EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA NIS360

Latest insights in the cybersecurity maturity and criticality of NIS sectors of high criticality

MAY 2026

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.

CONTACT

To contact the authors, please use NIS360@enisa.europa.eu.
For media enquiries about this publication, please use press@enisa.europa.eu.

AUTHORS

Jurgita Skritaite, Eleni Philippou, Ugne Komzaite-Kraujale, ENISA

ACKNOWLEDGEMENTS

We would like to thank all individuals and bodies who have contributed to this edition of the NIS360 report. In particular, Alessandro Ortalda, Azadeh Khaleghi, Steffen Grünewälder for their support with the NIS360 questionnaires and statistical analysis.

The NIS360 informal group of sectoral experts and in particular, Massimiliano Aschi, Francesco Binaschi, Douglas Hill, Gert Jan Olthof, David Jones, Oliver Schwabe and Taiyou Thomas Teramachi.

The NIS Cooperation Group members, sectoral workstreams and stakeholders who provided valuable insights and data for this report.

And of course, the European Commission DG CNECT, EBA, ESMA, EIOPA, ENTSOG, AVSEC, LANDSEC, MARSEC, EE-ISAC, EH-ISAC, FI-ISAC, TLD ISAC, Space ISAC, ISAC for Cities, Auto-ISAC EU, Rail ISAC and EU CISO Forum for Rail.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-792-4, DOI 10.2824/8928447, Catalogue nr. TP-01-26-009-EN-N

USE OF AI-ASSISTED TOOLS

AI-assisted tools were used in a limited capacity to support language refinement, terminology alignment, translation and preliminary document screening. All outputs were reviewed and validated by subject-matter experts. No AI-generated content was used without substantive human oversight.

Table of Contents

Executive Summary

This edition of the ENISA NIS360 report is **the third to assess the cybersecurity maturity and criticality of all sectors of high criticality as identified under Annex I of the NIS2 directive**. The assessment covers the entire ecosystem of a sector, where each sector is understood to comprise relevant actors (i.e., national authorities, entities, EU bodies) and applicable rules (EU legislation). The assessment relies on a structured methodology developed and continuously refined by ENISA. This methodology, takes into account the structural and gradually evolving nature of sectoral cybersecurity maturity and criticality, and builds on evidence gathered over time from: organisations operating in sectors that are within the scope of NIS2 and national authorities supervising those organisations, but also EU-level data, to reflect our latest evidence-informed understanding of where each sector stands.

Since the previous edition of this report, **cybersecurity maturity across sectors of high criticality in the EU, has been steadily improving** as organisations respond to evolving policy requirements and cyber threats they face. Banking, electricity and telecommunications remain the most mature and critical sectors, while **three sectors, trust services, aviation, and financial market infrastructures (FMIs) moved into the high maturity band**. **Four sectors strengthened their maturity within the moderate band: gas, road, maritime, and health**. Several compounding factors contribute to these improvements, including developments in cybersecurity legislation, increased political attention, but also progress across specific maturity dimensions assessed. Overall, maturity is steadily improving across critical sectors, but **progress still remains uneven both across and within sectors**. A number of factors contribute to these variations including **skill shortages, sector-specific characteristics and even organisational size**.

Sector criticality, under the ENISA NIS360, is assessed based on factors such as its level of digitalisation, the socioeconomic impact of incidents affecting it, and its time-criticality i.e. how quickly the impact of incidents affecting it can be felt on the ground considering interconnections with other sectors. As these factors typically change gradually, **criticality scores tend to remain relatively stable from year to year**. For instance, sectors such as banking, electricity, aviation, space, and digital infrastructure (including telecommunications, cloud, and data centres) remain the most critical. Nevertheless, in this NIS360 edition, limited adjustments were introduced to the criticality dimension of certain sectors to better reflect the evolving socio-economic conditions and threat landscape. In particular, the **criticality score for the space and railway sectors has been revised** to reflect changes in how society or other sectors depend on them, and the extent to which they are being targeted.

Combining and jointly interpreting the criticality and maturity dimensions helps identify mismatches between the two and helps define the risk zone. **The risk zone includes sectors with lower-than-average maturity and criticality that exceeds their maturity**. Its composition changes over time as overall maturity improves across sectors. This is one of the reasons why three sectors previously at the risk zone boundary - **rail, drinking water, and waste water are now within the risk zone.** The positive development is that **the gas sector has started moving out of the risk zone**. This shift is driven by improved information sharing, stronger collaboration, and better implementation of risk management measures that are to higher maturity.

It is expected that, as factors such as cybersecurity legislation, perceived cyber risk and threat exposure, past experience, interdependencies, and ecosystem expectations continue to act as key drivers for both cybersecurity investment and preparedness efforts, more sectors will be moving out of the risk zone.

SECTION 1

Cross-sector cybersecurity maturity overview

1. Cybersecurity maturity overview of NIS2 sectors of high criticality

1.1 Assessing progress in maturity and criticality of sectors

ENISA NIS360 is a tool designed to support EU-level informed prioritisation of sectors and national authorities in assessing the cybersecurity **maturity and criticality** of high criticality sectors[1] covered by the NIS2 directive. For this purpose, maturity is measured by how effectively and consistently the sector manages cybersecurity risks and develops capabilities over time (**overall preparedness of the sector**) whereas criticality is assessed by taking into account several elements, such as the importance of the sector to the economy and society, and how severe the consequences would be if it were attacked (**systemic relevance, exposure, and impact of disruption**)[2]. As a result, NIS360 provides both a comparative overview of sectors and a more detailed analysis per sector to help identify gaps and prioritise resources.

To assess sector maturity and criticality, ENISA uses **structured analytical models** each consisting of defined **dimensions and underlying indicators**. Unlike other maturity assessment tools that focus mainly on individual companies, **the NIS360 assesses the cybersecurity maturity of entire sector ecosystem**, including relevant actors (i.e., national authorities, entities, EU bodies) and applicable rules (EU legislation). In this regard, a sector's maturity under the NIS360 is determined by:

- Legislation and its effectiveness
- Companies and their preparedness
- Authorities and their institutional capacity
- Sectoral ecosystem structures and their effectiveness

It is important to note that each of these elements may evolve independently and such sectoral maturity evolution requires time to materialise. As a result, updating the evidence base on a regular basis ensures our assessment reflects the current state of the ecosystem. The criticality dimension, on the other hand, is assessed at the macro (socio-economic) level, taking into account the overall impact of sector disruptions on daily life (e.g. access to critical online services), as well as their effects on economic activity (e.g. halted operations, supply chain disruptions). These effects are considered both within the sector and across sectors, reflecting cross-sector interdependencies and cascading impacts. Overall, socio-economic factors are inherently more stable. Once the impact of disruptions has been assessed, the resulting scores tend to remain relatively stable, with only targeted updates required when material developments occur.

In order to identify material developments and update the NIS360 maturity and criticality assessment[3] accordingly, ENISA **collects evidence on an annual basis** from national authorities and companies through targeted surveys and the analysis of various sources, such as sectoral reports, the ENISA NIS Investment report[4], Eurostat and other EU-level sources.

The structured analytical model underpinning NIS360 allows for derived scores to be interpreted jointly, which helps identify areas where mismatches exist between criticality and maturity. These

[1] While the NIS2 Directive distinguishes between sectors and subsectors, this report generally refers to sectors for readability. The term subsector is only used when necessary to distinguish between a broader sector comprising of several subsectors and the subsectors themselves.
[2] While the NIS2 Directive already distinguishes between sectors of high criticality and other critical sectors, it does not differentiate within those categories to allow for a comparative analysis or prioritisation amongst them. The ENISA NIS360 thus takes on a more nuanced approach to assessing criticality.
[3] ENISA NIS360 2024 | ENISA (date accessed May 2026)
[4] NIS Investments 2025 | ENISA (date accessed May 2026)

areas are then used to define **the concept of a risk zone, which includes sectors with lower-than-average maturity and criticality that exceeds their maturity**. In other words, these sectors are more critical for the society and economy than they are currently prepared to manage cyber risks. The composition of the risk zone can change as overall maturity improves across sectors.

The next section provides a closer look at the assessment of maturity and criticality, explaining the factors that contributed to their evolution and progress over the last year.

1.2 Cross-sector progress overview

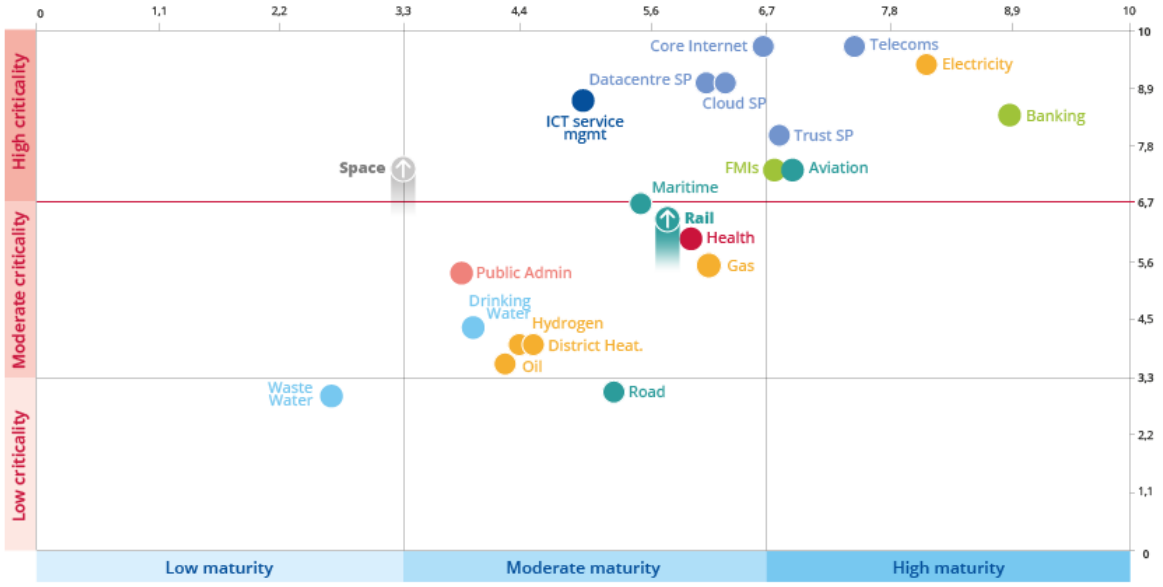
The section below provides separate analyses of maturity and criticality, showing how sectors compare with one another and the factors that have influenced their level of advancement over the past year[5]. It also includes a combined view of the two dimensions, thus helping to define a risk zone. Section Annex: NIS360 methodology**Annex:** NIS360 methodology further expands on the NIS360 methodology underpinning the assessment and the dimensions assessed to derive maturity and criticality scores.

Criticality dimension

The assessment of criticality is based on factors such as the level of digitalisation, the socioeconomic impact of incidents affecting it, and its time-criticality i.e. how quickly the impact of incidents affecting it can be felt on the ground considering interconnections with other sectors. As these factors typically change gradually, criticality scores tend to remain relatively stable from year to year. Nevertheless, limited adjustments were introduced to the criticality dimension of certain sectors to better reflect evolving socio-economic conditions and the threat landscape. In particular, the **criticality score for the space and railway sectors has been revised**. Figure 1 illustrates changes in criticality across sectors.

[5] The NIS360 study provides an EU-wide perspective on sectoral cybersecurity maturity and criticality. While we treat the EU as a collective whole for the purposes of this analysis, it is important to acknowledge that Member States have distinct regulatory and operational contexts and the sectors themselves are highly diverse. Entities within these sectors vary in size, operating models, risks they face, cybersecurity capability levels, cybersecurity resources etc. As a result, while the NIS360 assessment relies on a combination of perspectives, observations are often generalised to reflect the EU-wide landscape and may not accurately represent the status of individual entities or Member States.

Figure 1. NIS360 sectors' criticality change compared to last year



The higher a sector is positioned, the more critical it is considered. Sectors such as banking, electricity, aviation, space, ICT service management and digital infrastructures (including telecommunications, cloud, and data centres) are therefore considered the most critical. Space has joined this group this year, reflecting its growing role in society and across other sectors, which increases dependency, impact, and time criticality. The railway sector increased in criticality due to its growing role in military logistics[6], and the heightened exposure to cyber threat.

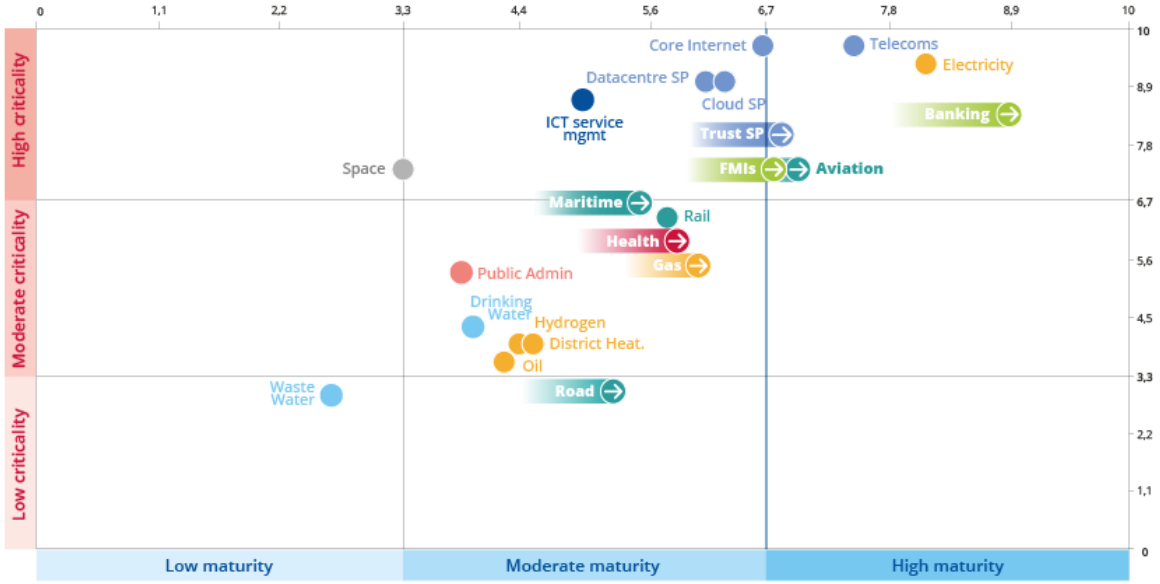
Maturity dimension

Maturity is assessed across four dimensions: firstly, policy frameworks, focusing on their effectiveness in supporting the sector and supervision under them by authorities. However, it is important to note that the effectiveness of legislation is not determined by the number of rules, but by their coherence and practical impact. Secondly, cyber risk management, covering both implementation by companies and supervisory insights on effectiveness as assessed by authorities; thirdly, information sharing and collaboration across companies, authorities, and between both; and finally, operational preparedness, based on evidence of readiness such as security assessments, incident response testing, and business continuity planning (BCP).

Since the previous edition of this report, **cybersecurity maturity across EU critical sectors seems to have been steadily improving** as organisations responded to evolving policy requirements and to the cyber threats they face. Figure 2 below shows slight progress, highlighting both the relative positioning of sectors and overall improvements in maturity.

[6] Report: Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness | European Commission (date accessed May 2026)

Figure 2. NIS360 sectors' maturity progress over a year



The further to the right a sector is positioned, the more mature it is considered. Banking, electricity, and telecommunications remain the most mature and critical sectors, as in previous years. Three sectors, trust services, aviation and financial market infrastructures (FMIs) moved into the high maturity band, while four sectors strengthened their maturity within the moderate band: gas, road, maritime, and health.

Several compounding factors contribute to these improvements including developments in cybersecurity legislation, increased political attention and progress across specific maturity dimensions assessed. Each of these factors are examined more closely below:

Developments in cybersecurity legislation

- Be it sector-specific like DORA or horizontal like the NIS2 directive, **cybersecurity legislation has certainly contributed to the progress observed across sectors**. Both banking and FMIs, for example, have improved their cybersecurity maturity, in part due to DORA reinforcing collaboration and information sharing amongst FMIs, and strengthening supervisory authorities enabling them to increase their expertise and further integrate cybersecurity into their supervisory activities.
- At the same time, findings from the 2025 ENISA NIS Investments[7] study indicate that **cybersecurity legislation has also acted as a key driver for investments in cybersecurity**, with organisations surveyed across critical sectors using it as a lever to secure resources to improve their cyber maturity and resilience, rather than adopting a 'form-over-substance' approach to it. This is supported by data showing that while 70% of organisations surveyed in the context of NIS Investments reported compliance as the main driver behind their cybersecurity investment in 2024[8], a substantial share has already realised benefits from that investment that extent well beyond compliance.
- Beyond its role in unlocking investments, **cybersecurity legislation seems to have also encouraged organisations to engage with strengthening their cybersecurity** maturity **in a more substantive way**. This is evidenced in the NIS2 areas organisations surveyed in the

[7] NIS Investments 2025 | ENISA (date accessed May 2026)
[8] According to the 2025 ENISA NIS Investments study, 70% of surveyed organisations identified regulatory compliance with frameworks such as NIS2, CRA, and DORA, as the main driver of their cybersecurity investment over the previous year.

context of the NIS Investments study identified as most challenging, namely: vulnerability and patch management, business continuity and disaster recovery, and managing supply-chain risk[9]. These areas go beyond the superficial aspects of compliance towards more substantive areas of cyber risk management, providing evidence that the NIS2 directive is successfully steering focus in the right direction.

- The findings also suggest that **organisations are increasingly viewing themselves as part of broader ecosystems, and are paying greater attention to interdependencies and supply chain risks**. According to the 2025 NIS Investments study, supply chain attacks are the second most cited concern for the future by the organisations[10] surveyed, with 90% of them reporting implementation of controls to better manage risks stemming from their supply chains[11].

Political attention and support

- **Greater political focus has also contributed to improvements in maturity recorded across certain sectors**, putting them in the spotlight, reinforcing the understanding that their cybersecurity must be improved, creating expectations around it, and increasing awareness. Examples include the European Health Action Plan that has driven the creation of guidance for making changes to cybersecurity policies, procedures and controls of sector entities. For instance, in the health sector the majority of entities surveyed in the context of the NIS360, indicated that in the past year they have made use of available guidance to inform changes to their cybersecurity policies, procedures or controls.
- Greater political attention has recently been given to sectors such as railway[12], maritime[13] and space due to their increased role in defence and military mobility, and the need to strengthen EU resilience and strategic autonomy. Over time, this is expected to further support improvements in maturity in these sectors.

Progress against specific maturity dimensions assessed

- Observed improvements in maturity have also been driven by progress across specific dimensions of maturity assessed particularly information sharing and collaboration, and operational preparedness
- In the latest NIS360 survey, many companies reported that they are more actively engaged in sectoral information sharing and analysis centres (ISACs), and we also observe an increasing number of EU ISAC members. At the same time, national authorities, confirmed the existence of mechanisms for structured collaboration among authorities. That said, information sharing and collaboration remains a challenge for sectors that are very diverse, operate across borders and across sectors or lack resources, such as ICT management services, cloud and data centres, space, public administrations, drinking and waste water.
- Another dimension where companies surveyed in the context of NIS360 last year have reported slight progress is operational preparedness particularly in terms of faster threat detection, and improved incident response and recovery capabilities, which are confirmed by the NIS Investment findings[14]. This dimension is also expected to further improve over time as

[9] Organisations surveyed in the context of the NIS Investments study identified the following three areas as the most challenging: vulnerability and patch management (50%), business continuity and disaster recovery (49%) and supply-chain risk management (37%).
[10] This concern was cited by 47% of entities surveyed and was the second most cited after ransomware which was cited by 55% of entities.
[11] These controls include: requiring suppliers to comply with security standards (63%), conducting supplier risk assessments or audits (54%) and including cybersecurity requirements in supplier contracts (48%).
[12] Guidelines on the resilience of critical entities, (2025) 6094 final, 11 September 2025
[13] EU Ports strategy, (2026) 112 final, 4 March 2026
[14] According to the 2025 ENISA NIS Investments study, 35% of surveyed organisations reported faster detection of incidents, and 26% reported improved incident response and recovery capabilities.

a result of the implementation of the Cyber Solidarity Act, which establishes a framework for strengthening EU-level cyber preparedness, detection, and response capabilities.

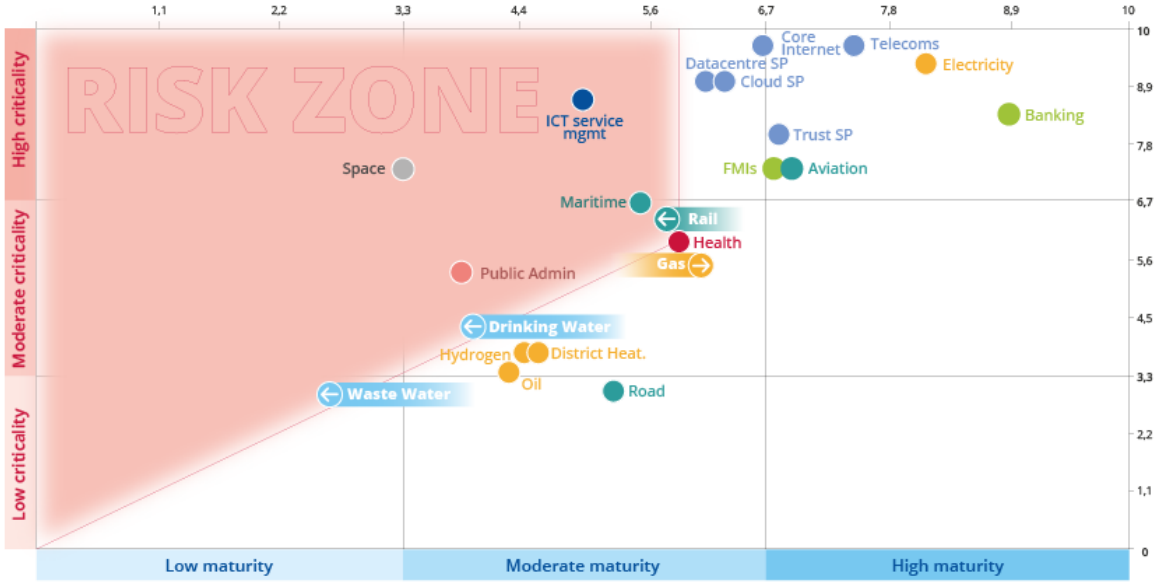
Based on their maturity and criticality level, sectors assessed in this report can be grouped into four categories:

I. **Sectors of high maturity and high criticality.** The telecommunications, electricity and banking sectors remain the backbone of our economy and society. Compared to the previous year, three new sectors joined this group: trust services, FMIs and aviation. The sectors in this group have been regulated for many years, with strong oversight from supervisory authorities which have integrated cybersecurity into their supervisory activities and enhanced their expertise in this area. All these sectors demonstrate advanced risk management, more consistent application of security measures, and a higher level of operational preparedness compared to other sectors. For instance, these sectors demonstrate not only a greater involvement of management in overseeing cyber-risk measures, but also their stronger cybersecurity expertise. Similarly, a higher percentage of companies within those sectors, are generally more proactive and focus more on preventing cyber incidents rather than reacting to them.

II. **Sectors of high criticality and upper-moderate maturity.** This category mainly includes several subsectors of the digital infrastructure sector that are digital-by-default such as core internet, data centres and cloud service providers. The increasing level of digitalisation across all sectors makes them more and more dependent on these digital-by-default subsectors. This interdependence makes these subsectors crucial for the functioning of all other sectors. There's no doubt that their criticality is high, however, their maturity still needs to be improved despite already being above the cross-sector average, and at the higher end of the moderate maturity band. Compared to the first group of sectors, these digital-by-default subsectors also demonstrate advanced risk management and strong management involvement, but less consistent application of security measures, and slightly lower level of operational preparedness. It is important to mention, that the regulation of these subsectors is complex particularly when they become subject to sectoral legislation as a result of the services they offer to other sectors. For instance, some cloud and data centre providers supporting financial entities are regulated not only under the NIS2 directive but also under DORA regulation. Such a policy environment means that requirements are not always easy to interpret, prioritise or operationalise consistently and often amplifies existing challenges companies in these sectors face An example of such a challenge is data security which companies surveyed within these sectors identified as the most challenging to implement, or testing of incident response plans where companies and authorities paint a very distinct picture with the former suggesting this happens regularly and the latter suggesting their supervisory activities do not give them that view.

III. **Risk zone sectors.** These are characterised by lower-than-average maturity but higher criticality relative to their maturity. As illustrated in Figure 3, sectors in the risk zone include health, railway, maritime, ICT management service, space, public administrations and drinking and waste water. The positive development is that the gas sector has started moving out of the risk zone.

Figure 3. NIS360 risk zone 2025



Maturity levels vary across and within the sectors in the risk zone because they are very different in terms of the size and capabilities of the organisations comprising them, their regulation and exposure to cyber risks.

- The health sector remains at the moderate cybersecurity maturity band, with some tangible progress observed across certain dimensions. This is partly driven by the stronger performance of certain entities within it (e.g. pharmaceutical manufacturers), and the increased political attention directed towards entities in greater need of support (e.g. hospitals and healthcare providers). Entities within the sector continue to face challenges – some common, stemming from the sector's increasing digitalisation (including the use of IoT and IoMT), growing dependence on third parties and suppliers, prevalence of legacy and obsolescence etc. and some less so, linked with resource constraints, lower levels of cybersecurity hygiene, lower levels of incident preparedness etc.
- The maritime and railway subsectors operate in inherently complex environments comprising several stakeholders that typically closely interact with each other e.g. infrastructure operators, transport service providers, technology providers etc. The reliance of these stakeholders on long-lived OT and IT systems as well as their dependence on supply chain and third-party providers, contribute to their overall exposure to cyber threats, while the sectors' increasing role in military logistics raises their strategic importance and potential attractiveness.
- The maturity of the ICT management service remains at a moderate level, with modest and mostly ad hoc progress over the past year due to its inconsistent application of security measures and limited improvements in operational preparedness. The sector is beginning to experience the practical implications of being in scope of the NIS2 directive. Despite that, many national authorities remain relatively new to overseeing the sector, often lacking the sector-specific and cybersecurity expertise that would enable them to do so effectively. At the same time, the wide diversity of entities operating in the sector means entities within it face distinct challenges when it comes to aligning with cybersecurity expectations. For some, these challenges arise in foundational areas such as patch management, network segmentation or data security. For others, particularly those operating across borders, challenges are compounded by complexities arising from coordinating response and recovery processes across different legal frameworks, jurisdictions etc. The sector's moderate maturity, is a concern for the sector itself but it is also a concern for other sectors relying on MSPs and MSSPs and their products/services.

- The public administrations sector is still at an early stage of cybersecurity maturity, as it is a newly regulated sector. Its maturity is at low-moderate level with reactive and uneven risk management and limited collaboration across entities. The sector is characterised by central, regional and local administrations and municipalities of varying sizes, which face different resource and expertise constraints, and therefore result in variations of maturity levels. The sector is also new for supervisory authorities, which are becoming acquainted with its specificities and might be slow in providing sector-specific support.
- The space sector remains at the lower end of the moderate cybersecurity maturity level demonstrating large variations in terms of cybersecurity practices. In part, this may be traced back to the different levels of obligations, oversight, guidance and prioritisation experienced across it, with some entities falling within the scope of the NIS2 directive while others do not, and some entities having chosen to adopt applicable cybersecurity standards, while others have not. The implications of the sector's low-moderate cybersecurity maturity are significant, particularly given its growing role in supporting Europe's strategic autonomy, the increasing complexity of the space ecosystem, and the ongoing transition to cloud infrastructures and software-defined nodes.
- The drinking and waste water sectors remain amongst the least mature sectors assessed, with drinking water scoring slightly higher than waste water in terms of cybersecurity maturity (low-moderate vs. low) partly owing to the former's earlier inclusion in scope of cybersecurity legislation. Despite their comparative differences, both sectors still have a long way to go in terms of managing cyber risks and attacks more effectively and uniformly with currently adopted approaches being largely reactive and ad-hoc. These are further hindered by heterogeneity, resource constraints, and the prevalence of legacy systems. Furthermore, both sectors engage in information sharing initiatives in a more limited way than other sectors.

IV. Other sectors. These are of low to moderate criticality and have moderate maturity. This group includes most energy subsectors, such as hydrogen, district heating, oil, and gas, and the road subsector. Oil remained stable in cybersecurity maturity, but the gas sector strengthened its maturity within the moderate band and has started moving out of the risk zone. Improved information sharing, stronger collaboration and better implementation of risk management measures drove this progress. The road subsector increased its maturity to a similar level as maritime, with progress largely driven by the automotive industry's strong practices in governance, risk management and comprehensive security assessments. As the hydrogen and district heating subsectors were not assessed due to very limited responses, their maturity scores were maintained at the same level.

Overall, despite maturity steadily improving across sectors, progress still remains uneven both across and within sectors. A number of factors contribute to these variations including, sector-specific characteristics, organisation-specific characteristics, but also skill shortages. For instance, while organisations across almost all sectors face similar challenges in aligning with the requirements of the NIS2 directive, the underlying causes of those challenges differ between sectors. Some sectors (e.g. electricity, oil, gas, maritime, railway, drinking, and waste water) point towards the prevalence of legacy systems within their infrastructures that are often unsupported yet difficult to replace, or their extensive reliance on operational technology (OT) and Industrial Control Systems (ICS) for which the patching and testing is often more challenging. Other sectors (e.g. ICT service management, space or manufacturing of pharmaceuticals) point towards complexities arising from having to operate across jurisdictions. At the same time, SMEs in sectors of high criticality consistently report greater difficulties than their larger counterparts across all dimensions of cybersecurity assessed. Finally, certain sectors (e.g. digital infrastructures, public administration) identify the lack of skilled personnel or internal expertise as the key barrier preventing them from successfully aligning with NIS2 requirements[15]. This highlights a key point: despite uniform NIS2 requirements, alignment efforts vary significantly across sectors due to the differing operational realities within each sector.

[15] These findings are also corroborated by data gathered in the context of the 2025 ENISA NIS Investments data companion – section 3.18 Main obstacles to implementing NIS2 requirements (Sectoral view).

1.3 Emerging context

Each of the sectors in scope of the ENISA NIS360 develops their cybersecurity maturity within an environment that is increasingly shaped by broader dynamics that influence both how entities and authorities operate, and the threats they face. Of these dynamics, three stand out as particularly influential:

- the rapid advancement of Artificial Intelligence (AI),
- the growing exposure to supply chain and third-party risks, and
- the intensifying geopolitical volatility

Each of these are discussed in more detail below:

The rapid advancement of AI undoubtedly presents significant opportunities for defenders and attackers alike. On the defenders' side, AI holds the promise for increased efficiency and accuracy of cyber threat detection and response, increased automation of workflows etc. On the attackers' side, AI makes advanced offensive capabilities more widely accessible while also increasing the success potential[16], scale and sophistication of attacks. With the benefits of AI thus far materialising faster for attackers than defenders, and the further proliferation and commoditisation of AI-enabled offensive capabilities being a matter of time, sectoral stakeholders are currently faced with mounting pressure when it comes to effectively adapting to the more dynamic threat environment brought forward by AI. In particular, sectoral stakeholders nowadays need to ensure they can detect and respond to cyber threats and manage vulnerabilities at significantly shorter timeframes than what has been traditionally required, ensuring they have the readiness and capacity to manage multiple concurrent waves of attacks at scale.

At the same time, **the increasing degree of interconnectedness and interdependence** of sectors across the EU nowadays, means that organisations today are faced with the growing imperative to effectively manage risks stemming beyond their narrow perimeter boundaries. Every time an organisation nowadays places its trust on a vendor or third-party provider, they are implicitly trusting everyone that vendor or provider trusted to build that component, develop that piece of code, host their data, deliver that service etc. What this implies, is that the compromise of one of those "trusted" links (be they part of more traditional or more modern supply chains[17]) can ripple through entire sector ecosystems much more easily nowadays than it used to, giving rise to a level of systemic risk that organisations have not experienced before[18]. What makes managing this risk even more challenging is that organisations nowadays need to deal with it, **in spite of existing limitations stemming from reliance on legacy infrastructure, technological obsolescence, technical debt, limitations stemming from OT, resource constraints** etc.

Finally, the way sectors across the EU approach **cybersecurity nowadays is also increasingly influenced by geopolitical volatility**. Indeed, in the interconnected environment sectors operate nowadays, geopolitical risk factors including sanctions, export controls, regional instabilities etc. have been seen to have a real impact on cybersecurity. This may take the form of increased exposure to geopolitically motivated attacks with organisations often being caught in the crossfire of nation-state conflicts. But it may also take the form of more pro-active efforts to reduce exposure to geopolitical volatility by looking into areas such as minimising concentration and dependency risks, data and digital sovereignty etc.

[16] Indeed, advancements in AI have been associated with more convincing social engineering attacks (through the use of deep-fakes, the development of more elaborated pre-texts and more polished phishing emails etc.) but also shorter time frames and greater success in terms of vulnerability discovery and exploitation.
[17] encompassing software vendors and SaaS suppliers, open-source ecosystems, cloud providers etc.
[18] An example of this comes from software supply chains. With software development nowadays often blending open-source components, third-party libraries, external integrations and increasingly AI-assisted development workflows, the compromise of a single trusted dependency has often been seen having widespread consequences that cascade not only across organisations and sectors but also across geographies.

Taken together, these three dynamics help us understand the broader context within which the sectors of high criticality across the EU assessed in the NIS360, are working to develop their cybersecurity maturity nowadays. Keeping this context in mind while reviewing the sectoral assessments in the section that follows, helps better understand not only factors influencing the risks these sectors are exposed to, but also the challenges they are faced with when it comes to building their cybersecurity maturity.

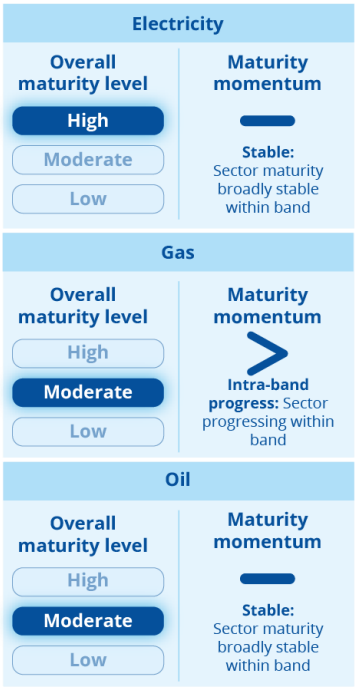
The next section provides a detailed analysis of each sector, covering the sector profile (scope and context), cybersecurity maturity insights, next steps, and offering an overview of key maturity dimensions.

SECTION 2

Sector-by-sector cybersecurity maturity overview

2. Sector-by-sector cybersecurity maturity overview

2.1 Energy[19]



The maturity of the energy sector varies across its subsectors. Electricity remains the most mature subsector, with well-established governance, and structured collaboration further strengthened through the implementation of additional sector-specific requirements under the Network code on cybersecurity. Gas follows with solid engagement and core cybersecurity structures, but continues to face constraints linked to OT environments, legacy infrastructure and implementation capacity. Oil remains comparatively less mature from a cybersecurity perspective, reflecting more limited sector-specific supervisory support, fewer dedicated mechanisms for cooperation and a more fragmented guidance landscape.

Sector profile: scope and context

The energy sector includes a broad range of entities engaged in the production, supply, transport, distribution and storage of energy across the Union. It consists of various subsectors:

- The **electricity** subsector includes entities responsible for the production, supply, transmission and distribution of electricity, as well as NEMOS, aggregators, demand response and storage providers and operators of recharging points
- The **gas** subsector includes entities engaged in the supply, transmission, distribution, and storage of gas, as well as LNG system operators, entities engaged in natural gas refinement and treatment.
- The **oil** subsector includes entities engaged in the production, refinement, treatment, storage and transmission of oil, as well as operators of oil transmission pipelines and central stockholding entities
- The sector also includes operators of **district heating or cooling** and entities engaged in the production, storage and transmission of **hydrogen**

Today, the cybersecurity of the energy sector is addressed at Union level via the NIS2 directive which mandates that sector entities within its subsectors align with the baseline cybersecurity requirements it sets out. For specific entities in the electricity subsector this is complemented by the Network Code on sector-specific rules for cybersecurity aspects of cross-border electricity flows[20] (NCCS) covering aspects such as cyber risk assessments, supply chain security, information security etc. Beyond this, energy sector entities may also have to align with the specific requirements stemming from other legislation such as the CRA etc.

The EU energy sector is **highly diverse** consisting of a wide range of entities across its subsectors. These entities often operate under very distinct operating models across MS and

[19] To avoid bias from a very small number of responses, hydrogen and district heating and cooling were not assessed separately this year, and their maturity scores were maintained at last year's level.
[20] Commission Delegated Regulation (EU) 2024/1366 of 11 March 2024 supplementing Regulation (EU) 2019/943 of the European Parliament and of the Council by establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows)

frequently depend on each other for the delivery of their services[21]. The sector is also **highly interdependent** relying on a number of other sectors to support its operations (including telecoms, transport etc.) and in turn serving as a key enabler for all other critical sectors to operate.

Against this backdrop, the energy sector is **increasingly digitalising** in an effort to more effectively integrate renewable energy sources, more reliably handle the fluctuations stemming from those, and more efficiently manage operations. Underpinning this digitalisation are: the closer integration of IT, IoT, IIoT and OT systems which enables the real-time, bi-directional flow of information among them but also increased remote-access capabilities. This foundation enables both:

- the continuous monitoring and maintenance of existing infrastructures by technicians and third-party service providers who can now remotely connect to geographically distributed assets even more easily; and

- the expansion of those infrastructures to include: renewable generation, EV charging infrastructures, Battery Energy Storage Systems (BESS) and systems to support the orchestration of distributed energy resources etc.

Taken together, all of the above paint a rather complex threat profile for the EU energy sector which is nowadays exposed to threats stemming not only from the traditional enterprise IT systems (e.g. data theft and ransomware etc.), but also, to threats affecting OT-adjacent systems (e.g. engineering workstations, Electric Vehicle Supply Equipment (EVSE), Open Charge Point Protocol (OCPP) networks etc.) and OT systems as such (e.g. exposed PLCs, RTUs etc.)[22],[23]. The sector's threat profile is only expected to become more complex looking ahead, given the increased volatility brought forward by AI-driven developments, geopolitical tensions, and deepening supply chain and third party interdependencies.

Cybersecurity maturity insights

This year's assessment shows that electricity continues to lead the energy sector in cybersecurity maturity, remaining in the high maturity band. This reflects its strong governance, well-established mechanisms for cooperation, and on-going sector-specific work linked to the NCCS Network code on cybersecurity.

Gas shows the most notable improvement compared to last year. While it remains in the moderate maturity band it has started moving out of the risk zone. The improvements are driven by stronger collaboration and information sharing, together with progress in risk management and its policy framework and guidance. Operational preparedness remained comparatively stable.

Oil remains at a moderate maturity band. Its results are less developed in policy framework and guidance, risk management and operational preparedness, while collaboration and information sharing show improvement.

The following key observations underpin this assessment:

- The energy sector has longstanding experience with regulatory supervision, which explains the existence of sectoral supervisory authorities, particularly in the electricity, gas and oil subsectors. However, supervisory experience in new sectors under the NIS2 directive such

[21] This interconnectedness comes with an increased volume of both operational and market data that need to be securely exchanged among operators across borders (e.g. nominations, allocations, balancing data). To this end, subsectors like electricity and gas have both focused on not only securing but also harmonising data exchanges, embracing distinct architectures built around Common Information Model (CIM) profile specifications for electricity, or in the case of gas standardised message formats such as Edig@s XML over AS4.

[22] Key recent developments in the sector in the EU and beyond include: the December 2025 attacks against 30 wind and photovoltaic farms in Poland, which exploited internet facing devices and weak credentials, deployed wiper malware, caused damage on RTUs, and disrupted communication between the facilities and DSOs without however affecting continuous energy production, threats relevant to widespread cybercrime e.g. attack against Endesa, or Conpet, and more recently the April 2026 U.S. joint advisory on Iranian-affiliated exploitation of internet-facing PLCs, and continued reporting on OT-focused threat activity

[23] Industry Attacks Surge, Mobile Malware Spreads: The ThreatLabz 2025 Mobile, IoT & OT Report | Zscaler (date accessed May 2026)

as hydrogen and district heating and cooling is limited, as reported by authorities. Governance structures are well established across companies, with defined roles and responsibilities, management involvement in cyber risk decision making, and approving policies covering key cybersecurity objectives. Amongst all the energy subsectors, electricity demonstrates a comparatively stronger position as regards management awareness, understanding of, and preparedness to manage cyber risks, with most surveyed entities within it reporting formal cybersecurity qualifications at management level, alongside the provision of regular cybersecurity training to management.

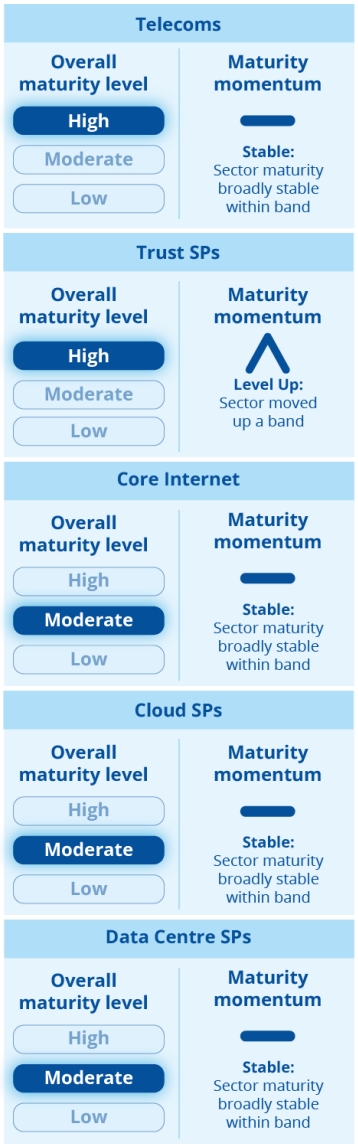
- Risk management practices are established across the sector, with most entities reporting structured approaches to identifying, and assessing risks. However, implementation of security measures to manage cyber risks varies. This variation can be traced back to several factors including but not limited to the prevalence of legacy, the inherent complexity of OT environments, and the extensive reliance of sector entities on third party providers and external suppliers. As a result of these factors, even where security patches are available, their deployment may not always be timely or feasible, visibility into OT environments is oftentimes limited, and the exposure of entities to risks outside their direct control increases.
- Across the sector, some entities are still working towards more consistent prioritisation and follow-up of cyber risks, especially where operational, safety or resource constraints make cyber risk management controls implementation more difficult. For instance, entities surveyed in the gas subsector reported facing challenges in asset management due to lack of skills and existence of legacy systems, while those in the oil subsector reported challenges in access management and conducting risk assessments for OT systems due to budget constraints and the wide prevalence of legacy systems.
- Capacity constraints and reliance on external providers remain structural factors across the sector. Shortages of specialised cybersecurity skills, combined with the complexity of OT environments, lead many entities to depend on third parties for operations, maintenance and incident response. In addition, there are variations across subsectors in how frequently cybersecurity assessments are conducted and the testing of incident readiness is carried out. This can affect how effectively risks are managed, particularly in relation to supplier access. These differences are also confirmed by national authorities, which note variations in the testing of incident readiness and the effectiveness of cybersecurity measures, with electricity performing more strongly and gas following closely. Overall, the stronger performance of the electricity and gas subsectors compared to oil may partly be explained by the fact that electricity and gas are more commonly combined within commercial utility groups, whereas oil companies have historically operated more independently.

Next steps

The sector could benefit from more support towards:

- **Improving consistency and follow-up of security assessments**. Strengthening how results are translated into actions, including clearer tracking of remediation, management follow-up, and the use of compensating controls where remediation is constrained.
- **Strengthening cybersecurity implementation in OT environments**. Prioritising OT asset visibility, governance of remote and supplier access, and monitoring in OT-adjacent environments, while ensuring that cybersecurity measures are compatible with safety and operational requirements.
- **Increasing the frequency of testing.** Entities could benefit from more regular incident response, recovery, and business continuity testing using OT-appropriate, non-disruptive approaches where needed, to better understand whether measures in place are working in practice.

2.2 Digital infrastructure



The digital infrastructure sector is central to the functioning of most essential services. It comprises telecommunications, core internet services, cloud services[24], data centres and trust services, which together provide the connectivity, data processing and trusted digital services needed across different sectors and borders. Telecommunications remain particularly important, as they provide the connectivity on which many other services depend.

The sector continues to perform relatively well in cybersecurity maturity, although there are differences between subsectors. Telecommunications and trust services remain the most mature, while core internet and cloud as well as and data centres are at an upper-moderate level. Most of the subsectors have well established information sharing communities, as well as generally well-developed governance structures and preventive practices.

At the same time, the sector still faces challenges. These include translating a complex regulatory landscape into clear actions, strengthening the effective prioritisation and follow-through of identified risks, and ensuring timely remediation of security gaps in areas such as vulnerability management, network segmentation and data security.

Sector profile: scope and context

The digital infrastructure sector brings together a set of services that underpin connectivity and enable the delivery of digital services across the EU. It covers telecommunications, core internet services, cloud computing, data centres and trust services. Together, these subsectors enable organisations to operate, exchange data and provide digital services across sectors and borders.

Under the NIS2 directive, the sector primarily covers providers of public electronic communications networks and publicly available electronic communications services, DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, trust service providers and electronic communications-related actors. These services form the technical foundation on which many essential and important entities depend.

The subsectors play different but closely connected roles. Telecommunications provide the connectivity layer, while core internet services support the basic functioning of the internet, including DNS, TLD registries, IXPs and content delivery networks. Cloud and data centre services provide the infrastructure and computing capacity needed to store, process and manage data at scale. Trust services support secure digital interactions through services such as electronic signatures, seals, timestamps, registered delivery and digital certificates.

The sector is characterised by strong interdependencies between its subsectors, as well as reliance on third-party providers and complex supply chains. In some areas, legacy technologies continue to be used alongside newer systems. These factors can make it more difficult to apply security measures consistently and can increase the potential impact of disruptions. Cybersecurity requirements for the sector are primarily set out in the NIS2 directive, which brings into its scope the main types of entities

[24] The term is used to collectively refer to the following categories of entities per NIS2 directive, Annex I: Internet Exchange Point (IXP) providers, Domain Name System (DNS) service providers excluding operators of root name servers, top-level domain (TLD) name registries, and content delivery network (CDN) providers.

across telecoms, core internet, cloud, data centres and trust services. This is complemented by the Commission Implementing Regulation (EU) 2024/2690 and supporting technical guidance from ENISA, that aim to clarify how requirements should be applied in practice. Additional frameworks also apply in specific areas, including the European electronic communications code for telecommunications and the eIDAS Regulation for trust services. Depending on the services provided, some cloud and data centre providers may also be subject to further requirements, such as DORA, as well as other rules linked to specific technologies and services.

Recent incidents show how disruptions in this sector can affect both the sector itself and the many services that rely on it. Outages at major cloud service providers have led to interruptions in downstream services, while damage to subsea fibre optic cables has affected connectivity, highlighting the sector's exposure to both cyber and physical risks. National authorities have also identified sector-specific risks, including physical threats such as accidental cable cuts, severe weather events and acts of vandalism. In June 2025, a disruption affecting Google Cloud and related internet services resulted in outages across multiple platforms and applications, illustrating how issues in large-scale cloud infrastructure can quickly impact a wide range of dependent services[25]. A comparable situation occurred in October 2025, when an outage involving Amazon Web Services disrupted thousands of websites and online services before operations were restored[26]. Targeted cyber activity, such as Salt Typhoon[27] exploiting vulnerable network devices to manipulate traffic[28], and the use of stealth malware such as *BPFdoor* within telecommunications networks[29], highlights the exposure of both telecoms and core internet infrastructure to persistent and coordinated threats. Operational incidents affecting providers such as Colt Technology Services further illustrate how disruptions in network services can have immediate downstream impacts. At the same time, physical incidents continue to affect connectivity, as shown by damage to a submarine optical fibre cable reported by Latvia State Radio and Television Centre in January 2025[30], which impacted data transmission capacity and underlined the importance of subsea infrastructure for cross-border data flows.

Cybersecurity maturity insights

The digital infrastructure sector maintains a relatively high level of cybersecurity maturity overall, though differences across subsectors remain. Telecommunications and trust services continue to operate at a high level of maturity, while core internet, cloud and data centres services remain at a moderate level, with no significant change compared to previous assessments. These differences reflect variations in regulatory experience, the diversity of entities in scope and the sector's role in supporting a wide range of essential services. However, it is important to note that the digital infrastructure sector overall has a strong cybersecurity baseline.

The following key observations underpin this assessment:

- Governance and risk management practices are generally well established, particularly in telecommunications and trust services. These subsectors benefit from longer regulatory experience, including under the European electronic communications code and eIDAS, and tend to show more structured and proactive approaches to cybersecurity governance and risk management. National authorities are generally strong and have a good understanding of the sector. While for some authorities, cybersecurity supervision is a relatively new responsibility, authorities supervising the digital-by-default sectors already have experience in this domain. As a result, national authorities report that the main challenge for them is resource constraints rather than a lack of cybersecurity skills.
- Risk follow-up remains uneven. Most companies surveyed in telecoms, core internet, and trust services prioritise identified risks, define treatment plans, and monitor progress over time. In contrast, around half of cloud and data centre providers report that risks are only recorded without being systematically prioritised or treated, indicating uneven application of risk

[25] Google suffers cloud outage, disruptions for many internet services (date accessed May 2026)
[26] Amazon says AWS cloud service back to normal after global outage | Reuters (date accessed May 2026)
[27] Colt Technology Services cyberattack report 2025 (date accessed May 2026)
[28] https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2026-04-07-cybersecurity-advisory.pdf?__blob=publicationFile&v=7 (date accessed May 2026)
[29] https://www.rapid7.com/blog/post/tr-bpfdoor-telecom-networks-sleeper-cells-threat-research-report/ (date accessed May 2026)
[30] LVRTC Submarine Optical Fiber Cable Damaged (Updated 01.02. at 10.00) - LVRTC (date accessed May 2026)

mitigation practices. This may be partly explained by resource constraints, complex environments, or service dependencies that make implementation more difficult.

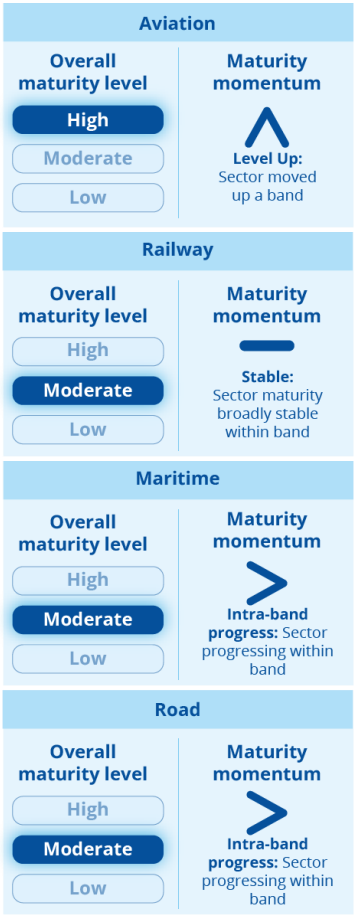
- Basic security measures are generally in place. All companies surveyed in the sector reported implementing security measures, with none indicating non-implementation, reflecting a strong cybersecurity baseline across the digital infrastructure sector. Variations relate mainly to the extent of implementation, ranging from partial to full implementation, with full implementation reported more frequently. It means that there are only a few areas where variations are more visible. For instance, network segmentation is reported as an area where implementation is more demanding for cloud and data centre service providers, which is partly linked to budget constraints. Also, partial implementation is more commonly observed in vulnerability management due to existence of legacy systems. However, data security is an area where challenges are observed across all subsectors.
- Operational preparedness remains relatively strong, supported by regular cybersecurity assessment, readiness testing and, awareness initiatives. Although overall readiness has improved, ensuring a consistent and routine exercising of response and recovery arrangements remains an area of focus, particularly for high-impact scenarios, as the sector is among the most frequently targeted by cyberattacks due to its critical role in essential services. Therefore, high standards of cybersecurity maturity are expected from this sector.

Next steps

The sector could benefit from more support towards the following.

- **To improve risk mitigation** entities should not only record risks, but also prioritise them and address them in practice through more consistent implementation of security measures. This is especially important for vulnerabilities patching, network segmentation and data security.
- **Strengthening structured cooperation where it is weaker**. Cloud and data centre services could benefit from more regular and structured cooperation formats, building on existing communities and better reflecting their dependencies with other sectors and providers.
- **Testing response and continuity arrangements more regularly**. Entities should test incident response and BCP/DR plans on a more regular basis and use the lessons learned to improve them. This would help move from having plans in place towards a better understanding as to whether they work in practice.

2.3 Transport



Cybersecurity maturity across transport subsectors varies. Aviation stands out as the most mature transport mode in cybersecurity. Compared to other transport modes, aviation shows stronger risk management, more consistent security practices, and better operational preparedness. Aviation authorities also have more developed supervisory capacity, with generally greater resources and expertise. Railway and maritime remain at a moderate level, with steady but gradual progress in areas such as information sharing and incident readiness. They continue to face some challenges linked to legacy systems, skills gaps, and limited resources. The road subsector is at a similar moderate maturity level to maritime, with progress largely driven by strong cybersecurity risk management practices in the automotive industry.

Sector profile: scope and context

The transport sector is characterised by a multi-stakeholder environment of diverse organisation sizes (infrastructure operators, transport service providers, logistics companies, technology providers, maintenance companies, and users). Although the NIS2 directive divides the transport sector into four key subsectors: aviation, railway, maritime, and road – each of them brings entities from across this broad ecosystem. Additional sectoral rules, such as the easy access rules for information security (Part-IS) and the common basic standards on aviation security (AVSEC) in aviation or UN regulations No 155 in automotive, extend the range of entities and authorities involved in this multi-stakeholder environment.

- The aviation subsector includes commercial air carriers providing passenger and cargo services, airport management organisations responsible for operating airports and their facilities and air traffic control operators ensuring the safe navigation of aircraft in controlled airspace.
- The railway subsector covers railway infrastructure managers responsible for developing and maintaining tracks, signalling systems, and associated infrastructure as well as railway operating companies that provide passenger and freight rail services. This subsector relies on companies specialised in electronic and computer systems, engineering systems and maintenance teams to manage the handling of trains and traffic management.
- The maritime subsector comprises maritime and inland water companies operating fleets for passenger and cargo services (excluding individual vessels operated by these companies), port authorities and operators managing maritime and inland ports, maritime traffic management services overseeing vessel movements and safety.
- The road subsector includes road management authorities responsible for traffic and infrastructure management, and smart transport system (ITS) operators deploying advanced digital technologies for traffic control and real-time information services. Although the automotive industry is defined as part of the manufacturing sector under the NIS2 directive, the industry tends to see itself as part of road transport. There is a close link between ITS systems and automated vehicles, which is why the automotive industry was included in this year's NIS360 assessment.

In addition to this, the transport sector is a complex sector due its dependency on a wide network of systems and technologies (i.e., IT, OT, IoT, AI driven systems) that need to operate in an integrated way. This can make it the effective implementation of cybersecurity measures challenging. For example, many OT systems are legacy systems that were not designed with cybersecurity in mind. This is further challenged by the fact that such systems often require maintenance contracts spanning many years or decades, meaning they must be retrofitted over time to comply with evolving cybersecurity standards and which often constrain the full implementation of security measures.

Furthermore, many components are integrated systems made by multiple companies that operate in different industries, which raises the need to understand supply chain risks.

- The aviation subsector relies on a wide range of OT systems, such as baggage handling, runway lighting, instrument landing systems (ILS), de-icing systems, fuel control systems, autopilot systems, aircraft tugs and boarding gates. These systems interact directly with the physical environment in real time, which creates specific security challenges. While most cyber incidents tend to affect IT systems, the strong interdependence between IT and OT means such incidents can pose indirect risks to operations. The recent cyberattack on Collins Aerospace's software[31], used for passenger check-in, boarding, and baggage tracking, showed how disruptions in IT systems can impact airport operations more broadly. In addition, emerging cyber-physical threats complicate the situation. Examples include spoofing activity affecting navigation signals and the disruptive use of drones in and around airports. Furthermore, increased reliance upon managed services providers and cloud service providers increases the risk of indirect data breaches, when these providers are targeted by malicious cyberthreat actors. Given the large number of users and customers in the aviation subsector, they are also exposed to risks, such as phishing campaigns. Fraudulent websites often mimic airline ticketing portals or booking platforms, making passengers direct targets.
- The railway subsector consists of numerous and heterogeneous subsystems including automatic train control, signalling systems, interlocking systems, radio-based control, and other OT systems. If they are compromised, they can affect passenger safety, cause a train accident or interrupt traffic, as it happened in Poland[32], when an attacker exploited a weakness in OT communication (radio layer), bringing a number of trains to a standstill for a couple of hours. Similar cyber-attacks are expected to increase as some actors[33] have expressed intent to target OT systems in the transport sector. In addition, the growing role of railway in supporting military mobility across Europe potentially makes them more attractive targets for both cyber and hybrid threats.
- The maritime subsector operations depend on OT, IIoT, IoT and IT systems that operate in a wide range of environments, from ports to open seas, and help crews navigate, manage cargo, maintain power and keep critical processes running safely. As this subsector becomes more digitalised, the tendency is to link newer digital tools with older equipment built for long service life, or to integrate OT systems with IT ones; for instance, cranes, video cameras, physical access controls and navigation systems now being connected to an organisation's network infrastructure, or to the cloud. In addition, increased reliance on satellite communications for remote monitoring and maintenance introduces new attack vectors. Unlike the road or rail transport, where the impact of cyber-attacks tends to be more localised, the potential impact of a cyber-attack in maritime could destabilise global supply chains. The NotPetya[34] attack and the ransomware data breach at Ferus Smit Shipyard[35] are just two examples that demonstrate the impact cyber-attacks may have in maritime transport. Furthermore, there is an increase in cyber-physical attacks in this sector, including spoofing of the automatic identification system (AIS)[36] used for vessel traffic monitoring.
- One of the characteristics of the road subsector is the growing number of IoT devices, such as smart traffic sensors for speed, density, weather, road pavement conditions, and the measurement of travel time. It includes also AI enabled CCTV cameras, license plate recognition cameras, connected vehicle telematic units, smart parking sensors, and similar technologies. Many of these devices have limited security as they are designed focusing on functionality and usability rather than security. For example, in the Netherlands, an ethical hacker identified vulnerabilities[37] in the network linking emergency services and traffic lights, which is intended to trigger green signals for approaching emergency vehicles. In this case, the attacker would be able to remotely control and switch traffic lights. These developments are also linked with connected and automated vehicles, as road ITS systems and vehicle systems are becoming part of the same digital ecosystem through vehicle-to-infrastructure (V2I) and cooperative intelligent transport systems (C-ITS). This interconnection also brings

[31] How a cyberattack on a software product brought EU airports to a halt - Industrial Cyber (date accessed May 2026)
[32] Poland investigates cyber-attack on rail network (date accessed May 2026)
[33] ENISA Threat Landscape 2025 | ENISA (date accessed May 2026)
[34] NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million (date accessed May 2026)
[35] maritimecybersecurity.nl/incident/XMYzQ1azd0 (date accessed May 2026)
[36] Systematic data analysis reveals false vessel tracks – SkyTruth (date accessed May 2026)
[37] Ready, steady, hack: traffic lights "can be switched remotely" - DutchNews.nl (date accessed May 2026)

the automotive industry directly into the cyber risk landscape of the road subsector, with potential impacts such as disruption to manufacturing, risks to customer data, and cascading effects across supply chains. This was recently illustrated by the ransomware attack on Jaguar Land Rover[38] forcing the shutdown of production across multiple plants and causing significant disruption to operations and suppliers across Europe.

Cybersecurity maturity insights

The data collected in 2025, shows that the aviation subsector, represented by larger companies, is leading the transport sector in cybersecurity maturity, moving from a moderate to a high maturity band. This reflects its advanced risk management, more consistent application of security measures, and higher level of operational preparedness compared to other transport subsectors. While large entities are generally mature and possess significant cybersecurity expertise and established procedures, small and medium-sized companies may have more limited levels of maturity and capability development.

The railway and maritime subsectors made slight progress in information sharing and operational preparedness, but remain at a moderate cybersecurity level and are still in the NIS360 risk zone, suggesting a need to further increase their maturity.

The road subsector has increased its maturity to a level similar to maritime; however, it is not in the NIS360 risk zone due to its lower criticality. Its maturity progress is largely driven by the automotive industry's strong practices in governance, risk management and comprehensive security assessments. The automotive sector operates under a mature cybersecurity framework, including international regulations for vehicle cybersecurity and software updates, as well as established engineering standards for secure vehicle development. These sector-specific requirements create a cybersecurity maturity profile distinct from other road and ITS stakeholders.

The following key observations underpin this assessment.

- The transport sector has been regulated for many years, with strong oversight from supervisory authorities, which have started integrating cybersecurity into their activities and strengthening their expertise in this area. Transport authorities are generally organised by mode rather than in a horizontal way, reflecting different subsector-specific regulatory regimes and characteristics. Overall, aviation authorities reported a stronger capacity to supervise and support regulated entities, despite this subsector encompassing a particularly broad range of company types. However, due to resource limitations, this progress is not uniform across all transport modes. Railway, maritime and road authorities face limited staff capacity and budget constraints, while maritime authorities face additional pressure, with more than half also reporting gaps in cybersecurity expertise.
- Key gaps identified by sector entities relate to the effectiveness of cybersecurity controls, such as access management. Access management remains a challenge in the railway, maritime, and aviation sectors due to limited skills, legacy systems and the large numbers of users and systems involved. This was also confirmed by the Aviation ISAC's CISO survey results[39], stating that identity management, authentication and access control continue to dominate the focus of CISOs in aviation. Our assessment also finds that aviation companies see room to further improve employee training, including phishing exercises and guidance on safe internet use. These observations are supported by the EATM-CERT which highlights the fact that the aviation sector has experienced credential leaks that were often linked to gaps in cyber hygiene. Other transport modes report fewer credential leaks, which may reflect differences in exposure rather than stronger cyber awareness. Beyond employees, all transport modes are also exposed to deceptive attacks targeting customers, such as phishing and fraudulent websites mimicking ticketing or booking platforms across aviation, railway, road, and maritime services.

[38] JLR hack 'is costliest cyber attack in UK history', experts say (date accessed May 2026)
[39] 2025 CISO survey results – Aviation ISAC (date accessed May 2026)

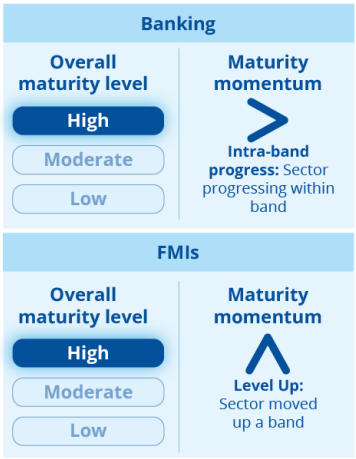
- Risk management is generally well developed across all transport modes, although gaps remain mainly due to legacy OT/IT systems. National authorities also highlight that these constraints can limit the full implementation of security measures. For instance, around two in five companies still exclude OT from cybersecurity assessments. However, greater inconsistencies across subsectors are observed in operational preparedness, largely driven by older and highly integrated multi-vendor systems that are difficult to fully map and secure, sometimes leading to gaps in OT/IT coverage and complicating coordination for patching, maintenance, and incident response. This helps explain why incident response testing remains an area for improvement, with these tests in many cases conducted rarely or only reactively in the railway, maritime, and road sectors. In aviation, security assessments are mostly conducted at regular intervals.

Next steps

The sector could benefit from more support in the following areas.

- **Strengthen supervisory capacity and sector-wide support.** The transport sector could benefit from more consistent supervision, particularly by reinforcing cybersecurity and OT expertise within national authorities. Targeted support is needed for subsectors such as maritime, where gaps are more pronounced.
- **Promote an IT/OT integrated risk management approach.** Further efforts could support the inclusion of OT systems in current risk management practises (security assessments, and testing of Security Operations Centres (SOCs) alongside the use of compensating security measures for legacy systems, where updates or retrofits may not be available options. Most subsectors would benefit from more tailored guidance and self-assessment tools that take into account the OT-related challenges and are aligned with the NIS2 directive.
- **Improve access management in multi-stakeholder environments.** Addressing the access management challenges in the complex, multi user or multi-company operational environments (such as EU ports, railway and airports) is key. Improving the management of third-party access is also important.
- **Support the uptake of existing cybersecurity requirements in transport supply chains in line with already established obligations**, such as the NIS2 directive, the Cyber Resilience act. The transport subsectors would benefit from the uptake of relevant standards and the integration of cybersecurity requirements into procurement and supplier management practices. Visibility across transport supply chains remains a challenge that needs to be addressed.
- **Encourage security testing and incident response capacity.** While there is progress in this area, further improvements could focus on more regular security assessments or testing of incident preparedness and response, though cyber exercises or stress tests, particularly in subsectors where these practices are still developing.
- **Enhance collaboration across subsectors.** The sector could benefit from strengthened mechanisms for collaboration, especially in the road subsector, involving infrastructure operators, ITS providers, municipalities, and public authorities. As vehicles become more connected and software-defined, cybersecurity extends beyond the vehicle to V2I systems and connected infrastructure. Stronger collaboration would improve resilience through better coordination, threat visibility, and consistent security across stakeholders.

2.4 Finance



The finance sector continues to demonstrate strong cybersecurity maturity, with banks retaining a high maturity level and FMIs advancing from upper-moderate to high. One of the key reasons for this positive development is compliance with DORA requirements, which has helped focus resources on strengthening the overall cybersecurity maturity of FMIs. As a result, risk management has become more structured and operational preparedness has improved. However, like any other economic sector, the finance sector is diverse in terms of company type and size, which leads to differences in maturity levels and explains why better performance is observed in the banking sector and among larger banks. Most companies in the finance sector are able to cope with DDoS attacks, however, persistent threats remain, particularly ransomware and data theft, alongside a growing number of fraud schemes, many of which rely on social engineering. A positive trend is that the sector recognises the need to continuously strengthen cybersecurity.

Sector profile: scope and context

Before the Digital operational resilience act (DORA), the NIS directive applied to the financial sector with a more limited scope, mainly covering banks and financial market infrastructures (FMI) such as central counterparties and trading venues. Since 17 January 2025, DORA has become the main cybersecurity framework for the financial sector, significantly expanding the scope vis a vis NIS2 directive. A broader range of entities, such as banks, trading venues and central counterparties but also insurance companies, investment firms, payment institutions, crowdfunding service providers, and others are regulated by DORA.

At the same time, DORA provides broader coverage of FMIs than the NIS2 directive. Under DORA, FMIs are covered through specific categories of financial entities, notably central counterparties, trading venues, central securities depositories, and trade repositories, as well as other financial institutions supporting core market functions. Given their critical role, disruptions in FMIs can have immediate and extensive negative effects on customers, such as failed payments or uncertainty over securities holdings.

The finance sector is highly digitalised, although the level of digitalisation varies depending on the type of activity. For instance, core financial services such as payments, trading, clearing, and banking operations are now almost fully digital, with many processes running in real time and relying on interconnected IT systems. This reliance increases exposure to supply chain risks. Recent incidents, such as the compromise of the LiteLLM AI library and vulnerabilities affecting CI/CD tools like Trivy[40], illustrate how attackers can exploit widely used dependencies. By targeting a single trusted component, these attacks can create broader exposure across multiple systems and sectors, including those supporting critical financial services.

At the same time, the finance sector itself is a frequent target for cyberattacks due to its high level of digitalisation, the large volumes of sensitive financial and personal data it processes, and the large number of customers using banking services, which creates opportunities for attackers to trick users into transferring money to fraudulent accounts. This is one of the reasons why most incidents are concentrated in banking, followed by payment institutions and insurance[41].

[40] Supply Chain Attack on Trivy, LiteLLM & Axios: AppSec Lessons for CISOs in 2026, (date accessed May 2026)
[41] Insurance falls outside the scope of the NIS360 assessment, although it was included in ENISA Threat Landscape 2025_v1.2.pdf (date accessed May 2026)

The main threats include DDoS attacks, ransomware, and data theft, alongside a growing number of fraud schemes, many of which rely on social engineering. Phishing, smishing, brand impersonation, and similar campaigns continue to be widely used and often reappear quickly even after being taken down, showing how easy they are to adapt and reuse. These schemes take different forms. For example, the Perseus Android banking malware has recently been observed targeting several European countries[42], including Italy, Germany, France, Poland and Portugal. It abuses Android accessibility features to gain control of infected devices, enabling attackers to steal banking credentials, monitor user activity in real time, and potentially authorise fraudulent transactions, while also extracting sensitive information such as stored passwords and recovery codes from apps. Another example of fraud schemes is an email scam abusing PayPal's 'subscriptions' billing feature to send legitimate PayPal emails containing fake purchase notifications embedded in the customer service URL field[43]. Fraudsters are also increasingly leveraging AI tools and deepfakes to expand social engineering opportunities. AI is used in phishing, vishing (voice phishing) and video calls to impersonate trusted contacts or officials. New technical schemes include relay attacks (terminal-to-terminal or card-to-terminal) and the use of fake base stations or 'SMS blasters' to facilitate large-scale smishing (SMS phishing)[44]. However, these campaigns can also rely on legitimate mobile networks where attackers send SMS messages using either spoofed sender identities or via third-party messaging services.

Cybersecurity maturity insights

The data collected in 2025 shows that the banking sector remains the most mature and critical sector while financial market infrastructures are catching up. The FMIs sector moved from a moderate to a high maturity band. One of the reasons for this is compliance with DORA requirements[45] which has partially directed efforts and resources towards strengthening the overall cybersecurity maturity of FMIs. As a result, risk management practices have become more structured and operational preparedness has improved.

The following key observations underpin this assessment:

- Overall, the finance sector is highly mature. The sector has long experience with regulation and supervision, meaning that compliance is expected, but no longer the main objective, in particular in the banking sector. Across the finance sector, cybersecurity maturity is gradually evolving beyond a primarily regulatory focus, with increasing attention to customer expectations, indicating a more forward-looking cybersecurity culture. The sector reports putting greater focus on better identification and mitigation of risks, improved incidence responses and better recovery capabilities. This is particularly important in this sector due to its high dependency on continuous operations and the potential systemic impact of disruptions on financial ecosystem, customer trust, and the functioning of other economic sectors.
- Improvements in this sector are driven by a combination of factors rather than a single reason or area. We have observed progress in all maturity dimensions. On the one hand, national authorities invested in cybersecurity skills and have strengthened their supervisory capabilities. On the other hand, companies also focused on enhancing the effectiveness of security controls. In addition, compared to last year, banks have improved information sharing. Effective information sharing and collaboration are crucial in the financial sector for addressing cross-border cybercrime, such as fraudulent transfers facilitated by a large number of mule accounts across Europe.
- The finance sector, like any other economic sector, is also diverse in terms of type and size of company, and level of digitalisation, which results in variations in maturity levels. This is illustrated by differences within the financial sector, including between banks and FMIs, and between larger and smaller companies, where better performance is observed in the banking sector and among larger banks. For instance, management involvement is greater in the larger banks, where senior management is actively engaged in cybersecurity

[42] New Perseus Android Banking Malware Monitors Notes Apps to Extract Sensitive Data (date accessed May 2026)
[43] Beware: PayPal subscriptions abused to send fake purchase emails (date accessed May 2026)
[44] Greece Arrests Chinese SMS Blaster Scammers | Commsrisk (date accessed May 2026)
[45] NIS Investments 2025 - Main report.pdf (date accessed May 2026)

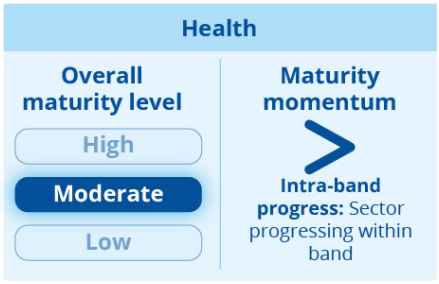
governance by setting clear cybersecurity priorities, allocating resources in line with risks, and promoting a culture of accountability across the company. In these companies, cybersecurity represents a company-wide risk. On the other hand, in FMIs it is an area requiring further improvement. FMIs can strengthen their governance arrangements by building leadership-level cybersecurity expertise. Vulnerability management, network security and data security are other areas where banks demonstrate better performance than FMIs, which often reported budget constraints and limitations related to legacy systems.

Next steps

The sector could benefit from more support in the following areas.

- **Strengthen governance and leadership engagement in weaker segments.** FMIs and smaller institutions should further enhance management-level cybersecurity expertise and governance structures, ensuring cybersecurity is treated as a company-wide risk rather than a technical function. This includes clearer prioritisation of risks and stronger alignment between cyber strategy and business objectives.
- **Address structural and resource-related gaps in weaker-performing entities.** Targeted support is needed for FMIs and smaller institutions to improve key technical areas such as vulnerability management, and data security, particularly where legacy systems and budget constraints remain a limiting factor.
- **Further enhance cross-border information sharing and operational resilience.** Building on progress already achieved, continued efforts should focus on strengthening information sharing and collaboration across the sector, particularly to better address cross-border and cross-sector cybercrime.

2.5 Health



The sector remains in the moderate cybersecurity maturity band, with some tangible progress observed across certain dimensions. This is partly driven by the stronger performance of certain entities within the sector (e.g. pharmaceutical manufacturers), and the increased political attention directed towards entities in greater need of support (e.g. hospitals and healthcare providers). Entities within the sector continue to face challenges – some common, stemming from the sector's increasing digitalisation, growing dependence on third parties and suppliers, prevalence of legacy systems etc. and some less so, linked with resource constraints, lower levels of cybersecurity hygiene, lower levels of incident preparedness etc. These challenges contribute towards a threat level for the sector that is unlikely to decrease any time soon and highlight the need to keep a sustained focus on the sector to ensure it can more uniformly continue to develop its maturity.

Sector profile: scope and context

The health sector includes a wide range of entities supporting the delivery of healthcare services across the EU, from hospitals and healthcare sites, to pharmaceutical manufacturers.

Today, the cybersecurity of the health sector is addressed at Union level via the NIS2 directive that brings into its scope:

- hospitals and other entities delivering healthcare services within Member States[46],
- pharmaceutical manufacturers,
- research and development entities focused on medicinal products,
- manufacturers of medical devices that are critical during public health emergencies,
- EU reference laboratories.

Beyond NIS2, several other regulatory instruments apply to sector entities addressing cybersecurity considerations in more specific areas. These include the Medical devices regulation, the European health data space, AI act, etc.

The health sector is characterised by its heterogeneity, consisted of entities of different sizes and capabilities ranging from national or regional healthcare service providers to pharmaceutical giants. These entities, although typically operating quite independently from one another, are often linked through the products or services they provide to one another (e.g. one medtech manufacturer could be offering their product to multiple healthcare providers across the Union, or one pathology services provider could be offering services to several hospitals within a region etc.).

The digital ecosystem upon which the sector relies to offer its critical services is also becoming increasingly more diverse with advancements such as the Internet of Medical Things (IoMT), AI in diagnostics, robotics in surgery etc. bringing about changes in how healthcare is being delivered across the EU.

These factors significantly expand the sector's attack surface, adding to the already high level of cyber risks it faces. The sector's attractiveness as a target stems predominantly from the critical nature of the services it offers, which attackers often use as a lever for pressure in their extortion attempts, but also the intrinsic value of the data it processes (patient records, pharmaceutical IP, etc.)[47]. This attractiveness, is already reflected in the volume of attacks targeting the sector annually and it is only expected to grow given the sector's increasing use of IoT and IoMT systems[48] and the impact of long-

[46] These were the sole focus of the NIS1 directive, under the health sector
[47] Zscaler ThreatLabz 2025 Mobile, IoT, & OT Threat Report (date accessed May 2026)
[48] According to Claroty's State of CPS Security: Healthcare Exposures 2025 and Zscaler ThreatLabz 2025 Mobile, IoT & OT Threat Report, as the healthcare sector embraces IoMT and IoT to drive efficiencies and automation, attackers are already

standing trends like BYOD[49] that make the sector even more accessible. At the same time, the sector faces a rising exposure as a result of its dependence on third-party and supply chain providers[50] that amplifies the potential impact of any possible attack against it[51].

Numerous incidents over the past few years have demonstrated that even if cyber-attacks against the healthcare sector do not typically have the cascading effect that attacks on other sectors do, they nevertheless have very real, felt consequences, often experienced as disruptions in service continuity and patient care, but also as the exposure of sensitive data[52].

Cybersecurity maturity insights

Analysis of the data collected in the most recent NIS360 cycle suggests the health sector's overall maturity remains at a moderate level, with some progress being observed in terms of available guidance, and a stronger political push to improve the cybersecurity of hospitals and healthcare providers building momentum. However, the health sector remains in the NIS360 risk zone. The following key observations underpin this assessment.

- The dense and maturing policy landscape within which the health sector operates, introduces a number of distinct obligations for sector entities. National authorities responsible for the supervision of health sector entities are increasingly in place, and technical guidance to support entities in the implementation of the NIS2 directive and alignment with legislation is increasingly available at EU and national levels, particularly following the introduction of the EU healthcare cybersecurity action plan, which also raises expectations for even more guidance to come.
- Despite that, the sector's expanded scope under NIS2 means national authorities often lack the sector-specific cyber expertise that would enable them to more effectively supervise it.
- The sector's heterogeneity is reflected both in the types of entities comprising it and in the variability of approaches towards cyber risk management and incident preparedness adopted by them. Amongst the various types of entities that comprise the sector, healthcare providers seem to be struggling more with aligning with best practices across the dimensions assessed, citing insufficient budgets and lack of skilled resources as compounding factors.
- Key gaps highlighted by sector entities concern implementing risk management processes, tracking assets, managing vulnerabilities (especially given the prevalence of legacy infrastructure), gaps in the coverage of threat detection and visibility but also inconsistencies in assessing the effectiveness of controls and incident readiness.
- Despite the existence of well-established structures for collaboration within the sector, including an EU-level ISAC, a dedicated NIS cooperation group workstream, and an annual cybersecurity conference organised by ENISA, the sector could still benefit from stronger peer collaboration and information sharing particularly among healthcare providers.

Next steps

The sector could benefit from more support towards the following.

adapting their approaches to targeting the sector. The Claroty report talks about the exposure of IoMT devices (e.g. those used for imaging), a number of which are running on legacy OS, to exploitable vulnerabilities that are often abused by ransomware groups. The ZScaler report suggests mobile phone-based attacks against the healthcare sector globally rose by 224% (all references accessed in May 2026).

[49] Ibid

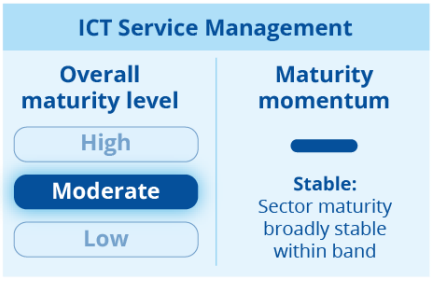
[50] Health ISAC's - 2026 Health Sector Cyber Threat Landscape suggests that although the primary threat facing the sector remains ransomware, the most concerning trend is the pivot of cyber threat actors towards supply chain compromises (data accessed in May 2026).

[51] The rationale here being: Why go after 100 hospitals separately when you can compromise the MSP, medical device manufacturer or electronic patient health record software provider that gives you access to all at the same time?

[52] Incidents against the sector in Europe and globally include an attack against two Belgian hospitals that resulted in the cancellation of surgeries and transfer of patients in January 2026 (The Register: Belgian hospitals refuse ambulances following cyberattack); the cyberattack against the Bank of Cyprus Oncology Centre that resulted in unlawful access to patient data on December 2025 (https://www.bococ.org.cy/en/news-and-blog/statement-cyber-attack-oncology-centre); the ransomware attack on pathology services provider Synnovis in 2024, delays as a result of which were cited by the UK NHS among the contributing factors to a patient's death (https://www.theregister.com/2025/06/26/qilin_ransomware_nhs_death/) etc. (all references accessed in May 2026)

- **Better understanding and alignment with applicable requirements** under the numerous legislative frameworks applicable to the EU health sector;
- **More uniform management of cyber risks** including those stemming from the prevalence of legacy systems, gaps in basic cyber hygiene, the exposure of entities to one another but also to supply chains and from the development of resilience against attacks and readiness;
- **Strengthening collaboration and information sharing** among health sector entities but also between entities and their suppliers.

2.6 ICT service management



The sector remains at a moderate level of cybersecurity maturity having made modest and mostly ad-hoc progress. It is now beginning to experience the effect of being within the scope of the NIS2 directive, which brings more structure and clarity around cybersecurity expectations, yet its approaches towards meeting those expectations remain largely inconsistent. The sector' s high diversity, extensive digitalisation, and central role as a service provider to other sectors, combined with fragmented cyber risk management and operational capabilities, uneven supervisory capacity and limited collaboration among entities, underline the need for more concerted support to help the sector get on a self-sustaining path to the development of cybersecurity maturity.

Sector profile: scope and context

The ICT service management sector includes a range of entities providing "business-to-business" services either as managed service providers (MSPs) or as managed security service providers (MSSPs).

- MSPs provide services in the areas of installation, management, operation and maintenance of ICT products, networks, infrastructure and applications.
- MSSPs provide cyber risk management services typically focused on the monitoring and management of systems and functions in the context of prevention, detection, analysis, incident response etc[53].

Today, the cybersecurity of the ICT service management sector is addressed at Union level via the NIS2 directive which mandates that 'essential' and '"important"' sector entities align with the baseline cybersecurity requirements it sets out. Layered on top of this, is DORA which as of 2025 applies to a handful of sector entities identified as 'critical ICT third-party providers' [54,55], and also other sector specific legislation, such as NCCS. Beyond NIS2, sector entities may also have to align with requirements stemming from legislation such as the CRA[56] or the AI act[57].

The EU ICT service management sector is highly diverse spanning players of various sizes (from small to large), different geographic scopes (national vs. cross border operations) and different service models (providers offering multiple services across multiple sectors vs providers offering multiple services to specific sectors vs providers offering a very narrow service scope across multiple sectors).

Across this spectrum, the sector is highly digitalised, relying on modern infrastructures, platforms, tools, products and processes to deliver its services efficiently. Over the past few years, AI has become a key driver of growth for entities within this sector who are increasingly seeking ways to embed AI into their operations to streamline service delivery and boost efficiency[58].

[53] More information on the EU MSS market (both demand and supply side) can be found in the ENISA report: Managed Security Services Market Analysis | ENISA (date accessed May 2026)
[54] The providers identified as critical under DORA are subject to direct supervision by one of the three European Supervisory Authorities (ESAs) who can potentially impose fines.
[55] https://www.eba.europa.eu/publications-and-media/press-releases/european-supervisory-authorities-designate-critical-ict-third-party-providers-under-digital (date accessed May 2026)
[56] As regards for example the mandatory software-bill-of materials (SBOM) for every managed product, the reporting of actively exploited vulnerabilities in products managed or developed by an MSP or with the CE marking is mandatory for all hardware or software sold by MSPs.
[57] Imposing requirements on AI systems particularly those used in critical infrastructure, and thus potentially affecting entities offering such systems in the ICT service management space.
[58] https://cybermagazine.com/articles/opentext-ai-main-driver-of-growth-for-msps-mssps (date accessed May 2026)

The ICT service management sector offers services and products underpinning many critical functions across the EU. Most notably, the sector has an important role to play in:

- Delivering the products, infrastructures and applications supporting the day-to-day operations of various critical sector entities.
- Enabling those entities to increase their cybersecurity capabilities and readiness to deal with cyber-attacks.
- Offering access to technical expertise, products and services to SMEs that are the backbone of the EU economy[59] in support of their digitalisation and cybersecurity efforts.
- Helping entities ensure that contracts, data residency, encryption keys and similar arrangements are managed in line with applicable EU law, and providing visibility and continuous monitoring of critical digital infrastructures.

The sector's pivotal role as a third-party provider makes it an increasingly attractive target for cyber threat actors who go after the sector[60] typically aiming at one of two outcomes:

- compromising the providers themselves typically as a means to exfiltrate client databases, or gain access to client or other important information which are then leveraged in high-stakes ransomware campaigns;
- compromising the providers as a stepping stone towards compromising their clients[61] e.g. via attacks aimed at stealing credentials and gaining access to multiple client environments, or leveraging vulnerabilities in products that MSPs and MSSPs use such as RMMs, VPNs, file transfer utilities, etc. to further adversarial objectives.

Notably, even in cases where threat actors do not intend to generate downstream effects, incidents affecting MSPs and MSSPs may have tangible impacts on their clients.

Cybersecurity maturity insights

Drawing on the analysis of the data collected in the most recent NIS360 cycle, the EU ICT service management sector remains at a moderate level of cybersecurity maturity and is still in the NIS360 risk zone. This suggests that more support is needed to ensure the sector's cybersecurity maturity continues to evolve in line with its criticality.

Overall, progress observed across the sector is modest and mostly ad-hoc, with largely inconsistent improvements noted particularly in the area of operational preparedness. The following key observations underpin this assessment.

- The sector is beginning to experience the practical implications of being within the scope of the NIS2 directive. National authorities responsible for the supervision of MSPs and MSSPs are increasingly in place, and technical guidance to support entities in the implementation of the directive is available bringing greater clarity and structure around cybersecurity expectations for entities.
- Despite that, many national authorities remain relatively new to overseeing the sector, often lacking the sector-specific and cybersecurity expertise that would enable them to do so effectively.

[59] According to Eurostat SMEs made up 99.8% of the total enterprises across EU in 2022, with 99% being micro and small businesses responsible for generating 32% of its turnover (€12.2 trillion in net turnover). More here: Large businesses generated half of EU's net turnover - News articles - Eurostat- (date accessed May 2026)

[60] In recent years, several high-profile data breaches have been enabled by the exploitation of vulnerabilities in products typically used by MSPs and MSSPs and their clients such as RMMs (e.g. ConnectWise Screenconnect, SimpleHelp), VPNs and gateways (Ivanti Connect Secure, SonicWall), file transfer utilities (Cleo, Fortra's GoAnywhere MFT, and Progress MOVEit Transfer etc.).

[61] The supply-chain attack against an MSP publicised by Sophos in May 2025, is a recent example of such an attack. In this instance the threat actor gained access to the MSPs RMM tool, SimpleHelp, and then used it to gather and exfiltrate information on multiple client networks managed by the MSP, and deploy DragonForce ransomware to leverage a double extortion tactic to pressure victims into paying ransom. (The Register: DragonForce used MSP's RMM software to distribute ransomware • The Register.) (date accessed May 2026). We note, that if attacks against MSPs and MSSPs have significant cascade potential, attacks against their supply chains represent an even higher risk (as they can propagate across multiple MSPs or MSSPs or service environments increasing both the impact and the magnitude of potential compromises).

- At the same time, the wide diversity of entities operating in the sector means MSPs and MSSPs within it face distinct challenges when it comes to aligning with cybersecurity expectations. For some, these challenges arise in foundational areas such as patch management, network segmentation or data security. For others, particularly those operating across borders, challenges are compounded by complexities arising from coordinating response and recovery processes across different legal frameworks, jurisdictions, SLAs, liability arrangements etc.
- Although some progress has been noted in terms of MSPs and MSSPs assessing the effectiveness of cybersecurity controls and operationalising readiness for incident and crisis, this was often fragmented and ad-hoc.
- Significant room for improvement remains around structured collaboration[62] and information sharing in the sector among MSPs and MSSPs, among authorities tasked with supervising the sector and between the sector and other interdependent sectors.

The sector's moderate maturity, is a concern for the sector itself, as many MSPs and MSSPs rely on each other, often rely on the same third party and supply chain providers, and continue to face challenges stemming from technical debt[63]. At the same time, it is also a concern for other sectors relying on MSPs and MSSPs, as their vulnerability could affect the ability of other sectors operate effectively.

Next steps

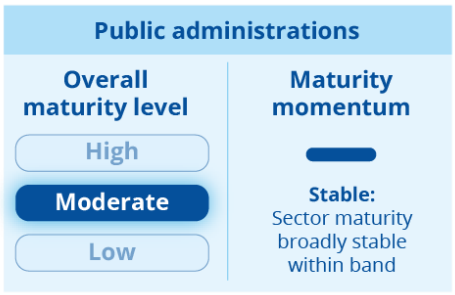
Against this backdrop, the sector could benefit from further support towards:

- **More consistent implementation of existing guidance** and a more uniform alignment with applicable requirements, including those stemming from legislation beyond NIS2, e.g. DORA;
- **Increasing the capacity of national authorities to effectively supervise the sector**, addressing challenges related to a lack of sector-relevant experience, cyber knowledge and resources;
- **Establishing more structured collaboration and information sharing** among authorities supervising the sector (particularly where those engage in cross-border supervision) and also among MSPs and MSSPs themselves.

[62] Collaboration at the EU-level for example, is mostly ad hoc and no structured mechanisms exists to consistently bring sector entities or authorities together. But an ad hoc working group has been established by ENISA in 2025, following the adoption of the amendment to the EU Cybersecurity act, for the drafting of the European certification scheme for managed security services. The new ad hoc working Group on EUMSS kicks-off – European Union Cybersecurity Certification (date accessed May 2026)

[63] The term is used to describe the outcome of choosing an "easy" short-term fix now, instead of a more sustainable one that would require more time or resources. Technical debt in MSPs and MSSPs is often the result of acquisitions which may for example result in a provider running different versions of similar tools to ensure they can continue servicing their client base, but they could also be the result of for example, relying on legacy codebases or technology, which would require a lot of effort or investment to modernise and are thus not prioritised.

2.7 Public administrations



The sector remains at a moderate level of cybersecurity maturity having made modest progress in operational preparedness. One of the challenges for the sector is the variety in its types of entities. These entities have different objectives and operational contexts, and they also vary from one Member State to another, which leads to differences in maturity levels. At the same time, the public administration sector remains the most targeted and is likely to continue to be so. This underlines the need for continued support across all maturity dimensions, from governance and risk management to information sharing.

Sector profile: scope and context

The NIS2 directive primarily applies to public administrations at the central government level. However, Member States can extend its scope to regional and local public administrations, leading to a wide variety of public entities being included. At the same time, constitutional and governance differences across Member States further contribute to this diversity. The estimated number of identified public administration entities under the NIS2 directive in Member States ranges from just over a hundred to several thousand across Member States. However, the overall number of public administrations is expected to be much higher.

In some countries, the scope remains largely limited to central bodies such as ministries, authorities and agencies, that can enforce decisions or are tasked with implementing laws, policies, and administrative functions in the public interest. Meanwhile in other jurisdictions it is broadened to include regional and local administrations, such as municipalities, and local authorities providing essential services, such as emergency, fire and rescue. This explains the significant variation in the types of public entities included within the scope across Member States. Differences are also visible in the size of authorities, as similar institutions—such as ministries—may range from around 50 staff in one country to several hundred in another. The entities surveyed in 2025 were mainly smaller organisations, which indicates that this sector may consist of a higher share of smaller administrations and municipalities that face varying constraints on their resource and expertise, resulting in differences in maturity levels. This trend will be further observed in the coming years to assess whether it can be confirmed.

The services they provide and the level of digitalisation can also vary, reflecting national administrative structures. The same digital services can be delivered at both central and local government levels and refer to public services provided through online platforms, enabling users to access, submit, and manage administrative processes electronically, such as applying for permits, certificates, ID cards, filing taxes, or accessing social security and healthcare information. Therefore, although the central government experiences a higher number of attacks (69%)[64], the attacks on local administrations (24%) have a similarly significant impact on citizens.

Overall, the public administrations sector is the most targeted sector and is likely to remain so in the short to medium term. This sector is particularly attractive to state-nexus actors due to the strategic value of the information they hold for economic and defence purposes. Although cyberespionage campaigns accounted for only a small share of incidents in 2024 (around 2.5%), their potential impact on national security remains significant[65]. In terms of volume, hacktivist activity dominates, representing nearly 63% of incidents, often aiming to attract attention and disrupt services, with targets including municipal websites and ministry portals.

In addition, data breaches are continuously increasing accounting for almost 18%. Data breaches in some cases resulted in the unauthorised exposure of personal or operationally sensitive

[64] ENISA SECTORIAL THREAT LANDSCAPE (data accessed in May 2026)
[65] Ibid

information[6667]. Cybercrime actors account for around 16% of incidents and phishing[68] remains a common initial access vector across attack types. While no specific statistics are available, elected politicians are also relevant in this context, as their accounts are frequently subject to attacks[69].

Cybersecurity maturity insights

This year's assessment shows that the public administrations sector is still at an early stage of cybersecurity maturity with its overall maturity remaining at a moderate level. The public administration sector is still part of the NIS360 risk zone, meaning that more support is needed to ensure the sector's cybersecurity maturity continues to evolve in line with its criticality.

Overall, progress observed across the sector is modest, with largely inconsistent improvements noted in the area of operational preparedness. This reflects the broader reality that public administrations across EU Member States operate at differing levels of maturity, and exposure to threats, resulting in a highly diverse public sector landscape. Such diversity creates an additional challenge, as varying capabilities, resources, and levels of readiness can complicate coordination, resilience-building, and the consistent implementation of cybersecurity rules. The following key observations underpin this assessment:

- Compared to other sectors, public administration is among those with the lowest level of management involvement and expertise. Around one third of public administrations have no structured approach to ensuring cybersecurity expertise at management level. Furthermore, when this is combined with findings on management training – where about half do not provide cybersecurity training – it highlights a concerning gap. Strong management expertise is important to ensure that risks are properly understood, prioritised, and resourced, and that cybersecurity is embedded in decision-making rather than treated as a purely technical issue, particularly as the public administration sector remains the most targeted sector.
- Access control in this sector is around the cross-sector average. However, when combined with the weaker performance of the sector in cyber hygiene, this becomes a concern. This is particularly important as phishing remains a common way for attackers to gain initial access, often leading to credential theft. At the same time, attackers are increasingly using more advanced techniques, such as spear-phishing, exploiting email servers, and targeting remote access services.
- Most public administrations are already identifying vulnerabilities in near-real time or during scheduled assessments and prioritise patching based on severity. However, patching often takes over three months, and in addition only about one third of public administrations conduct full, regular security assessments. Slow patching and limited or ad-hoc security checks are currently identified as weak points.
- The areas where we observe slight improvement are threat monitoring and detection, and to some extent, in the testing of incident readiness. Public administrations are the most active users of the Support Action, which may have contributed to progress in these areas. However, the sector still remains below the cross-sector average. The frequency of short, repeated DDoS waves affecting public administrations, along with the presence of ransomware, also highlights the need for stronger operational readiness.
- Finally, the new evidence shows that the sector faces challenges in information sharing and collaboration. The sector is relatively new, with new types of entities being identified and included within its scope. There is a high diversity of entities, including ministries, municipalities, parliaments, and public service authorities. These entities have different objectives and operational contexts, and they also vary from one Member State to another. As a result, it takes time to build effective mechanisms for cooperation and trust.

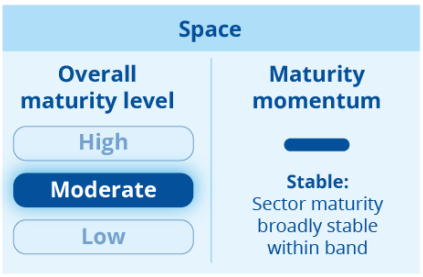
[66] French Ministry confirms data access to 1.2 Million bank accounts (date accessed May 2026)
[67] French interior ministry targeted in massive cyberattack, minister confirms | Euronews (date accessed May 2026)
[68] Dutch Police discloses security breach after phishing attack (date accessed May 2026)
[69] President of German parliament hit by Signal hack, report says – POLITICO (date accessed May 2026)

Next steps

The sector could benefit from more support in the following areas.

- **Increasing the capacity of national authorities to effectively supervise the sector**. Challenges related to a lack of sector-relevant experience, cyber knowledge and resources need to be addressed.
- **Strengthening management-level cybersecurity capability and training.** Public administrations should develop a more structured approach to ensuring cybersecurity expertise at management level, including targeted training for leadership. This is important to ensure cybersecurity risks are properly understood, prioritised, and integrated into decision-making.
- **Improving cyber hygiene practices across all employees.** Given the link between weak cyber hygiene and successful attacks, further efforts should focus on reinforcing basic security practices, including regular awareness activities and practical guidance for day-to-day behaviour, particularly around email use and credential protection.
- **Establishing more structured collaboration and information sharing** among authorities supervising the sector, but also among various types of public administrations. **Establishing more structured collaboration and information sharing**. Better collaboration and information sharing among authorities supervising the sector, and also among various types of public administrations, needs to be established.

2.8 Space



The sector remains at the lower end of the moderate cybersecurity maturity band demonstrating a large variability in terms of cybersecurity practices. This variability can partly be traced to uneven regulatory requirements and oversight of sector entities, with some falling within the scope of the NIS2 directive while others do not. These factors are compounded by the sector's increasing diversity, ongoing cloudification, the growing use of commercial-off-the-shelf (COTS) products, and a sustained shift towards software-defined components. Differences across the sector are evident in cyber risk management practices, operational capabilities and collaboration and information sharing and point to the need for more targeted support to help the sector more uniformly develop its cybersecurity maturity.

Sector profile: scope and context

The space sector consists of a range of players operating across the space value chain. The players operating on the upstream portion of the chain are typically engaged in activities aimed at building hardware and launching it into space. These players are typically involved in the manufacturing of satellites, spacecraft or other equipment necessary to support space-related activities, or in supporting launch operations (rockets, launch pads etc.). The players operating on the downstream portion of the chain are typically focused on taking the signals or data from space and turning those into end-user-oriented services or products. These players are typically involved in operating and maintaining hardware in orbit, receiving and processing data transmitted from space assets to ground stations, but also delivering products or services built around space-based data for end-users to consume.

To date, the cybersecurity of the EU space sector has only been partially addressed at Union level via the NIS2 directive[70], the scope of which only covers operators of ground-based infrastructure that support space-based services and manufacturers engaged in the production of satellites and equipment crucial for supporting space activities[71].

The EU Space Programme

At the heart of the EU space sector, lies the EU Space Programme which relies on upstream players to build and launch the hardware that makes it possible, and creates 'big data' that downstream players use to deliver value to end-users. The programme itself is built around three key pillars[72], earth observation supported by Copernicus, satellite navigation supported by Galileo and EGNOS, and secure communication supported by GOVSATCOM and the newly initiated IRIS^2.

An increasingly diverse sector

Historically, the upstream portion of the space value chain in the EU was mainly characterised by the dominance of a few large aerospace firms[73] that had the resources and capabilities it took to partake in it, with the downstream portion demonstrating somewhat more diversity. Over the past several years however the growing momentum of the 'New Space' paradigm has acted as a catalyst for increasing the diversity of the EU space sector, lowering the barriers to entry and broadening access to space-based activities to players beyond the 'traditional' ones. 'New Space' players rely predominantly on private funding, operate on a do-more-with-less and 'fail fast' mentality, make use of COTS components to make going to market faster and cheaper, and put on the market products and services at the forefront

[70] The potential adoption of the EU Space Act stands to change this.
[71] Under Annex I: Operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks. Under Annex II: Manufacture of air and spacecraft and related machinery and Manufacture of computer, electronic and optical products
[72] OBSERVER: The EU Space Programme Explained | Copernicus (date accessed May 2026)
[73] Analysis: Current structures of the European space manufacturing industry - Eurospace (date accessed May 2026)

of digital innovation (e.g. miniaturised satellites, satellite constellations, space-data driven analytics, etc.) [74].

Today, space sector activities underpin a wide range of critical societal and economic functions in the EU that are only expected to increase as new applications such as autonomous vehicles, e-road infrastructures, drone logistics, smart ports, satellite-to-cell etc. become more ubiquitous. These include:

- Positioning and navigation – with applications today ranging from navigation and positioning information on end-user smartphones and vehicle navigation systems, to those leveraging High Accuracy Services (HAS)[75] e.g. precision agriculture[76];
- Precision timing and synchronisation - required for timestamping instructions in the context of financial systems (e.g. used for trading), but also for essential synchronisation in the context of telecommunications or power grids[77];
- Earth observation – vital for emergency response e.g. wildfire or flood tracking, but also relevant during search and rescue mission planning (where in combination with positioning data can enable teams to locate and rescue people in distress)[78] and other activities supporting border and maritime surveillance, observation of atmosphere, climate change, etc.;
- Secure communications **–** relevant in times of crisis, emergencies or remote settings where terrestrial networks are unavailable, to ensure availability of secure, reliable communications for public authorities engaged in managing critical missions or infrastructure[79].

At the same time, the sector is increasingly being regarded as a cornerstone for Europe's resilience and strategic autonomy[80,81] particularly against the current backdrop of geopolitical instability. This is in recognition of the sector's crucial role in supporting the EU in achieving energy independence and diversification, reducing its dependence on imported raw materials, securing communications in times of crises, ensuring food security, etc.[82]

Against this backdrop, a number of factors help explain why the sector is becoming an increasingly attractive target for cyber threat actors.

- As the sector becomes a key pillar of EU strategic autonomy it also transforms into a strategic target which opens the sector up to more state-aligned and politically motivated attacks, hacktivism, and also attacks such as GNSS jamming.
- As it increasingly digitalises, it also becomes more susceptible to different types of attacks. The evolution from ground to cloud where many modern ground stations rely on cloud processing, or the transition from legacy hardware-centred operations towards software-defined satellites and software-defined user terminals, all come with increased cyber risk.
- As its reliance on COTS and global supply chains grows so too do the threats of compromised components cascading through the entire sector.
- As it becomes more open and more deeply integrated, avenues for compromising it leveraging inconsistent cybersecurity practices also increase (e.g. instead of targeting one of the large primes directly, attackers could foreseeably go after a 'trusted' New Space start-up that provides a specialised COTS component)[83].

[74] OECD (2023), Harnessing "New Space" for Sustainable Growth of the Space Economy, OECD Publishing, Paris, https://doi.org/10.1787/a67b1a1c-en (date accessed May 2026).
[75] https://www.gsc-europa.eu/galileo/services/galileo-high-accuracy-service-has (date accessed May 2026)
[76] EGNOS_GALILEO_Agriculture.pdf (date accessed May 2026)
[77] New Galileo Timing Service Message Operational Service Definition is out | EU Agency for the Space Programme (date accessed May 2026)
[78] OBSERVER: How the EU Space Programme supports Search and Rescue – Galileo SAR Meet 2025 | Copernicus (date accessed May 2026)
[79] https://www.copernicus.eu/en/news/news/observer-eu-space-programme-explained (date accessed May 2026)
[80] *https://www.copernicus.eu/en/news/news/observer-security-competitiveness-and-access-space-discussed-18th-european-space* (date accessed May 2026)
[81] EU Space a bedrock for building a more autonomous Europe | EU Agency for the Space Programme (date accessed May 2026)
[82] Ibid.
[83] According to ASD Eurospace data, the space manufacturing sector in Europe is at the same time very fragmented and very concentrated. The 30 largest space units in Europe make up almost 70% of total employment in the sector. The remaining

Cybersecurity maturity insights

Drawing on the analysis of the data collected in the most recent NIS360 cycle, the EU space sector remains at the lower end of the moderate cybersecurity maturity level and is still part of the NIS360 risk zone. This suggests that more support is needed to ensure that the sector's cybersecurity maturity begins to evolve in line with its criticality.

The following key observations underpin this assessment.

- The EU space sector continues to present a highly uneven picture of cybersecurity maturity, with substantial variations observed in how sector entities apply cybersecurity frameworks. This may in part be traced back to the different levels of obligations, oversight, guidance and prioritisation experienced across it, with some entities falling within the scope of the NIS2 directive while others do not, and some entities having chosen to adopt applicable cybersecurity standards, while others have not, etc.
- When it comes to cyber risk governance and the implementation of measures to manage cyber risk, these vary widely across the sector, with some entities demonstrating advanced capabilities, and others struggling in foundational areas such as defining cybersecurity roles and responsibilities, managing the cybersecurity of their assets, implementing network segmentation and managing vulnerabilities.
- At the same time, wide variability is also evident in how sector entities go about ensuring their operational readiness, with some entities demonstrating mature, proactive, regularly tested incident detection, response and recovery capabilities and others remaining mainly reactive and limited to untested plans.
- Despite the existence of a few initiatives aimed at fostering collaboration among entities (e.g. the EU Space ISAC), or national space agencies occasionally coming together for the development of standards, collaboration and information sharing within the sector in the context of cybersecurity remain limited. At the same time, collaboration with counterparts in other sectors is also limited, despite the space sector's growing importance in enabling the operations of other sectors.

The implications of the sector's low moderate cybersecurity maturity are significant, particularly given its growing role in supporting Europe's resilience and strategic autonomy, the increasing complexity of the space ecosystem, the ongoing transition to cloud infrastructures and software-defined nodes, and the increasing integration of AI into attacker tradecraft. Taken together, these factors amplify the potential impact of cyber-attacks and highlight the need for more targeted support for the sector to enable it to more uniformly develop its cybersecurity maturity.

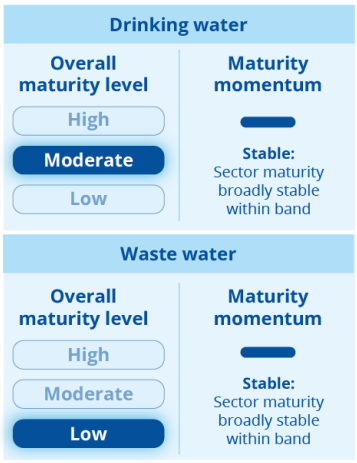
Next steps

In particular, the sector could benefit from further support as follows.

- **A more consistent approach to cybersecurity** is required both in terms of what entities in the space sector do and in terms of how they do it. Achieving this may require raising awareness, clarifying expectations for key sector players and making it easier for sector SMEs to manage cyber risks.
- **More uniformity in managing supply chain risks is needed**, including the risks stemming from the sector's increasing reliance on COTS and software-defined components.
- **Collaboration and information sharing needs strengthening**, both within the sector (among entities and among national authorities), and between the space sector and other sectors.

smaller players represent barely 30% of employment. What is interesting to note is that most smaller players work almost exclusively as subcontractors to the largest players.https://eurospace.org/the-29th-edition-of-the-annual-facts-figures-report-is-out/#:~:text=When%20a%20reply%20is%20missing,very%20fragmented%20and%20very%20concentrated (date accessed May 2026)

2.9 Drinking and Waste water



The drinking and waste water sectors remain amongst the least mature sectors assessed, with drinking water scoring slightly higher than the waste water in terms of cybersecurity maturity (low-moderate vs. low) partly owing to the former's earlier inclusion in scope of cybersecurity legislation. Despite their comparative differences, both sectors still have a long way to go in terms of managing cyber risks and attacks more effectively and uniformly with approaches as currently adopted being largely reactive and ad hoc. These are further hindered by heterogeneity, resource constraints, and the prevalence of legacy systems. Both sectors have moved into the NIS360 risk zone reflecting the need for more targeted support to ensure the evolution of their cybersecurity maturity can continue in line with their criticality.

Sector profile: scope and context

The drinking and waste water sectors include a range of entities providing essential services across the Union.

- The drinking water sector is predominantly focused on ensuring the reliable supply of safe, potable water to end users. Entities operating in this sector manage the abstraction, treatment, storage, quality monitoring and distribution of water intended for human consumption[84]. They include *water utilities*, *water treatment plants* but also *entities responsible for oversight* at national, regional or local levels.
- The waste water sector is predominantly focused on public sanitation and protecting the environment. Entities operating in this sector manage the collection of urban, domestic or industrial waste water, its appropriate treatment so that it does not harm the environment once it is returned, the treatment of sewage sludge, the management of rainwater to limit adverse effects (e.g. flash floods) or meet demands (e.g. irrigation, urban cleaning etc.) but also recovering resources from waste water (e.g. nutrients, biogas, energy etc.)[85]. They include entities engaged in the *operation of sewerage systems, waste water treatment plants* but also *entities responsible for the oversight* of the above at national, regional or local levels.

At EU-level, these sectors are both individually and jointly regulated[86]. The cybersecurity of both is currently addressed at Union level via the NIS2 directive which mandates that “essential” and “important” entities operating in these sectors align with baseline cybersecurity requirements. Despite that, the two sectors have different experiences of being regulated from a cybersecurity standpoint with drinking water having been in scope of cybersecurity legislation since the introduction of the first NIS directive, unlike waste water. That said, neither of the two sectors has

[84] Abstraction refers to the collection of water from surface or groundwater sources, whereas treatment covers elements such as membrane filtration, desalination etc. More here: https://eureau.org/wp-content/uploads/2021/07/the-value-of-water-services.pdf (date accessed May 2026).
[85] According to Eureau, modern sanitation services are becoming essential parts of the circular economy, serving as bio-factories where electricity and heat are generated, valuable nutrients and clean water are recovered from waste water and fertilisers are produced. Treated water can be reused in industrial processes, agriculture etc. More here: https://eureau.org/wp-content/uploads/2023/09/the-value-of-sanitation-services.pdf (date accessed May 2026).
[86] The Water Framework Directive or WFD (Directive 2000/60/EC) constitutes the main law for water protection in Europe. The directive sets out objectives for Member States to ensure the protection and restoration of water bodies on the basis of established River Basin Management Plans through the implementation of a programme of measures including measures required inter alia under the Drinking Water Directive (80/778/EEC) as amended by Directive (98/83/EC); the Urban Waste-water Treatment Directive (91/271/EEC); and the Sewage Sludge Directive (86/278/EEC) which are applicable to the sectors.

enjoyed the level of focus other sectors have at EU-level to this day, which does in part explain their comparatively lower maturity scores.

Beyond their essential role in protecting human health and the environment, both the drinking and the waste water sector nowadays serve as key enablers for the activities of other sectors, thereby supporting both sustainable development and economic growth. Sectors that heavily rely on water services across the EU include the following.

- In the energy sector the link is very much bidirectional. Energy production requires a lot of water particularly for the cooling of fossil fuel or nuclear power plants[87]. In turn, water-related activities such as drilling, purification, desalination, treatment and distribution require a lot of energy[88].
- In the agriculture sector water services contribute towards irrigation, livestock management, as well as the recovery of substances like phosphorus and nitrogen from wastewater to reduce the environmental damage caused by fertilizers[89].
- In the manufacturing sector[90]large quantities of water are required to produce numerous items we use nowadays, from the clothes we wear, to the devices, plastics and papers we use, to the cars we drive, etc.
- All sectors underpinning the EU's digitalisation where water is required not only for the production of the hardware itself but also for the generation of electricity needed to run it, and for the cooling needed for its efficient operation[91].

Nowadays, both the drinking water and the waste water sectors in the EU increasingly rely on complex infrastructures that integrate OT, IoT, IIoT and IT for monitoring and controlling physical processes (e.g. pumps, valves, motors, dosing controllers, aerators, etc.), the real-time collection of data from distributed assets, and support for information management, administration and predictive maintenance.

This growing reliance of both sectors on digital infrastructures, however, has not always come hand in hand with a growing focus on cybersecurity. In fact, both sectors are currently faced with challenges including a dependency on legacy systems, weak cyber hygiene, limited infrastructure visibility and external exposure, particularly of OT infrastructures. These challenges are further exacerbated by a lack of skilled cybersecurity professionals and the heterogeneity of the sectors themselves. All these factors contribute to the increasing exposure of the sectors to cyberattacks.

Over the past five years, cyber-attacks observed against both sectors were predominantly linked to hacktivism and cybercrime most attacks going after IT infrastructure, although spill-overs to OT infrastructure were also observed[92]. In terms of impact, this has ranged from the unavailability of

[87] Based on 2022 data, the greatest volumes of water abstracted in the EU go to supporting power generation cooling. In fact, it is estimated that during the period running from 2000 to 2022, 34.1% of all water abstracted within the EU was used towards the cooling of power plants. Source: Water Atlas 2025: Data and facts about the basis of life | Heinrich Böll Stiftung | Brussels office - European Union (date accessed May 2026)

[88] According to a December 2025 - EurEau briefing note 'The criticality of energy security to achieve resilient water services – the sector is not only reliant on energy but also reliant on the stable supply of it'

[89] Agriculture is the largest consumer of water globally, with 72% of the world's water consumption being used towards the production of food. Across the EU, the sector was responsible for the consumption of less than a third of all water abstracted – with numbers varying significantly amongst MS. Source: Water Atlas 2025: Data and facts about the basis of life | Heinrich Böll Stiftung | Brussels office - European Union. More on wastewater treatment can be found here: EurEau – The value of waste water services, 2022.

[90] Based on 2022 data, 14.7% of all water abstracted within the EU was used towards manufacturing – beyond that, we should consider that manufacturing also relies on primary sources such as metals like copper or lithium which also require water when they are mined. Source: Water Atlas 2025: Data and facts about the basis of life | Heinrich Böll Stiftung | Brussels office - European Union

[91] Much of today's digitalisation for example, relies on data centres that have a water footprint that is quite large. It is estimated that by 2030, 90,000,000 litres of water per annum will be needed to cool data centres in Europe. Water Atlas 2025: Data and facts about the basis of life | Heinrich Böll Stiftung | Brussels office - European Union

[92] Attacks observed against the sector (within but also beyond the EU) include: the 2021 attack that compromised Voluetech a Norwegian software provider for water utilities that spread into the networks of 200 municipal water supply companies (without impacting water supply as such); the attack against Reitzner AG another IT supplier, in 2022 that led to the disruption of water and sewerage services in multiple municipalities; the attack against US Maine wastewater whereby the company's SCADA were affected and a switch to manual processes was performed until system restoration concluded etc.

utility websites, to disruptions of billing and customer interfaces, to compromises of customer data, to interference with control operations that necessitated switching to manual processes, etc.

Cybersecurity maturity insights

Drawing on the analysis of the data collected in the most recent NIS360 cycle, the drinking water sector remains at the lower end of the moderate maturity level, whereas the waste water sector remains at a low maturity level. Both sectors have now moved into the NIS360 risk zone, highlighting that more support is needed to ensure their cybersecurity maturity begins to evolve in line with their respective criticality.

The following key observations underpin this assessment.

- The two sectors have historically experienced different levels of regulatory oversight from a cybersecurity standpoint, with drinking water having been within the scope of cybersecurity legislation since the introduction of the first NIS directive, unlike waste water. This has at least in part, contributed to the somewhat higher overall level of maturity of the drinking water sector, although both sectors have received comparatively less attention than others.
- Across both sectors, entities report struggling to effectively manage cyber risks and attacks, more so than entities in other sectors. Key challenges cited seem to be affecting sector entities to varying degrees and reflect an approach to risk assessment that is mostly reactive and ad hoc, an approach to risk management that often lacks validation, lower levels of cybersecurity awareness overall, limited ability to detect cyber-attacks against infrastructures, and mostly reactive and untested response and recovery arrangements.
- These challenges seem to be exacerbated by constrained budgets, shortages of personnel with relevant cybersecurity skills, the prevalence of legacy systems within both sectors, and also extensive reliance on third-party products and services albeit with insufficient third-party risk management arrangements in place.
- Collaboration and information sharing is limited across both sectors and noticeably lower than other sectors assessed, with entities in the waste water sector engaging in collaboration and information sharing even less than their drinking water peers. Despite the existence of European associations such as EurEau bringing together sector entities from both the private and public sectors, currently no dedicated forum exists at EU-level that focuses specifically on the topic of cybersecurity as it relates to these two sectors.

With the level of reliance of both sectors on digital technologies and their level of interconnectedness steadily increasing, the need for more targeted support to ensure they can both work more uniformly towards strengthening their cybersecurity maturity becomes evident. In working towards that goal, both sectors must crucially consider the impact that developments such as geopolitical volatility, deepening third-party and supply-chain reliance, but also AI-enabled offensive capabilities have on foundational assumptions that have underpinned the way cyber risk has been managed to date.

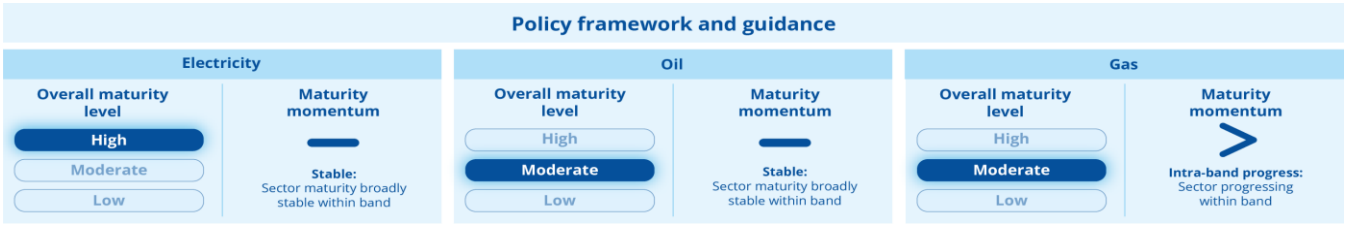
Next steps

In particular, both sectors could benefit from further support.

- **A more consistent approach to cyber risk assessment and management**, both in terms of what entities do and in terms of how they do it, is vital. A key part of this should be raising awareness around cybersecurity obligations within both sectors, clarifying what those mean for key sector players and making it easier, particularly for sector SMEs, to take action to future-proof their cybersecurity arrangements.
- **Collaboration and information sharing needs to be strengthened** within the sectors (among entities and among national authorities) in order to facilitate the exchange of experiences and best practices, tailoring approaches to the size of facilities etc.
- **The foundations for incident detection, response and recovery need to be laid** through practical, proportionate guidance.

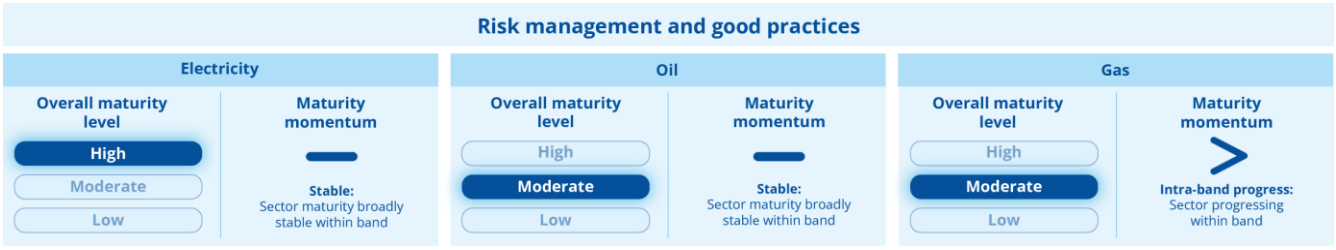
A Annex: Overview of maturity dimensions per sector

A.1 Energy

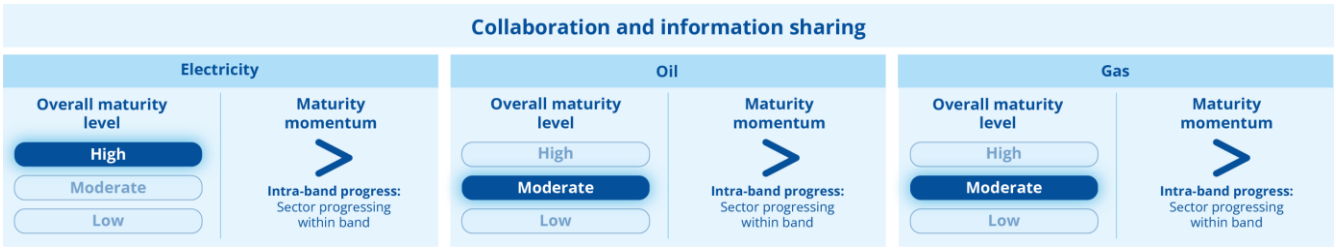


Indicators	*What are we seeing?*
Legislation	**A well-established cybersecurity policy landscape** ✓ The NIS2 directive is the main cybersecurity framework for the sector complemented by technical implementation guidance by ENISA. ✓ Electricity is additionally covered by the Network code on cybersecurity, providing more sector-specific requirements for cross-border electricity flows. ✓ Some entities may also be subject to additional EU requirements (e.g. for digital products or supply chains). ✓ Energy security framework is under review[93]. This framework may include revision of the Gas security of supply regulation and the Electricity risk preparedness regulation. However, a high level of alignment with existing legislation should be ensured to avoid increased regulatory complexity and reduced efficiency.
Supervision & Support	**Supervisory support is strongest in electricity** ✓ Electricity benefits from established supervisory engagement and structured interaction between authorities, regulators, and key sector stakeholders. ✓ Gas shows a similar but slightly less mature pattern, with more variation across authorities and Member States. ✓ Oil relies more on horizontal or cross-sector supervisory arrangements, with less sector specific support. ✓ Supervisory experience in hydrogen and district heating and cooling is limited, as reported by authorities.
Guidance	**Good uptake of guidance across the sector** ✓ Gas and electricity entities report active use of guidance. Majority of them reviewed guidance and made changes to their cybersecurity policies, procedures or security controls ✓ Oil has fewer dedicated sector-specific outputs and relies more on cross-sector guidance.

[93] EU energy security framework (revision) (date accessed May 2026)



Indicators	*What are we seeing?*
Governance	**Governance structures are largely in place** ✓ In electricity and gas, governance arrangements are well established, with senior management involved in cyber risk decision making and clear allocation of cybersecurity responsibilities. However, in the electricity subsector more companies reported that management has formal qualifications in cybersecurity and receives regular cybersecurity training. ✓ All three subsectors have defined roles and responsibilities and policies in place.
Risk assessments & Good practices	**Risk treatment remains inconsistent** ✓ Risk assessments are widely conducted and risks are documented across the electricity, gas and oil subsectors. ✓ Differences in risk assessment practices are observed across companies, particularly in relation to OT systems. In this area, the oil subsector appears more uneven in maturity, with variations reported in the assessment of OT-related risks.
Security measures	**OT and legacy constraints continue to affect implementation** ✓ Electricity entities generally report stronger asset tracking, vulnerability management, access control, and network segmentation, however there's still room for improvement. ✓ Gas shows similar practices, but with more variation and slower implementation particularly in asset management due to a lack of skills and the existence of legacy systems. ✓ Oil reports weaker access management and limited OT security due to budget constraints and the wide prevalence of legacy systems.

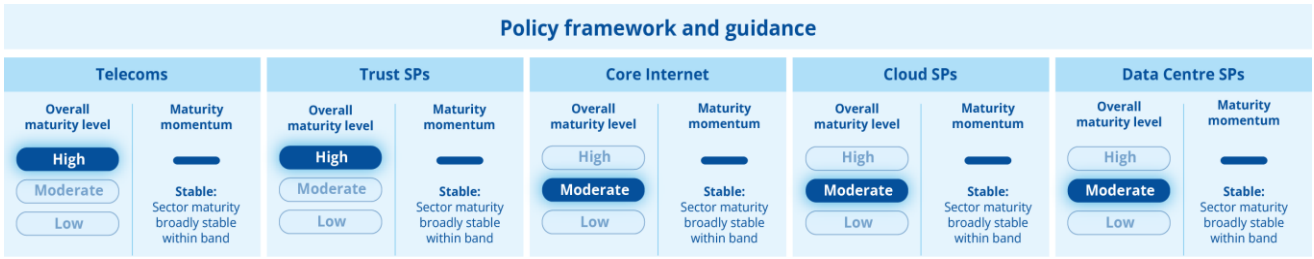


Indicators	*What are we seeing?*
Information sharing arrangements	**Information sharing is strongest in electricity and gas** ✓ Electricity benefits from a mature information sharing environment, including sector specific European and national platforms (EE-ISAC, European Network for Cyber Security (ENCS). ✓ Gas also benefits from structured information sharing arrangements and close engagement with public authorities (ENTSOG, the European Association for the Streamlining of Energy Exchange – gas (EASEE-gas) and Gas Infrastructure Europe (GIE). ✓ The oil subsector relies more heavily on energy sector information-sharing platforms, rather than specific oil subsector mechanisms.

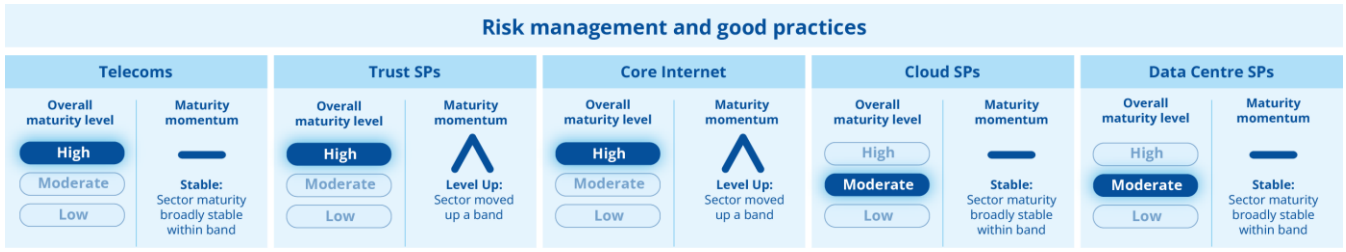
Structured collaboration mechanisms	**Structured collaboration is uneven across sectors** ✓ Electricity and gas have regular coordination formats, such as the NIS cooperation group workstream on Energy. ✓ Oil has fewer dedicated structured exchanges and relies more on broader sector formats. ✓ Wider energy events or conferences and cross-sector conferences support additional exchanges across the sector, including the ENISA annual cybersecurity conference in energy.

Indicators	*What are we seeing?*
Prevention	**Testing of controls is mostly conducted on an ad-hoc basis** ✓ In all three subsectors, security assessments are carried out on an ad hoc basis as reported by 65% of the companies surveyed while the remaining 35% conduct security assessments at set intervals covering all critical systems. This may partly be explained by the fact that in sectors such as energy, where OT environments are present, safety and operational continuity limit how security testing can be conducted, so organisations rely more on safer, non-disruptive testing methods.
Detection	**Threat detection practices are uneven across subsectors** ✓ More than half the electricity companies surveyed reported stronger threat detection practices with both prevention and detection measures applied across all relevant systems with continuous monitoring. ✓ Gas shows similar practices, although detection is more frequently limited to high-risk areas. ✓ Oil shows less consistent threat detection, with even more selective monitoring of critical assets.
Response & Recovery	**Incident response readiness is uneven, while BCP testing is generally strong** ✓ In the electricity subsector, 65% of the companies surveyed regularly conduct incident readiness and business continuity testing. ✓ In the gas and oil subsectors, around half of entities take a reactive approach, testing incident readiness plans after significant events, which was also confirmed by supervisory authorities. ✓ On a positive note, both subsectors test business continuity and crisis response arrangements annually or semi-annually.

A.2 Digital Infrastructure

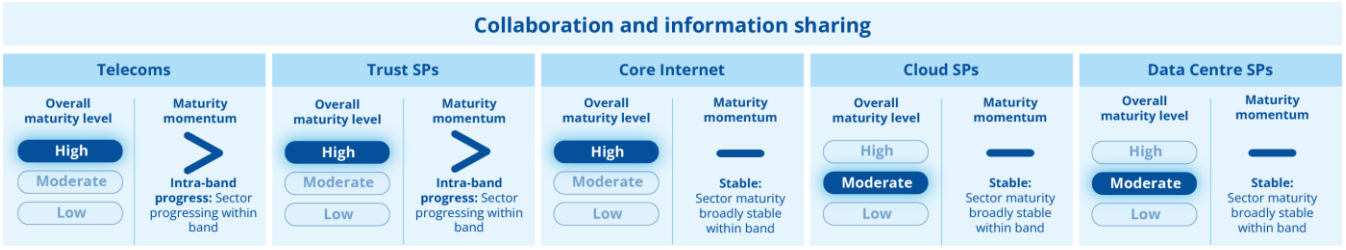


Indicators	*What are we seeing?*
Legislation	**A common baseline, with several additional frameworks** ✓ The NIS2 directive provides the main cybersecurity framework for the digital infrastructure sector complemented by technical implementation guidance by ENISA. ✓ Additional sector specific legislative frameworks exist for telecommunications (the European electronic communications code) and trust services (eIDAS). ✓ Some cloud and data centre providers may also fall under DORA, depending on the services they provide.
Supervision & Support	**Mandates are clear, but capacity remains a constraint** ✓ National authorities report that supervisory responsibilities for digital infrastructure are generally well defined across all subsectors, although in practice supervision and support do not always match the level of responsibility due mainly to limited staff capacity and budget constraints.
Guidance	**Guidance available but unevenly applied** ✓ Entities in telecommunications more often report using guidance to drive concrete updates to policies, procedures and controls. ✓ In cloud, responses are more mixed, with some entities making changes and others limiting their actions to reviewing guidance. In core internet, data centres and trust services, entities more frequently report reviewing guidance without implementing changes. ✓ This limited implementation is mainly due to operational constrains, where recommendations do not always align with existing security frameworks and operating models, and available resources are not always sufficient to support additional measures.



Indicators	*What are we seeing?*
Governance	**Governance structures largely in place but resources affect implementation** ✓ Governance across the digital infrastructure sector is generally well established, with most entities reporting defined roles and responsibilities and the presence of formal cybersecurity policies. ✓ Cyber-risk measures are typically approved at management level, supported through regular briefings and consultation with internal security teams. Furthermore, management receives regular training to ensure sufficient awareness of the organisation's cyber risk exposure. ✓ While governance frameworks are in place, their implementation is not always consistent across entities, partly due to budget limitations, with available resources often only partially covering cybersecurity needs and objectives.
Risk assessments	**Regular risk assessments in place but follow-up varies**

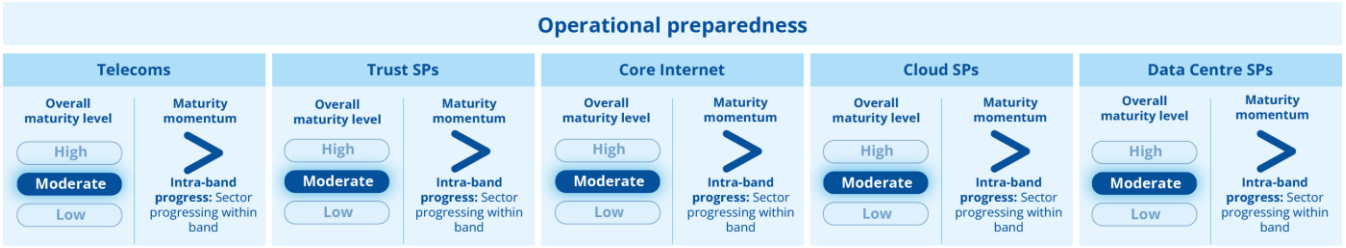
& Good practices	✓ Most entities across the digital infrastructure sector conduct cyber risk assessments on a regular basis, typically at least annually, and maintain risk registers. ✓ A majority of the companies surveyed in telecoms, core internet and trust services subsectors (60%) prioritise identified risks, define treatment plans and monitor progress over time. ✓ Half of the cloud and data centre providers surveyed, report that risks are recorded without being systematically prioritised or treated, indicating uneven application of risk assessment practices across subsectors.
Security measures	**Basic security measures in place** ✓ All companies in the sector reported implementing security measures, with none indicating non-implementation. However, the extent of implementation differs across subsectors. National authorities confirmed that cybersecurity measures are implemented most effectively in the telecommunications and trust service subsector, while other subsectors follow closely behind. ✓ Most entities across all subsectors actively track their assets, while a smaller share (30%) report only partial coverage, suggesting gaps in completeness rather than the absence of asset management practices. ✓ Similarly, many entities identify vulnerabilities in near real time and apply patching based on severity, while others rely on scheduled assessments and prioritisation of high-risk issues Legacy constraints, along with limited budgets, remain key barriers to timely remediation, especially in telecommunications. ✓ Access management is well developed across the sector, with most entities reporting controlled, reviewed and enforced access across systems. Only limited cases were observed in the data centre services subsector where consistency is less strong, partly due to skills and budget constraints. ✓ Network segmentation is reported as an area where implementation is more demanding for cloud and data centre service providers, which is partly linked to budget constraints. ✓ Environmental and physical protection measures are broadly in place and regularly tested. At the same time, the sector's critical role increases exposure to physical threats, requiring continued oversight of facilities and physical access controls to reduce the risk of wider disruption[94].



Indicators	*What are we seeing?*
Information sharing arrangements	**Mature information-sharing culture in telecoms, trust service and core internet subsectors** ✓ Telecommunication, trust service and core internet companies engage more systematically in ISACs and industry associations. Cloud and data centre services, in contrast, exhibit lower levels, although many companies reported participation in information-sharing activities at national, regional or EU levels. ✓ Across the sector, entities benefit from various cybersecurity-focused events such as the Telecom and Digital Infrastructure Security Forum and the Trust Services and eID Forum.
Structured collaboration mechanisms	**Stronger structures in telecoms and trust services** ✓ Structured collaboration mechanisms are most developed in telecommunications and trust services, where established sector communities and formal cooperation arrangements support regular and organised exchange (e.g. existing NISCG workstreams for digital infrastructures, 5G, trust services and telecommunications).

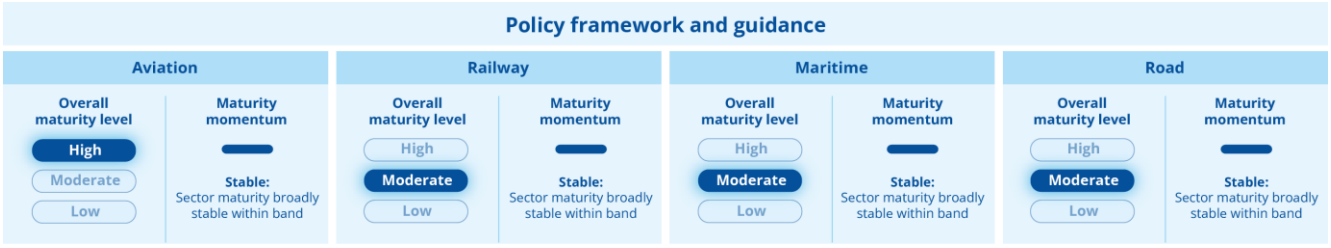
[94] The report on the cybersecurity and resilience of Europe's communications infrastructures and networks emphasised the need to extend physical stress testing to digital infrastructure. As a result, in 2025 the digital infrastructure sector, in particular fixed networks and submarine cable infrastructure, was included in the coordinated preparedness testing call under the Digital Europe Programme (DEP). The outcomes of the call are not yet available and are expected to be reflected in the next NIS360 report (all references accessed in May 2026).

	✓ Core internet services benefit from largely community-driven arrangements for collaboration. ✓ Less dedicated structures exist in the cloud and data centres service subsectors, where collaboration is more often channelled through broader cross-sector or industry fora, with more limited visibility of dedicated, sector-specific mechanisms.

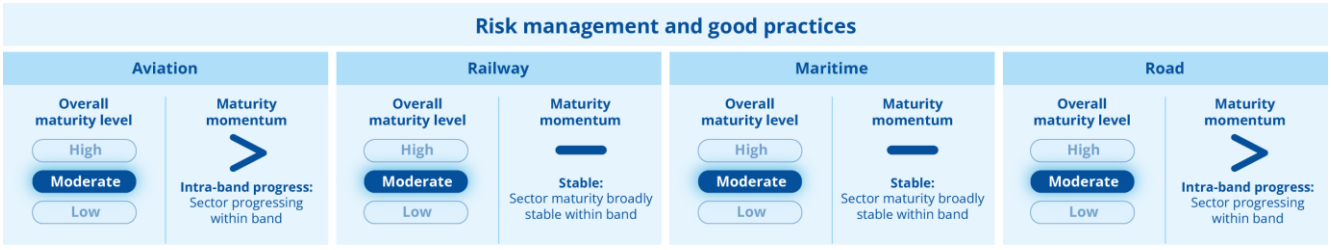


Indicators	*What are we seeing?*
Prevention	**Preventative practices are largely in place** ✓ Security assessments are generally well established, with most entities conducting them at defined intervals and using the results to inform improvements.
Detection	**Detection measures are widely used but coverage varies** ✓ Most entities report detection controls across relevant systems with continuous monitoring, while others apply detection more selectively in higher-risk areas. ✓ Widespread cyber hygiene measures and awareness initiatives are fully implemented across the sector. By implementing widespread cyber hygiene measures, the sector demonstrates a clear understanding of its high exposure to cyberattacks due to its critical role in essential services, which reinforces its focus on strengthening baseline resilience against common attack vectors. ✓ Most entities also provide cybersecurity training for management and specialised functions, helping strengthen overall preparedness.
Response & Recovery	**Response and recovery testing is common but not fully consistent** ✓ Most entities test incident and crisis response, as well as BCP/DR arrangements, on a regular basis and incorporate lessons learned into their processes. This is one of the few sectors where national authorities confirm a high level of maturity in readiness testing. ✓ A smaller group remains more event-driven in testing. For instance, 35% of telecommunications and cloud providers surveyed test BCP/DR arrangements only after significant events. ✓ While overall readiness has improved, ensuring consistent and routine exercising of response and recovery arrangements remains an area of focus, particularly for high-impact scenarios.

A.3 Transport

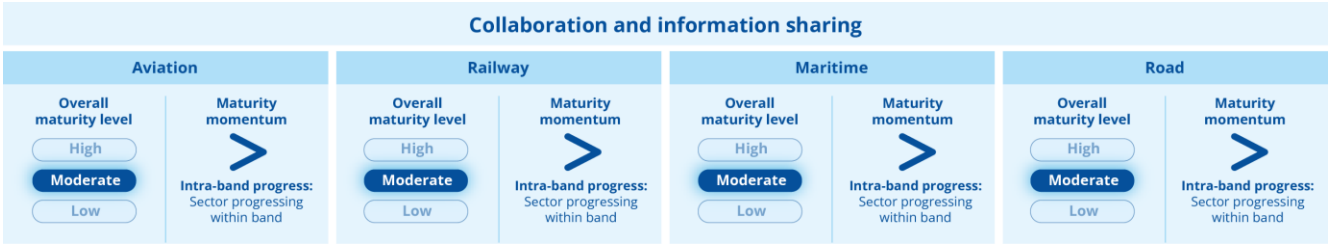


Indicators	*What are we seeing?*
Legislation	**An established cybersecurity policy landscape** ✓ The NIS2 directive is the main cybersecurity framework for the sector complemented by a technical implementation guidance by ENISA. ✓ However, additional rules exist in the aviation (PART-IS, AVSEC) covering a broader range of entities and authorities. ✓ The automotive sector is regulated by international rules, such as UN regulation No 155 and No 156, and established automotive cybersecurity engineering standards (ISO/SAE 21434). ✓ The transport sector's increasing reliance on IoT, IIoT, OT and AI driven systems also makes the Cyber Resilience act and the AI act relevant.
Supervision & Support	**Varying capacity across transport authorities, with cybersecurity gaps in maritime** ✓ Capacity constraints remain a common challenge across transport national authorities. ✓ While limited staffing affects most authorities, maritime authorities face additional pressure, with more than half also reporting gaps in cybersecurity expertise, which is a lesser concern for other transport modes. ✓ Aviation authorities appear relatively well positioned, reporting a stronger capacity to supervise and support regulated entities, despite this sector encompassing a particularly broad range of company types.
Guidance	**Positive uptake of guidance, but also increasing focus on sector's involvement in its own development** ✓ Overall, the transport sector is aware of available guidance and when it is relevant, it has been reviewed and accordingly incorporated in corporate cybersecurity policies. ✓ A positive trend is also seen with regards to the involvement of the transport sector in the development of such guidelines. The aviation and railway subsectors are more active in developing sector-specific guidance. Aviation focuses on mapping cybersecurity requirements to support practical compliance with EU legislation, while the railway sector emphasises standardisation through International Electrotechnical Commission (IEC) standards aligned with the NIS2 directive. ✓ As a result, these sectors score higher than maritime and road. ✓ In 2026, the EU ports strategy was adopted, foreseeing a revision of guidance on ports security. In addition, the action plan on inland transport is planned for the period 2028-2034. However, these new initiatives should be assessed in terms of how they contribute to the overall efficiency of the legislative framework.



Indicators	*What are we seeing?*
Governance	**Management is responsible for approving cyber risk measures** ✓ In the aviation and road sectors, management oversees cyber-risk measures with cybersecurity expertise obtained through regular trainings.

	✓ In many railway and maritime companies, management involvement is below the cross-sector average. They primarily rely on internal expertise, which provides valuable support, but greater management involvement would be needed to further strengthen the supervision of cyber-risk.
Risk assessments & Good practices	**Risk treatment is generally strong, with some gaps reflecting legacy OT systems** ✓ Aviation leads in annual cyber-risk assessments and systematic risk management, with rail and road close behind. ✓ Maritime is catching up and remains above the cross-sector average overall. ✓ Around 3 in 5 railway companies include OT systems in their cyber-risk assessments. ✓ The ENISA 2025 threat landscape report[95] indicates that some actors have expressed intent to target OT systems in the transport sector, highlighting the need to further strengthen this area.
Security measures	**Entities still struggle with security measures, notably access management and third-party supplier management** ✓ Across the transport sector, national authorities highlight that reliance on legacy systems and difficulties securing OT remain key challenges, often constraining the full implementation of security measures. ✓ Most transport companies detect vulnerabilities in near real-time; however, in the railway, maritime, and aviation sectors, critical vulnerabilities are patched more slowly due to legacy systems. ✓ Access management remains a challenge in the railway, maritime, and aviation subsectors due to limited skills, legacy systems and the involvement of many users and systems. While access is generally controlled, it is not always regularly reviewed or consistently enforced, which is notable given that aviation and maritime sectors face a higher likelihood of cyber-attacks. ✓ Physical security is a challenge in the maritime subsector, with most companies applying risk-based measures only to certain critical assets or areas. ✓ Aviation and road companies largely ensure full encryption of sensitive data, but in railway and maritime subsectors, encryption is often partial, constrained by legacy infrastructure. ✓ Railway, aviation and maritime subsectors lag behind the cross-sector average in procurement management, reflecting uneven implementation of cybersecurity requirements in IT/OT acquisitions. This is further challenged by the fact that such systems often require maintenance contracts spanning many years or decades, meaning they must be retrofitted over time to comply with evolving cybersecurity standards, which increases the complexity.



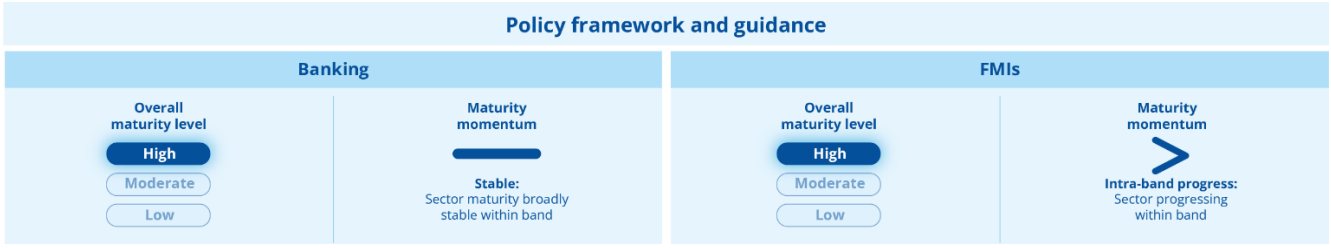
Indicators	*What are we seeing?*
Information sharing arrangements	**Entities demonstrate good information sharing practices** ✓ Aviation and maritime companies engage more systematically in ISACs and industry associations. Railway have strengthened information-sharing as well. ✓ The road subsector improved information-sharing largely under the influence of initiatives in the automotive industry.
Structured collaboration mechanisms	**Well-established EU-level mechanisms for structured collaboration** ✓ Aviation, maritime and railway have well-established mechanisms for collaboration and are maintaining similar performance to previous years: Aviation (SAGAS, Aviation ISAC, Aviation workstream and EASA), Maritime (SAGMAS and Maritime ISAC) and Railway (LANDSEC, Rail ISAC, Railway CISO Forum as well as expert groups in railway-related associations (EIM, CER, UNIFE), and an annual conference co-organised by ENISA and ERA.

[95] ENISA Threat Landscape 2025_v1.2.pdf (date accessed May 2026)

	✓ Collaboration in the road subsector remains limited. The Automotive ISAC provides an established collaboration model for vehicle manufacturers and suppliers. There are no mechanisms for structured collaboration for road authorities and ITS operators, except LANDSEC.

Indicators	*What are we seeing?*
Prevention	**The effectiveness of controls is inconsistently assessed** ✓ In aviation, security assessments are mostly (80%) conducted at regular intervals and cover all critical systems, with results feeding into continuous improvement. ✓ The road subsector performs at a slightly lower (65%) but comparable level. ✓ Railway and maritime apply security assessments more unevenly—ranging from regular (35%) to ad hoc (50%) — placing them below the cross-sector average.
Detection	**Threat detection is active** ✓ Across all transport modes, both prevention and detection are applied either across all systems or selectively in high-risk areas, while prevention-only approaches are rare (10%), which is a positive development. ✓ Appropriate cyber awareness and hygiene practices are generally evident across transport sectors, with most providing cybersecurity training for employees, except in aviation, where companies see opportunities to further improve employee training programmes. ✓ Most transport sector companies have a separate and more specialised training for management; however there is room for improvement in the railway and maritime subsectors.
Response & Recovery	**Incident response and continuity testing is uneven** ✓ Incident response testing continues to be a weak area, with readiness tests rarely conducted or only reactively in the railway (35%), maritime (20%), and road (45%) subsectors, as confirmed also by national authorities. Aviation stands out with 60% of companies testing their incidents readiness annually or semi-annually. ✓ Most aviation and maritime entities conduct regular BCP/DR testing, while it is limited in the railway (25%) and road (45%) subsectors. ✓ Only the maritime subsector showed relatively high participation in cybersecurity exercises. However, at EU level both maritime and railway are included in the Cyber Europe 2026 exercise. In addition, both subsectors will be included in the coordinated preparedness testing call under the Digital Europe Programme (DEP) in 2026.

A.4 Finance

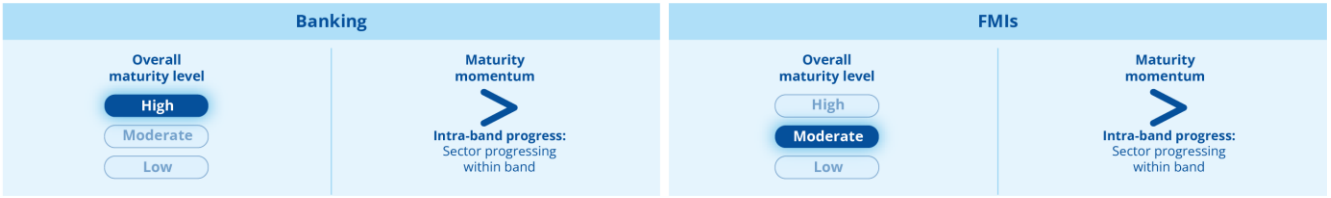


Indicators	*What are we seeing?*
Legislation	**A well-established cybersecurity policy landscape** ✓ DORA is the main cybersecurity framework for the sector; it is complemented by Regulatory technical standards (RTS) and implementing technical standards (IT). ✓ DORA is a *lex specialis* for the financial entities, meaning that DORA specific requirements take precedence over the NIS2 directive. ✓ However, should DORA not provide specific provisions, the requirements of NIS2 directive continue to apply (e.g. cross-sector cooperation).
Supervision & Support	**National authorities integrate cybersecurity in their activities** ✓ FMIs authorities have strengthened their supervisory and cybersecurity skills capacity, although some resource constrains remain. ✓ Financial authorities (covering both sectors) are increasingly integrating cybersecurity into their activities. They also carry out some additional activities beyond those of NIS2 authorities, including TLPT/TIBER testing and related community engagement.
Guidance	**Positive uptake of guidance** ✓ Overall, the finance sector is aware of available guidance; its companies review it and incorporate it in corporate cybersecurity policies. ✓ However, existing cybersecurity guidance is applied more consistently in the banking sector than among FMIs.

Indicators	*What are we seeing?*
Governance	**The banking sector demonstrates a higher level of management involvement compared to FMIs** ✓ In the banking sector, management oversees cyber-risk measures with solid cybersecurity expertise, while in many FMIs, management involvement remains below the cross-sector average, representing an area for improvement. ✓ Many banks have at least one management member with formal cybersecurity qualifications in addition to internal expertise, which is not the case for FMIs where management does not often have cybersecurity qualifications.
Risk assessments & Good practices	**Risk assessment is consistent in both sectors** ✓ Most entities in both sectors assess cyber risks annually and maintain a systematic risk management process.
Security measures	**Banking shows higher maturity in security controls than FMIs** ✓ Banks generally track all assets, in contrast to FMIs, where tracking is partial due to budget limitations.

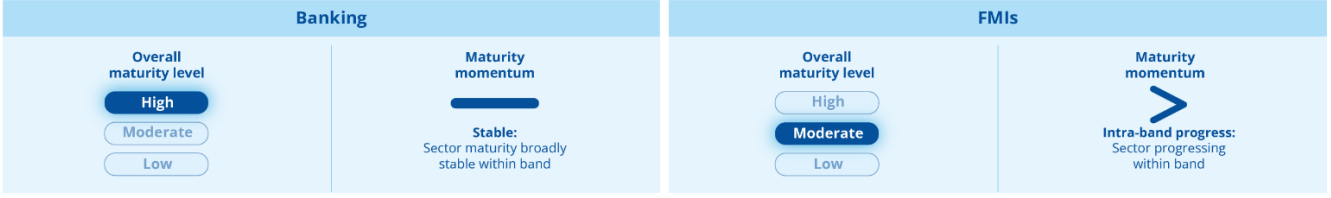
	✓ Most banks detect vulnerabilities in near real-time, whereas many FMIs rely on scheduled assessments and patch critical vulnerabilities more slowly due to legacy systems or budget constraints. ✓ Most banking networks are segmented with security controls and continuous monitoring. FMIs show uneven network security, from proper segmentation to none. ✓ While the majority of banks encrypt all sensitive data, most FMIs apply encryption partially, reflecting a shortage of skilled staff. ✓ Access management is a strong area for both sectors, with controlled, reviewed, tested, and enforced access across all systems. ✓ Although physical security measures are in place and regularly tested, cyber criminals increasingly leverage physical infrastructure. Entities should therefore enhance oversight and safeguards to prevent criminals from exploiting business or company facilities for illicit purposes.

Collaboration and information sharing



Indicators	*What are we seeing?*
Information sharing arrangements	**Information sharing improved considerably in both sectors** ✓ Given the critical role of information sharing in combating cross-border cybercrime, the banking sector has made significant improvements, supported by active engagement in ISACs and industry associations. FMIs have also enhanced their information-sharing practices, although only just over half reported active participation in those formats.
Structured collaboration mechanisms	**EU-level structured collaboration mechanisms exist** ✓ While structured collaboration (ISACs, expert groups and conferences) is present in both sectors, it is more developed in the banking sector, with more members involved. ✓ Efforts within the financial sector to comply with DORA and NIS2 requirements have contributed to more structured collaboration between DORA and NIS2 national authorities. At the same time cross-sector cooperation at the EU level, including links between the European supervisory authorities and the NIS cooperation group, is still developing.

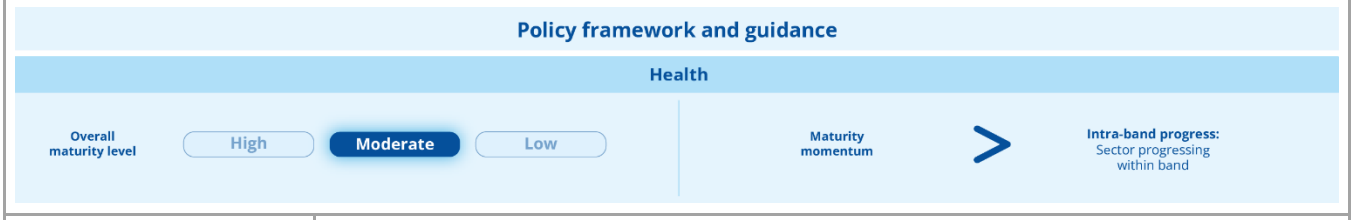
Operational preparedness



Indicators	*What are we seeing?*
Prevention	**The effectiveness of controls is consistently assessed** ✓ 90% of banks and 75% of FMIs surveyed reported conducting regular (at least annual) security assessments, demonstrating a proactive and systemic approach to auditing, scanning, evaluating and testing their IT infrastructures, applications and policies as part of a cyclical process.
Detection	**Both sectors show a high level of maturity in detection capabilities** ✓ 90% of banks and 75% of FMIs surveyed reported implementing proactive prevention and detection controls across all systems, with continuous monitoring. They combine advanced analytics, threat intelligence and human expertise to detect anomalous and malicious activities rather than relying solely on security alerts. This aligns with DORA's requirements for timely detection and response capabilities.

	✓ Strong cyber awareness and hygiene practices are evident in both sectors, with most offering separate cybersecurity training to management and all other staff. 80% of banks and 70% of FMIs provide dedicated cybersecurity training for management and specialised roles.
Response & Recovery	**Response and recovery readiness is mature in both sectors** ✓ Incident readiness tests are conducted regularly by almost all banks and most companies in the FMI sector. ✓ However, national authorities observed that FMIs tended to perform better than banks. This could be explained by the fact that FMIs generally involve fewer companies than the banking sector and are typically systemically important. The banking sector, by contrast, is more diverse and includes companies of varying size and systemic relevance, from small local banks to large systemically important ones, leading to more diverse responses from the authorities. ✓ Regular BCP/DR testing is conducted across most companies in both sectors. ✓ Participation in EU-level and national cybersecurity exercises was higher among banks than FMIs.

A.5 Health



Indicators	*What are we seeing?*
Legislation	**A dense but maturing policy landscape** ✓ The NIS2 directive is the main cybersecurity framework for the sector; it is complemented by several other policy instruments addressing more specific areas (e.g. the Medical device regulation, European health data space, AI act) and creating a more complex policy environments for sector entities to navigate.
Supervision & Support	**National authorities under growing pressure** ✓ National authorities play a central role in supervising and supporting health sector entities. ✓ The sector's expanded scope under NIS2 has increased the complexity of oversight for authorities who already had to deal with challenges such as limited staff capacity, budget constraints, and gaps in sector-specific cyber expertise.
Guidance	**Availability of guidance is improving** ✓ Guidance for sector entities is available at both EU and national levels, with recent political developments around the EU healthcare action plan, creating expectations for even more to come. **Uptake of guidance varies by entity type** ✓ The majority of entities surveyed indicated that in the past year they have made use of available guidance to inform changes to their cybersecurity policies, procedures or controls. ✓ Nevertheless, uptake varies by entity type with healthcare providers presenting a mixed picture compared to for example pharmaceutical manufacturers that consistently reported having used the guidance to drive change.

Indicators	*What are we seeing?*
Governance	**Management is responsible for approving cyber risk measures** ✓ The majority of entities surveyed indicated their management is responsible for approving measures to manage cyber-risk, citing consultations with either internal or external experts as the most prevalent ways used to ensure management has the understanding to do so effectively. **Roles are assigned, but responsibilities may be unclear** ✓ Most entities surveyed tend to fall into one of two categories: a) those that have assigned some of the cybersecurity roles they need without having defined responsibilities clearly, and b) those that have clearly defined, documented and assigned all the cybersecurity roles they need. ✓ More than half of healthcare providers fall in the first category, whereas more than half of pharmaceutical manufactures fall in the second. **Budget constraints limit ability to attain cyber objectives** ✓ Most entities indicate that current cybersecurity budgets are insufficient or only partially sufficient to meet their cybersecurity needs. The pressure is more acute among healthcare providers.

Risk assessments & Good practices	**Risk assessments are conducted but risks are not consistently addressed** ✓ While most entities report conducting risk assessments at least annually, one in two entities (including the majority of healthcare providers) suggest that they either don't follow a specific process for handling the risks identified or that they record the risks identified but do not necessarily follow up on them. This view aligns with the observations shared by roughly one in two of the authorities surveyed. ✓ Encouragingly, some of the hospitals who suggested they do not follow a specific process for risk management mentioned that they are in the process of establishing it, in line with the requirements of NIS2.
Security measures	**Entities still struggle with foundational security measures** ✓ Across the sector, entities struggle most notably with: asset management (more than half say they track only some of their assets) as well as an inability to perform continuous vulnerability management (predominantly focused on high-severity findings), inconsistent data security arrangements and an uneven integration of security considerations in procurement. ✓ All of these issues are more acute for healthcare providers who cite lack of resources and skilled personnel and the prevalence of legacy systems among the key challenges they are facing.

Collaboration and information sharing

Health

Overall maturity level: **High** | Moderate | Low

Maturity momentum: ^ **Level Up:** Sector moved up a band

Indicators	*What are we seeing?*
Information sharing arrangements	**Information sharing takes place, but is uneven** ✓ Most entities surveyed suggest they engage in information sharing. The proportion of entities surveyed who do not engage in information sharing or collaboration initiatives is highest among healthcare providers.
Structured collaboration mechanisms	**Strong collaboration exists at EU-level** ✓ The sector benefits from well-established structures for collaboration, including an EU-level ISAC, a dedicated NIS cooperation group workstream and an annual cybersecurity conference organised by ENISA. **Peer collaboration could be further strengthened** ✓ While national authorities cooperate effectively with entities, structured collaboration between entities still has room for improvement. ✓ At the same time, the collaboration among different authorities having oversight of the sector at national level under differing legal frameworks, also needs to be improved.

Operational preparedness

Health

Overall maturity level: **High** | Moderate | Low

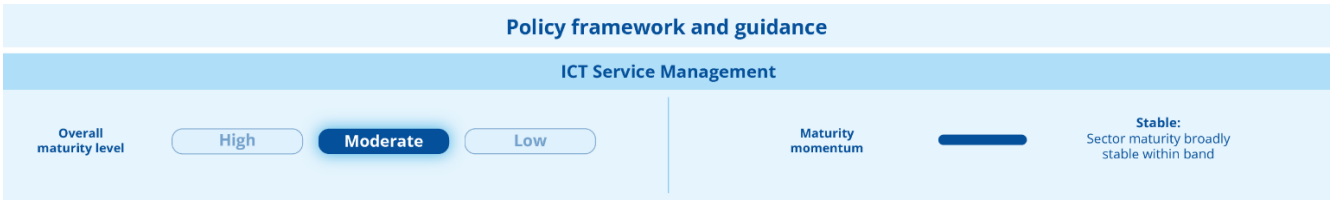
Maturity momentum: ^ **Level Up:** Sector moved up a band

Indicators	*What are we seeing?*
Prevention	**Effectiveness of controls is inconsistently assessed** ✓ Most entities surveyed suggest they run security assessments at regular intervals to determine the effectiveness of their controls, however nearly 60% of authorities characterise testing practices as ad hoc suggesting uneven practices across the sector. ✓ Looking more closely at healthcare providers, most of the entities surveyed suggested that testing of controls is often ad hoc, limited in scope or not conducted at all.
Detection	**Detection capabilities exist, but coverage is uneven** ✓ The majority of entities surveyed suggest that both preventive and detection measures are applied across their systems, with active monitoring for threats.

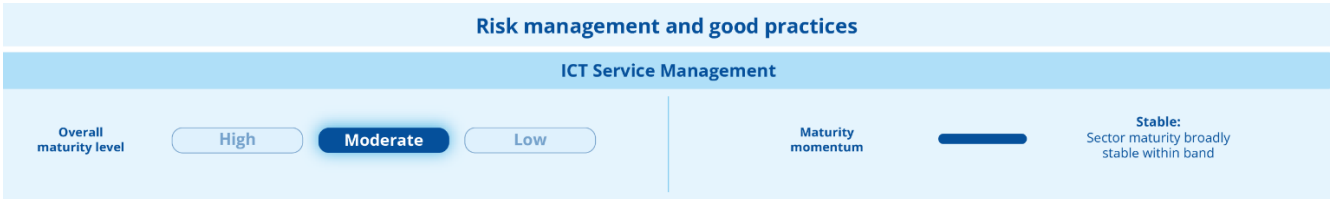
	✓ For healthcare providers however the situation is more uneven, with more than half stating that they are either focused on their prevention or their detection capability is limited to high-risk areas, leaving gaps in their coverage. **Depth of management training is often inconsistent** ✓ Despite management training taking place across the majority of sector entities, the content and objectives of this training appear to be inconsistent, with some entities saying the content their management is trained on is highly introductory and lacks sufficient depth for them to be able to better understand, govern and act on cyber risk.
Response & Recovery	**Incident response and continuity testing is uneven** ✓ Testing of incident response and BCP/DR arrangements happens inconsistently among entities surveyed, with some saying it takes place at set intervals, others describing a more ad hoc, reactive approach and others stating it takes place but may have limited scope (e.g. only testing backups). This view is largely echoed by national authorities. ✓ Large variability is observed in the incident response practices of both healthcare providers[96] and pharmaceutical manufacturers – whereas the picture for BCP/DR arrangements among manufacturers is more consistently mature.

[96] The health sector, in particular hospitals, was included in the coordinated preparedness testing call under the Digital Europe Programme (DEP) in 2025. The outcomes of the call are not yet available and are expected to be reflected in the next NIS360 report.

A.6 ICT service management



Indicators	*What are we seeing?*
Legislation	**An established cybersecurity policy landscape** ✓ The NIS2 directive is the main cybersecurity framework for the sector; it is complemented by a technical implementation guidance by ENISA. ✓ Many sector entities are also within the scope of the CRA or sector-specific legislation like DORA which introduce additional obligations.
Supervision & Support	**National authorities constrained by limited experience and resources** ✓ National authorities play a central role in supervising and supporting entities under NIS2; however given the relatively recent inclusion of the sector under regulatory oversight, authorities have limited experience in supervising this sector. ✓ The challenges created by lack of experience are, according to authorities, compounded by a) limited staff capacity, b) budget constraints and c) lack of cybersecurity expertise.
Guidance	**Slow uptake of available guidance** ✓ Roughly one in two entities report being aware of available guidance but not having reviewed it or having reviewed the guidance but not having acted upon it, with some citing an inability to bridge the provisions of the guidance with their existing cybersecurity arrangements, and others citing a lack of resources.



Indicators	*What are we seeing?*
Governance	**Management is responsible for approving cyber risk measures** ✓ The majority of entities surveyed indicated their management is responsible for approving cyber-risk management measures, with one in two entities indicating their management also has relevant cyber qualifications. **Risk management efforts are challenged by lack of resources** ✓ Across the sector, inadequate budget is identified as a key barrier to effectively meeting cybersecurity objectives, however national authorities feel other challenges are more pressing (e.g. shortage of skilled cybersecurity personnel, risks from third party suppliers etc.).
Risk assessments & Good practices	**Risk treatment is inconsistent** ✓ The majority of the entities surveyed stated they run risk assessments at least once per year. ✓ Despite that, roughly one in two entities said they either have no formal process to manage identified risks or when they do, the treatment of risk is not necessarily prioritised or performed systematically.
Security measures	**Entities still struggle with foundational security measures** ✓ Sector entities struggle most notably with timely patching, network segmentation, and data security, citing lack of budget and prevalence of legacy systems amongst the key reasons.

Collaboration and information sharing

ICT Service Management

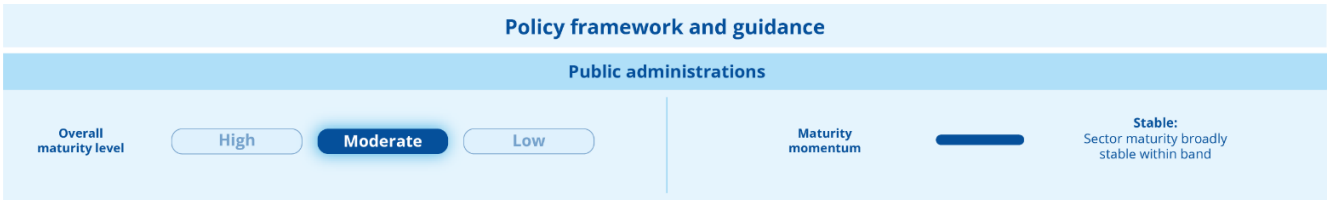
Indicators	*What are we seeing?*
Information sharing arrangements	**Information sharing is uneven among entities** ✓ Entity engagement in information sharing initiatives is inconsistent, with smaller entities within the sector being less involved in such initiatives than larger ones. ✓ National authorities indicate efforts are made to facilitate information exchanges with other sectors (sharing reports, threat intelligence etc.).
Structured collaboration mechanisms	**Lack of EU-level mechanisms for structured collaboration** ✓ At the EU-level no mechanisms exist that consistently bring sector entities or authorities together to discuss on topics of cyber relevance (e.g. ISACs, workstreams, expert groups, conferences). That said, an ad hoc working group on EUMSS was established in 2025, to support the drafting of the EUMSS scheme foreseen under Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024, amending Regulation (EU) 2019/881 as regards managed security services.

Operational preparedness

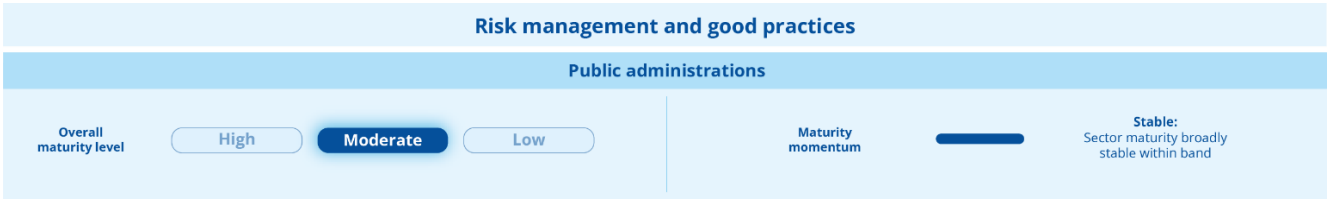
ICT Service Management

Indicators	*What are we seeing?*
Prevention	**The effectiveness of controls is assessed inconsistently** ✓ More than half of the entities surveyed in the sector suggested they either do not conduct security assessments or when they do, those have limited coverage or are done on an ad hoc basis, a view that is corroborated by national authorities. That raises concerns particularly when considering the prevalence of sector entities as third-party suppliers to other sectors.
Detection	**Detection capabilities exist** ✓ The majority of entities surveyed suggest that both preventive and detection measures are applied across their systems, with active monitoring for threats. While prevention-only approaches remain relatively rare (10%), this share is still considered relatively high for the ICT service management sector, given its widespread role as a third-party supplier to other sectors.
Response & Recovery	**Response and recovery readiness is uneven** ✓ Across the sector, readiness to respond to and recover from incidents is inconsistent, with a notable number of entities indicating they feel underprepared to deal with cyberattacks stemming from their supply chain or causing IT/OT degradation. ✓ Roughly one in two entities across the sector indicate that their arrangements for incident response undergo limited testing or are undertaken reactively (after incidents); this is corroborated by national authorities. ✓ Similarly, 37% of entities in the sector say they only test their BCP/DR arrangements in a limited manner or reactively.

A.7 Public administrations

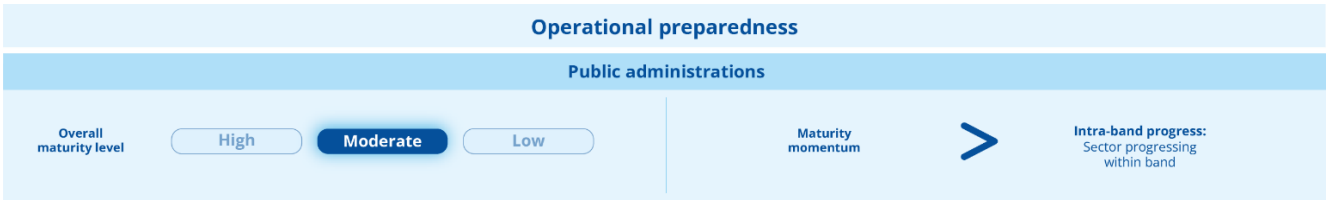


Indicators	*What are we seeing?*
Legislation	**An established cybersecurity policy landscape** ✓ The NIS2 directive is the main cybersecurity framework for the sector; it is complemented by a technical implementation guidance by ENISA.
Supervision & Support	**National authorities constrained by limited experience and resources** ✓ Cybersecurity responsibilities are often assigned to horizontal national authorities, which need time to manage a wide range of entities and at the same time have limited resources and experience in supervising a new sector.
Guidance	**Good uptake of available guidance** ✓ Roughly three in four public administrations report being aware of available guidance and making changes to their cybersecurity policies. Administrations that indicated that they either had not reviewed the guidance or had not acted upon it, cited a lack of resources or insufficient support mechanisms to facilitate implementation.



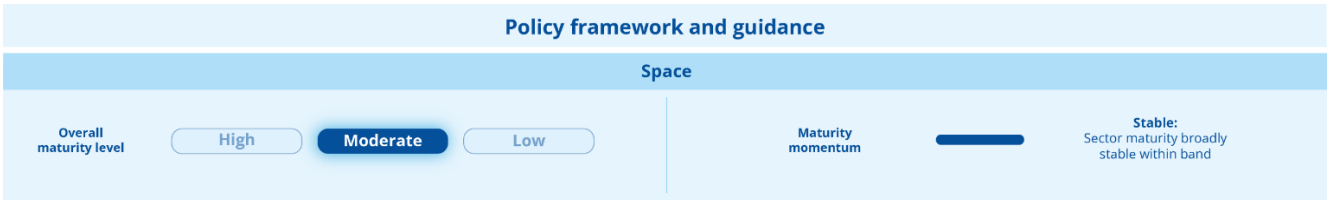
Indicators	*What are we seeing?*
Governance	**Opportunity to enhance management cybersecurity expertise** ✓ While in three out of five public administrations surveyed management is responsible for approving cyber-risk management measures, they have limited cybersecurity expertise. Only one in four reported that their management has relevant cyber qualification. Furthermore, one third have no structured approach to ensuring management cybersecurity expertise. **Policies and roles are defined inconsistently** ✓ About half of surveyed public administrations have limited or no formal policies, indicating that the sector has only just started implementing the NIS2 requirements. ✓ Similarly, about half of surveyed public administrations have limited or no clearly defined cybersecurity roles, often remain handled by IT functions.
Risk assessments & Good practices	**Risk treatment is inconsistent** ✓ Many public administrated reported that they assess risks at least once a year, however risk handling practices are inconsistent. One fourth have no formal process in place, while about half identify, prioritise, and treat risks but don't have a formal risk register, or have risk registers but risk treatment is not necessarily prioritised or carried out systematically. Inconsistencies in risk treatment were also confirmed by national authorities. ✓ Majority of entities that rely on OT systems for their operations, include them in the risk assessment, which shows that the sector is following good practices to cybersecurity risk management.
Security measures	**Entities struggle with foundational security measures** ✓ Sector entities struggle most notably with access management, network segmentation, data security, and timely patching, which typically takes three months or longer, citing lack of skills, budget and prevalence of legacy systems amongst the key reasons.

Indicators	*What are we seeing?*
Information sharing arrangements	**Information sharing is limited among entities** ✓ Half of public administrations do not engage in information sharing and collaboration due to the lack of such mechanisms or the high diversity of entities in the sector, including ministries, municipalities, parliaments, and public service authorities. These entities have different objectives and operational contexts and they vary from one Member State to another. ✓ At the moment collaboration is limited to NIS2-mandated information sharing with authorities.
Structured collaboration mechanisms	**Lack of EU-level structured collaboration mechanisms** ✓ Structured collaboration exists mainly at the municipal level (e.g. ISAC4Cities, CEMR, Major Cities) but does not extend to central government administrations or collaboration among national authorities.

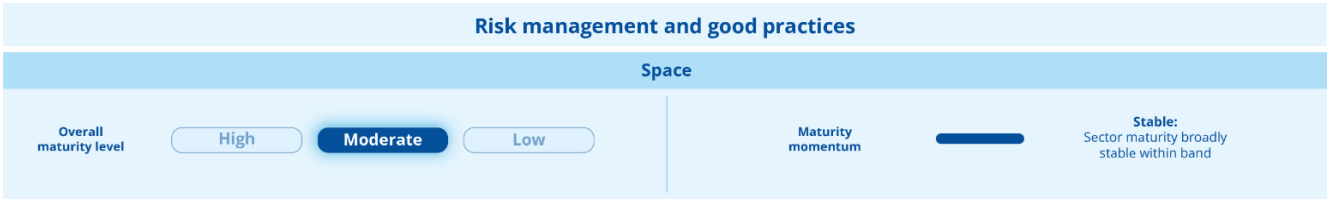


Indicators	*What are we seeing?*
Prevention	**The effectiveness of controls is inconsistently assessed** ✓ One fifth of the entities surveyed in the sector do not conduct security assessments and about half of them rely on ad-hoc or limited assessment, a view that is also corroborated by national authorities. However, some public administrations have a structured and systematic process that begins with clearly defining the scope and objectives of the assessment. This involves identifying the systems, applications, and networks to be tested, as well as the specific goals to be achieved, such as detecting vulnerabilities, assessing the effectiveness of controls, and improving overall security posture.
Detection	**Threat detection capabilities exists, but could further improved** ✓ About 40% of public administrations surveyed reported implementing proactive prevention and detection controls across all systems, with continuous monitoring, and only small group relies on prevention only. **Cyber hygiene initiatives and management training are still developing** ✓ One third of public administrations do not run cybersecurity awareness and cyber hygiene initiatives for employees, and about a half of them don't have cybersecurity training initiatives for management. Some provide general training, monthly briefings, and alerts, some organise the same training for all employees, with no tailored courses for management. This reflects an inconsistent approach to cybersecurity training and it is particularly concerning, as phishing remains a common initial access vector across attack types in this sector.
Response & Recovery	Response and recovery readiness is uneven ✓ The testing of plans for incident response and BCP/DR is below the average with many entities testing rarely or only after major events, which is also confirmed by the supervisory authorities. It is another concerning area, as this sector remains the most targeted sector. ✓ A positive trend is that public administrations are the most active users of the Support Action. Furthermore, the sector will be included in the coordinated preparedness testing call under the Digital Europe Programme (DEP) in 2026.

A.8 Space



Indicators	*What are we seeing?*
Legislation	**Uneven obligations and uneven practices** ✓ The NIS2 directive remains the main cybersecurity framework for the sector[97] however its scope is limited to only specific entities operating in the sector. NIS2 is complemented by standards and guidelines of relevance to specific entities operating in the sector[98]. ✓ The CRA also introduces cybersecurity obligations that are relevant to the wider sector.
Supervision & Support	**Support structures exist but cyber experience varies** ✓ The sector's cybersecurity efforts are supported by EU bodies (e.g. EUSPA), national space agencies and industry associations. ✓ National authorities have an important role to play under NIS2; however their sector-specific experience and cyber expertise are still limited and often constrained by a lack of resources (staff and budgets).
Guidance	**Use of available guidance is inconsistent** ✓ One in two entities surveyed in the sector indicate that while they have reviewed available guidance, they have not ended up using it.



Indicators	*What are we seeing?*
Governance	**Management approves cyber risk management measures** ✓ Most entities indicate their management approves cyber risk management measures citing various ways they use to ensure management has the relevant understanding to do so effectively (consultations with experts internally or externally, regular briefings etc.). **Roles and responsibilities are inconsistently defined or assigned** ✓ Most entities say that roles and responsibilities around cybersecurity are inconsistently defined and assigned within their entity. **Wide differences in budgets affect ability to attain objectives** ✓ Entities present a very fragmented view as regards the adequacy of their budgets to meet their cybersecurity objectives with some indicating it is adequate, others suggesting it is not, and others stating that it only partially suffices. ✓ Insufficient budget is also among the top three most cited challenges hindering the sector's cybersecurity efforts according to authorities (after shortage of skilled personnel and limited awareness of cybersecurity best practices).
Risk assessments & Good practices	**Risk management practices vary** ✓ Although most entities say they conduct cyber risk assessments at least once per year, systematically tracking and managing identified risks, national authorities provide different

[97] This may change with a potential adoption of the EU Space Act a proposal for which was announced by the European Commission in June 2025. The proposal introduces, among other things, obligations on cyber resilience for entities operating in the EU space sector and it is currently being negotiated under the standard legislative procedure. Should it be adopted, the act would serve as a *lex specialis* with respect to NIS2. In its current form the proposal foresees a number of requirements for sector entities including 'all hazards' risk management, asset mapping, physical resilience, detection mechanisms, protection and preventive measures, supply chain risk management, training, incident handling, business continuity, response and recovery measures, testing, etc. The proposal was open to public consultation from July to November 2025 and its proposed entry into force date is January 2030. https://defence-industry-space.ec.europa.eu/eu-space-act_en (date accessed May 2026)

[98] Examples include: ECSS-E-ST-80C – Space engineering – Security in space systems lifecycles, July 2024 and ECSS-E-ST-40C Rev.1 DIR1 – Space engineering – Software" - April 2025.

	views of the sector. These confirm entities implement risk management procedures, but suggest that these are limited in scope and mostly reactive.
Security measures	**Entities still struggle with foundational security measures** ✓ The entities surveyed present an inconsistent view when it comes to the implementation of security measures. Areas where most such inconsistencies appear include: asset management, network segmentation, vulnerability management and physical security. *It is worth noting that all of these areas are included in Annex VII of the EU Space Act proposal in recognition of their importance in the context of space operations across segments.*

Collaboration and information sharing

Space

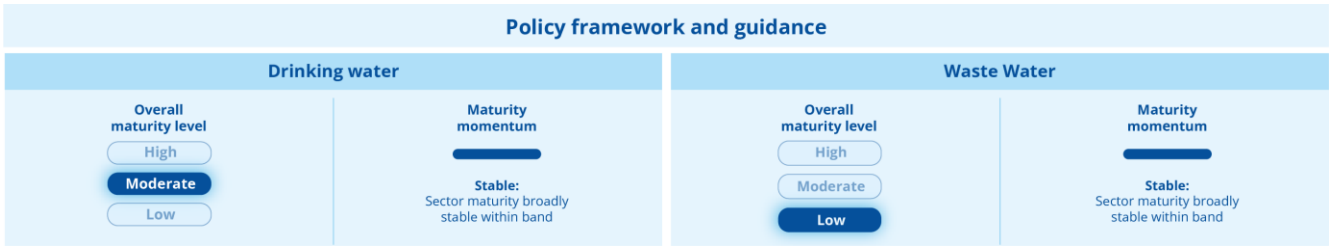
Indicators	*What are we seeing?*
Information sharing arrangements	**Information sharing is uneven among entities** ✓ The EU Space ISAC was established in 2024, as a membership-driven initiative and working groups have already been established among its members to work on specific topics (threats in the space environment and standardisation of space-related policies).
Structured collaboration mechanisms	**Structured mechanisms for collaboration within the sector and across it are limited** ✓ Currently, structured mechanisms that consistently bring sector entities or authorities together to discuss topics of cyber relevance are still limited. National space agencies occasionally interact during the development of standards or policy discussions; however, their exchanges are not necessarily focused on cybersecurity. ✓ At the same time, collaboration of entities or authorities within the sector with counterparts from other sectors is also limited.

Operational preparedness

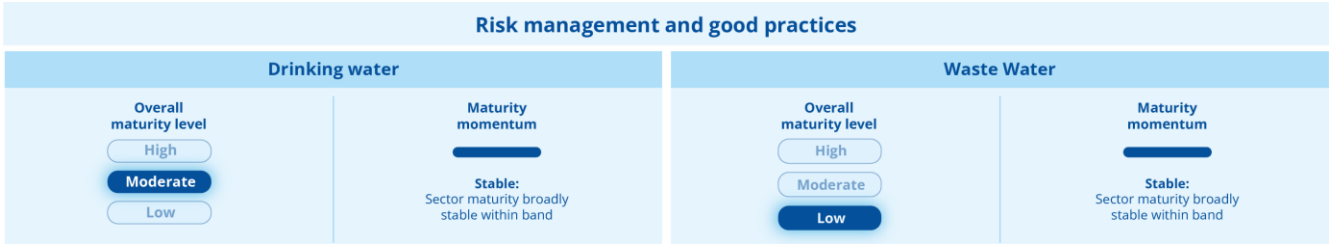
Space

Indicators	*What are we seeing?*
Prevention	**The effectiveness of controls is assessed inconsistently** ✓ Testing the effectiveness of implemented controls takes place inconsistently across the sector with roughly one in two entities indicating that it is done regularly covering all critical systems, compared to the other half that says it only happens on an ad hoc basis, focusing on high-risk areas.
Detection	**Threat detection capability is uneven** ✓ Approaches to detection are also inconsistent with some entities suggesting their primary focus is on prevention, others stating that they implement both preventive and detection controls albeit with a limited scope, while others describe more advanced detection capabilities.
Response & Recovery	**Response and recovery readiness is uneven** ✓ In a similar vein, readiness to respond to incidents and recover from attacks also varies, with most entities saying they have incident response and BCP/DR plans in place, but they all follow different approaches to testing them (some more reactive, others more proactive). ✓ This view is corroborated by national authorities most of whom confirm sector entities have relevant plans but do not necessarily test them.

A.9 Drinking water and Waste water



Indicators	*What are we seeing?*
Legislation	**Common baseline, limited support** ✓ Both the drinking water and waste water sectors are subject to the NIS2 directive but have received limited attention when it comes to cybersecurity, compared to other sectors. ✓ Neither sector benefits from a dedicated EU-level authority or sector body supporting its cybersecurity efforts.
Supervision & Support	**National authorities with uneven experience** ✓ National authorities play an important role, but their experience is inconsistent. ✓ The drinking water sector benefits from more experienced national supervision, as it was also in scope of NIS1.
Guidance	**Lack of awareness and resources hinder the use of guidance** ✓ One in five entities surveyed in both sectors are not aware of guidance available to help them align with NIS2 requirements. ✓ Roughly one in five entities in each of the sectors are aware of such guidance, have reviewed it, but have not acted upon it, with the majority citing lack of resources as the reason.



Indicators	*What are we seeing?*
Governance	**Management approves cyber risk management measures** ✓ The majority of entities surveyed indicate their management is responsible for approving cyber-risk management measures. ✓ Consultation with external experts was cited as the most common way management in both sectors ensures they have the understanding needed to make cyber decisions. **Roles and responsibilities are inconsistently defined or assigned** ✓ Across both sectors, most entities report that cybersecurity roles and responsibilities are not formally assigned and are often assumed by other roles (e.g. IT). ✓ Where some roles are assigned, entities report gaps or overlaps. **Risk management efforts challenged by lack of resources** ✓ Across both sectors inadequate budget is identified as a key barrier to effectively meeting cybersecurity objectives. The view is corroborated by national authorities. ✓ Top five most cited challenges facing both sectors according to authorities: a) shortage of skilled personnel, b) insufficient budgets, c) risks from third-party suppliers, d) limited awareness and e) dependence on legacy systems
Risk assessments & Good practices	**Risk assessments are infrequent and mostly reactive** ✓ Across both sectors, one in three entities surveyed report that they have never conducted a risk assessment.

	✓ Of those that have, the majority have done so only after specific events or emergencies. This reactive approach is corroborated by national authorities. ✓ The majority of entities in both sectors don't have a formal process in place for managing the risks identified.
Security measures	**Lack of resources hinders the implementation of core measures** ✓ Across both sectors, entities struggle most notably with vulnerability and patch management, network segmentation and data security. Those challenges are predominantly attributed to a lack of budget or expertise.

Collaboration and information sharing

Drinking water		Waste Water	
Overall maturity level: High / Moderate / **Low**	Maturity momentum: **Stable:** Sector maturity broadly stable within band	Overall maturity level: High / Moderate / **Low**	Maturity momentum: **Stable:** Sector maturity broadly stable within band

Indicators	*What are we seeing?*
Information sharing arrangements	**Limited information sharing among entities** ✓ The engagement of entities in information sharing initiatives is limited across both sectors and at noticeably lower levels than other sectors assessed. ✓ Entities in the waste water sector report lower levels of engagement than their drinking water peers. ✓ National authorities say efforts are made at the level of authorities to engage with other sectors through information exchange and participation in joint initiatives.
Structured collaboration mechanisms	**Lack of EU-level structured collaboration mechanism** ✓ Neither sector benefits from the existence of EU-level structured mechanisms that bring entities or authorities together for discussion on topics of cyber relevance (e.g. ISACs, workstreams, expert groups, conferences).

Operational preparedness

Drinking water		Waste Water	
Overall maturity level: High / **Moderate** / Low	Maturity momentum: **Stable:** Sector maturity broadly stable within band	Overall maturity level: High / Moderate / **Low**	Maturity momentum: **Stable:** Sector maturity broadly stable within band

Indicators	*What are we seeing?*
Prevention	**Effectiveness of controls is weakly validated** ✓ Across both sectors, most entities report that they either do not assess the effectiveness of the controls they have implemented or when they do, the scope of their assessments is limited. ✓ The issue is more prevalent among entities in the waste water sector.
Detection	**Readiness to prevent or detect attacks remains low** ✓ Nearly two in three entities surveyed suggest they are not running cybersecurity training and awareness raising initiatives for their employees or management – thus limiting the potential of their staff to prevent or at least detect attacks. ✓ Roughly one in two entities across both sectors report focusing primarily on preventive rather than detection controls. ✓ Where detection controls are implemented, those are often selectively deployed, resulting in inconsistent visibility across assets.
Response & Recovery	**Response and recovery are mostly reactive**

	✓ Across both sectors, readiness to respond to and recover from incidents is limited, although entities in the drinking water sector report relatively higher confidence in their readiness to deal with specific scenarios, than entities in the waste water sector. ✓ Roughly one in three entities across both sectors report they either do not have or have never tested their incident response arrangements, whereas more than half state that they only test in a limited way or reactively (after incidents). ✓ Similarly, nearly one in two entities across both sectors do not have or have never tested their BCP/DR arrangements, whereas a notable proportion suggest they only test limitedly or reactively. ✓ National authorities corroborate these views, suggesting preparedness testing is often absent. ✓ Participation in national or EU-level cybersecurity exercises remains rare.

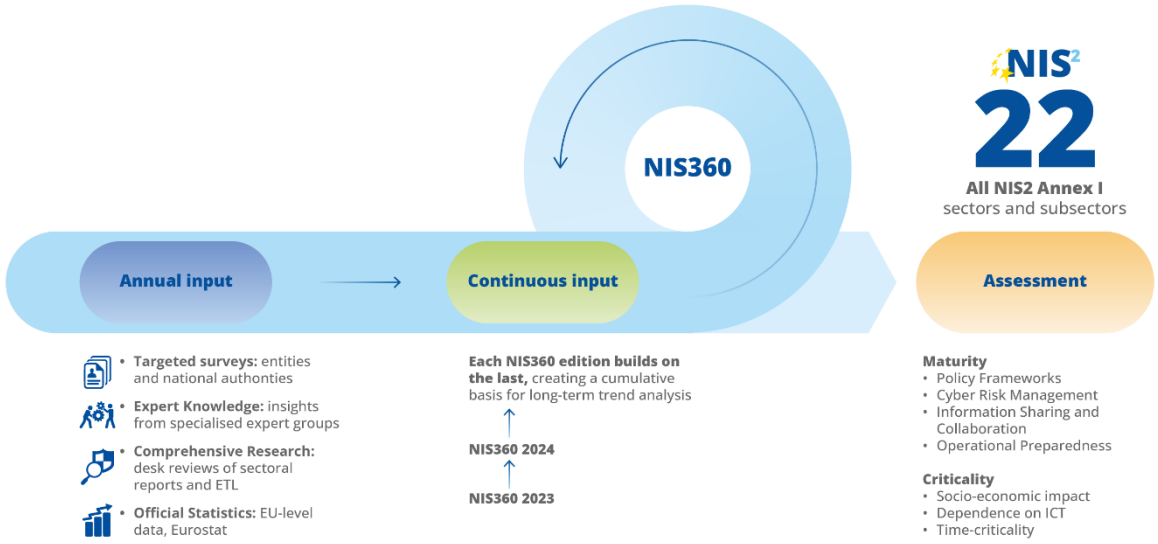
B Annex: NIS360 methodology

This Annex outlines the methodology used to **assess sector maturity and criticality**.

This year marks the **third edition of NIS360**, focusing on where each of the 22 sectors and subsectors of high criticality under NIS2 directive, stand in terms of maturity, criticality and year-on-year progress[99]. The first edition was not formally published in 2023 but was presented to Member States and received positive feedback, which led to the continuation and publication of subsequent editions.

Although the NIS360 is an **annual assessment**, it builds on the foundation established by ENISA's previous assessments, providing a stable baseline for comparison over time. Each year, new evidence is collected through surveys, reports, and other sources to support the assessment, identify material developments, and evaluate whether progress has been made across sectors. The methodology also takes into consideration other factors, such as the threat landscape or market pressures, that may influence behaviours shaping cybersecurity practices. Figure 4 illustrates this continuous cycle.

Figure 4. NIS360 maturity and criticality assessment cycle



Unlike other tools for assessing cybersecurity maturity that focus mainly on individual companies, NIS360 assesses the maturity of the entire sector ecosystem. In this regard, maturity of a sector under the NIS360 is interpreted as consisting of four parts:

- Legislation and its effectiveness
- Companies and their preparedness

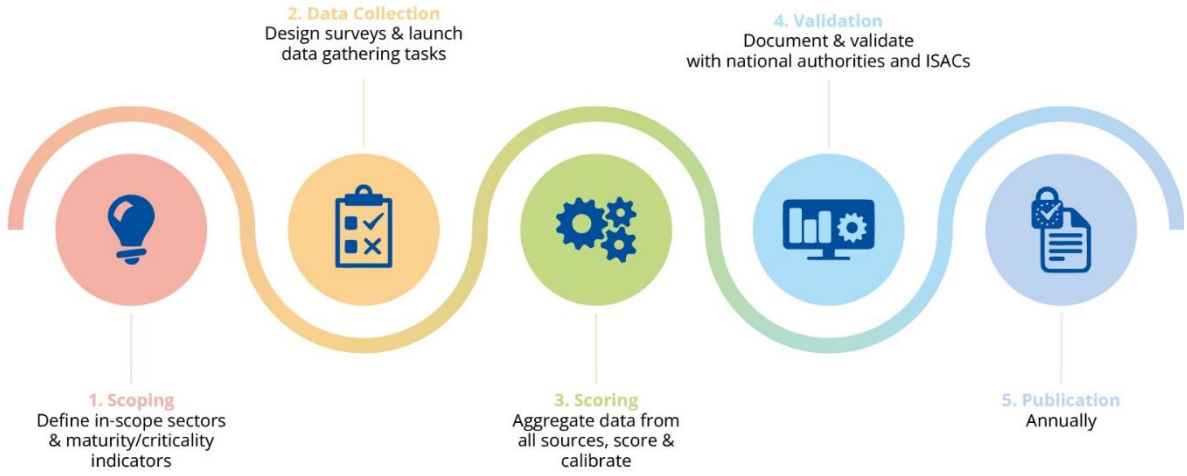
[99] The scope of the NIS360 study has been progressively expanded since its first edition, so that it now covers all sectors and subsectors of high criticality under the NIS2 Directive. Our current efforts are focused on increasing the study's efficiency while ensuring its quality and consistency. A future gradual expansion of the scope of the study is foreseen, subject to resources, capacity and stakeholder engagement.

- Authorities and their institutional capacity[100]
- Sectoral ecosystem structures and their effectiveness

The aim is to provide insights that help Member States and national authorities understand where each sector stands in terms of cybersecurity maturity and criticality, how this has evolved over time, and where gaps and strengths remain. The analysis supports the identification of areas for action, while recognising that observed cybersecurity maturity reflects both the implementation of regulatory requirements and sector-specific operational, technical, and organisational contexts. In addition, the NIS360 may also serve as an evidence-based input to support the selection and prioritisation of sectors for EU actions, including sectoral action plans, sectoral coordinated preparedness testing under Digital Europe Programme calls for proposals, as well as to inform the identification of priority sectors for large-scale cybersecurity exercises, such as Cyber Europe.

The process is structured into distinct phases, each contributing to a comprehensive evaluation of the cybersecurity maturity and criticality of the sectors.

Figure 5. NIS360 assessment phases



1. Scoping

The assessment begins with an initial phase where the indicators to be used for assessing both the maturity and criticality of the sectors are defined. To enable trend analysis over time, a set of core dimensions and indicators are kept consistent across NIS360 editions, while certain indicators are updated annually to reflect evolving threats and practices. For this reason, **structured analytical models are used** each consisting of defined **dimensions and underlying indicators**. These indicators are mapped against specific maturity and criticality dimensions:

Maturity Dimensions

Maturity measures improvements through a combination of indicators, including developments in cybersecurity legislation, the efforts organisations make towards strengthening their cybersecurity risk management, resilience and preparedness, and the capacity of authorities to support the sector. In other

[100] It is clarified that the assessment of authorities' institutional capacity is intended to support national authorities' own understanding of maturity gaps within their sector, and does not constitute a supervisory or compliance assessment of national competent authorities.

words, it seeks to assess how effectively and consistently the sector manages cybersecurity risks and capabilities over time (overall preparedness of the sector) using several dimensions.

- **Policy framework and guidance**. We evaluate the maturity and effectiveness of the policy and legislative framework for the sector. Key aspects considered are the legislative framework driving cybersecurity objectives, the availability and the extent to which guidance is accessible and facilitates compliance. However, the effectiveness of legislation is not determined by the number of rules, but by their coherence and practical impact. In addition, this dimension takes into consideration the institutional setup at EU-level, the existence and experience of national authorities,

- **Risk management and good practices**. We assess the level of understanding of cyber risks and steps taken towards their mitigation by sector entities, national authorities, and at the EU level. Key aspects considered are risk identification, risk management practices and security measures adopted by entities, the perceived effectiveness of these practices as assessed by their supervisory authorities, and the role of EU-level initiatives promoting risk management and good practices.

- **Collaboration and information sharing**. We evaluate the level of collaboration and information sharing within the sector i.e. between entities, between entities and authorities, and among authorities at national and EU level. This includes evaluating the practices adopted by sector entities and national authorities, as well as the existence of EU-level initiatives encouraging collaboration and information sharing.

- **Operational preparedness**. We assess key indicators such as the practices entities adopt to build and test preparedness, including threat detection, security assessments, incident response testing, business continuity planning, as well as the preparedness levels as evaluated by supervisory authorities.

Criticality Dimensions

The criticality dimension, is assessed at the macro (socio-economic) level, taking into account the overall impact of sector disruptions on daily life (e.g. access to critical online services), as well as their effects on economic activity (e.g. halted operations, supply chain disruptions). These effects are considered both within the sector and across sectors, reflecting cross-sector interdependencies and cascading impacts.

- **Socio-economic impact of significant incidents**. We examine the sector's potential socio-economic impact in the event of a significant incident. This considers its economic footprint across the EU (e.g. employment figures, number of enterprises) where available, impact of previous incidents[101] and the availability of alternatives to the sector's services.

- **Dependency on ICT**. We evaluate the reliance of sector entities on ICT systems for their core functions and operations, also taking into account the interdependencies between the sector and other sectors.

- **Time Criticality**. We assess how quickly the impact of a significant incident affecting the sector would be felt in society and the economy and/or the impact on other sectors, taking into account the existence of alternatives and the time sensitivity of the sector’s operations.

[101] It is noted that ENISA does not solely rely on incident figures to assess criticality, in recognition of the fact that such figures oftentimes include confirmed, alleged, and de-bunked events that do not necessarily provide a direct measure of realised compromise.

2. Data collection

The next phase involves designing and conducting surveys, performing desk research, and consulting with experts to collect the qualitative and quantitative data necessary for the assessment.

The report integrates three complementary perspectives:

- **Entity input**, collected through targeted questions designed to capture the perspectives of public and private sector organisations on their cybersecurity maturity, and discussed with expert groups through dedicated workshops;
- **National authority input**, captured via a dedicated survey that reflects supervisory perspectives on sectorial maturity and resilience;
- **EU-level input**, including ENISA insights into sector-wide progress and challenges, sectorial threat landscape and reported incidents; and data gathered from sources such as Eurostat.

Data is collected via an online platform using two structured questionnaires, designed to assess cybersecurity maturity by combining insights from the private sector with perspectives from national authorities. For instance, in 2025, surveys were more granular and closely aligned with NIS2 security requirements and measures, providing a more standardised and comparable dataset.

The survey was conducted from June to October 2025.

This report focused on organisations from all high-criticality sectors and subsectors identified under the Annex I of the NIS2 directive, a total of 22. However, it is important to mention that the sector definitions are not always fully aligned with the NIS2 directive for several reasons:

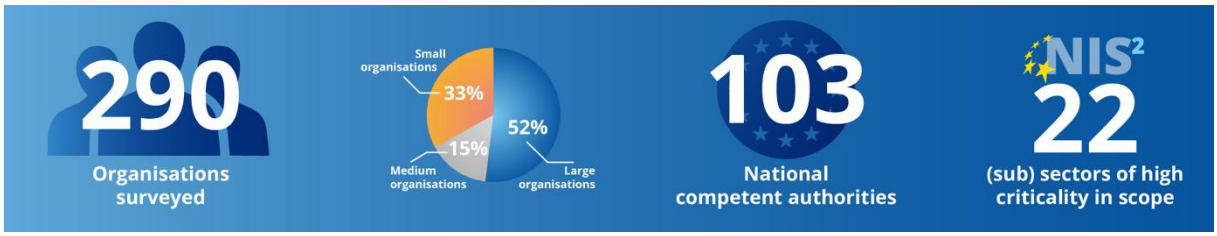
- First, participation in the survey is voluntary, so entities self-identifying with a sector are included in that sector's assessment but this cannot be independently verified.
- In addition, some sectors, such as the automotive sector, have requested to be added in the NIS360 assessment under the road transport sector. While under the NIS2 directive, the automotive industry is part of the manufacturing sector, it is often considered by the industry itself as part of road transport. In addition, given the close link between ITS systems in road transport and automated vehicles, the automotive industry was therefore included in the NIS360 assessment under road transport.

As a result, the NIS360 interprets sector definitions in a broader way, covering the following:

- Energy: electricity, district heating and cooling, oil, gas, hydrogen
- Transport: aviation, railway, maritime, road, including automotive
- Finance: banking, financial market infrastructures (FMIs)
- Health
- Drinking and Waste water
- Digital infrastructure: core internet[102], cloud and data centres, telecoms, trust services
- ICT service management
- Public administrations
- Space

[102] The term is used to collectively refer to the following categories of entities per NIS2 directive, Annex I: Internet Exchange Point (IXP) providers, Domain Name System (DNS) service providers excluding operators of root name servers, top-level domain (TLD) name registries, and content delivery network (CDN) providers.

In 2025, around 300 companies from 25 Member States and 100 national authorities responded to the survey. It reflects a diverse set of entities of **different sizes drawn from several Member States**, which is sufficient to assess sector-level maturity trends and patterns across the EU.



Participation by companies and authorities is voluntary, so the composition and size of the sample naturally vary from year to year and are expected to continue to do so. To reduce the impact of these variations, the following actions are taken.

- A structured analytical model and a continuous assessment approach is used and supported by a solid base of data built up over several years and updated annually with new evidence, where the data collected each year serves as evidence to confirm existing patterns.
- NIS360 surveys are carefully designed to ensure that the data collected every year remains comparable and reflects overall patterns. As a result, the findings are not highly sensitive to variations in the sample.
- Data reliability was assessed using statistical methods, such as 95% confidence intervals, which indicate the precision of the reported averages. This approach is appropriate because individual scores are normally distributed, independent, and show limited variation.
- Consultations and desk research are conducted in parallel.

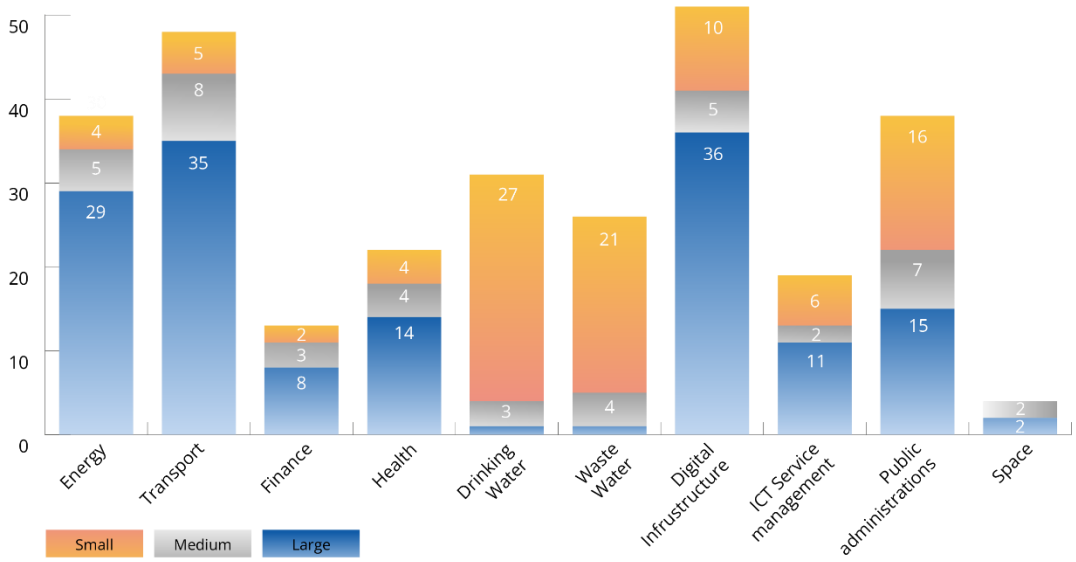
For instance, to avoid data bias, two subsectors, such as hydrogen and district heating, were not assessed due to very few responses, and their maturity scores were maintained at the same level. However, consultations with the experts from the sectors were conducted to confirm the results.

Organisations within the scope of the NIS2 directive are mainly medium and large entities, so our assessment of sector maturity focuses on these companies. This approach ensures that maturity assessment reflects the practices and experiences of entities with the most complex operations, interdependencies, and cybersecurity requirements. Typically, those are the companies facing higher risk and holding greater systemic importance within their sectors. These organisations are often critical to the functioning of the economy and society, making their cybersecurity maturity, resilience and preparedness key indicators of sectoral maturity.

However, in certain sectors or cases as determined by the NIS2 directive, the rules also apply to entities of all sizes, including small ones. Their inclusion in the maturity assessment is therefore necessary for a complete picture, as the NIS2 directive recognises that SMEs are increasingly targeted through supply chain attacks due to less mature cybersecurity practices and limited resources, which can have cascading effects on larger entities.

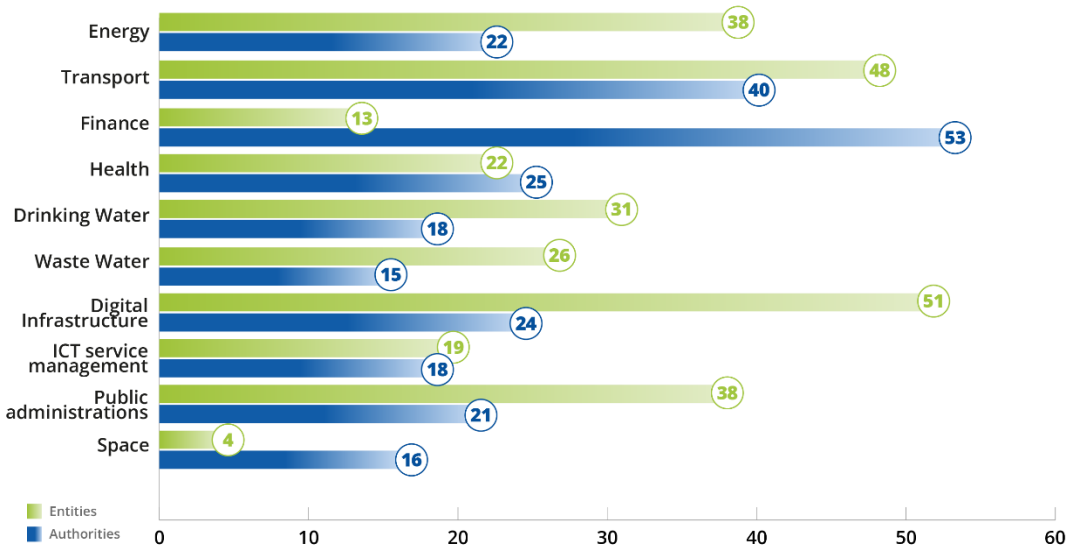
In parallel, responses received in 2025 show that some sectors, such as public administrations and drinking and waste water, naturally have a higher proportion of smaller organisations. In addition, around one third of ICT service management companies participating in the NIS360 survey are small entities, demonstrating that small companies are a notable component of this sector's overall structure. These entities were therefore taken into account in the maturity assessment to broaden our understanding of cybersecurity practices across a wider range of organisational types, highlighting differences in approach, resources and risk exposure.

Figure 6. Organisations by size represented in 2025 ENISA NIS360 survey



In addition, it is important to note, that **entity-level responses are complemented by input from national authorities**. As authorities typically oversee multiple entities at national level, their participation broadens geographic coverage and strengthens the EU-wide perspective of the assessment, even where entity participation is uneven across Member States. Figure 7 demonstrates that several sectors, such as finance and space, were assessed with stronger participation from authorities, helping to corroborate the views of organisations and provide a more balanced assessment.

Figure 7. Sectors represented in 2025 ENISA NIS360 survey



3. Scoring

This phase revolves around the aggregation of data previously collected, its mapping to defined indicators using a structured scoring algorithm, and conducting post-scoring analysis to identify sectors falling within the risk zone.

- **Data aggregation.** The collected data is analysed to identify key insights and scores are assigned based on these findings using a scoring algorithm to ensure consistency in the evaluation process. This phase provides the foundation for understanding the maturity and criticality of the sectors assessed.

- **Scoring.** The scoring algorithm plays a crucial role in ensuring a structured and comparable evaluation of the data. Each maturity and criticality dimension is assessed through a series of indicators identified during the initial phase of the NIS360 methodology. For each indicator, a corresponding data source is identified and a scoring algorithm is specified that defines how the collected data will be translated to a score. The algorithm ensures the scoring process is consistent across all indicators - and all sectors assessed - and that each sector is assessed based on a standardised framework that allows for comparisons and insights into the maturity and criticality of sectors under review.

- **Calibration.** This becomes necessary when biases or significant variations are observed among different sources of assessment e.g. evaluations by authorities or observable sector performance metrics at the EU-level.

  These variations typically stem from two primary sources.

  - **Assessment perspective gaps**

    - Inherent biases in self-assessment, stemming from different perspectives, the Dunning-Kruger Effect,
    - Varying interpretations of maturity/criticality criteria,
    - Possible effects of survey fatigue on response consistency.

  - **Variations in contextual understanding**

    - Limited knowledge of the cross-sectoral context,
    - Incomplete understanding of sector-specific challenges,
    - Varying levels of sector expertise among respondents.

  To address these issues, a calibration element is included in the scoring algorithm to allow for the adjustments necessary to allow for cross-sectoral comparability despite disparate assessment perspectives, taking into account sector-specific contextual factors.

  The ultimate goal is to achieve a state where initial assessments are naturally aligned, rendering calibration unnecessary. To progress towards this, we aim to continually refine survey questions, raise awareness and foster a shared understanding among stakeholders. Until then, this structured calibration process remains essential to ensure a fair and accurate representation of reality.

- **Post-scoring analysis**. To derive conclusions after the scores are assigned, each sector is examined individually – but also in comparison to all the others both in the context of the subsectors of a specific sector, but also across the board, positioning all sectors on the

NIS360 quadrant. This step goes beyond simply categorising sectors as having 'low', 'moderate' or 'high' maturity or criticality.

Combining and jointly interpreting the criticality and maturity dimensions helps identify areas where mismatches exist between criticality and maturity and thus define a risk zone. The risk zone includes sectors with lower-than-average maturity and criticality that exceeds their maturity. Determining the **risk zone** helps prioritise sectors that require immediate attention. Unlike sectors in the upper half of the maturity dimension, which, regardless of criticality, are progressing well and are better equipped to manage challenges, sectors in the 'risk zone' have lower maturity levels by comparison, indicating significant gaps that may require additional supports to address.

4. Validation

The pre-validation phase involves consulting a group of experts from various sectors to review and provide feedback specifically on the results and sector-specific recommendations from the perspective of the private sector.

The subsequent validation phase focuses on documenting the outcomes of the assessment and reviewing them with stakeholders from the NIS Cooperation Group and EU-ISACs, refining the results as necessary.

5. Publication

The final phase focuses on the activities relevant to the publication of the report presenting the outcomes of the annual NIS360 assessment.

C Annex: Abbreviations and key legislation

Acronyms and abbreviations

BCP/DR – Business continuity plan and disaster recovery
BYOD – Bring your own device
CDN – Content delivery network providers
CERT - Computer emergency response team
CSIRT – Computer Security Incident Response Team
COTS - Commercial-off-the-shelf components
DNS – Domain name system service providers
DSO – Distribution system operator
FMIs – Financial market infrastructures
ICS – Industrial Control Systems
IIoT – Industrial Internet of things
IoT – Internet of things
IoMT – Internet of medical things
IT – Information technology
IXP – Exchange point providers
LNG – Liquefied natural gas
MSPs – Managed service providers
MSSPs – Managed security service providers
NIS CG – NIS cooperation group
OT – operational technology
TLD – Top-level domain name registries
TSO – Transmission system operator
V2I – Vehicle-to-infrastructure

List of legal acts

NIS2 directive – Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union[103]

Commission Implementing Regulation (EU) 2024/2690 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements for cybersecurity risk management measures and further specification of cases in which an incident is considered significant[104]

ENISA NIS2 Technical Implementation Guidance[105]

AI act – Artificial intelligence act – Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence[106]

CER directive – Critical entities resilience directive - Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities[107]

CRA – Cyber resilience act - Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements[108]

Cyber Solidarity Act - Regulation (EU) 2025/38 of the European Parliament and of the Council on measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694[109]

DORA – Digital Operational Resilience Act – Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector[110]

EECC – Electronic Communications Code - Directive (EU) 2018/1972 of the European Parliament and of the Council establishing the European Electronic Communications Code (recast)[111]

eIDAS regulation – Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market[112]

Guidelines on the resilience of critical entities – Communication from the Commission on the resilience of critical entities C/2025/4990[113]

NCCS – Network Code on Cybersecurity – Commission Delegated Regulation (EU) 2024/1366 establishing a network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows[114]

EU ports strategy – Communication from the Commission on EU ports strategy COM (2026) 112 final[115]

Part-IS – Easy Access Rules for Information Security (Regulations (EU) 2023/203 and 2022/1645)[116]

[103] Directive - 2022/2555 - EN - EUR-Lex (date accessed May 2026)
[104] Implementing regulation - EU - 2024/2690 - EN - EUR-Lex (date accessed May 2026)
[105] NIS2 Technical Implementation Guidance | ENISA (date accessed May 2026)
[106] Regulation - EU - 2024/1689 - EN - EUR-Lex (date accessed May 2026)
[107] Directive - 2022/2557 - EN - CER - EUR-Lex (date accessed May 2026)
[108] Regulation - 2024/2847 - EN - EUR-Lex (date accessed May 2026)
[109] Regulation - EU - 2025/38 - EN - EUR-Lex (date accessed May 2026)
[110] Regulation - 2022/2554 - EN - DORA - EUR-Lex (date accessed May 2026)
[111] Directive - 2018/1972 - EN - eecc - EUR-Lex (date accessed May 2026)
[112] Regulation - 910/2014 - EN - e-IDAS - EUR-Lex and consolidated version: EUR-Lex - 02014R0910-20241018 - EN - EUR-Lex (date accessed May 2026)
[113] EUR-Lex - 52025XC04990 - EN - EUR-Lex (date accessed May 2026)
[114] Delegated regulation - EU - 2024/1366 - EN - EUR-Lex (date accessed May 2026)
[115] EUR-Lex - 52026DC0112 - EN - EUR-Lex (date accessed May 2026)
[116] Easy Access Rules for Information Security (Regulations (EU) 2023/203 and 2022/1645) - Revision from December 2025 — Available in PDF, online, and XML format | EASA (date accessed May 2026)

AVSEC – Commission Implementing Regulation (EU) 2019/1583 laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity measures[117]

UN regulation No 155 – Uniform provisions concerning the approval of vehicles with regards to cybersecurity and cybersecurity management system [2021/387][118]

ISO/SAE 21434 – Road vehicles — Cybersecurity engineering[119]

EHAP – European Health Action Plan – Communication from the Commission on European action plan on the cybersecurity of hospitals and healthcare providers[120]

MDR - Medical Devices Regulation – Regulation (EU) 2017/745 of the European Parliament and of the Council on medical devices [121]

EHDS - European Health Data Space - Regulation (EU) 2025/327 of the European Parliament and of the Council on the European Health Data Space[122]

[117] Implementing regulation - 2019/1583 - EN - EUR-Lex (date accessed May 2026)
[118] EUR-Lex - 42021X0387 - EN - EUR-Lex (date accessed May 2026)
[119] ISO/SAE 21434:2021 - Road vehicles — Cybersecurity engineering (date accessed May 2026)
[120] ehealth_com_2025-10_act_en.pdf (date accessed May 2026)
[121] Regulation - 2017/745 - EN - Medical Device Regulation - EUR-Lex (date accessed May 2026)
[122] Regulation - EU - 2025/327 - EN - EUR-Lex (date accessed May 2026)

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
Agamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union