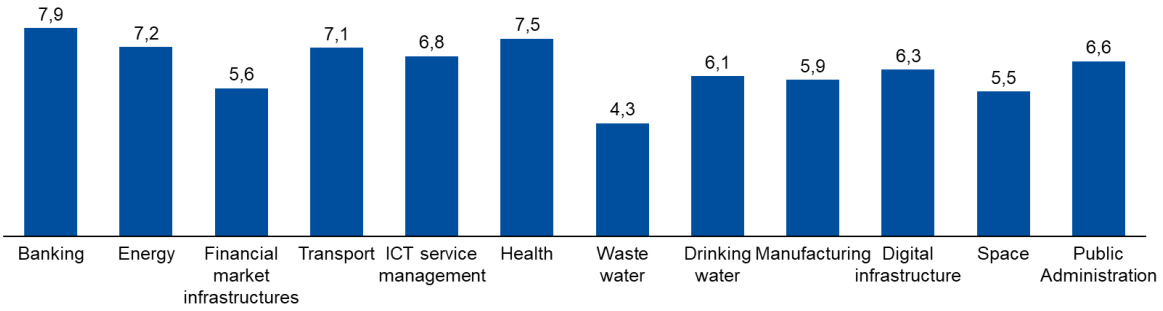


Figure 64: Network and information security perceived maturity, per NIS 2 Sector



5.6 INFORMATION SHARING

Survey Question: Does your organisation participate in national or EU-level Information Sharing and Analysis Centres (ISACs) or in any other forms of information sharing?

74% of surveyed entities exchange information with their national competent authority, while just over a third utilise EU ISACs or industry associations as key channels for information-sharing.

22% of organisations do not engage in any collaboration or information-sharing initiatives.

Entities in sectors not previously covered by the NIS Directive, such as ICT service management, Waste water, Manufacturing, Space and Public administration, report higher rates of non-participation in information-sharing initiatives compared to other sectors.

Figure 65: Participation in information sharing activities among surveyed entities

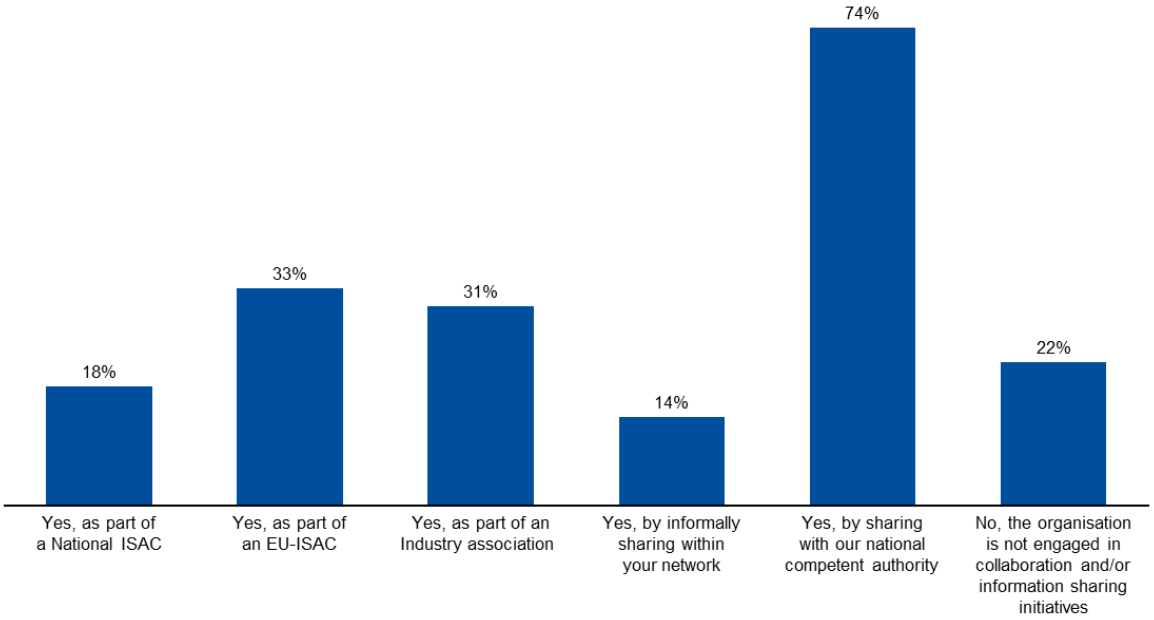


Figure 66: Participation in information sharing activities, per Member State

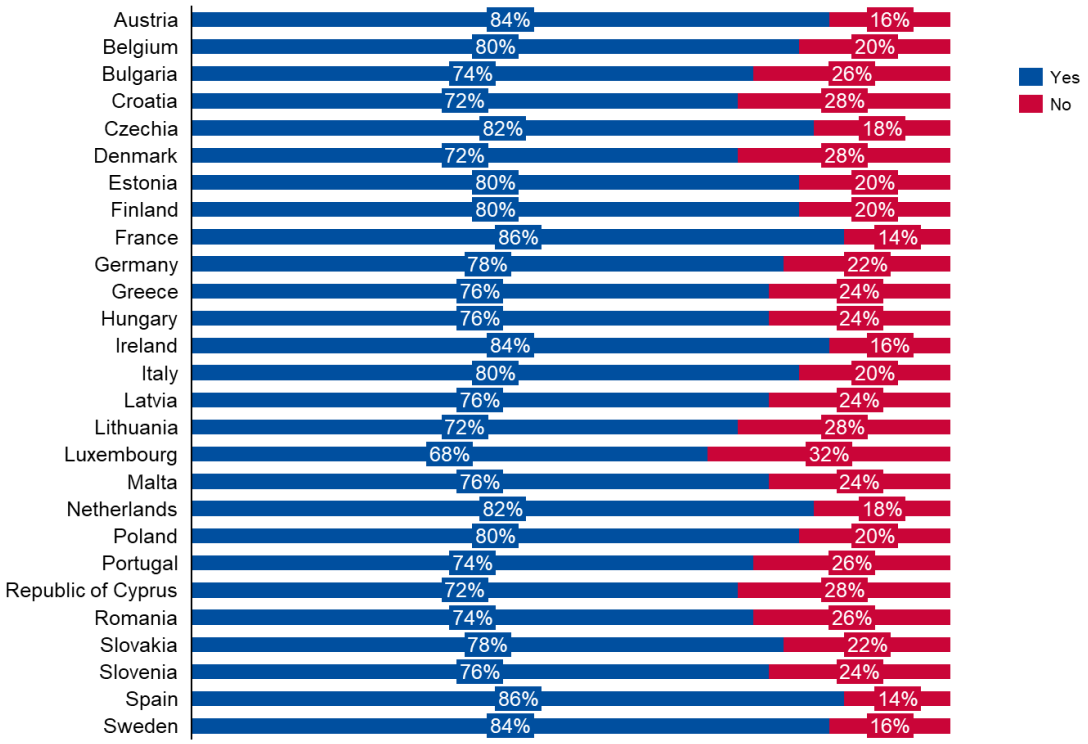


Figure 67: Participation in information sharing activities, per NIS2 sector

- Yes, as part of a National ISAC
- Yes, as part of an EU-ISAC
- Yes, as part of an Industry association
- Yes, by informally sharing within your network
- Yes, by sharing with our national competent authority
- No, the organisation is not engaged in collaboration and/or information sharing initiatives

5.7 CYBER RESILIENCE ACT (CRA)

Survey Question: Are you developing products that will be in scope of the Cyber Resilience Act (CRA)?

24% of respondents indicated that they are developing products within the scope of the Cyber Resilience Act (CRA)[36].

75% of entities in the ICT service management and 62% of entities in the Digital infrastructure sectors suggested they are developing such products.

Figure 68: CRA Product Development

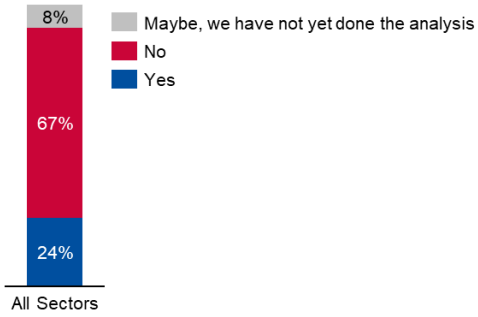
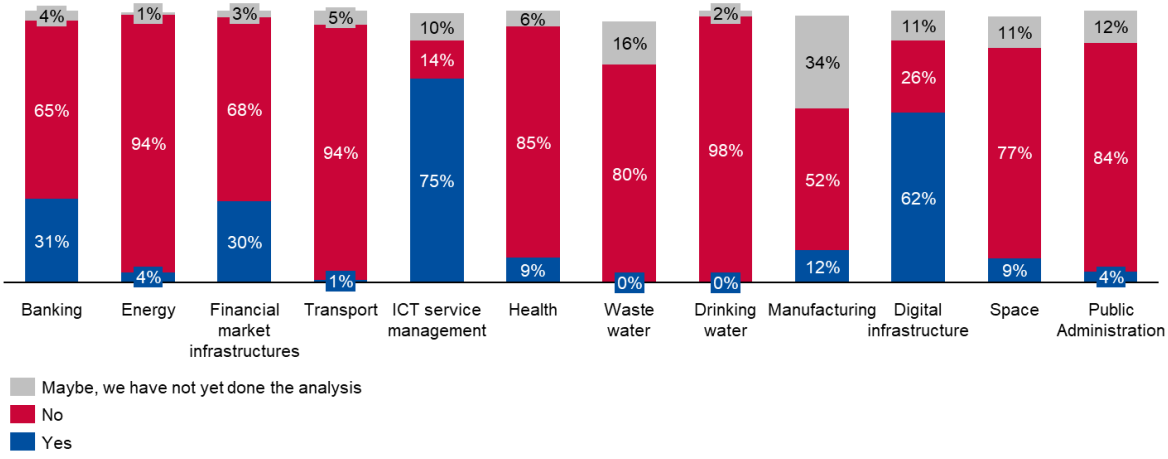


Figure 69: CRA Product Development, per NIS 2 sector

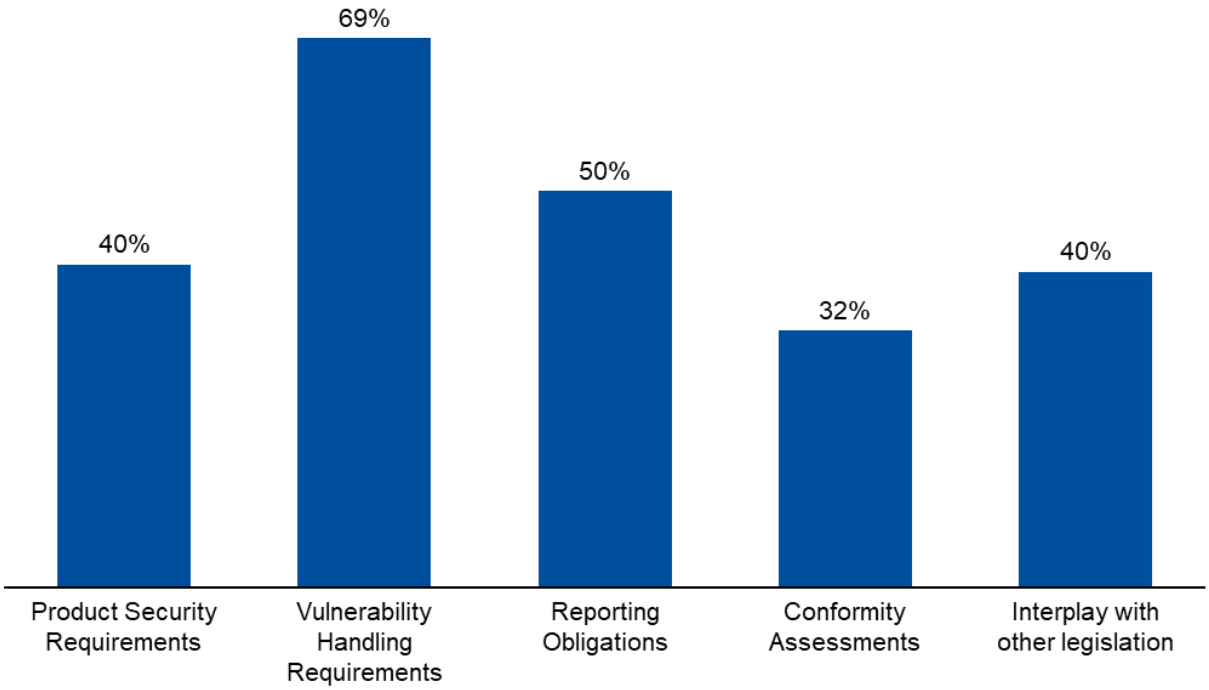


Survey Question: Which of the below areas of the CRA would you most appreciate further guidance in?

69% of the organisations developing products in scope of the CRA would appreciate further guidance on Vulnerability Handling Requirements and 50% on Reporting Obligations.

[36] European Commission. (n.d.). Cyber Resilience Act. Available at: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

Figure 70: Guidance about CRA requirements

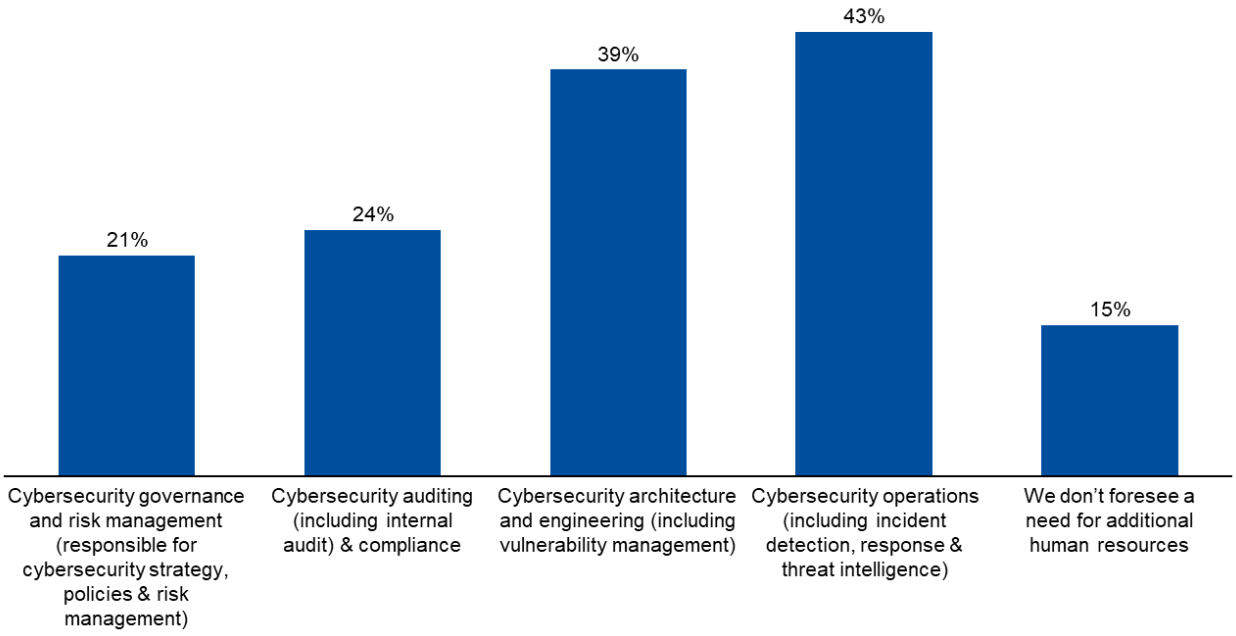


n=329. only for organizations developing products in scope of CRA

Survey Question: For which of the following area will you need additional human resources to comply with the Cyber Resilience Act?

43% of the organisations developing products within the CRA scope foresee the need for additional human resources in cybersecurity operations and 39% in cybersecurity architecture and engineering. 15% of the organisations do not foresee the need for additional human resources.

Figure 71: Cybersecurity human resources to comply with the Cyber Resilience Act



n=329. only for organizations developing products in scope of CRA

5.8 EU CYBERSECURITY CERTIFICATION

Survey Question: In your industry sector, would an EU cybersecurity certification for products with digital elements be valuable for supply chain risk management?

Among the surveyed organisations, 86% expressed that an EU cybersecurity certification for products with digital elements would be beneficial for their sector.

This sentiment is particularly strong in the Banking sector, where 99% of respondents indicated its value. The Waste water sector has the lowest proportion of respondents who believe such a certification would be valuable, with only 52% of entities identifying it as beneficial.

Figure 72: Interest in EU cybersecurity certification for products with digital elements

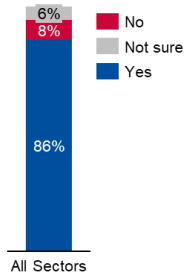
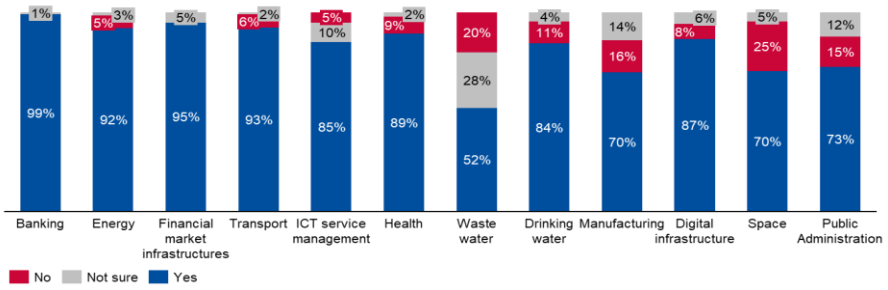


Figure 73: Interest in EU cybersecurity certification for products with digital elements, per NIS2 sector



6. CYBER ATTACK EXPECTATIONS AND PREPAREDNESS

Key Figures
90% of surveyed organisations expect an increase in cyberattack costs, volume, or both in the next year.
Sectors previously covered by NIS reported higher perceived maturity in detecting and responding to cyberattacks (7.1 vs. 6.3) compared to new sectors.
When it comes to participation in cybersecurity preparedness initiatives 74% of the surveyed entities engage in internal initiatives, with new sectors exhibiting consistently lower engagement and higher non-participation than existing sectors.

6.1 CYBER ATTACK EXPECTIONS

Survey Question: In the coming year, what does your organisation expect to face?

When asked to predict the evolution of security threats in the coming year, the majority (53%) of organisations anticipate an increase in cyberattacks. 19% foresee **both** a higher volume and increased costliness of these attacks.

Only 10% of organisations expect no significant changes in the volume or costliness of cyberattacks. This expectation is most prevalent in the Drinking water (53%), Waste water (36%), and Manufacturing (32%) sectors.

Figure 74: Cyberattack expectations in the coming year

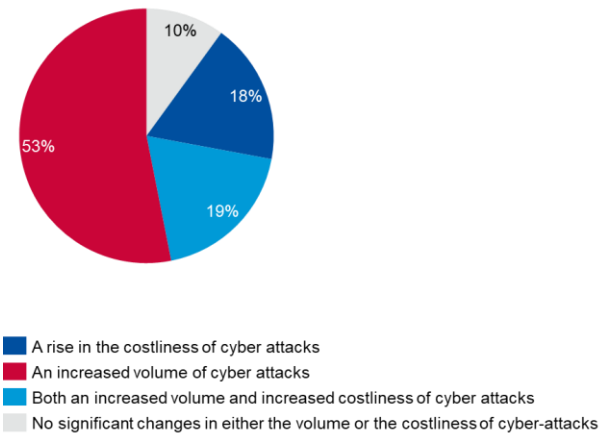
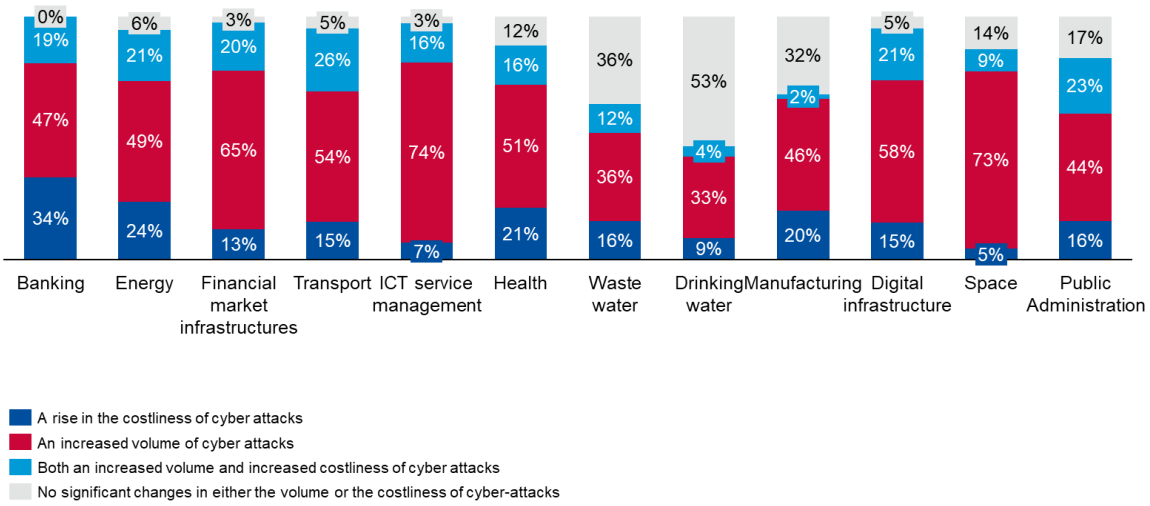


Figure 75: Trend about security threat, per NIS2 sector



6.2 PERCEIVED CYBER-ATTACK DETECTION AND RESPONCE CAPABILITY MATURITY

Survey Question: On a scale from 1 to 10, please rate your organisation's capability to detect and respond to sophisticated cyber-attacks

Survey respondents were asked to perform a self-assessment of their capability to detect and respond to sophisticated cyber-attacks based on the following scale definitions:

- Score = 1 – Our capability to detect and respond to any type of cyber-attack is minimal.
- Score = 5 – Our capability enables us to detect and respond to many simple cyber-attacks on some parts of our infrastructure. However, improvement is still needed before we can effectively detect more sophisticated attacks against our infrastructure.
- Score = 10 - Highly Mature: Our capability enables us to detect and respond to most sophisticated cyber-attacks across most parts of our infrastructure. We are continuously testing and improving our processes, automating as much as possible.

The figures that follow illustrate the results of this self-assessment.

Overall, the score across all sectors is 6.9, indicating that surveyed organisations perceive having capabilities to detect and/or respond to **many simple** and **some sophisticated** cyber-attacks **on most parts of their infrastructure**.

The analysis per sector shows that entities in the Banking perceive their detection and response maturity to be the highest (at 8.1), followed by entities in the Health sector that self-assess their maturity at 7.6. Entities in the Energy and Transport sector follow self-assessing their maturity at a 7.2. Only the Waste water (4.4) sector has indicated a score below 5 meaning they perceive being able to respond only to simple to attacks and probably not on all their infrastructure.

Figure 76: Capability to detect and respond to sophisticated cyber-attacks

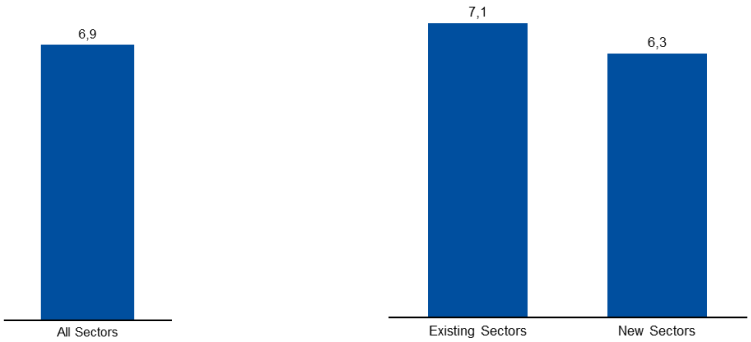


Figure 77: Capability to detect and respond to sophisticated cyber-attacks, per Member State

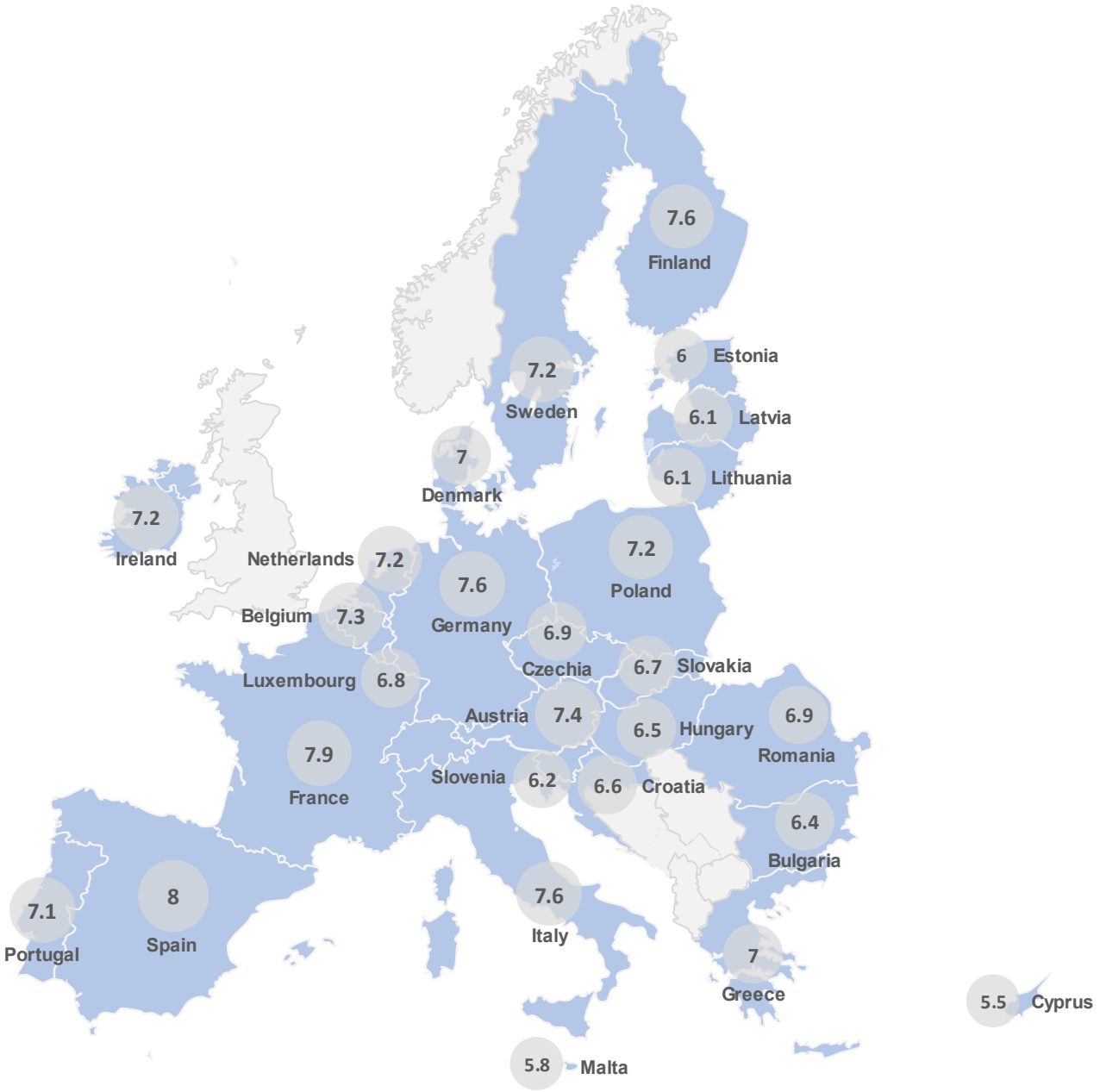
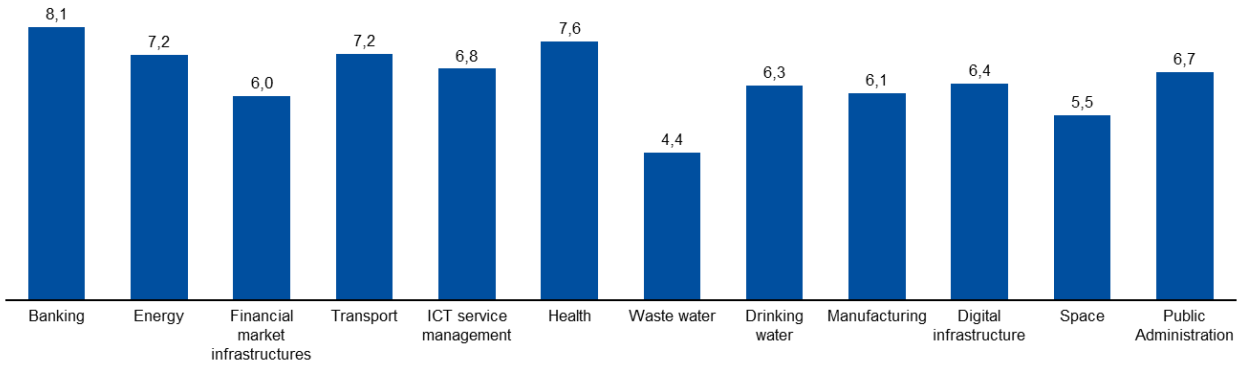


Figure 78: Capability to detect and respond to sophisticated cyber-attacks, per NIS2 sector



6.3 PARTICIPATION TO CYBERSECURITY PREPAREDNESS INITIATIVES

Survey Question: Does your organisation participate in cybersecurity preparedness initiatives?

When it comes to participation in cybersecurity preparedness initiatives, 74% of the surveyed entities indicated that they engage in such activities within their organisations. Participation in national-level cyber drills and exercises was notably low at just 12%. Whereas 17% of organisations reported that they do not engage in any cybersecurity preparedness initiatives.

When comparing the responses of new sectors to existing ones, it is evident that new entities consistently show lower engagement in these initiatives, with a higher overall percentage of non-participation.

Figure 79: Participation to cybersecurity preparedness initiatives

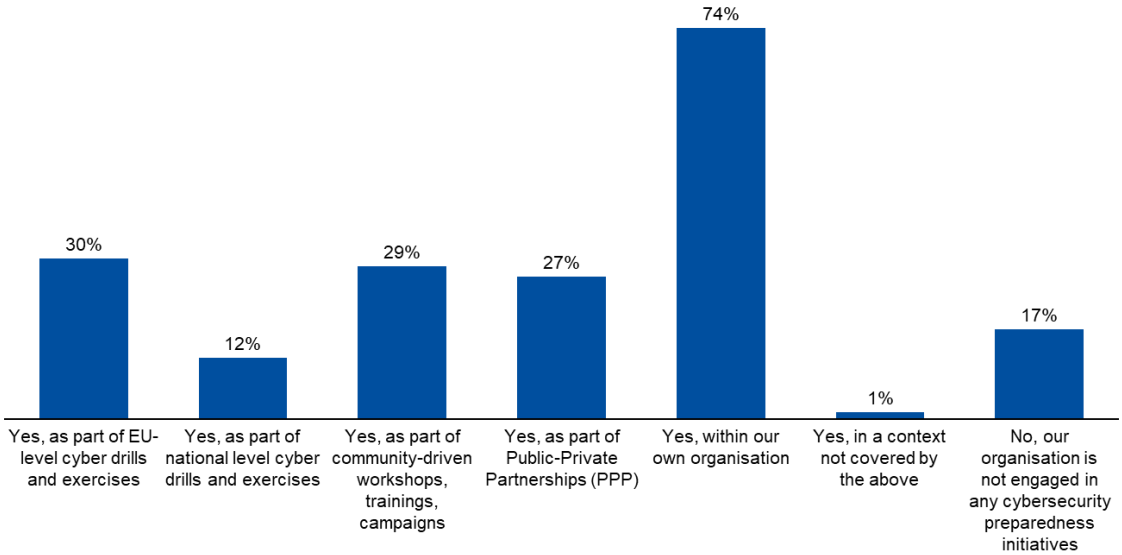
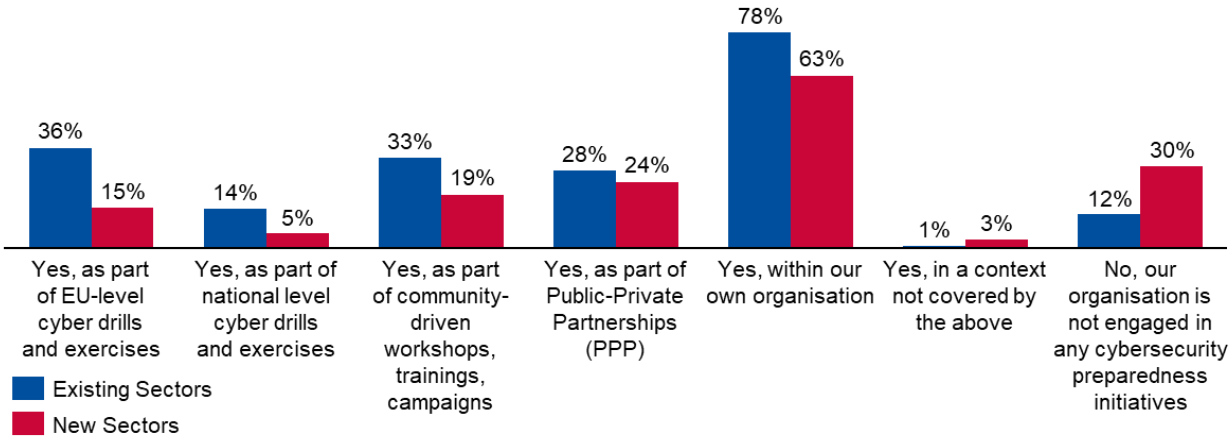


Figure 80: Participation to cybersecurity preparedness initiatives, in existing and new NIS sectors



7. SECTORAL ANALYSIS: DIGITAL INFRASTRUCTURE

Digital Infrastructure forms the technical foundation of Europe's digital economy. It encompasses providers of Core Internet services (IXPs, DNS, TLD, CDN), providers of Cloud computing and Data centre services, providers of Trust services and providers of Telecommunication networks and/or services. Internet infrastructure providers maintain the technical backbone that supports online services. Trust service providers offer services that enhance the security of online transactions and communications and telecommunications operators ensure connectivity through fixed and mobile networks relied upon daily by millions of Europeans.

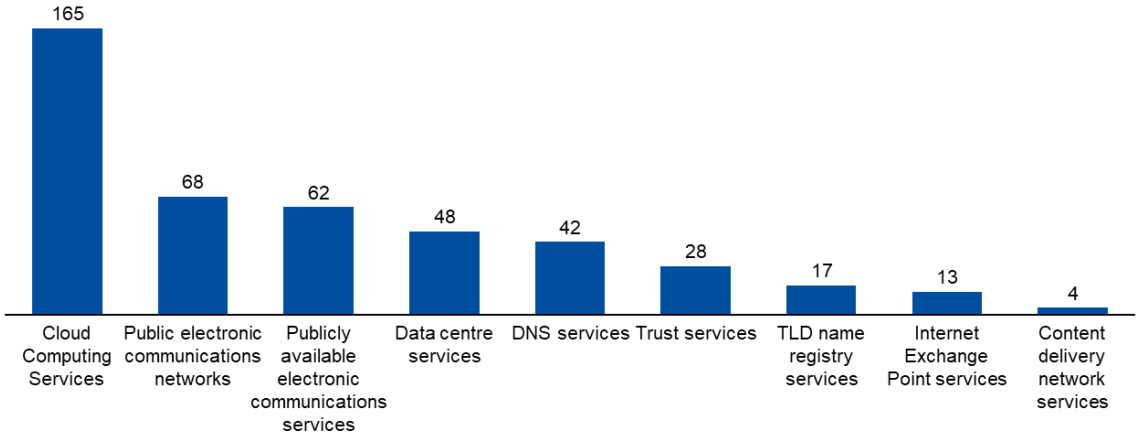
This section examines the Digital Infrastructure sector's strategic priorities, focusing on three critical aspects: incident reporting obligations, implementation of cybersecurity frameworks, and risk management approaches regarding high-risk vendors.

7.1 DIGITAL INFRASTRUCTURE SERVICES

Survey Question: Which of the following services does your organisation provide?

For the purposes of this deep dive, 261 organisations were surveyed in the Digital infrastructure sector. The following figure provides a detailed breakdown of the digital infrastructure services offered by each of the surveyed organisations.

Figure 81: Digital Infrastructure Services



n=261. only Digital Infrastructure Sector

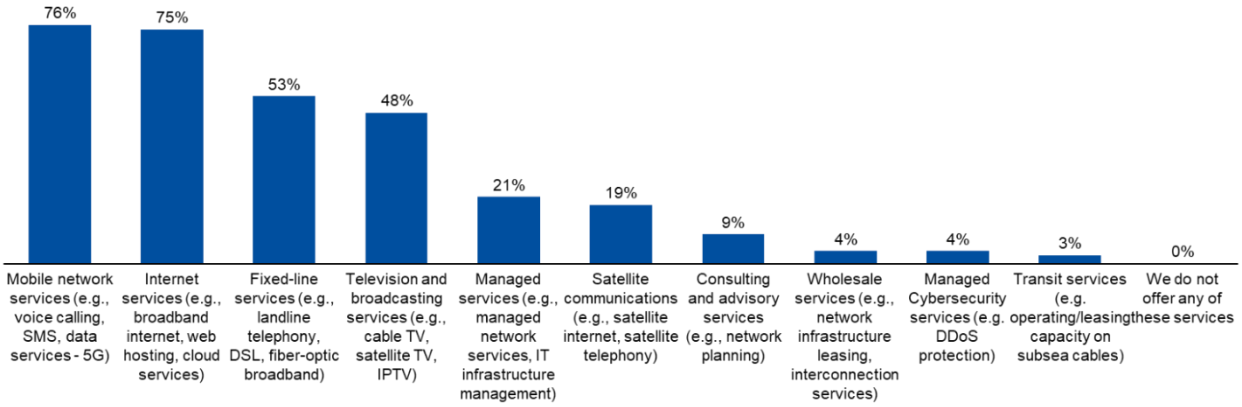
7.2 TELECOMMUNICATION SERVICES

Survey Question: Which of the following types of services do you offer?

76% of the seventy five organisations delivering publicly available electronic communications services or public electronic communications networks offer mobile network services, while 75% provide internet services.

Figure 82 provides a breakdown of the telecommunications services offered by these entities.

Figure 82: Telecommunication Services



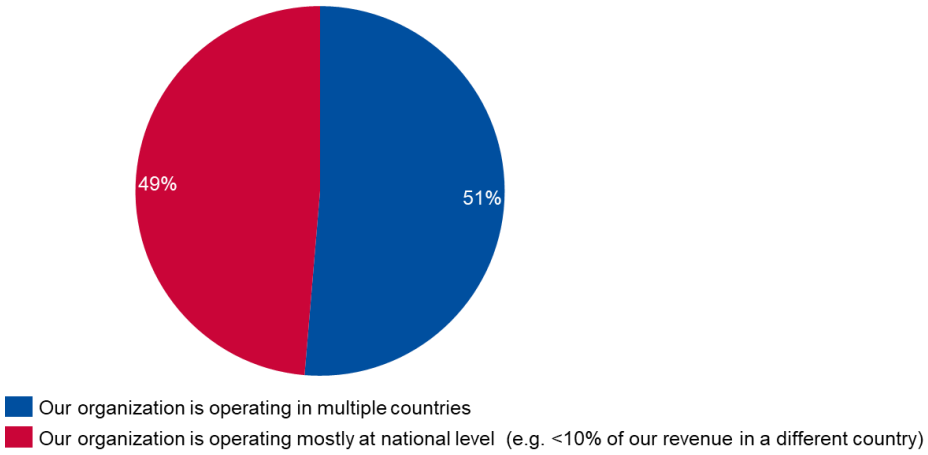
n=75. only Publicly available electronic communications services and Public electronic communications networks

7.3 SCOPE OF OPERATIONS

Survey Question: Does your organisation operate cross-border or mostly nationally?

In our survey sample, there is a comparable representation of digital infrastructure entities operating nationally (49%) and cross-border (51% entities with more than 10% of their revenue in a different country).

Figure 83: Scope of operations



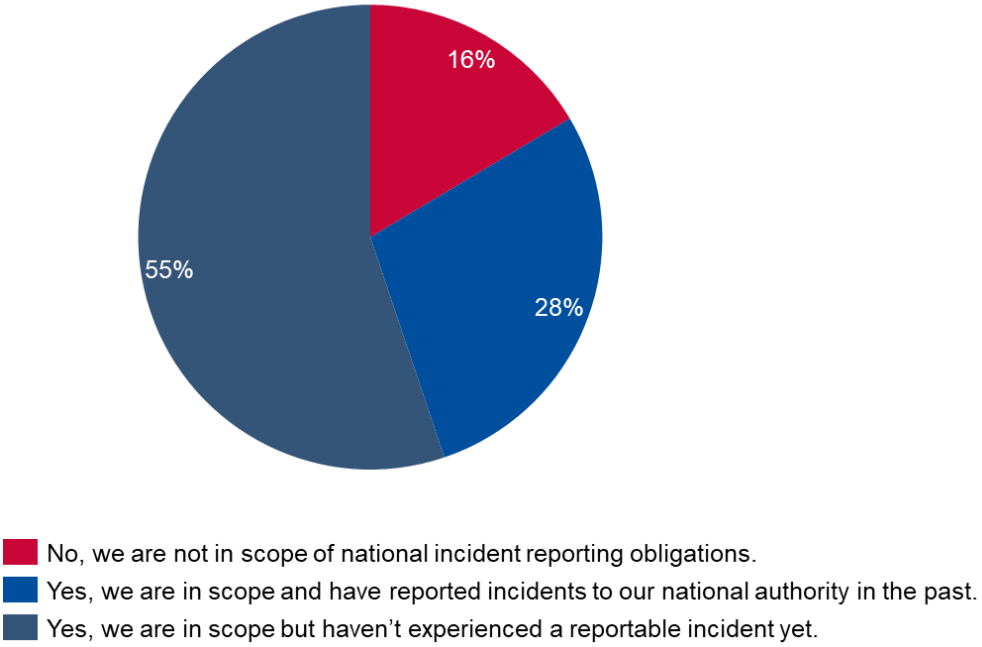
7.4 INCIDENT NOTIFICATION OBLIGATIONS

Survey Question: Are you in scope of national incident reporting obligations and have you reported any incidents?

The majority of digital infrastructure organisations (55%) declared being subject to national incident reporting obligations but not yet having experienced a reportable incident, while 28% suggested having reported incidents in the past.

16% of the Digital Infrastructure entities declared not being in scope of national incident reporting obligations.

Figure 84: Reporting obligations

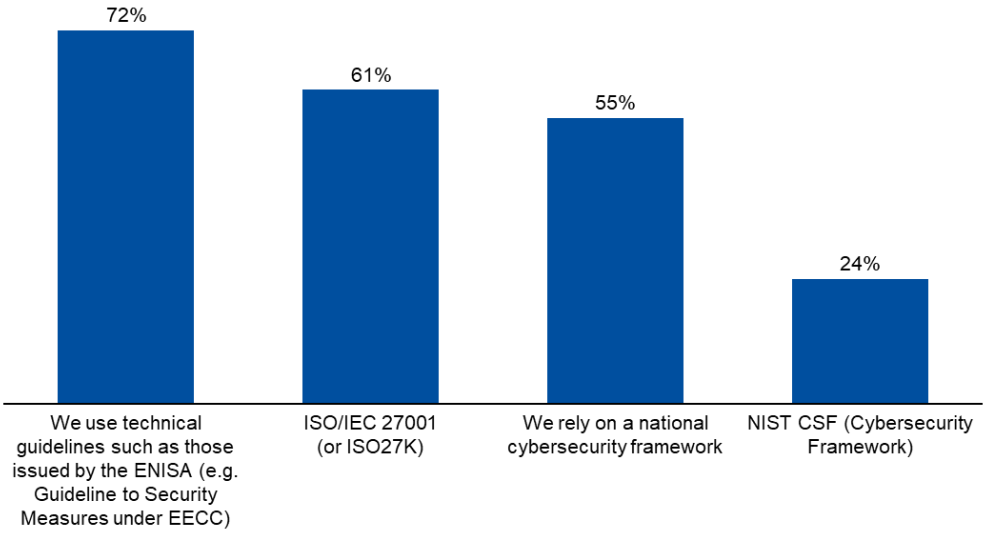


7.5 CYBERSECURITY FRAMEWORKS

Survey Question: Which security frameworks does your organisation rely on for ensuring robust cybersecurity measures?

Most respondents (72%) indicated that they rely on technical guidelines to ensure they implement robust cybersecurity measures.

Figure 85: Information security frameworks

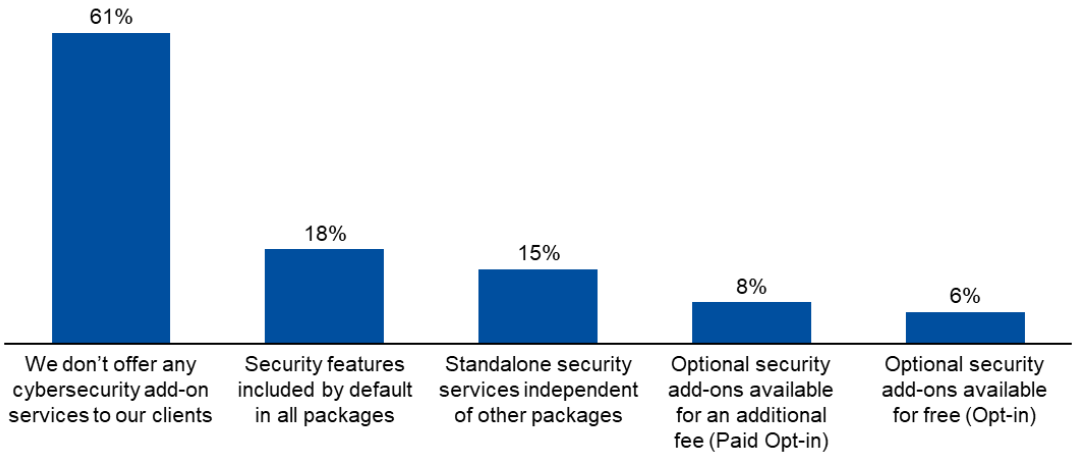


7.6 CYBERSECURITY SERVICES

Survey Question: Do you offer any cybersecurity add-on services to your clients? If so, what is the nature of those services?

Most of the digital infrastructure entities (61%) do not offer cybersecurity add-on services to their clients. 18% of respondents indicated that they include security features by default in all packages, while 15% propose standalone security services independently.

Figure 86: Security Services



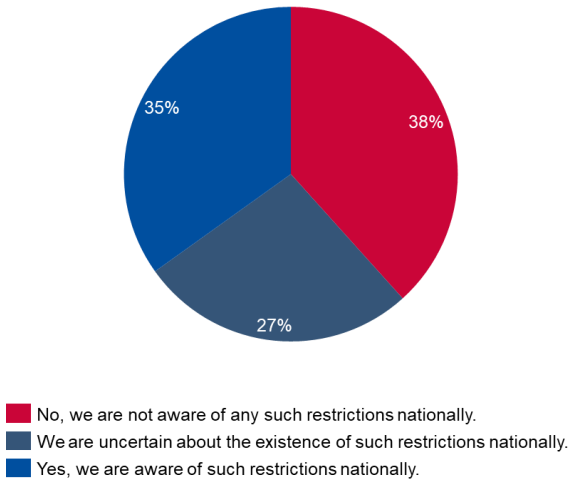
7.7 HIGH RISK VENDORS

Survey Question: Are you aware of any national restrictions regarding the use of high-risk vendors?

There is significant uncertainty surrounding national restrictions on the use of high-risk vendors, with 27% of respondents unsure about the existence of such restrictions.

38% of respondents are not aware of such restrictions nationally, while 35% are aware of them.

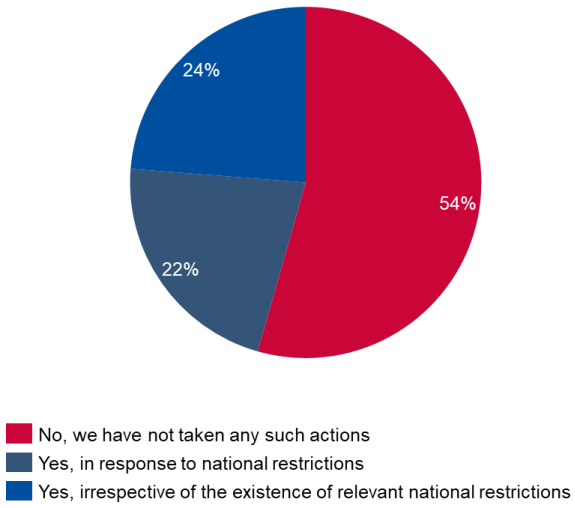
Figure 87: Awareness around national restrictions regarding high-risk vendors



Survey Question: Have you taken any actions to minimise risks associated with high-risk vendors?

46% of the respondents have taken some form of action with regards to high-risk vendors.

Figure 88: Actions to minimise risks associated with high-risk vendors

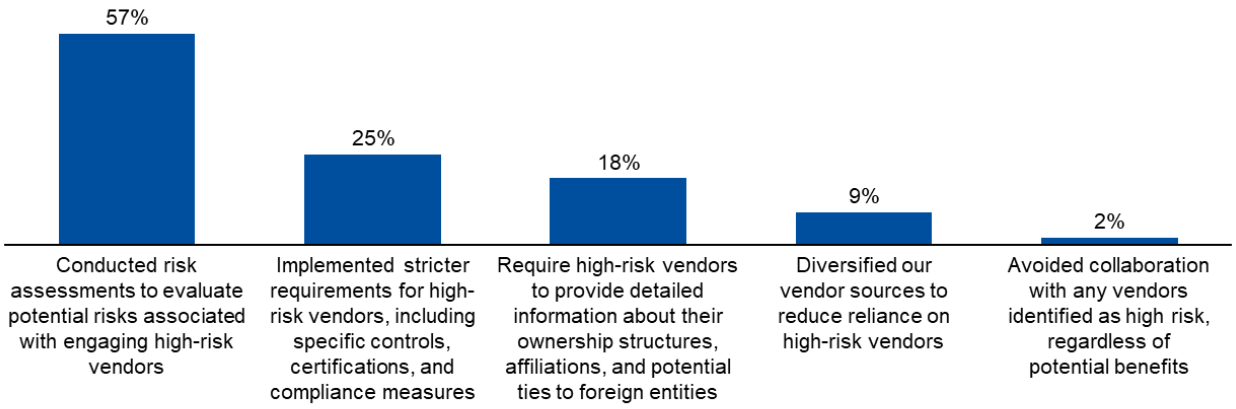


Survey Question: Which measure(s) has your organisation implemented to minimise risks associated with high-risk vendors in line with guidelines at national or EU level (e.g. 5G Toolbox)?

Among organisations that have taken measures, a majority (57%) have conducted risk assessments to evaluate potential risks associated with engaging high-risk vendors. 2% of the

respondents suggested having completely avoided collaboration with any vendor identified as high risk, regardless of potential benefits.

Figure 89: Measures implemented to minimise risks associated with high-risk vendors



n=119. only entities that have taken action

8. SECTORAL ANALYSIS: SPACE

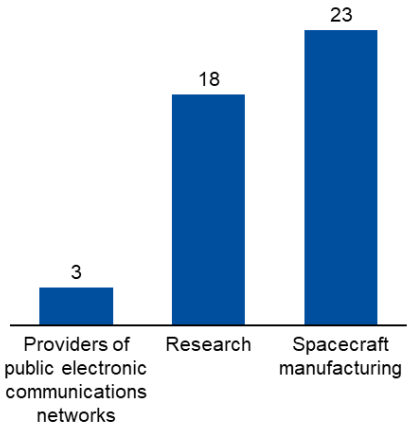
This section analyses data gathered from entities within the Space sector that fall directly under the NIS 2 Directive's scope, such as operators of ground-based services, along with other critical actors in the Space sector economy—including spacecraft manufacturers, satellite operators and service providers, and research organisations.

For the purposes of this study and because the number of operators in Space that meet the criteria for essential entities under NIS 2 was low, additional operators from the Space sector were surveyed.

8.1 SPACE ENTITIES PROFILE

Out of the 44 organisations surveyed from the Space sector, there are 23 operating in spacecraft manufacturing, 18 in research and 3 are providers of public electronic communications networks.

Figure 90: Space Entities Profile



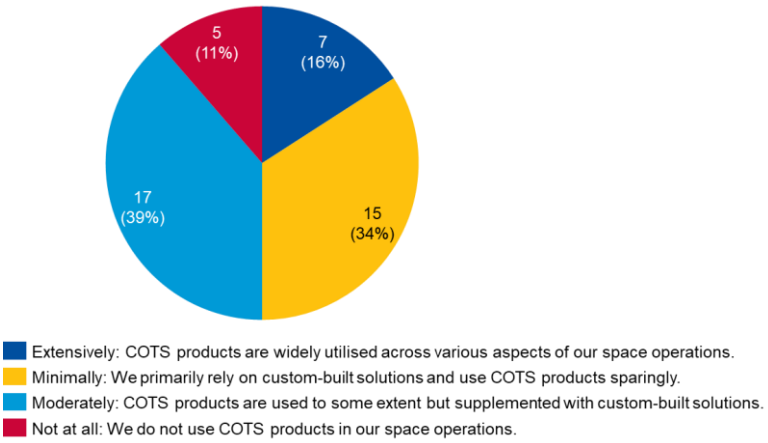
8.2 COTS (COMMERCIAL OFF THE SHELF) USAGE

Survey Question: To what extent does your organisation rely on Commercial Off-The-Shelf (COTS) products in your space operations? Space operations cover both space and ground segments.

Overall, the data indicates that a substantial majority (89%) of space sector organisations incorporate COTS applications into their operations to some degree. This widespread adoption suggests a growing acceptance of commercial solutions within the traditionally specialised Space sector.

The breakdown indicates that 16% of organisations declare extensive use of COTS applications across their space operations. 39% utilise COTS moderately, while 34% use them minimally. Only 11% do not employ COTS products to support their space operations.

Figure 91: COTS in Space

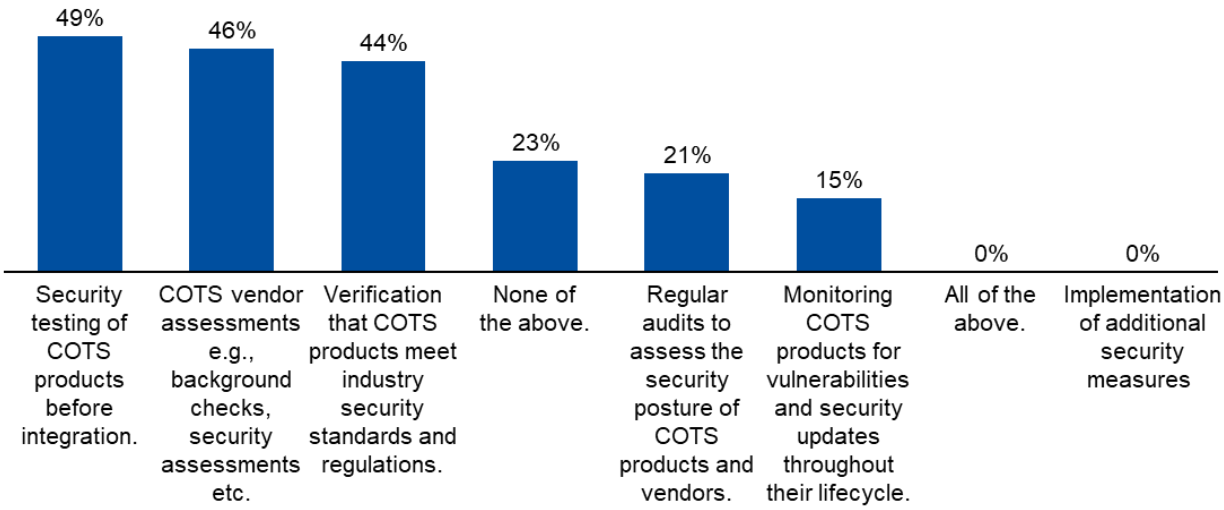


8.3 SECURITY OF COTS PRODUCTS

Survey Question: How does your organisation ensure the security of Commercial Off-The-Shelf (COTS) products supporting your operations across the various segments (user, ground, space etc.)?

Nearly half of the organisations (49%) that use COTS in the Space sector perform security testing of the products before integration. 46% execute COTS vendor assessments and 44% verify that COTS products meet industry security standards and regulations.

Figure 92: Security of COTS product

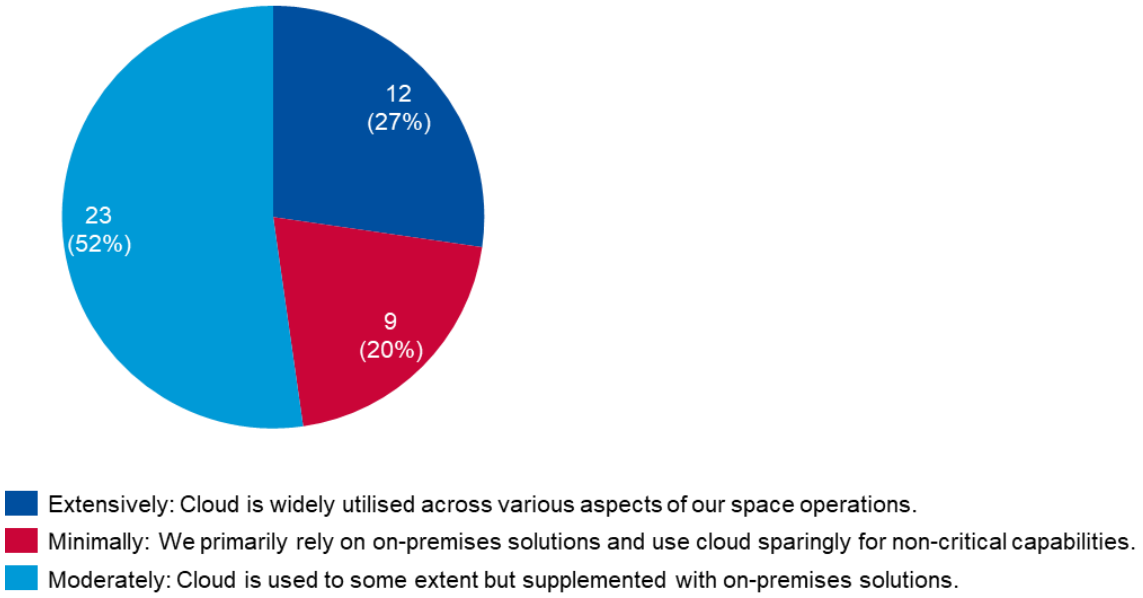


8.4 USE OF CLOUD SERVICES

Survey Question: To what extent does your organisation rely on the use of Cloud services?

All organisations operating in the Space sector are using cloud services to some extent. Figure 94 below shows the breakdown per intensity of sage.

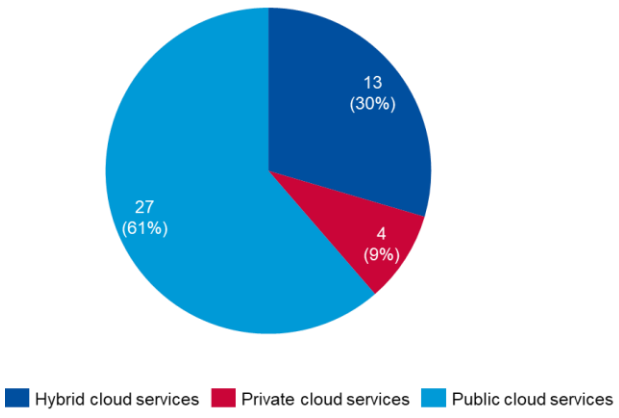
Figure 93: Use of cloud services in Space



Survey Question: What type of cloud services do you primarily use?

Public cloud services are primarily used by the space entity with 61% of organisations and only 4% prefer private cloud services. No organisation has indicated using sovereign cloud services or industry cloud services.

Figure 94: Type of cloud services

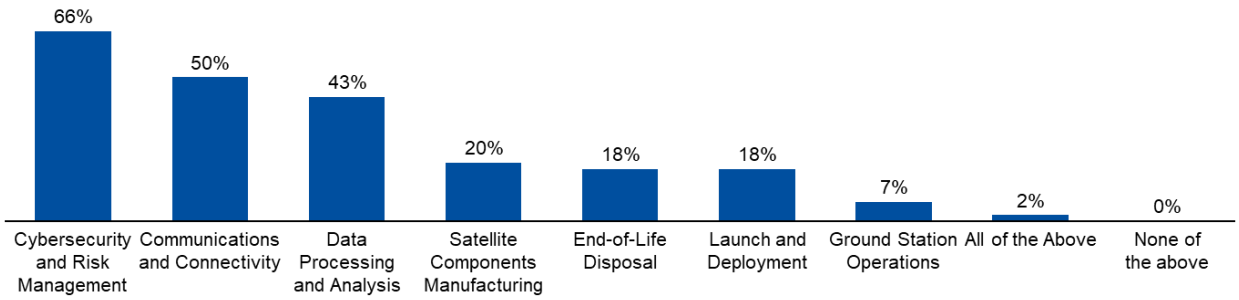


8.5 USE OF 3RD PARTY SUPPLIERS

Survey Question: For which of the below do you rely on Third Party Suppliers?

66% of the space respondents indicated using third party suppliers for Cybersecurity and Risk Management, 50% for Communications and Connectivity and 43% for Data Processing and analysis.

Figure 95: Use of 3rd party suppliers

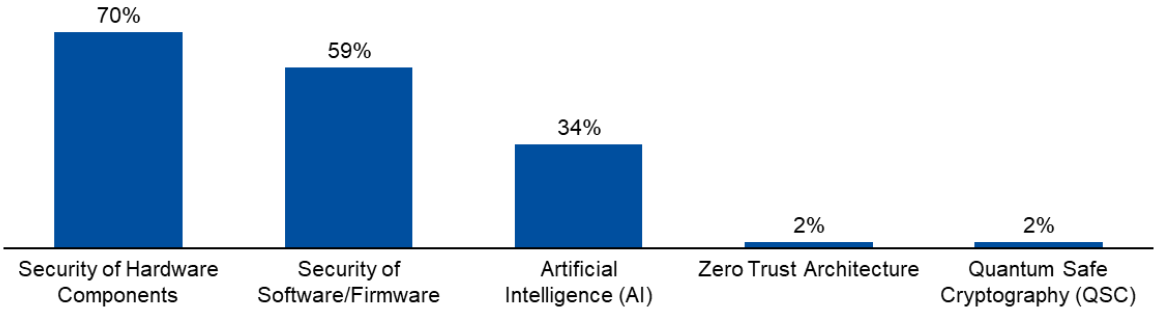


8.6 CYBERSECURITY POSTURE STRENGTHENING

Survey Question: Which of the below technologies is your organisation considering in the context of strengthening its cyber-posture?

While traditional security measures dominate the space sector's priorities, with 70% focusing on hardware security and 59% on software/firmware security, there is a notable gap in the adoption of emerging security technologies, as only 2% of organisations prioritise advanced approaches like Zero Trust Architecture and Post-Quantum Cryptography (PQC), despite 34% considering AI implementation for security enhancement.

Figure 96: Cybersecurity posture strengthening



9. COMPARING SMES AND LARGE ENTERPRISES

This chapter aim to provide additional insights on the data collected through the lens of the organisation size, breaking down key figures for SMEs and Large Enterprises (LE).

Figure 97: Small Medium Enterprise (SME) vs Large Enterprise (LE) distribution

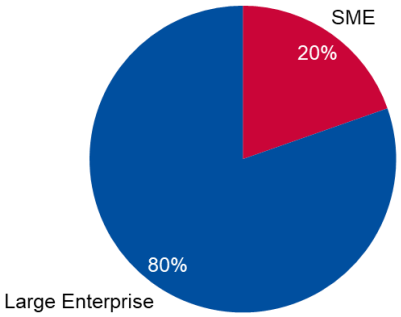


Figure 98: SME vs LE distribution across sectors

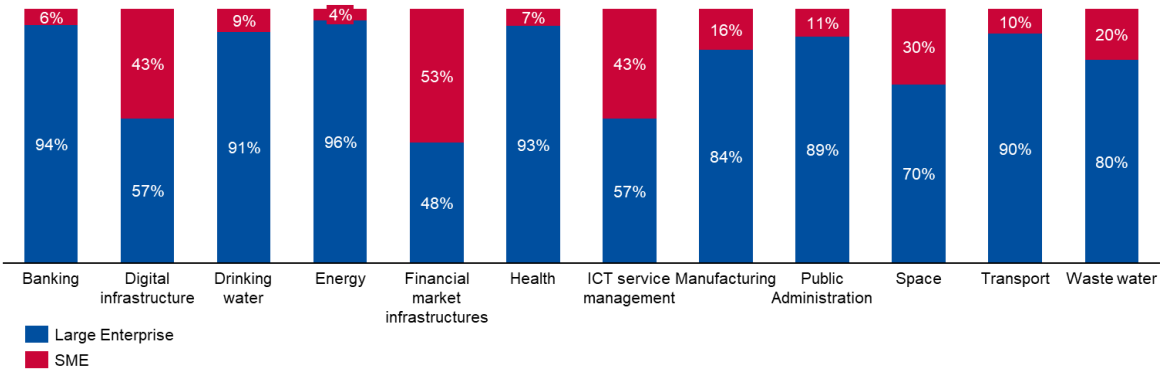
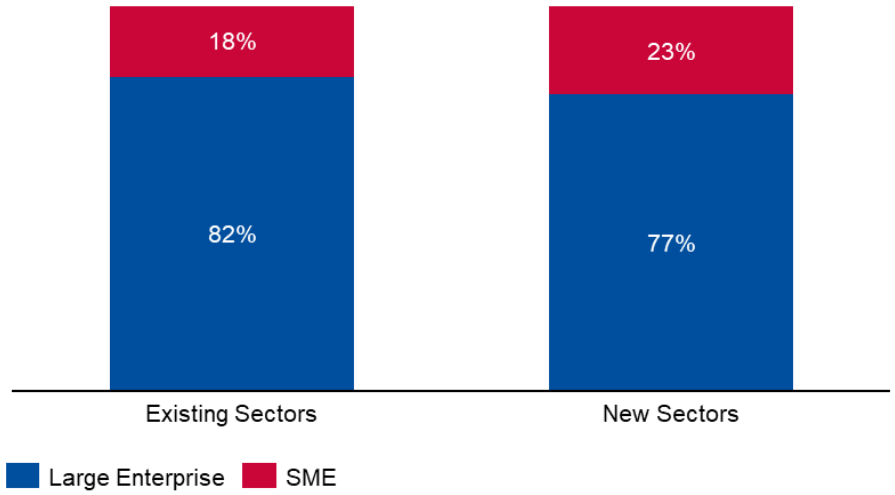
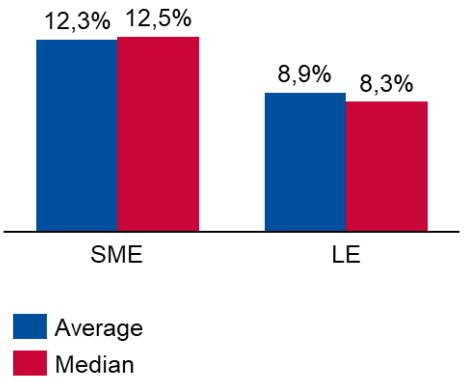


Figure 99: SME vs LE distribution in new and existing NIS sectors



The distribution of surveyed SMEs and LEs appears to be similar for both existing and new NIS 2 sectors.

Figure 100: IS spending as a share of IT spending for SMEs and LEs



The IS spend as a share of IT spend continues to grow year-on-year for both SMEs and LEs. Consistent with past years' data, the corresponding figure for SMEs appears larger than LEs, which is attributed to the need for certain baseline investments on cybersecurity – regardless of the organisation's size – which take up a substantial part of the budget. In that sense, LEs tend to benefit from the respective economies of scale

Figure 101: IS FTEs as a share of IT FTEs for SMEs and LEs

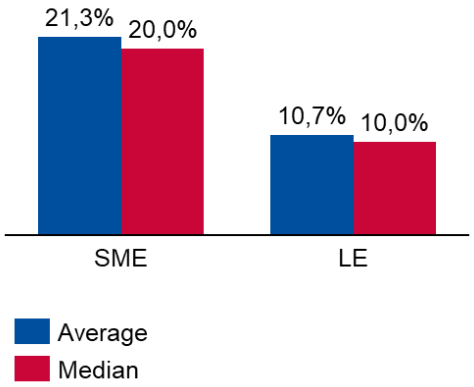
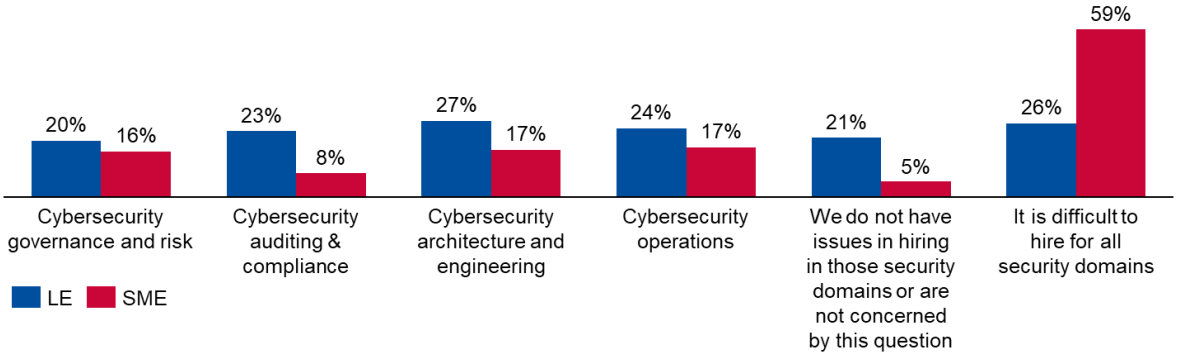


Figure 102: Hiring difficulties for SMEs and LEs



A key observation when it comes to difficulties in hiring cybersecurity staff is that SMEs continue to struggle in finding suitable experts in all domains, with the respective number significantly increasing compared to last year's data from 32% to 59%.

Figure 103: Leadership training in cybersecurity for SMEs and LEs

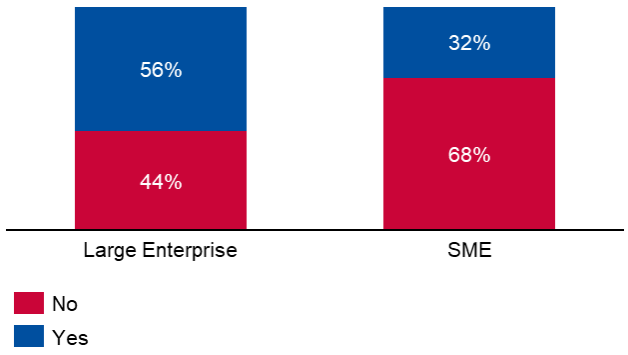


Figure 104: Leadership involvement in approval of cybersecurity measures for SMEs and LEs

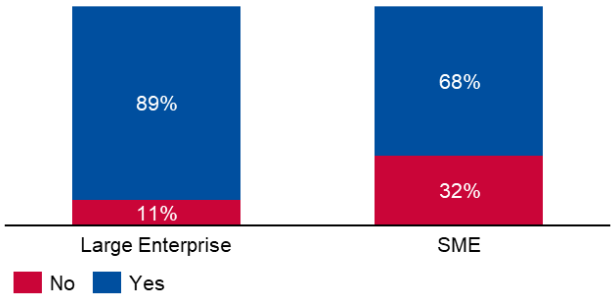
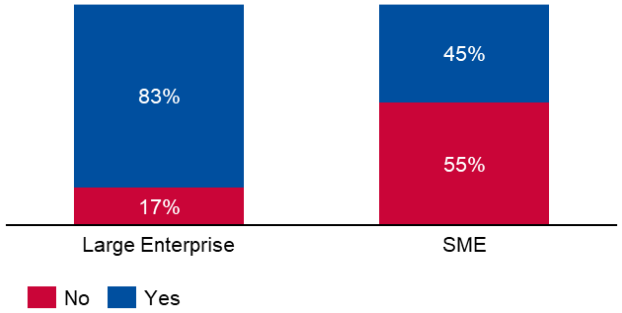


Figure 105: Cybersecurity risk management policy for third parties for SMEs and LEs



While all three metrics concerning leadership involvement and 3rd party risk management have improved for SMEs compared to last year, a substantial gap in maturity between SMEs and LEs in that regard is still noticeable.

Figure 106: NIS2 Directive awareness for SMEs and LEs

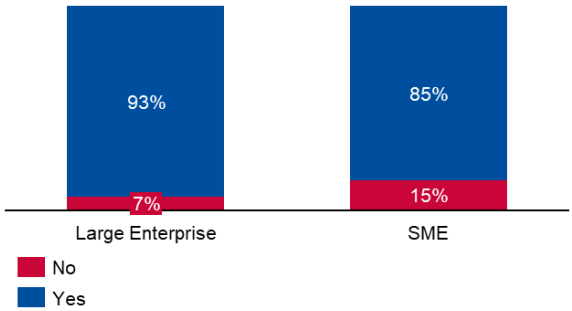
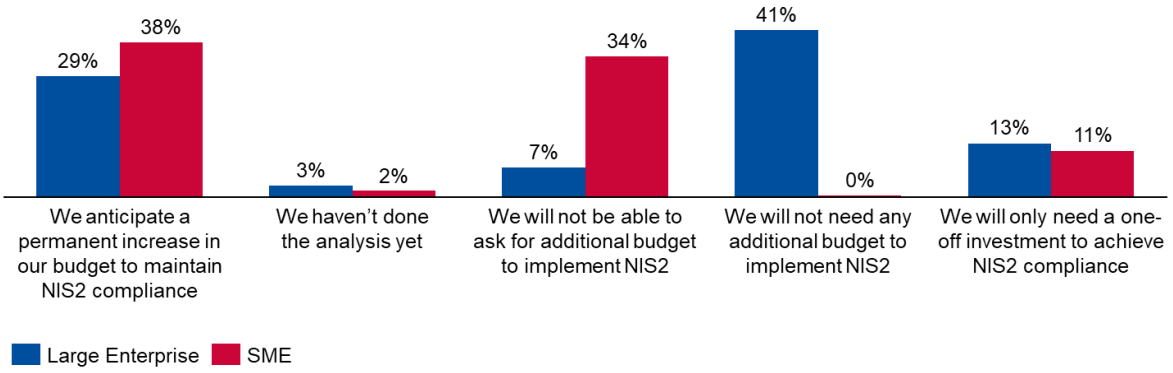


Figure 107: NIS2 Directive budget arrangements for SMEs and LEs



While all SMEs declare a need for increased investments in cybersecurity to comply with NIS 2, a significant percentage in the order of 34% will not be in a position to secure this funding.

Figure 108: Challenging NIS2 requirements for SMEs and LEs

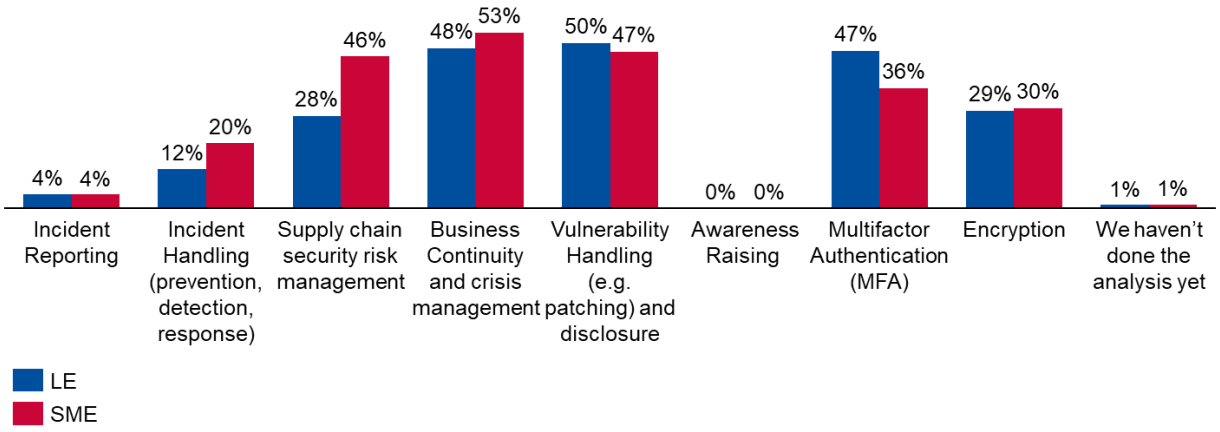


Figure 109: Perceived capability to detect and respond to attacks for SMEs and LEs

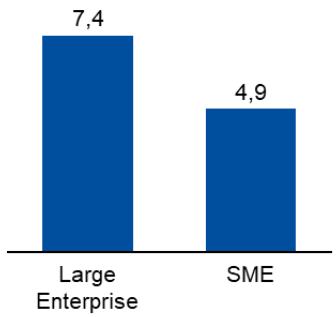


Figure 110: Perceived cyber risk management maturity for SMEs and LEs

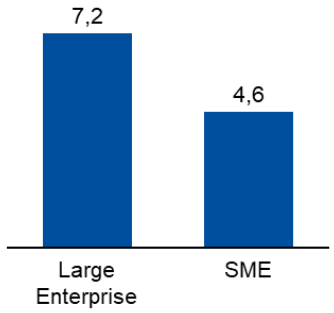


Figure 111: Perceived network and information systems cybersecurity maturity for SMEs and LEs

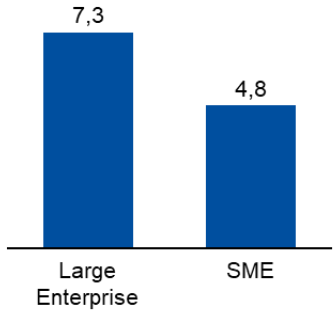


Figure 112: Information sharing for SMEs and LEs

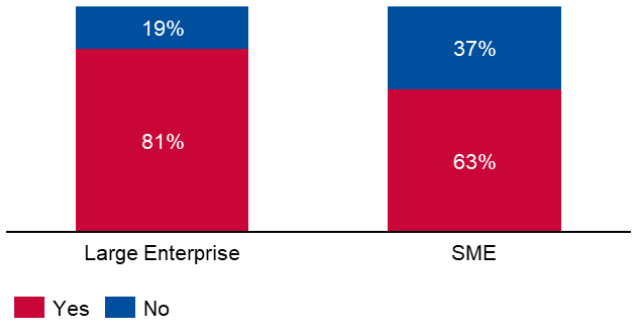
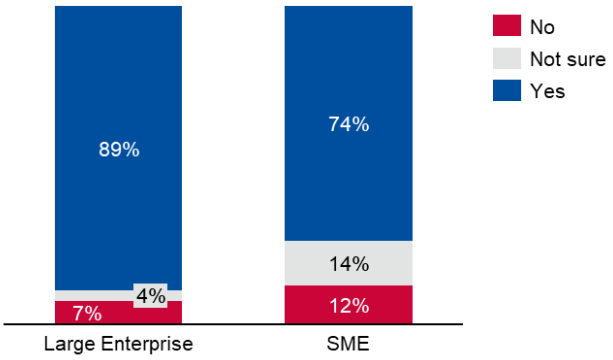


Figure 113: Interest in certifications for SMEs and LEs



10. CONCLUSIONS

This report marks the fifth iteration of ENISA's Cybersecurity Policy Assessment (CSPA) work, which aims to provide EU and national policy makers with evidence to support them in assessing the effectiveness of the existing EU cybersecurity policy framework. This year's report marks a significant change from the previous iterations in that it no longer focuses primarily on the operators in scope of the NIS Directive but rather extends its survey sample to include sectors and entities that will be in scope of NIS 2, which as of October 2024, replaced the NIS Directive. In total, 1350 entities covering all sectors of high criticality of NIS 2, as well as the manufacturing sector, were surveyed to produce this year's dataset. This coverage allows for the maintaining of historical data for sectors and entities that were in scope of the NIS Directive and remain in scope of NIS 2, but also provides a snapshot of the cybersecurity maturity status of new entities and sectors before the transposition of NIS 2. The latter is of particular value as the continuous assessment of key cybersecurity maturity and investment metrics over the next years will provide clarity on the concrete impact of NIS 2 on these sectors and entities. Moreover, recent years have been characterised by a proliferation of cybersecurity legislative initiatives that have recently entered, or will soon enter into force, including for example the CRA and sectorial initiatives such as DORA and NCCS, which directly affect a number of entities in scope of the survey. This report attempts to provide relevant data for the readiness of entities to comply with these new legislations as well.

A summary of the main findings and conclusions is presented below.

Compared to 2022, the median spending on IT for organisations increased to EUR 15 million while the median spending on information security also increased from EUR 0.7 million to EUR 1.4. **The percentage of IT investments that organisations in the EU allocate to information security was 9.0% a significant increase of 1.9 percentage points compared to 2022**. This substantial increase marks the **second year in a row with increasing investments in cybersecurity** following the pandemic and highlights the increasing attention paid by organisations to cybersecurity. Moreover, data shows that the **new NIS 2 sectors in fact fare well** in that regard with their investments in cybersecurity being comparable to those of entities that already had to comply with the NIS Directive. These investments seem to focus on developing and maintaining baseline cybersecurity capabilities, however **not as much attention seems to go to emerging areas such as post quantum computing** where only 4% of surveyed entities are investing and an additional 14% plan to invest in the near future. This may illustrate a gap that new policy initiatives in the area may seek to address.

At the same time, **the percentage of IT FTEs allocated to information security is in decline for the fourth year in a row, dropping from 11.9% to 11.1%** among organisations. While seemingly contradictory to the overall increase in cybersecurity spending, this finding can be correlated with the difficulties that organisations face when it comes to recruiting cybersecurity experts. **32% of organisations face difficulties in hiring in all cybersecurity domains**, with the more technical skillsets, i.e. in the cybersecurity architecture and engineering (25%) and cybersecurity operations (23%) domains remaining the more challenging ones for recruitment. The issue is even more striking for smaller organisations with **59% of SMEs reporting challenges in hiring in all domains**. Additionally, many cybersecurity roles are filled by employees without formal qualifications, with **76% of cybersecurity** staff in the EU **lacking certified training**. The growing demand for expertise in areas like AI and cloud security further compounds the challenge, leaving many organisations struggling to build resilient security teams capable of addressing evolving threats.

The recruitment challenges should also be viewed in light of the new compliance obligations for entities stemming from the evolving EU cybersecurity legislative framework. Notably, **89% of organisations will require more cybersecurity staff to comply with NIS 2**, primarily in the cybersecurity architecture and engineering (46%) and cybersecurity operations (40%) domains. Combined with the reported challenges in recruiting particularly in these domains, enabling easier access for entities to these skillsets should be considered to facilitate compliance with NIS 2. Similar conclusions can be drawn when looking beyond NIS 2 and into the recruitment needs of the respective entities in scope to comply with the CRA (85%), DORA (84%) and NCCS (81%).

As transition to NIS 2 is ongoing, the overall level of awareness among entities in scope is encouraging, with **92% of entities surveyed from NIS 2 sectors being aware of the directive's general scope or specific provisions**. Still, there is a noticeable percentage of entities within certain new NIS 2 sectors that are not aware of the NIS 2 Directive, most notably in the Waste water (40%), Manufacturing (38%) and Public administration (27%). This hints to a potential need for more awareness campaigns and targeted actions by National Competent Authorities. Among the various obligations for NIS 2 entities, two stand-out as most challenging, namely Business continuity and crisis management and Vulnerability handling and disclosure (both top of the list at 49%). There seems to be a direct link between this and the perceived skills gap and challenges in recruitment in the domains most associated with these requirements, namely cybersecurity architecture and engineering and cybersecurity operations. When it comes to budgetary needs for compliance, **the majority of organisations anticipate a one-off or permanent increase in their cybersecurity budgets for compliance with NIS 2**. Although new NIS 2 sectors score well in terms of cybersecurity spending, they report the most needs for permanent increase in their relevant budgets. Notably, **a substantial number of entities will not be able to ask for the required additional budget, a percentage that is especially high for SMEs (34%)**.

It is worth noting that the CRA, another key piece of the horizontal EU cybersecurity policy framework has recently been adopted and will soon enter into force. In fact, 24% of organisations in the survey sample indicated that they are developing products within the scope of the CRA. Notably, 75% of entities in the ICT service management and 62% of entities in the Digital Infrastructure sectors suggested they are developing such products. However, **only 12% of entities in the manufacturing sector reported developing products in scope of the CRA with an additional 34% claiming they had not yet done the analysis** at the time of the survey. While the surveyed entities in the Manufacturing sector include subsectors that are not in fact in scope of the CRA, these percentages appear particularly low indicating a potential lack of awareness of the CRA provisions among these organisations. In terms of compliance challenges with the CRA, organisations developing products in scope of the CRA indicated that **further guidance is needed on Vulnerability Handling Requirements (69%) and on Reporting Obligations (50%)**.

In terms of cybersecurity governance, the percentage of organisations reporting **leadership participation in dedicated cybersecurity training in line with NIS2 requirements has increased** to 51%, up from 50% last year. Regarding supply chain and third-party risk management, 75% of organisations have established policies to manage these risks, with **trust in the IT and OT supply chain primarily based on vendors' credentials and certifications** (55%) **and stringent procurement criteria** focused on information security (49%). A notable observation is that **entities in sectors already covered by NIS perform better** across various cybersecurity governance, risk and compliance metrics compared to those newly included under NIS 2. Specifically, **several entities in new sectors report non-participation rates in leadership training exceeding 70%**. Furthermore, **at least 20% of entities in these new sectors admit to trusting their supply chains implicitly** and not conducting any assessments. This observation is also reflected in self-assessments of cyber-risk management and network and information security maturity, with **sectors previously covered by NIS**

reporting higher perceived maturity in both areas (6.8 vs. 6.2 for cyber-risk management; 7 vs. 6.3 for network and information security). Similarly, **over 60% of entities in new NIS 2 sectors report non-participation in information-sharing initiatives**, which is substantially higher than in existing sectors.

Regarding projected cyberattack trends and preparedness, **90% of entities expect an increase in cyberattacks in the coming year**. Despite this, **participation in cybersecurity preparedness initiatives is predominantly internal**, with 74% of organisations engaging in such activities within their own companies. In contrast, **participation in national or EU-level preparedness initiatives is notably lower**, **highlighting a potential gap in response capabilities for cross-sectoral and large-scale incidents at the national, regional, or EU levels**. This gap underscores a critical area for improvement, as effective cross-border cooperation in managing large-scale incidents can only be achieved at these higher levels. Notably, entities in new sectors, lag behind in various cybersecurity preparedness areas, **consistently demonstrating lower engagement and higher non-participation rates in cybersecurity preparedness initiatives** compared to their counterparts in existing sectors. This observation is also reflected in self-assessments of attack detection and response capability maturity, with **sectors previously covered by NIS reporting higher perceived maturity** than those in new NIS 2 sectors (7.1 vs. 6.3).

The sectorial deep dive into the Digital infrastructure sector revealed that 55% of entities are subject to national reporting obligations but have not yet experienced a reportable incident, while 28% have reported incidents to their national authority in the past. Most sector respondents rely on technical guidelines, such as those issued by ENISA, including the Guideline to Security Measures under the EECC, to implement robust cybersecurity measures. There is **notable uncertainty regarding national restrictions on high-risk vendors**, with 27% of respondents being unsure if such restrictions exist. **Nevertheless, 46% of respondents have taken steps to mitigate risks associated with high-risk vendors**, with the most commonly reported approach being conducting risk assessments to evaluate potential risks arising from their engagement with these vendors.

The sectorial deep dive on Space revealed **all surveyed entities utilise cloud services to some extent, predominantly public cloud (61%), with minimal reliance on private or sovereign options.** Additionally, a substantial portion of entities **depend on third-party suppliers, particularly for cybersecurity and risk management needs.** While traditional security practices, such as hardware and software security, remain central to cybersecurity efforts, only a small proportion (2%) are adopting emerging technologies like Zero Trust Architecture and Post-Quantum Cryptography, highlighting a potential for broader advancements in cybersecurity within the sector.

11. ANNEX A – DEMOGRAPHICS

Figure 114: Sectorial distribution per Member State

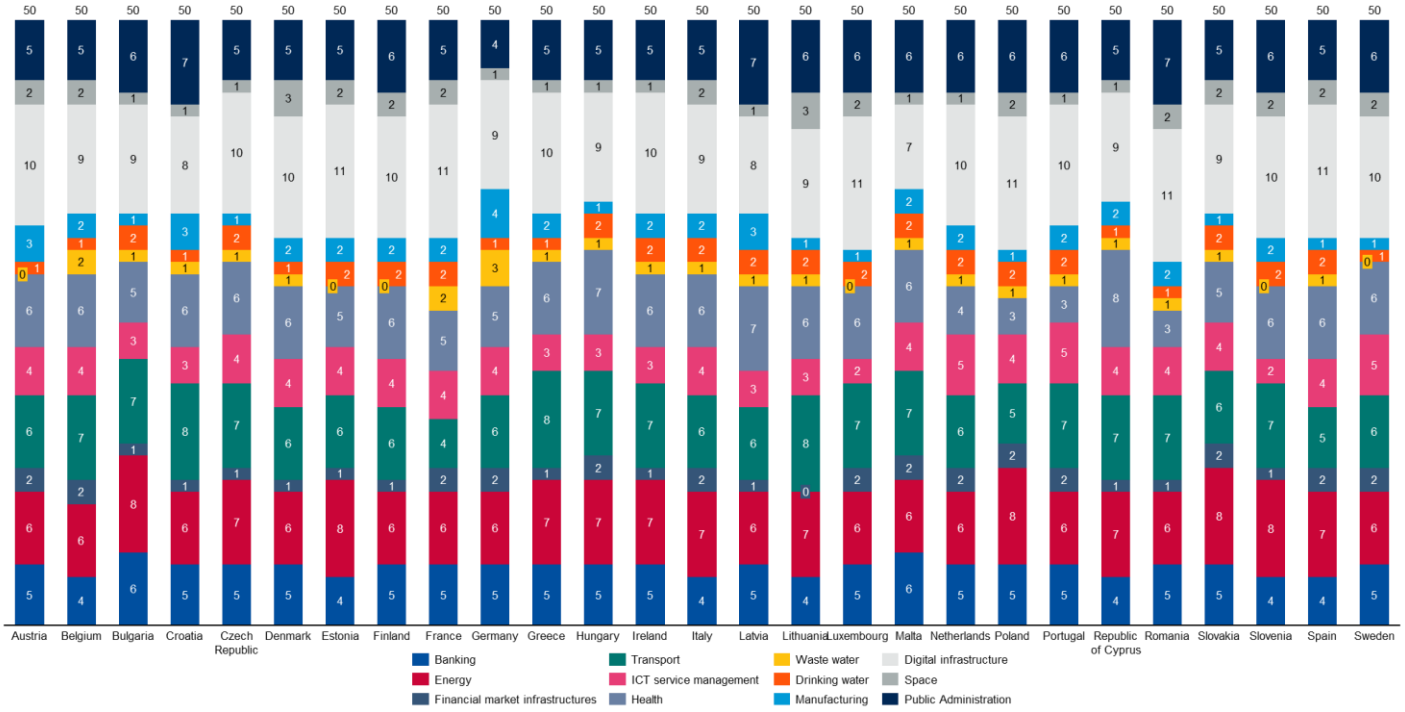


Figure 115: Revenue per sector

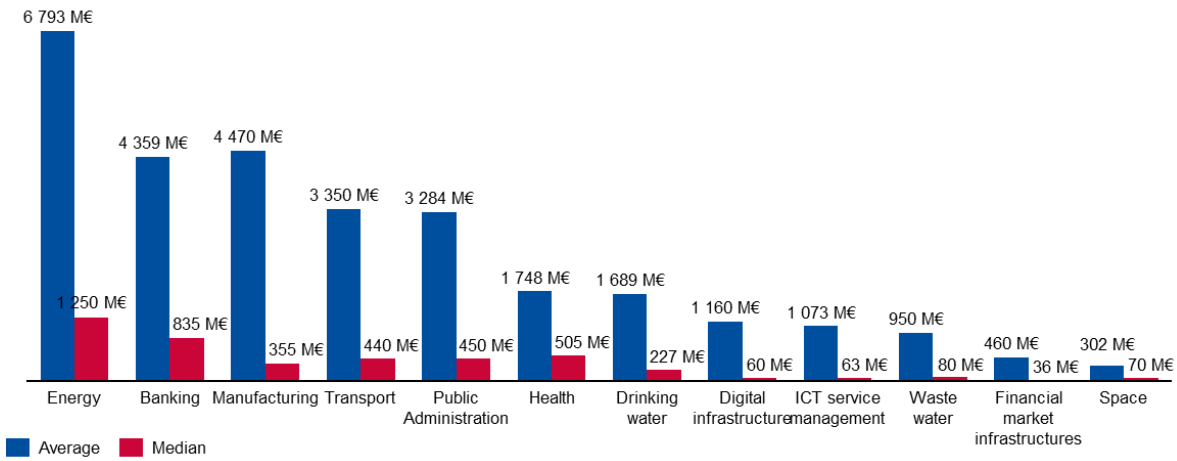
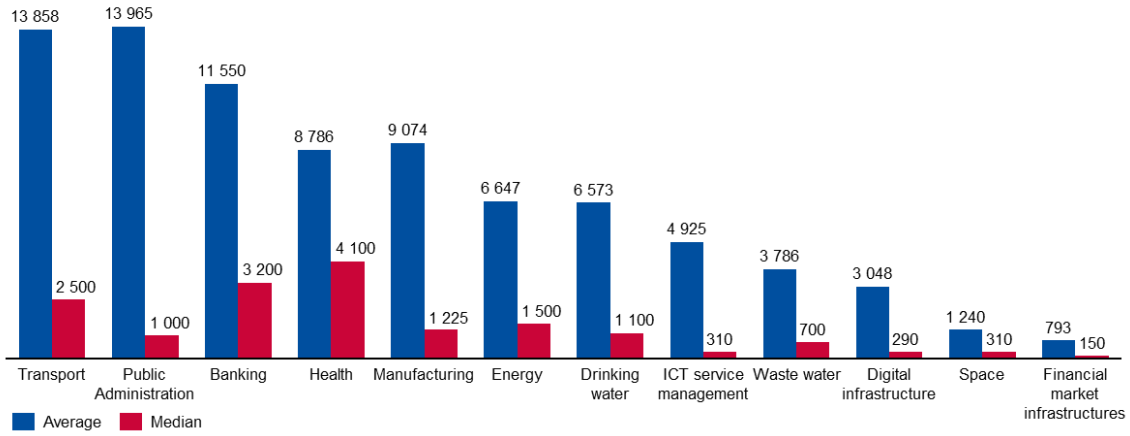


Figure 116: Employees per sector



12. ANNEX B – DEFINITIONS

12.1 MEDIAN AND AVERAGE DEFINITIONS

Median: the median is the value separating the higher half from the lower half of a data sample, a population, or a probability distribution. For a dataset, it may be thought of as **"the middle" value**. It is a robust measure of central tendency that is less sensitive to outliers (extremely large or small values) compared to the mean.

The basic feature of the median in describing data compared to the mean (often simply described as the "average") is that it is not skewed by a small proportion of extremely large or small values, and therefore provides a better representation of a "typical" value.

Median income, for example, may be a better way to suggest what a "typical" income is, because income distribution can be very skewed.

Average or Arithmetic mean: the arithmetic mean is the sum of all measurements divided by the number of observations in the dataset.

Type	Description	Example	Result
Arithmetic mean	Sum of values of a dataset divided by number of values	(1 + 2 + 2 + 3 + 4 + 7 + 9)/7	4
Median	Middle value separating the greater and lesser halves of a dataset	1, 2, 2, 3, 4, 7, 9	3

12.2 CAGR DEFINITION

The compound annual growth rate (CAGR) is the annualised average rate of revenue growth between two given years, assuming continuous compounding. It provides a consistent measure of growth over a period, even if the actual growth rate fluctuates from year to year.

To calculate the CAGR between years X and Z, where N is the number of years between the two, we use the following formula:

- CAGR, year X to year Z = [(value in year Z/value in year X) ^ (1/N)-1]
- For example, the CAGR for 2006 to 2011 is calculated as: [(value in 2011/value in 2006) ^ (1/5)-1]

12.3 SME DEFINITION[37]

The main factors determining whether an enterprise is an SME are:

- staff headcount

[37] European Commission. (2020). User guide to the SME definition. Available at: https://op.europa.eu/en/publication-detail/-/publication/756d9260-ee54-11ea-991b-01aa75ed71a1

- either turnover or balance sheet total

Organisation category	Staff headcount	Turnover	Balance sheet total
Medium-sized	< 250	≤ € 50 m	≤ € 43 m
Small	< 50	≤ € 10 m	≤ € 10 m
Micro	< 10	≤ € 2 m	≤ € 2 m

12.4 MAPPING OF ECSF PROFILES TO SECURITY DOMAINS

The table below maps the ECSF cybersecurity profiles to the security domains used in the analysis. The profiles of Cybersecurity Educator and Cybersecurity Researcher are excluded from this mapping.

Security domain	ECSF profiles
Cybersecurity governance and risk	Chief Information Security Officer (CISO) Cybersecurity Risk Manager
Cybersecurity auditing & compliance	Cybersecurity Auditor Cyber Legal, Policy and Compliance Officer
Cybersecurity operations	Cyber Incident Responder Cyber Threat Intelligence Specialist Digital Forensics Investigator Penetration Tester
IT security architecture and engineering	Cybersecurity Implementer Cybersecurity Architect

TP- TP-01-24-001-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-676-7
ISSN 2600-4712
DOI: 10.2824/5220134