EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA NIS360 2024

ENISA Cybersecurity Maturity & Criticality Assessment of NIS2 sectors

FEBRUARY 2025

ABOUT ENISA

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

CONTACT

To contact the authors, please use enisa-nis-directive@enisa.europa.eu.
For media inquiries about this report, please use press@enisa.europa.eu

ACKNOWLEDGEMENTS

We would like to express our gratitude to the NIS Cooperation Group members, sectorial workstreams and stakeholders who provided valuable insights and data for this report. Special thanks to European Commission DG CNECT, EASA, ERA, EMSA, EBA, ESMA, EIOPA, ENTSOG, AVSEC, ECASEC, LANDSEC, MARSEC, EE-ISAC, EH-ISAC, FI-ISAC, TLD ISAC, EU Space ISAC, ISAC for Cities, Auto-ISAC EU and EU CISO Forum for Rail.

AUTHORS

Marnix Dekker, Jurgita Skritaite, Eleni Philippou, Rossen Naydenov, ENISA

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-687-3, DOI: 10.2824/1378797, Catalogue nr. TP-01-25-002-EN-N

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The NIS360 is a new ENISA product that assesses the maturity and criticality of sectors of high criticality under the NIS2 Directive, providing both a comparative overview and a more in-depth analysis of each sector. The NIS360 is designed to assist Member States and national authorities in identifying gaps and prioritising resources. Our analysis is based on data from national authorities with a horizontal or sectorial mandate, data from companies within the in-scope sectors, and insights from EU-level sources such as Eurostat. Key findings include:

- Three sectors stand out above the rest in terms of overall maturity and criticality: **electricity**, **telecoms**, and **banking**. Over time, these sectors have benefited from significant regulatory oversight, global investments, political focus, and robust public-private partnerships. Their resilience is crucial for societal and economic stability.
- **Digital infrastructures**, including core internet services, trust services, data centres, and cloud services, are among the higher-ranking sectors in terms of maturity and criticality, however they still have challenges to navigate due to their inherent heterogeneity, cross-border nature and the inclusion of previously unregulated entities within their scope.
- Four sectors and two subsectors are in the '**risk zone**': **ICT service management, space, public administrations, maritime, health** and **gas**. These sectors need extra attention to ensure their maturity gaps are addressed in a way that enables them to effectively deal with the added challenges posed by their respective criticality levels.
- The **ICT service management** sector, faces key challenges due to its cross-border nature and diverse entities. Strengthening its resilience is vital and requires close cooperation between authorities, reduced burdens for entities subject to both NIS2 and DORA, and harmonised cross-border supervision.
- The **space** sector faces challenges due to stakeholders' limited cybersecurity knowledge and its heavy reliance on commercial off-the-shelf components. Enhancing its resilience requires better cybersecurity awareness, clear guidelines for pre-integration testing of components, and stronger collaboration with other sectors e.g., telecoms due to the growing convergence of 5G and satellite communications.
- The **public administrations** sector is still in the early days of developing its cybersecurity maturity, lacking the support and experience seen in more mature sectors. Being a prime target for hacktivism and state-nexus operations, it should aim to strengthen its cybersecurity capabilities leveraging the EU Cyber Solidarity Act and explore shared service models among sector entities on common areas e.g., digital wallets.
- The **maritime** sector continues to face challenges with OT and could benefit from tailored cybersecurity risk management guidance that focuses on minimising sector-specific risks, as well as an EU-level cybersecurity exercises to enhance coordination and preparedness in both sectorial and multi-modal crisis management.
- The **health** sector, with an expanded scope, that further decreases its homogeneity, continues to face challenges such as the reliance on complex supply chains, legacy systems, and poorly secured medical devices. Strengthening the sector's resilience across the board, requires the development of practical procurement guidelines to help organisations acquire secure services and products, tailored guidance to help overcome common issues e.g., gaps in basic cyber hygiene, and staff awareness campaigns.
- The **gas** sector, needs to continue working towards developing its incident readiness and response capabilities, through the development and testing of incident response plans at national and EU levels but also through enhanced collaboration with the electricity and manufacturing sectors.

Overall, all sectors covered by the NIS360 face challenges in building their maturity and meeting NIS2 requirements. To better support them, stronger collaboration within and across sectors is recommended, along with sector-specific guidance on implementing cyber risk management measures. Upskilling and reskilling national authorities could be key to a more harmonised NIS2 implementation, while cross-border cybersecurity exercises could enhance crisis response and help mitigate the cascading effects of cyber incidents.

1. INTRODUCTION

The NIS2 Directive[1] covers a wide range of sectors, each with its own challenges and cybersecurity needs. To allow for more effective prioritisation and a clear understanding of these needs, in 2023 ENISA developed the NIS360 methodology[2], to assess, on an annual basis, the **cybersecurity maturity** and **criticality of** these **sectors from a Union-wide perspective**.

This report presents the outcomes of the **2024 NIS360 study**, which now covers all highly critical sectors under NIS2[3]. The study integrates three complementary perspectives:

- **Industry input**, gathered through targeted questions aimed at capturing entity perspectives on their cybersecurity maturity, as part of a broader annual survey launched by ENISA4.
- **National authority input**, captured via a dedicated survey that reflects supervisory perspectives on sectorial maturity and resilience.
- **EU-level inputs**, including ENISA insights into sector-wide progress and challenges, sectorial threat landscape and reported incidents; and data gathered from sources such as Eurostat.

1.1 GOAL AND TARGET AUDIENCE

This report offers both a **cross-sectoral** overview and a detailed **sector-by-sector** analysis of the criticality and maturity of assessed sectors. Building on the insights gathered, it highlights the *strengths of* and *challenges faced by* each sector assessed, identifies discrepancies in maturity perceptions, and provides a clear view of the *impact of cybersecurity policy* implementation on sectorial maturity and resilience across the EU. The goal of this report is to support sectorial stakeholders by enabling prioritisation, highlighting areas for improvement, and facilitating the tracking of sector progress over time. It aims to achieve this by providing input to the:

- **ENISA NIS Strategy:** ENISA developed a strategy to support the EU Member States with the implementation of the NIS Directive, balancing horizontal and sectorial activities. The NIS360 provides input to this strategy.
- **Authorities cooperating at EU-level**: The NIS360 aims to inform the NIS CG's prioritisation and planning of future work in support of sectorial implementation of cybersecurity policy, including **union-wide risk evaluations** and **stress testing**.
- **Authorities at MS-level:** The NIS360 aims to inform national authorities' prioritisation and planning of future work in support of sectorial implementation of cybersecurity policy.
- **Biennial report on the state of cybersecurity in the Union.** The NIS360 study provides input to the biennial report on the state of cybersecurity in the union and ensuing policy recommendations.

[1] DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive) - https://eur-lex.europa.eu/eli/dir/2022/2555
[2] Initially designed and piloted in 2023 across a limited number of sectors, the ENISA NIS360 methodology has since been refined and was applied in full for the first time, in 2024.
[3] The 2024 NIS360 study focuses on sectors of high criticality as defined in DIRECTIVE (EU) 2022/2555 – Annex I, unless otherwise specified. Future iterations of this study—once the current framework has been standardised—could potentially expand to include Annex II sectors. However, such an expansion is not planned in the near term.
[4] NIS investments 2024

1.2 SCOPE AND METHODOLOGY

In scope of the 2024 NIS360 study, were the following 22 (sub)sectors identified as highly critical under the NIS2 Directive (Annex I):

- Energy: electricity, district heating and cooling, oil, gas, hydrogen
- Transport: aviation, railway, maritime, road
- Finance: banking, financial market infrastructures (FMIs)
- Health
- Drinking and waste water
- Digital infrastructure: core internet[5], cloud and data centres, telecoms, trust services
- ICT service management
- Public administrations
- Space

The cybersecurity maturity and criticality of each of the above sectors were assessed against defined **maturity and criticality dimensions**, in accordance with the NIS360 methodology detailed in Annex 3.ANNEX A The assessment draws from insights gathered from:

- **the industry (i.e., companies across the EU) –** via dedicated qualitative and closed quantitative questions included in a large-scale double-blind survey run as part of a broader study run by ENISA aimed at understanding how cybersecurity policy influences entity decisions across the Union. *Notably, the survey focused on sectors rather than subsectors and predominantly included large organisations, with 93% of respondents being large enterprises.*
- **national authorities (supporting/supervising the sectors across the EU) –** via a dedicated survey including both qualitative and quantitative questions aimed at understanding the current state of each sector's cybersecurity maturity and criticality from a supervisory perspective. *Notably, some authorities were newly appointed under the NIS2 Directive and may not have had full visibility or in-depth knowledge of the sector.*
- **EU-level inputs** – via consultation with ENISA experts directly supporting NIS2 sectors at EU-level; from relevant ENISA work including sectorial threat landscapes, bimonthly SITAW[6] reports and CIRAS[7] reported incidents – but also via consultation of relevant Eurostat datasets pertaining to the sectors under evaluation.

Each sector's performance against the defined maturity and criticality dimensions is assessed through a series of indicators. 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 use of the algorithm aims to ensure that each sector is assessed based on a standardised framework that allows for comparisons among the sectors – where necessary this incorporated a calibration to enable cross-sectoral comparability or to account for sector-specific context.

Once scores are assigned per sector, post-scoring analysis take place to identify what the NIS360 methodology describes as '**risk zone'** sectors. These are the sectors that rank comparatively lower than others in terms of maturity, but have a criticality score that is higher than their maturity score. Identifying the 'risk zone' enables prioritisation. Sectors outside the

[5] 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.
[6] Situational awareness (SITAW) reports compiled by ENISA gathering, analysing and interpreting information about cyber threats, vulnerabilities, incidents etc. of relevance to a particular sector on a bimonthly basis.
[7] CIRAS, the Cybersecurity Incident Reporting and Analysis System, is maintained by ENISA to support member states in submitting incident reports – CIRAS is available here: https://ciras.enisa.europa.eu/ciras-visual

risk zone are either on track to developing maturity in line with their criticality, or not yet at a stage where cybersecurity risks pose a significant threat to their core operations.

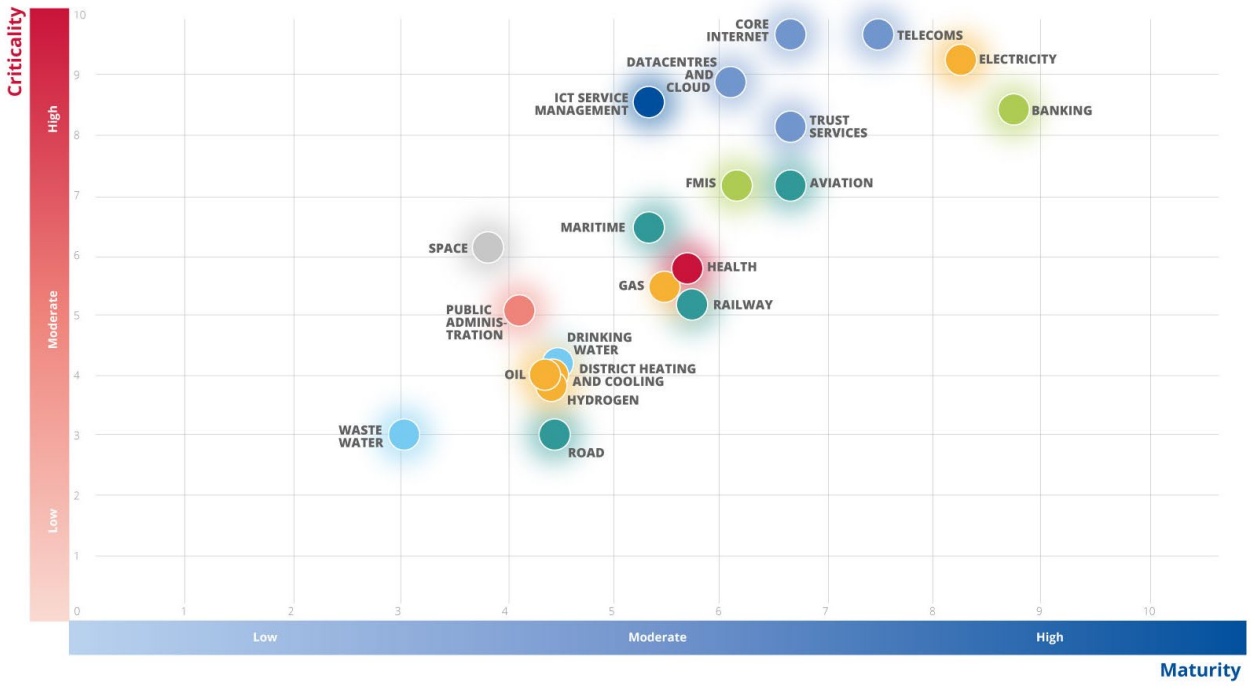
Following the analysis, key observations were documented and shared with national authorities through the NIS Cooperation Group (NISCG) and with entities via the EU Information Sharing and Analysis Centres (EU-ISACs) for **validation**.

1.3 DISCLAIMER

This study provides an EU-wide perspective on sectorial 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.

2. SECTOR MATURITY & CRITICALITY OVERVIEW

ENISA NIS360 Quadrant



2.1 MATURITY OVERVIEW

Three sectors stand out above the rest: **electricity**, **telecoms**, and **banking**. These sectors form the foundation of a resilient and interconnected economy, ensuring stability, connectivity and financial security. Over time, these sectors have benefited from significant regulatory oversight, global investments, political focus, and robust public-private partnerships, enabling them to achieve a higher level of maturity.

Digital infrastructure sectors, such as **core internet, trust services, data centre** and **cloud services**, are also among the higher-ranking sectors in terms of maturity. These sectors provide foundational support for other industries, serving as the backbone for communication, connectivity, and data services. Given that digital is their primary domain of service, it is perhaps unsurprising that these sectors score highly in certain of the cybersecurity maturity areas assessed. That said, these sectors are also faced with several challenges when it comes to aligning with NIS2 requirements, stemming from their inherent heterogeneity (for instance, the SaaS subsector includes both SMEs and some of the world's largest companies) and their cross-border nature. Additionally, the inclusion of previously unregulated entities in scope presents a dual challenge: the requirements are entirely new for these companies, and national authorities are often unfamiliar with the market they are now required to oversee.

The **ICT service management** sector, while sharing some similarities with digital infrastructure –particularly given MSPs and MSSPs operate primarily in the digital domain to support entities with technology and cybersecurity - has a distinct maturity profile. The sector is assessed at moderate maturity, but ranks notably lower than the rest of the digital-by-default sectors. As a newly regulated sector under NIS2, the ICT service management sector faces several

challenges, particularly the lack of standardised processes, consistency and resources to keep pace with the growing complexity of supporting digital operations across other sectors. This is compounded by the lack of familiarity with the sector among the authorities responsible for its oversight, the presence of cross-border players within the market, and the weak collaboration among them with implications on both the entities themselves but also others relying on them.

The **space sector** presents an even more distinct challenge. Despite its role in enabling global connectivity—facilitating data transmission, internet access, television broadcasting, navigation, and real-time communication— it falls just within the "moderate" maturity range and ranks among the lowest compared to other sectors in terms of maturity. As a newly regulated sector under NIS2, it is still in the early stages of aligning with the directive's requirements which present challenges for both entities and national authorities responsible for sector oversight. The sector's heavy reliance on supply chains and commercial off-the-shelf products, combined with its limited investment in cybersecurity, further exacerbate these challenges. At the same time, collaboration and information sharing within the sector remain nascent despite the establishment of the EU Space ISAC in 2024. Recent advancements, such as Eutelsat's 5G Non-Terrestrial Network (NTN) trial with low Earth orbit satellites[8], demonstrate the potential for satellite-based 5G services, especially in remote areas. However, these advancements highlight the need for stronger cybersecurity measures and improved cooperation both within the sector and across other sectors, like telecommunications.

A similarly diverse landscape emerges when analysing the maturity levels of subsectors within specific EU sectors. In the **energy sector**, the **electricity** subsector demonstrates high maturity, ranking among the top tier of all assessed sectors, while **gas** shows moderate maturity, and ranks closer to the middle. In contrast, **district heating and cooling, hydrogen,** and **oil** lag significantly, ranking in the low end of maturity among all sectors assessed. The transport sector shows similar variation, with **aviation** ranking in the top tier for maturity, **railway** and **maritime** falling closer to the middle, and **road** having a notably lower score. Within the finance sector, **banking** exhibits higher maturity than **FMIs**, though both rank high when compared to other subsectors. Finally, in the Water sector, **drinking water** demonstrates higher maturity than **waste water** with both sectors' scores being on the lower end of the maturity scores ranking.

The discrepancies among subsectors can be attributed to several key factors including but not limited to differences in:

- **cybersecurity policy frameworks** whereby one subsector may be subject to comprehensive policy frameworks than others e.g., **electricity** stands to benefit from the Network Code on Cybersecurity[9] and its targeted guidance towards enhancing the sector's cyber resilience.
- **the level of support and oversight provided to sector entities** whereby entities in certain subsectors receive significantly more support and guidance than those in others. For example, **aviation** entities benefit from robust backing by EASA at the EU level and experienced authorities at the national level, whereas **road** entities lack comparable support structures. Similarly, **banking** institutions have undergone EU-wide stress tests conducted by the ECB to assess the adequacy of their risk and incident management arrangements, while **FMIs** have not participated in equivalent exercises.
- **political attention** whereby specific subsectors within a sector may receive greater political focus than others. In 2024, for example, **electricity** and **gas** received more focus than the remaining energy subsectors which in turn translated to targeted actions such as a Union-wide risk assessment and Cyber Europe 2024 focusing on them.

[8] Eutelsat OneWeb
[9] Delegated regulation - EU - 2024/1366 - EN - EUR-Lex

The **health sector** sits at upper end of the “moderate” maturity range and mid-level across all maturity rankings. Under NIS2, the sector’s scope has been expanded substantially, adding complexity to an already highly heterogeneous sector (consisted of larger entities that typically demonstrate stronger cybersecurity postures, and smaller entities that often struggle even with basic cyber hygiene). The sector faces several key challenges. One of the most pressing is the disparity in understanding among sector entities of cyber risks facing them - with larger ones having a better grasp and thus more robust measures to deal with risks - than smaller ones. The sector's fragmented nature and inadequate understanding of the cyber risks facing it further complicates things. Additionally, the sector’s reliance on complex supply chains as well as its dependence on legacy systems and inadequately secured medical devices, further exacerbates the situation. Finally, operational preparedness levels are also inconsistent across the sector with gaps also highlighted during the Cyber Europe 2022 exercise.

The **public administration** sector is among the least mature sectors assessed despite its role in ensuring the effective governance and delivery of services to society. Newly regulated under the NIS2 directive, the sector is still very much in the early stages of aligning with its requirements and lacks the well-established support and experience seen in more mature sectors. At the EU level, there is no comprehensive, sector-wide understanding of the risks facing public administration and still not a clear understanding of what is in scope of the sector, common assets, and threats it faces, further complicating effective risk management practices.

By examining the overall maturity scores of the sectors and the factors that have shaped them, one can observe that sectors with higher maturity levels benefit from:

- more substantial cybersecurity guidance which could include sector-specific legislation, relevant standards, or tailored guidance, while carefully considering the balance between general frameworks and sector-specific requirements;
- stronger oversight and support at EU and national levels from authorities familiar with the sector and its challenges;
- deeper understanding of their sector’s risk landscape which usually leads to the implementation of more effective risk management measures to safeguard their increasingly digitalised infrastructures.
- stronger collaboration and information sharing among all sector stakeholders (entities and authorities) and at all levels (entity, national, EU).
- better developed operational preparedness through well-tested plans exercised at entity, national and EU level.

All sectors assessed under the NIS360 are diverse, meaning that within each sector, there are various types of entities, ranging from highly critical to less critical, and from very large to small. These entities also exhibit varying levels of cybersecurity maturity and cyber risk postures. In general, larger entities tend to have a higher level of cybersecurity maturity, but they are often also more critical to the sector's overall operations.

2.2 CRITICALITY OVERVIEW

The **telecoms, electricity, core internet, and cloud & data centres** are the four most critical sectors for the economy and society. Telecoms, core Internet, and cloud and data centres rely heavily on digital technologies, as it is their primary domain of operations. The electricity sector is heavily dependent on ICT for its operations, particularly Distribution System Operators (DSOs). Incidents in these sectors have immediate and severe impacts. A telecoms disruption would halt emergency services and disrupt sectors like digital payments and online businesses. Disruptions at national TLDs, DNS providers, IXPs, or CDNs would slow internet traffic, affecting businesses and digital services. A cyberattack on a cloud provider could lead to widespread business interruptions and financial losses. Similarly, a power outage would disrupt electronic payments, halt sales and services, and impact telecoms networks, compounding the economic

disruption. These sectors have high time-criticality, with impacts felt almost immediately, severely affecting sectors reliant on digital infrastructure and electricity.

The **ICT service management, trust,** and **finance sectors** are vital to the EU economy, supporting financial stability, digital services, and growth. They form the second group of critical sectors, with ICT service management and trust inherently digital, and finance fully reliant on ICT for operations. The banking sector depends on digital infrastructure for payments and inter-banking services, while financial market infrastructures (FMIs), like stock exchanges and clearing houses, rely on ICT for real-time data, risk management, and trading. A major incident in this sector could halt payments, impacting businesses and individuals. For example, a series of attacks[10] on over 100 financial institutions worldwide led to cumulative losses of over 1 billion euros. Similarly, the 2020 ransomware attack on Cognizant[11], a major MSP provider, impacted sectors like healthcare and banking, causing losses of about €45 million for the company. Disruptions in the trust sector could impact online services reliant on web certificates, triggering spill over effects across sectors requiring offline processes. With high time-criticality, the impact of significant incidents against these sectors is felt quickly, with dependent sectors also being affected.

The **aviation**, **maritime**, and **space** sectors are essential to the EU economy, with air transport handling 13.1% of passenger travel and maritime managing 67.8% of freight, supporting global trade and tourism. The space sector is growing, providing critical services to sectors like transport, finance, and energy, with increasing reliance on satellite systems like 5G-satellite convergence and GPS. All three sectors depend heavily on ICT. Air transport is the most digitally advanced, using systems like EUROCONTROL's System Wide Information Management and sophisticated Air Traffic Management. Maritime faces challenges with outdated technology, while the space sector relies heavily on ICT for most of its core processes. Cyber incidents in these sectors are time-critical (e.g., NotPetya[12]) delays in responding to them may result in wider impacts including on other sectors. In the space sector, disruptions can affect aviation, maritime, and emergency services, all reliant on precise satellite data.

The **health** sector plays an important role in the EU economy, accounting for 7.4 % of businesses, and on average 8.4% of employment, and 6.2% of total business value added[13]. However, its direct cross-sectoral impact is lower compared to other sectors. While it heavily relies on ICT systems, the effects of cyber incidents are typically manageable, with supply chain vulnerabilities amplifying risks. Cyberattacks like ransomware can incur substantial costs (e.g., the 2021 HSE breach[14]) but have minimal impact on the broader economy. Despite this, significant incidents still require a prompt response to avoid disruptions, maintain operations and safeguard sensitive services. Given the high sensitivity of patient health data and the potentially devastating impact of cyberattacks on healthcare services, it is essential to ensure a swift and effective response to cybersecurity incidents in order to protect patient safety and maintain the sector's critical functions.

The **railway, gas** and **public administrations** sectors are moderately important to the economy, with disruptions generally affecting national rather than EU-wide operations. Rail-transferred freight constitutes 5%[15] of the EU market, while the central public administration sector accounts for 2.0% of GDP[16], with nearly half of the population relying on digital public services. The gas sector is interconnected with various industries, including electricity

[10] Mastermind behind EUR 1 billion cyber bank robbery arrested in Spain | Europol
[11] https://www.zdnet.com/article/cognizant-expects-to-lose-between-50m-and-70m-following-ransomware-attack/
[12] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[13] Eurostat
[14] https://en.wikipedia.org/wiki/Health_Service_Executive_ransomware_attack
[15] Eurostat
[16] Eurostat

generation, heating, and manufacturing, which amplifies the potential impact of disruptions. Dependency on ICT is moderate, with ongoing digitisation offset by widespread legacy systems and reliance on suppliers and third parties for updates and maintenance. While a significant incident may cause temporary service suspensions and moderate socio-economic disruptions, long-term damage is unlikely. Cyberattacks can disrupt service availability, but manual backups help mitigate societal impacts, keeping short-term effects manageable. However, a cyberattack in the gas sector could lead to widespread economic consequences. The impact of significant incidents within these sectors is typically felt within hours by the society or other dependent sectors.

Drinking water, district heating, oil, hydrogen, road transport and waste water are the remaining six sectors having lower criticality. Their reduced reliance on digital infrastructure and the availability of alternative solutions helps mitigate the immediate impact of cyber incidents. All these sectors utilise Operational Technology (OT) in varying degrees to control, monitor, and maintain critical infrastructure and operations. However, the complexity and scope of OT systems can vary significantly across them, with sectors like oil and drinking water being more dependent on OT for safety and efficiency than others like road transport or hydrogen. Incidents in these sectors, while often carrying operational and societal consequences[17], are unlikely to cause widespread disruptions or cross-sector spill overs.

The criticality of sectors is evaluated through several key factors: their socio-economic impact, potential to cause disruptions across other sectors, reliance on ICT, and the time-criticality in terms of how long it would take for the impact of the incident to felt within the society/economy or affect other sectors[18]. Overall, sectors with higher socio-economic importance and greater interconnectivity and ICT dependence, such as electricity, telecoms, and finance, typically face more severe consequences in the event of cyber incidents, requiring quicker responses to prevent widespread impact. On the other hand, sectors like drinking water, district heating, oil, hydrogen, road transport, and waste water, although important, tend to be less critical in the immediate aftermath of cyberattacks. These sectors, with their lower reliance on digital infrastructure and available contingency measures, tend to recover more slowly, but without causing long-term disruption or significant cross-sector effects.

2.3 RECOMMENDATIONS

While many sectors face several common challenges in enhancing cybersecurity resilience to meet NIS2 requirements — such as the need for better information sharing, tailored guidance, upskilling and reskilling efforts, and cross-border cybersecurity exercises — this section specifically focuses on providing detailed recommendations for six sectors identified as being in the 'risk zone' of the quadrant[19].

Sectors in the 'risk zone' are those that exhibit lower comparative maturity, but have a criticality score that is higher than their maturity score[20]. These sectors are ICT service management,

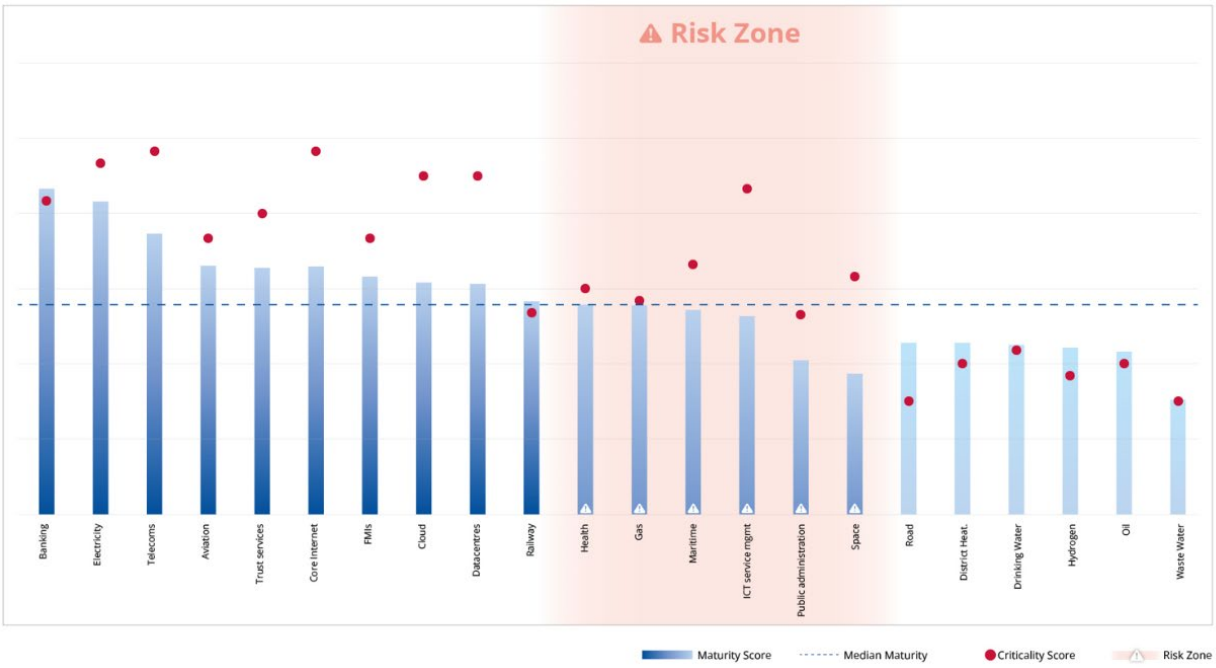
[17] https://danskfjernvarme.dk/aktuelt/nyheder/2022/cyberangreb-blev-wake-up-call-for-naestved-fjernvarme, https://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter.html and https://databreaches.net/2022/08/10/scoop-ista-international-takes-systems-offline-in-wake-of-ransomware-attack-daixin-team-claims-thousands-of-servers-encrypted/

[18] In assessing criticality, these dimensions were evaluated without considering the sector's potential value in more military-relevant contexts. For example, when assessing the criticality of the transport sector, the role of transport infrastructure in facilitating military mobility was not taken into account. While this remains an important consideration, as highlighted in the Action Plan on Military Mobility 2.0 (c3d3067c-6d9a-4f95-9a69-4dd99c340188_en), it falls outside the scope of this assessment.

[19] A larger version of the Risk Zone visual below, can be found in Annex F

[20] Determining the 'risk zone' helps prioritise sectors that require immediate attention. A sector falls into the 'risk zone' if its maturity ranks in the lower end, and its criticality exceeds its maturity. Unlike sectors in the upper end of the maturity rankings—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 support to address. Appendix A, describes the full NIS360 methodology, including how the 'risk zone' is determined.

space, public administrations, maritime, health and gas and could be considered as candidate sectors for coordinated preparedness testing at the Union level[21]. Additionally, further actions are recommended to enhance their cybersecurity maturity.



The **ICT service management sector's** cross-border nature, combined with its critical role in supporting other sectors, heightens its vulnerability to cyberattacks, making it essential to enhance cyber resilience.

- It is crucial to ensure close collaboration between the ICT service management sector's competent authorities (CAs) and those of other sectors, given their interconnectedness. A cyber incident against entities in this sector, can disrupt critical services across multiple sectors. To mitigate such risks, a coordinated approach between CAs is essential, to ensure consistent response efforts across sectors, reducing the cascading impact of cyber threats.
- To ensure consistent application of the DORA and NIS2 frameworks for overlapping ICT service management entities, mapping the cybersecurity requirements from both frameworks will enhance clarity, and minimise redundancy.
- Additionally, aligning the certification scheme for managed security services under the EU Cyber Solidarity Act[22] with the DORA RTS and ITS is essential to maintain consistency and coherence across these regulatory frameworks.
- Cross-border supervision within the ICT service management sector, also governed by frameworks like DORA, should be harmonised to promote best practices, ensure consistent regulatory compliance, and strengthen sector resilience.

The **space sector**, newly included under NIS2, faces challenges due to its reliance on off-the-shelf components and the lack of cybersecurity knowledge among its stakeholders, with only 57% of respondents in our 2024 NIS Investments survey[23], being familiar with the directive. Cyber threats to space systems could impact critical sectors like transport, energy, and finance, underscoring the need to improve cybersecurity maturity to match its critical role.

- Launch a NIS2 knowledge campaign for the space sector, organising workshops, webinars, and training sessions aimed at increasing awareness and improving cybersecurity skills.

[21] As mentioned in the Cyber Solidarity Act
[22] Cyber Solidarity Act
[23] NIS investments 2024

- Develop guidelines and best practices to ensure comprehensive security analysis and testing of components before integration into the production environment. These guidelines should encourage stakeholders in the space and satellite industries to conduct thorough security evaluations, as nearly half (49%) of organisations using COTS products currently lack this practice.
- Promote collaboration and information exchange within the space sector and with other sectors, such as telecommunications, due to the growing convergence of 5G and satellite communications.

The **public administrations** should focus on building effective remediation capabilities to meet NIS2 requirements.

- One way to achieve this is through shared service models with other public entities, which can help optimise resources and enhance cybersecurity capabilities. Given the common regulatory frameworks and similar operational needs across public administrations, such collaborative models are particularly well-suited for this sector. This approach can also better facilitate addressing the growing needs for digital wallets, which are associated with higher cyber threats, necessitating stronger protections to maintain public trust.
- Public administrations can strengthen their cybersecurity capabilities by leveraging the EU Cyber Solidarity Act, which provides financial support for enhancing detection, response, and remediation efforts. By combining this funding with investments in necessary technologies, modernising legacy systems, and investing in training, and staffing, they can significantly improve their ability to manage cybersecurity risks and meet NIS2 obligations.

The **maritime sector** is vital for global trade, relying on operational technology (OT) to ensure safety and efficiency. However, outdated OT systems make it vulnerable to cyberattacks, highlighting the need to enhance cybersecurity maturity and resilience.

- Develop tailored guidance for maritime entities to implement robust cybersecurity risk management controls aligned with NIS2 and applicable sector-specific legislation. This guidance should prioritise the integration of secure-by-design principles and proactive vulnerability management within maritime OT and connected systems, addressing sector-specific risks effectively.
- Conduct an EU-level cybersecurity exercise focusing on an intermodal scenario involving maritime transport. Such an initiative would improve crisis response capabilities by linking sectoral crisis management structures with national and EU-level frameworks. The exercise should simulate cross-border incidents and cascading effects to enhance coordination and preparedness in both sectoral and multi-modal crisis management.

The **health** sector faces significant cybersecurity challenges due to its diverse range of entities, devices, and technologies, with many organisations struggling with basic security measures, resource gaps, and outdated practices.

- Develop practical guidelines to assist healthcare organisations in the secure procurement of services, products, and infrastructure, addressing both immediate and long-term cybersecurity needs.
- Develop targeted guidance on essential cybersecurity practices tailored to the healthcare sector, addressing its unique challenges such as diverse entities, devices, and technologies. Additionally, create sector-specific methodologies to help healthcare providers implement these practices effectively, focusing on overcoming common issues like resource gaps, outdated security measures, and gaps in basic security hygiene.
- Launch awareness campaigns to enhance the cybersecurity culture and ensure staff are prepared to address sector-specific vulnerabilities, while promoting secure product design for diverse healthcare technologies. Leverage information-sharing platforms like the European

Health ISAC to facilitate collaboration between healthcare providers and manufacturers, addressing cybersecurity risks, particularly within the supply chain.

- Additionally, encourage healthcare organisations to actively engage with national operational initiatives, tools, and collaboration frameworks to strengthen threat detection, response capabilities, and overall cybersecurity resilience.

Note: During the drafting of this report, the European Commission unveiled an action plan aimed at strengthening the cybersecurity of hospitals and healthcare providers[24]. By enhancing threat detection, preparedness, and response capabilities, this action plan aims to contribute to a safer and more secure environment for both patients and healthcare professionals. That said, the scope of the health sector assessed for the NIS360, extends beyond hospitals and healthcare providers to include other types of entities (e.g., EU reference laboratories, research and development entities for medicinal products, pharmaceutical manufacturers, manufacturers of medical devices). While the action plan is not explicitly tailored to them, these entities could still benefit from its outcomes and leverage this momentum as an opportunity for their own cybersecurity development.

The **gas** sector's reliance on digital systems for control and its interconnectedness with industries like electricity and manufacturing make it vulnerable to cyberattacks, potentially causing widespread economic impacts. However, its cybersecurity maturity remains insufficient, particularly in post-incident preparedness and response, where it lags behind the more advanced electricity sector.

- Enhance the gas sector's resilience by developing robust, sector-specific incident response plans and regularly testing them at both national and EU levels.
- Promote collaboration with the electricity and manufacturing sectors to ensure coordinated cyber defence, share best practices, and conduct joint exercises to strengthen the sector's ability to quickly detect, respond to, and recover from cyber incidents, minimising potential economic disruptions.

[24] European action plan on the cybersecurity of hospitals and healthcare providers | Shaping Europe's digital future

3. NEXT STEPS

The 2024 iteration of NIS360 assessed all high-criticality sectors under NIS2 to provide a comprehensive understanding of their cybersecurity maturity and criticality. This year marked the first time we integrated the industry perspective into the assessment, transitioning to an indicator-based evaluation. Additionally, we introduced dual validation of outcomes by both authorities and the industry, enhancing the credibility and robustness of our findings.

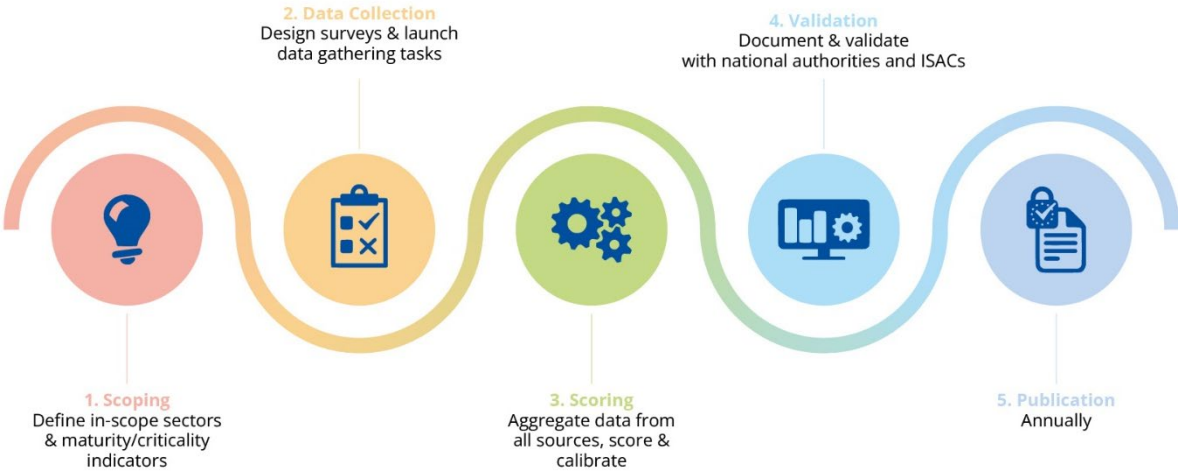
Looking ahead to 2025, we plan to build on this work by continuing the NIS360 assessment for all highly critical sectors under NIS2, adopting a holistic approach that considers improvements at every level—from the EU, to national authorities, and individual entities—thereby contributing to enhanced security across the board.

The value of this work lies in establishing a dynamic framework that allows us to assess the current state of in-scope sectors, prioritise maturity-building actions effectively, identify areas where targeted improvements can have the greatest impact, drive more informed decision-making to strengthen sectorial resilience, and enable the ongoing monitoring of progress over time.

We will also continue refining this framework to ensure it fulfils these ambitious objectives and remains a valuable tool for strengthening cybersecurity across sectors.

ANNEX A THE NIS360 METHODOLOGY

This annex outlines the NIS360 methodology employed to assess the cybersecurity criticality and maturity of sectors under the NIS2 Directive. The process is structured into distinct phases, each contributing to a comprehensive evaluation of the sectors' cybersecurity posture.



1. Scoping

The assessment begins with an initial phase where the sectors in scope for the current year's evaluation are determined. During this phase, we also define the types of indicators to be used for assessing both the maturity and criticality of the sectors. These indicators are mapped against specific maturity and criticality dimensions:

Maturity 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 institutional setup at EU-level, the existence and experience of national authorities, the level of interaction between entities and these authorities, and the availability of guidance to support compliance.

- **Risk Management and Good Practices** – We evaluate 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 management practices adopted by entities, the perceived effectiveness of these practices as assessed by both entities and 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 evaluate the level of preparedness of the sector to handle large-scale incidents and crises. Key aspects considered include the practices entities adopt

to build and test preparedness, their ability to detect and respond to cyberattacks, the organisation of sector-specific EU-level cyber exercises, and the preparedness levels as evaluated by supervisory authorities.

Criticality Dimensions

- **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, 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, taking also 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 the society and economy and/or impact other sectors, taking into account the existence of alternatives and the time sensitivity of the sector's operations.

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.

Data is drawn from three perspectives:

- **Industry**: Input from sector entities gathered through a survey.
- **National authorities**: Input from national supervisory authorities (horizontal or sector-specific) gathered through a survey.
- **EU-level**: Input from ENISA experts and EU-level repositories and deliverables.

This phase includes:

- **Survey Engineering:**
  Surveys are carefully designed to collect data from industry stakeholders and national authorities.
- **Data Collection:**
  Surveys are launched while consultations and desk research are conducted in parallel to ensure that all relevant data points are collected.

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.

On calibration:
Calibration becomes necessary when significant variations are observed among different assessment sources e.g.:

- Entity self-assessments
- Authority evaluations
- Observable sector performance metrics at EU-level

These variations typically stem from two primary sources:

- **Assessment Perspective Gaps**
  - Inherent biases in self-assessment, stemming from different perspectives.
  - Knowledge gaps
  - Varying interpretations of maturity/criticality criteria

- **Variations in Contextual Understanding**
  - Limited knowledge of the cross-sectoral context
  - Incomplete understanding of sector-specific challenges
  - Varying levels of sector expertise among respondents
  - Varying interpretations of maturity/criticality criteria

To address these issues, a calibration element is included in the scoring algorithm to allow for 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 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/ criticality. It also involves evaluating *sector rankings* in terms of maturity and criticality.

Considering rankings rather than just broad categories provides a more precise and meaningful comparison across sectors. A sector considered to have “moderate” maturity for example, may still be lagging significantly compared to others, while another in the same category could be much closer to the higher end. Rankings enable the identification of relative positioning, ensuring that the analysis doesn’t just focus on sectors that score “low” or “low-moderate” in absolute terms, but also on sectors that underperform compared to others. This allows for a more nuanced understanding of where the biggest gaps exist and where targeted interventions are most needed.

In fact, *ranking* forms the foundation of an important step of the NIS360 process – the determination of sectors in the **‘risk zone’**.

Determining the **'risk zone'** helps prioritise sectors that require immediate attention. A sector falls into the 'risk zone' if its maturity ranks in the lower half[25], and its criticality exceeds its maturity. Unlike sectors in the upper half of the maturity rankings—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 support to address.

4. Validation

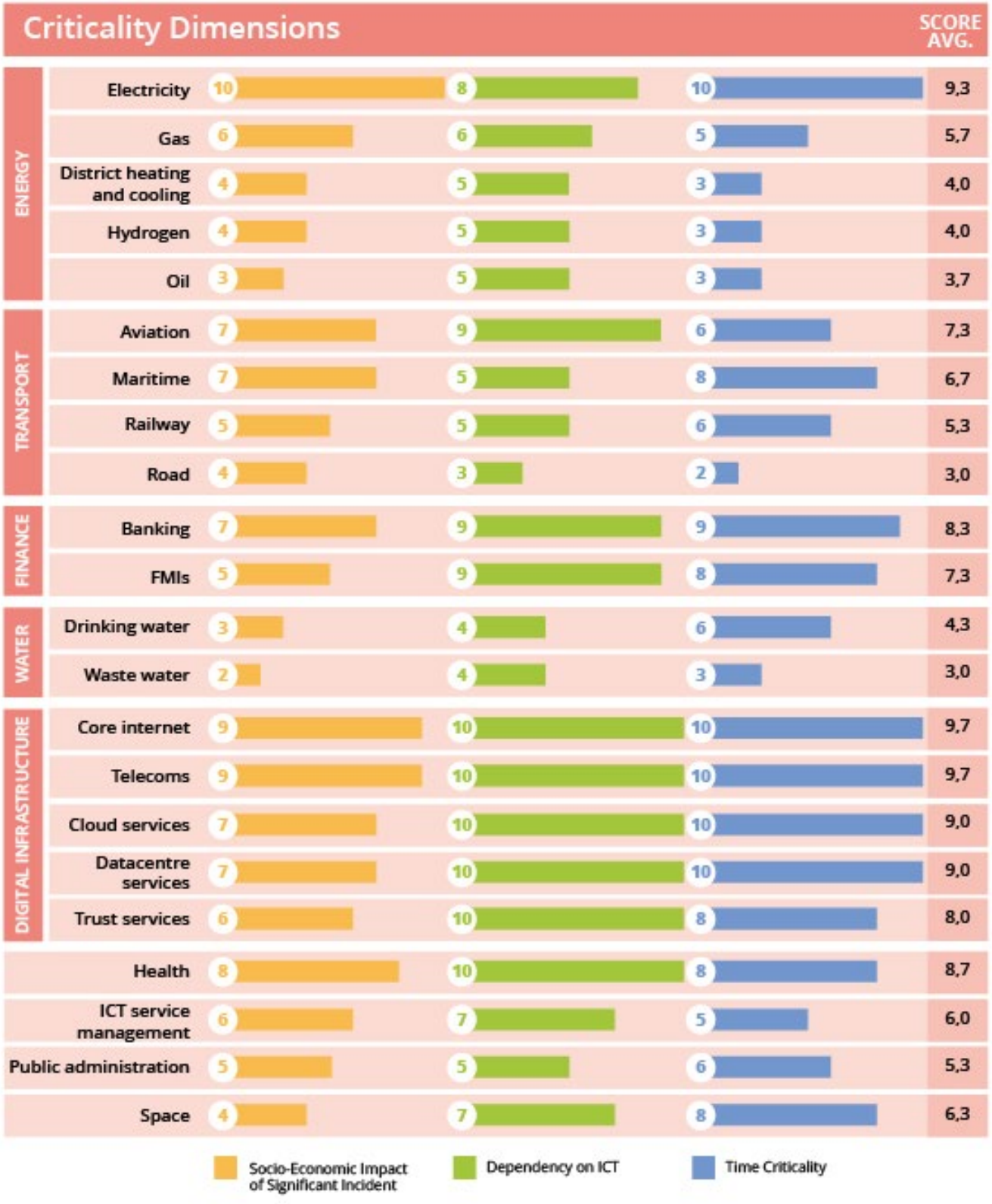
This phase involves documenting the outcomes of the assessment and validating the results with stakeholders from the NIS Cooperation Group and EU-ISACs, refining as necessary.

5. Publication

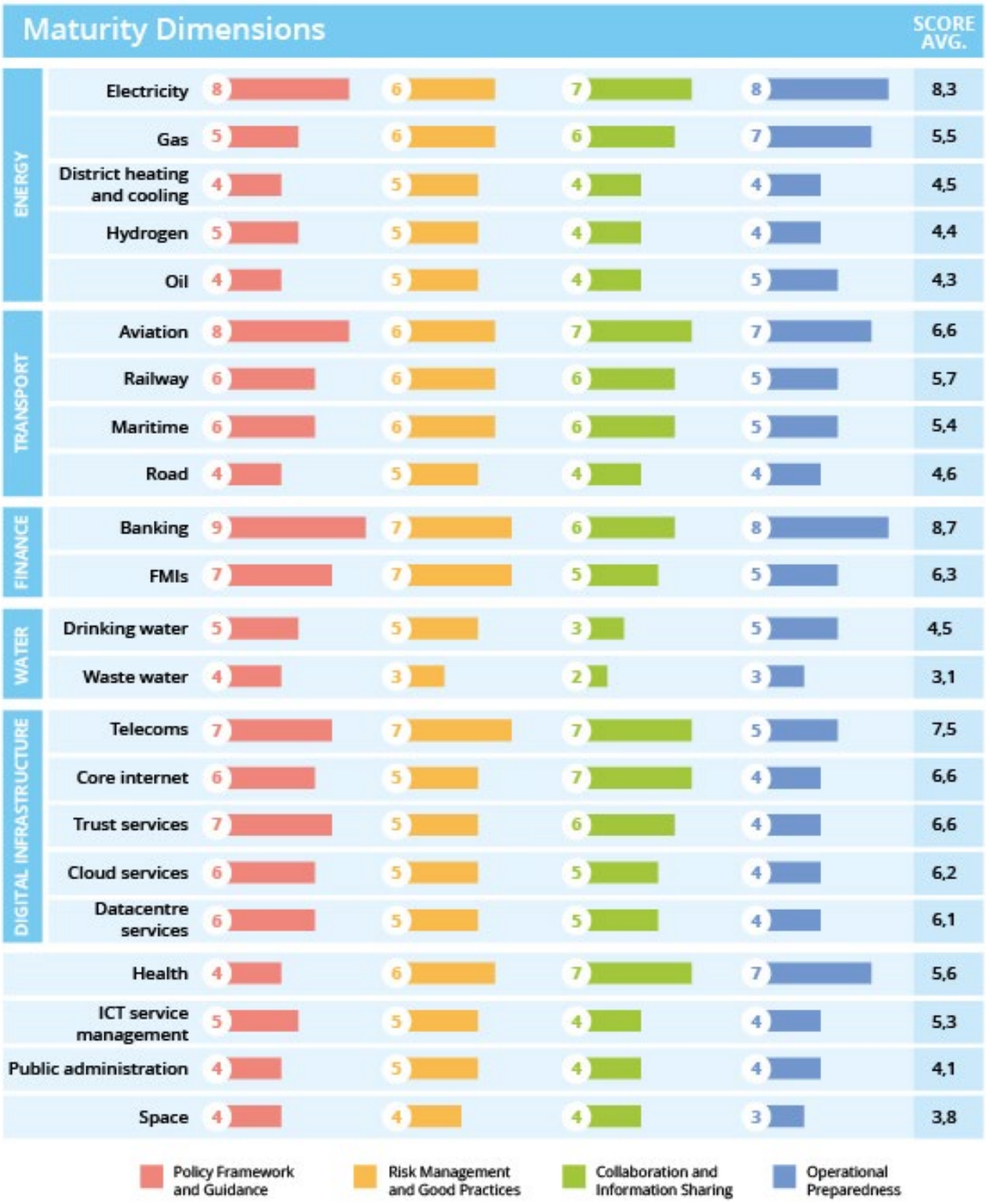
The final phase focuses on the activities relevant to the publication of the report presenting the outcomes of the annual NIS360 assessment.

[25] To define the "risk zone" in a set of 22 maturity rankings, we took a conservative approach based on the median. With an even number of rankings, the middle two sectors—ranked 11th and 12th—fall into a "grey area." To ensure a cautious stance, both of these sectors are included in the lower half of the ranking.

ANNEX B CRITICALITY BREAKDOWN BY SECTOR



ANNEX C MATURITY BREAKDOWN BY SECTOR



ANNEX D SECTOR BY SECTOR ANALYSIS

D.1 ENERGY SECTOR

D.1.1 Sector scope

The energy sector includes a broad range of entities responsible for generating, transmitting, distributing, and managing energy across various subsectors, such as electricity, district heating and cooling, oil, gas, and hydrogen. Each subsector and the entities within it play a distinct role in the broader energy ecosystem, contributing to the efficient and reliable delivery of energy.

- The **electricity** subsector includes:
  - **producers** generating electricity.
  - **Transmission System Operators** (TSOs) managing transmission over long distances,
  - **Distribution System Operators** (DSOs) delivering electricity to consumers,
  - **retail electricity providers** selling electricity to consumers,
  - n**ominated electricity market operators** facilitating trading in electricity markets,
  - entities providing **energy storage, demand response,** and **aggregation services**,
  - **operators of recharging points**, supporting electric vehicle infrastructure.

- The **district heating and cooling** subsector includes:
  - Operators managing systems that distribute thermal energy to buildings and facilities.

- The **oil** subsector includes:
  - operators of **production** facilities,
  - **refineries**,
  - **storage** facilities,
  - **long-distance transmission pipelines**
  - **central stockholding** entities responsible for maintaining strategic reserves.

- The **gas** subsector focuses on the exploration, production, and distribution of natural gas, which is used for heating, electricity generation, and industrial processes. It includes:
  - **supply undertakings** carrying out the function of supply,
  - **natural gas undertakings** managing production and refinement,
  - **TSOs** overseeing high-pressure pipelines,
  - **DSOs** ensuring local delivery to consumers.
  - **storage system operators** maintaining reserves
  - **LNG system operators** managing liquefied natural gas facilities.

- The **hydrogen** subsector is expanding to support decarbonisation and sustainability, focusing on:
  - **production**, **storage**, and **transmission** to integrate hydrogen into energy systems and industry.

D.1.2 Maturity

Each of the energy subsectors has its distinct level of maturity influenced by policy frameworks and guidance, risk management practices, collaboration and information sharing, and operational preparedness.

Policy framework and guidance:

- **Electricity** ranks highest in this dimension, guided by the NIS Directive and the sector-specific Network Code on Cybersecurity (NCCS), which became effective on 13 June 2024. The NCCS aims to enhance cyber resilience in electricity networks while providing a clear framework and practical guidance for the sector. Additionally, EU-level bodies such as European Union Agency for the Cooperation of Energy Regulators (ACER), European Network of Transmission System Operators for Electricity (ENTSO-E), and Association of European Distribution System Operators (E.DSO) play a crucial role in supporting the subsector's efforts to advance its cybersecurity maturity.
- **Gas** and **hydrogen** follow with comparable scores. Gas benefits from the support of European Network of Transmission System Operators for Gas (ENTSO-G), which has increasingly emphasised cybersecurity in its initiatives over the past year. In contrast, **hydrogen** is still in the early stages of building its cybersecurity institutional framework at EU-level. The formation of ENNOH, the European Network of Network Operators for Hydrogen, in 2024 aims to foster coordination among hydrogen transmission operators, though its specific role in advancing cybersecurity remains undefined as it moves toward operational status in 2025.
- **Oil** and **district heating and cooling** rank lower in this dimension. While also covered under NIS2, coordinated efforts towards supporting them achieve better alignment with NIS2 requirements is yet to have been seen.
- Across the energy sector, all entities benefit from supervision and support by experienced national and/or sector-relevant authorities. While this oversight is generally viewed positively, sector entities suggest that more opportunities exist to further enhance the level of support offered.

Risk management and good practices:

- Across the energy sector, many entities report implementing robust cyber risk management practices. These include securing leadership approval for cyber risk management controls, adopting supply chain cybersecurity policies, and deploying measures to enhance trust within the supply chain. Sector entities also indicate a solid understanding of cyber risks, effective mitigation measures, and strong security practices for managing vulnerabilities and legacy systems in both IT and OT.
- National and sector-relevant supervisory authorities highlight differences across subsectors, with **electricity, gas**, and, to some extent, **oil** making meaningful progress in implementing NIS2-aligned measures to identify, protect against, and detect cyber threats. **Electricity** stands out with its higher performance, supported by EU-level initiatives such as the subsector-relevant EU-wide risk assessment conducted by the NISCG in 2024 and the risk management provisions in the NCCS, which align with industry standards. In contrast, entities in the **district heating and cooling**, and **hydrogen** subsectors are reported to have made limited advancements. Authorities also note that entities across all energy subsectors tend to perform better in pre-incident measures compared to post-incident ones.
- **Gas**, while trailing electricity, has also benefited from targeted efforts aimed at supporting the sector develop its cyber risk management capacity over the period, with a “train the trainer”

programme for gas TSOs, based on ENISA's "AR-in-a-box" framework, delivered to the sector in 2023.
- In contrast, **oil, district heating, and hydrogen** did not have equivalent EU-level initiatives, contributing to their comparatively lower maturity.

Collaboration and information sharing:
- Across the energy sector, many entities report participating in information-sharing and collaboration initiatives, primarily through industry associations, EU-ISACs, and national ISACs, with nearly all engaging with their national competent authority. National-level supervisory authorities of energy sector entities, also participate in such initiatives at both national and EU levels, but less so than for other sectors. At the EU level, ENISA supports these efforts through bi-monthly SITAW updates shared with the sector.
- **Electricity** stands out for its higher maturity in this area, supported by an active EU-level ISAC (EE-ISAC[26]), the European Network for Cyber Security (ENCS) established by grid operators, and national authorities' involvement in NIS Cooperation Group workstream on Energy. Additionally, the sector benefits from sector-specific cyber-relevant events, such as the annual cybersecurity conference co-organised by key EU-level bodies. The 6th edition of this event took place in October 2024.
- At the same time, **gas** has benefited from a range of initiatives in 2023 including the organisation of a joint workshop among ENTSOG, the European Association for the Streamlining of Energy Exchange – gas (EASEE-gas) and Gas Infrastructure Europe (GIE) on data exchange and cybersecurity in the gas sector, the creation of a common task force among ENTSOG/GIE to among other things develop a common understanding on various policy files, the development of a framework for deeper collaboration between ENTSOG and EASEE-gas etc.
- In contrast, **oil, district heating,** and **hydrogen** lack similar EU-level initiatives, which constrains their ability to achieve comparable maturity in information-sharing and collaboration.

Operational preparedness:
- Across the energy sector, entities engage in preparedness-building activities, most commonly within their own organisations, and to a lesser extent via EU-level exercises and community-driven workshops and training sessions. Sector entities generally report that their current detection and response capabilities enable them to manage some sophisticated attacks on most parts of their infrastructure.
- From a supervisory authority standpoint, **electricity** subsector entities are seen as the most prepared for incidents or crises (among all subsector entities), with many having documented and tested plans and processes through cyber exercises. **Oil** and **gas** entities follow, with many having documented plans that may however not always be tested. In contrast, entities in the **district heating and cooling** and **hydrogen** subsectors are viewed as less prepared, with fewer having established and tested plans.
- From an EU-level standpoint the 2024 Cyber Europe exercise focused on the electricity and gas sectors.

D.1.3 Criticality

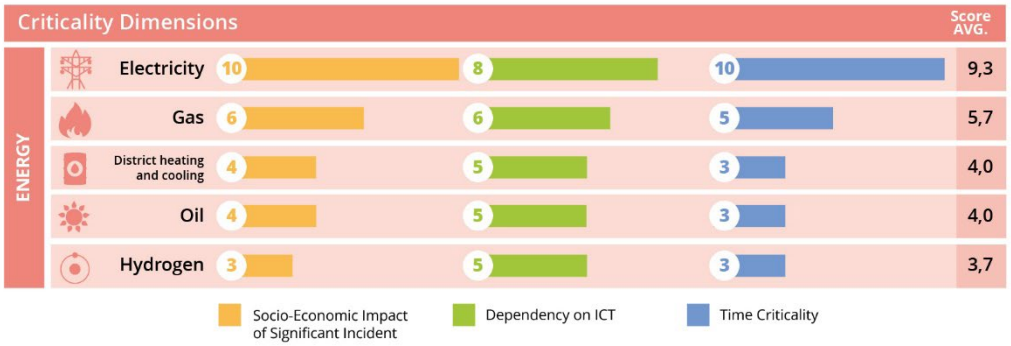
The EU energy sector's digital transformation is accelerating, driven by advances in technology, declining costs, and widespread connectivity. **Electricity networks** are at the forefront of this evolution, becoming smarter and enabling greater efficiency, improved reliability, and better integration of renewable energy sources. Meanwhile, the **gas, oil, district heating and cooling**, and **hydrogen** subsectors are steadily adopting digital solutions to enhance

[26] European Energy Information Sharing & Analysis Centre - https://www.ee-isac.eu/

operational processes including production (e.g., processing equipment, heat generation units), monitoring (e.g., pipeline monitoring) and maintenance (e.g., predictive maintenance).

While these advancements bring operational and sustainability benefits, the growing reliance of the EU energy sector on ICT and interconnected systems makes it increasingly vulnerable to a range of cyber threats. According to ENISA's 2024 Threat Landscape report[27], the sector accounted for 3.27% of all recorded events during the reporting period, with DDoS and ransomware emerging as the most common threats. On the CIRAS[28] platform, the energy sector reported 10% of all incidents in 2023, 36% of which were attributed to malicious activities.

Despite these shared challenges, the criticality of EU energy subsectors varies based on several factors. These include not only the level of ICT dependency within each subsector, but also the potential socioeconomic impact of cyber-attacks against them and the speed at which such an impact would be felt. For instance, electricity, given its central role in energy distribution and the functioning of other sectors, has a higher criticality than for example hydrogen.



Socio-economic impact:

- The **electricity** subsector stands out with the highest impact score, reflecting its central role within the energy sector and its importance to the broader economy. A major cybersecurity incident in this subsector could cause widespread disruptions, including power outages that would not only affect consumers directly, but also disrupt other highly critical sectors like telecoms, where many systems rely on electricity.
- The **gas** subsector follows in terms of impact reflecting its dominant position as a source of energy for households across EU[29]. While cybersecurity incidents could result in temporary service disruptions, the effects would be less widespread than those of a similar event in the electricity subsector, with fewer ripple effects across other sectors.
- In contrast, the **oil**, **district heating and cooling,** and **hydrogen** subsectors are considered to have a more limited socio-economic impact in the event of a cybersecurity breach. Disruptions in these subsectors would likely be isolated and have a more contained effect, with minimal broader economic consequences compared to electricity or gas.

Dependency on ICT:

- The **electricity** subsector stands out as the most reliant on digital technologies, especially with the ongoing digital transformation of power grids. This shift is driving greater convergence between IT and OT systems, which are crucial not only for real-time monitoring of power generation, transmission, and distribution networks, but also for balancing supply and demand, preventing overloads, and enabling rapid responses to emergencies.

[27] ENISA THREAT LANDSCAPE 2024
[28] Incident reporting — CIRAS
[29] Gas factsheet | www.acer.europa.eu

- The **gas** subsector follows with significant, though somewhat lower, dependence on ICT. As the sector becomes more digitally integrated, its reliance particularly on operational technology is growing, especially in areas such as extraction, processing, and distribution. However, the level of digitalisation in this subsector is still behind that of electricity.
- In contrast, the **oil, district heating and cooling,** and **hydrogen** subsectors are less dependent on ICT, with digital adoption progressing more slowly. While these subsectors are incorporating digital technologies to enhance efficiency and operations, many processes remain only partially digitalised. The **hydrogen** subsector is still in early digitalisation stages, and district heating and cooling are advancing at a slower and smaller scale compared to electricity and gas.

Time Criticality:

- The **electricity** subsector ranks highest, as a significant incident would have immediate impacts due to its central role in daily life and interdependencies with critical sectors like telecoms and transportation, potentially causing cascading effects.
- The **gas** subsector has moderate time criticality, with incident impacts typically felt within hours, potentially allowing some time for mitigation. Its broader economic effects are generally less severe than those of electricity disruptions.
- In contrast, the **oil, district heating and cooling,** and **hydrogen** subsectors exhibit lower time criticality. Incidents in these areas tend to have delayed and more limited effects, impacting only a few sectors, and generally result in less widespread disruption than electricity incidents.

D.1.4 Areas for improvement

Based on the above, the following areas of improvement/interventions are proposed to help the sector further develop its cyber maturity:

- **Help national authorities deepen their understanding of the less mature energy subsectors unique challenges** to ensure more effective support and supervision of entities within it particularly in the oil, district heating and cooling and hydrogen space. This could be supported via a mapping of stakeholders within those sectors and an identification of their diverse cybersecurity needs considering their level of digitalisation.
- **Equip national authorities to effectively support entities in implementing and harmonising requirements outlined in NIS2 and other applicable legislation (e.g., NCCS)**, ensuring consistent support towards in-scope entities across Member States.
- **Support the development/strengthening of the energy sector's risk management capacity.** For the electricity sector, this is expected to happen through targeted support towards the development of cybersecurity risk assessment methodologies, the identification of controls to mitigate applicable risks and the promotion of their implementation as foreseen via the NCCS.
- **Strengthen information sharing and collaboration** among sector entities in the electricity and gas sectors, and continue to share sectorial situational awareness updates with stakeholders. Explore ways of reaching a broader set of energy sector stakeholders.
- **Support sector entities in developing and implementing robust incident response and crisis management plans** and strengthen the capacity of national authorities to respond to cross-border incidents by improving their understanding of available tools and mechanisms and validating their application through practical exercises.

D.2 TRANSPORT SECTOR

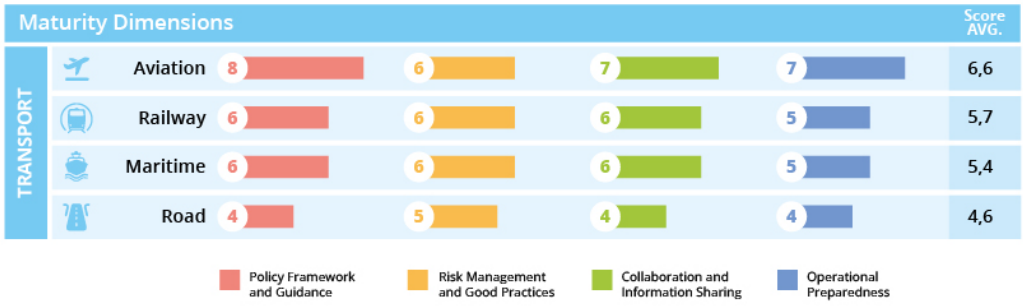
D.2.1 Sector scope

The transport sector consists of a broad range of entities that collectively form the backbone of Europe's transportation network. Under the NIS2 Directive, this sector is divided into four key subsectors: aviation, railway, maritime, and road. Each subsector comprises critical entities essential to maintaining the efficiency, safety, and connectivity of Europe's transport infrastructure. In particular,

- the **aviation** subsector includes:
  - commercial **air carriers** providing passenger and cargo services,
  - **airport management organisations** responsible for operating airports and their facilities
  - **air traffic control operators** ensuring the safe navigation of aircraft in controlled airspace.
- the **railway** subsector includes:
  - railway **infrastructure managers** responsible for developing and maintaining tracks, signalling systems, and associated infrastructure
  - **railway operating companies** that provide passenger and freight rail services.
- the **maritime** subsector comprises:
  - maritime and inland **maritime 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[30]:
  - **road management authorities** responsible for traffic and infrastructure management and
  - **smart transport system operators** deploying advanced digital technologies for traffic control and real-time information services.

D.2.2 Maturity

The EU transport sector is made up of subsectors that exhibit varying levels of maturity, all within the Moderate maturity range.



Policy framework and guidance:

- **Aviation**: Aviation leads in cybersecurity, being covered by both the NIS2 Directive, the sector-specific Regulations (EU) 2023/203 and 2022/1645[31] *as well as from cybersecurity provisions for certified aeronautical products*[32]. This regulatory package has a broader scope

[30] Although the NIS2 Directive includes *Manufacturers of motor vehicles, trailers and semi-trailers* and *Manufacturers of other transport equipment* under Annex II, these were outside the scope of our study. The *Road Transport sub*sector, as covered under Annex I of the directive, does not encompass the automotive industry.
[31] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023R0203 & https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32022R1645
[32] https://www.easa.europa.eu/en/document-library/agency-decisions/ed-decision-2020006r

within the aviation subsector than the NIS Directive, defining detailed rules for identifying and managing information security risks for aviation organisations and competent authorities. The subsector is supported by EU-level bodies such as European Union Aviation Safety Agency (EASA), which contribute to advancing cybersecurity maturity through oversight, and guidance. In 2024, EASA participated in a dedicated subgroup under the NIS CG, to identify overlaps and gaps between Part-IS[33], NIS2 and the AVSEC information security requirements[34] and published updated guidance on how to demonstrate compliance with Part-IS[35].

- **Railway:** Railway ranks next, with the NIS2 Directive and the CRA[36] serving as its primary cybersecurity policy framework. While the directive represents a step forward, its effective and harmonised implementation across Member States remains to be seen. Harmonisation is crucial to ensure that sector entities, particularly those operating cross-border, are not overburdened by varying compliance requirements. The sector benefits from the support of EU-level bodies such as the European Union Agency for Railways (ERA), which actively contribute to its cybersecurity maturity development efforts. At the same time, a mapping of regulatory requirements with international standards is currently on-going with the intention to further support the sector towards its cybersecurity maturity development efforts in line with NIS2 requirements.
- **Maritime**: Maritime ranks next, with the NIS2 Directive serving as the sector's primary cybersecurity policy framework. The sector benefits significantly from the support of the European Maritime Safety Agency (EMSA), which plays a key role in advancing cybersecurity maturity. In 2024, EMSA published the Handbook Guidance on Maritime Security for Member States' Competent Authorities[37]. This document offers guidance to assist Member States in achieving a harmonised and effective implementation of EU law in maritime security, specifically addressing Regulation (EC) No 725/2004 on ship and port facility security and Directive 2005/65/EC on port security. While the Handbook includes provisions for addressing cyber risks, it does not provide specific guidance on implementing the NIS2 Directive.
- **Road**: The sector lacks targeted support, hindering its cybersecurity maturity compared to others.

Risk management and good practices:

- Across the transport sector, many surveyed entities have implemented robust cyber risk management practices, including securing leadership approval for risk controls, adopting supply chain cybersecurity policies, and deploying measures to build trust within the supply chain. These entities report a solid understanding of cyber risks, effective controls, and strong security practices for managing vulnerabilities and legacy systems across both IT and OT. However, national and sector-relevant authorities note that all sectors still have work to do in fully implementing NIS2-aligned measures, with aviation being the most aligned, road the least and railway and maritime still relying heavily on legacy systems.
- The higher maturity scores in **aviation, railway, and maritime** are supported by EU-level initiatives that help these subsectors better understand and manage the cyber risks they face. **Aviation** benefits from EASA regulations and standards developed by EUROCAE[38] (e.g., ED-204A)[39]. **Railway** leverages technical specifications addressing cybersecurity risks, such as CENELEC CLC/TS 50701:2023[40], along with guidance documents from ENISA[41], with further

[33] The term "Part-IS" represents the information security management system (ISMS)requirements laid down in the Regulations of the European Union (EU) 2022/1645 (Delegated Regulation) and (EU) 2023/203 (Implementing Regulation).
[34] https://www.easa.europa.eu/community/topics/unvex-2024-cybersecurity-aviation-uas
[35] https://www.easa.europa.eu/community/sites/default/files/2024-07/Guidelines%20-%20ISO%2027001%20add-on.pdf and https://www.easa.europa.eu/en/document-library/acceptable-means-of-compliance-and-guidance-materials/amc-gm-part-isar-issue-1
[36] Regulation (EU) 2024/2847 - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847
[37] https://www.emsa.europa.eu/we-do/safety/maritime-security/item/4828-eu-marsec-handbook.html
[38] European Organisation for Civil Aviation Equipment - https://www.eurocae.net/
[39] https://www.easa.europa.eu/community/content/regulations-standards
[40] CENELEC CLC/TS 50701:2023- "Railway applications - Cybersecurity" provides a framework for managing cybersecurity risks associated with railway applications, covering both the rolling stock (trains, locomotives) and fixed installations (signalling, communication, power supply systems).
[41] https://www.enisa.europa.eu/publications/zoning-and-conduits-for-railways

developments expected from IEC 63452 beginning 2026. **Maritime** is advancing in cybersecurity maturity with the support of the European Maritime Safety Agency (EMSA), which offers training courses[42] and leads working groups focused on emerging threats such as AIS spoofing[43] and GPS jamming.

- The **road** subsector ranks lowest in this dimension. Although some awareness and risk management efforts exist within the sector, limited action at the EU level has been taken to address and manage cybersecurity risks systematically.

Collaboration and information sharing:

- Across the transport sector, several entities report active participation in information-sharing and collaboration initiatives, primarily through industry associations, EU-ISACs, and national ISACs, with nearly all engaging with their national competent authority. National-level supervisory authorities for transport entities also participate in such initiatives at both national and EU levels, though this is less widespread compared to other sectors. ENISA supports these efforts at the EU level through bi-monthly SITAW updates shared with the transport sector.
- **Aviation** leads in this area, reflecting robust EU-level initiatives that strengthen collaboration and information-sharing on cybersecurity. These efforts include the Stakeholders' Advisory Group on Aviation Security (SAGAS), which advises the European Commission on legislative proposals, policy initiatives, and the implementation of aviation security legislation. Workshops on cybersecurity-relevant topics, such as GNSS jamming and spoofing, are organised at national, EU, and international levels. Additionally, events like the Aviation Cybersecurity Summit, hosted by the A-ISAC, and work by key task forces and working groups promoted or led by the European Union Aviation Safety Agency (EASA) (e.g., the Part-IS Implementation Task Force, the European Centre for Cybersecurity in Aviation (ECCSA), and the Network of Cybersecurity Analysts (NoCA)) contribute to the sector's high performance in this domain.
- **Maritime** follows, reflecting similar EU-level but also national and regional[44] initiatives aimed at strengthening collaboration and information-sharing among stakeholders. These include the Stakeholders' Advisory Group on Maritime Security (SAGMAS), which advises the European Commission on matters related to maritime and port security, as well as the European Maritime ISAC. EMSA contributes through initiatives such as the annual Maritime Cybersecurity Conference and working groups focused on threats like AIS spoofing and GPS jamming.
- **Railway** shows comparable scores to maritime, driven by active EU-level efforts to enhance collaboration across the sector. The Expert Group on Land Transport Security (LANDSEC) supports the European Commission in shaping policies related to land transport security. Sector stakeholders convene in the LANDSEC group, managed by DG-MOVE, with ENISA providing regular cybersecurity briefings. Collaboration is further supported by the European CISO Forum for Rail, which brings together CISOs from European Rail Infrastructure Managers and Railway Undertakings. ERA and ENISA also co-host the annual Cybersecurity in Railways conference to address challenges, best practices, and advancements, most recently held in October 2024.
- **Road** ranks last as collaboration within this subsector remains relatively underdeveloped compared to other transport modes. While the auto-ISAC[45] exists, it focuses on car manufacturers (which are not in scope of the road transport sector as defined in NIS2 Annex I) and excludes many other critical entities, such as road authorities and operators of intelligent transport systems.

[42] https://www.emsa.europa.eu/we-do/safety/maritime-security/item/5068-part-time-course-on-maritime-cybersecurity-now-completed.html
[43] https://www.emsa.europa.eu/we-do/safety/maritime-security/item/5358-wg-ais-spoofing.html
[44] Other initiatives exist such as https://www.france-cyber-maritime.eu/en/ and https://www.normacyber.no/
[45] https://automotiveisac.com/europe

Operational preparedness:

- Across the transport sector, surveyed entities engage in preparedness-building activities, most commonly within their own organisations, and to a lesser extent via EU-level exercises and community-driven workshops and training sessions. Sector entities generally report that their current detection and response capabilities enable them to manage some sophisticated attacks on most parts of their infrastructure.
- From a supervisory authority standpoint, **aviation** subsector entities are seen as the most prepared for incidents or crises (among all subsector entities), with many having documented and tested plans and processes through cyber exercises including at EU level. **Railway and maritime** entities follow, with many having documented plans that may however not always be tested. In contrast, entities in the **road subsector** are seen as less prepared, with fewer having established and tested plans. Attacks within the road sector are generally perceived to have a primarily national or regional impact. However, there is a lack of comprehensive information on preparedness at the national level, making it difficult to form a clear picture of the overall situation. While the subsector may face some cross-border risks, these are not typically EU-wide.

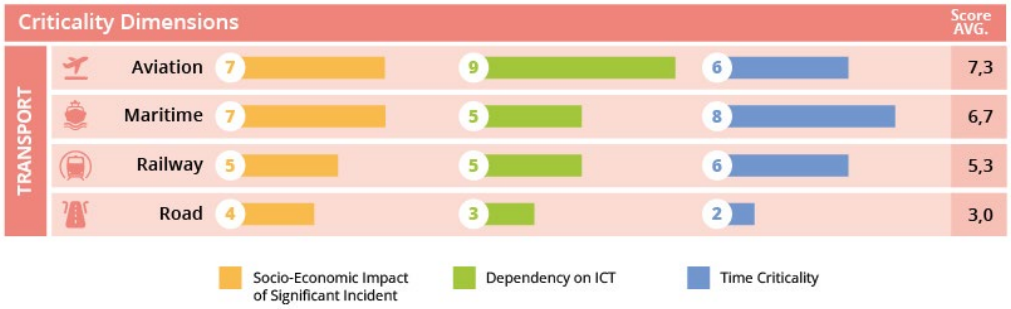
D.2.3 Criticality

The EU transport sector exhibits varying levels of digitalisation across its subsectors, reflecting the technological evolution and operational complexities unique to each mode of transport. **Aviation** stands out as the most digitally advanced subsector, characterised by sophisticated air traffic management systems, automated flight operations, and integrated passenger handling systems. **Maritime and railway** are also making significant strides in digitalisation. The maritime sector increasingly relies on digital systems for port operations, vessel tracking, and maritime traffic management, including the introduction of the European Maritime Single Window environment[46]. The railway sector is progressively adopting digital signalling, automated systems, and smart operational platforms, with the European Rail Traffic Management System[47] (ERTMS) implemented across major corridors to enhance efficiency. In contrast, the **road** sector remains the least digitally advanced of the four modes, despite the gradual deployment of Intelligent Transport Systems (ITS) aimed at improving traffic management and real-time information services.

The EU transport sector faces sustained pressure from threat actors, ranking as the second most targeted sector in ENISA's 2024 Threat Landscape report[48], making up 11.19% of recorded events during the reporting period. Distributed Denial of Service (DDoS) attacks emerged as the most prevalent, accounting for 8.75% of transport sector incidents, followed by ransomware at 1.54%. On CIRAS[49], the sector reported 16% of all incidents in 2023—the second highest across sectors—with 60% attributed to malicious actions.

Despite these shared challenges, EU transport subsectors have different levels of criticality, shaped by the socio-economic impact of incidents, their reliance of ICT, and their time-criticality.

[46] European Maritime Single Window environment - EMSA - European Maritime Safety Agency
[47] European Rail Traffic Management System (ERTMS) | European Union Agency for Railways
[48] ENISA THREAT LANDSCAPE 2024
[49] Incident reporting — CIRAS



Socio-economic impact:

- Cybersecurity incidents in the **air and maritime sectors** have the highest socio-economic impact among all transport subsectors, owing to their critical roles in passenger movement and freight logistics. In **aviation**, a significant incident can cause widespread flight delays or cancellations, impacting thousands of passengers, business travel, tourism-dependent industries, and global supply chains - aircraft being the second most used mode of transport in the EU for passengers, after cars. The financial losses can be substantial for airlines, airport operators, and associated businesses such as cargo handlers and retailers, particularly when disruptions occur at major European hub airports. Similarly, in **maritime**, where over two-thirds of EU freight movement depends on maritime systems, cybersecurity incidents affecting ports or maritime traffic management can severely disrupt supply chains, delay cargo, and drive up costs. These disruptions have ripple effects across the economy, potentially affecting just-in-time manufacturing processes, retail operations, and energy security, particularly as ports handle critical resources like oil, gas, and essential raw materials.
- The socio-economic impact of cybersecurity incidents in the **railway sector** is considered moderate, owing to its lesser share of both passenger and freight traffic in the EU[50]. While a significant incident affecting the sector could disrupt local and regional travel and logistics, causing inconvenience for commuters and delays in supply chains, the scale of impact remains more limited compared to air and maritime.
- Despite cars being the most common mode of passenger transport and the second most common for freight, **road** has a lower socio-economic impact from cybersecurity incidents due to its relatively lower levels of digitalisation. Although the introduction of advancements like Intelligent Transport Systems (ITS) is gradually enhancing road infrastructure, the sector's current reliance on digital systems is not yet significant enough for disruptions to cause severe socio-economic consequences. However, as digitalisation continues to grow, the sector's vulnerability to cyber threats is expected to increase.

Dependency on ICT:

- **Aviation** stands out as the most digitally advanced sector among all transport sectors, leveraging highly sophisticated Air Traffic Management (ATM) systems, and advanced data analytics to enhance both passenger services and operational efficiency. Initiatives like EUROCONTROL's System Wide Information Management (SWIM) have significantly improved information sharing across European airspace. While modern digital interfaces drive progress, the sector still relies on specialised OT systems—such as radar, navigation equipment, and ground control infrastructure—that often incorporate legacy components requiring careful integration and protection.
- **Railway and maritime** share comparable levels of digitalisation (albeit lower than that of aviation), with a mix of legacy systems and modern solutions. Railway has progressively adopted the European Rail Traffic Management System (ERTMS) and advanced signalling solutions. However, challenges remain in integrating legacy OT infrastructure with modern

[50] Rail accounted for 7% of passenger transport and 5.5% of freight movement in the EU, in 2021. Key figures on European transport – 2023 edition

systems and maintaining strict safety and reliability standards. Similarly, the maritime sector has embraced automated cargo handling, vessel traffic management systems, and smart ports, employing technologies like digital twins and AI-driven optimisation tools.

- **Road** remains the least digitally mature of all transport modes, largely due to the limited integration of ICT systems in its infrastructure. While technologies like Intelligent Transport Systems (ITS) and smart traffic management solutions are gradually being introduced, their adoption is not yet widespread. Many traffic management systems still rely on older protocols and hardware that were not originally designed to meet modern cybersecurity standards. This lack of advanced digitalisation, particularly when compared to other transport sectors, limits the sector's reliance on digital systems and, consequently, its exposure to cyber risks.

Time criticality:

- **Maritime** demonstrates the highest level of time criticality. Significant cyber incidents affecting port operations—such as delays in berthing, unberthing, and cargo handling—can produce immediate and widespread repercussions. Time-sensitive cargo, including perishable goods, depends on efficient processing to maintain quality, while delays can disrupt supply chains, creating cascading financial and logistical challenges. **Rail and aviation** follow, with the impact of significant incidents affecting these sectors typically materialising within a few hours. For railway, disruptions to signalling systems or operational networks can quickly lead to delays in passenger services and freight movement. Similarly, in aviation, incidents affecting flight schedules, passenger services, or air traffic management systems can generate cascading delays across airports, with broader repercussions for travellers, cargo operations, and the aviation sector—although freight impacts are less severe than those in maritime due to lower volumes transported by air. In contrast, **road** exhibits the lowest time criticality. The sector's relatively lower reliance on digital infrastructure and the inherent redundancy in road networks help mitigate the immediate societal and economic consequences of a significant cyber incident, containing its overall impact.

D.2.4 Areas for improvement

Based on the above, the following areas of improvement/interventions are proposed to help the sector further develop its cyber maturity:

- **Provide tailored guidance for entities across all transport subsectors to implement cybersecurity risk management controls aligned with NIS2 and applicable sector-specific legislation.** This could include the development of self-assessment tools, encouraging cooperation with standardisation bodies for the development of sector-specific security standards for road transport etc.
- **Conduct EU-wide sectorial risk assessments** to better understand the risks facing the transport sector at EU-level.
- **Facilitate EU-level cybersecurity exercises**, particularly for subsectors that have not yet participated, to improve crisis response capabilities and link sectoral crisis management structures to national and EU-level frameworks. Focus on simulating cross-border incidents and cascading effects to improve sectorial and multi-modal crisis management coordination among authorities and the between authorities and the private sector. Document outcomes and lessons learned to drive improvement.
- **Continue the production and dissemination of sector-specific situational awareness** reports and continue prioritising cybersecurity discussions in forums such as SAGAS, SAGMAS, LANDSEC, ECCSA and NoCA.
- **Develop and distribute updated good practice guides** to assist entities in addressing evolving cybersecurity threats effectively. These could incorporate case studies inspired by previous incidents and be focused on various topics of relevance to the sector including cyber-physical system interdependencies countering common threats etc.
- **Further support the road sector to better align with NIS2**, and foster a stronger stakeholder community to address current gaps, through sector specific training programs and facilitating the exchange of best practices among different actors in the sector.

D.3 FINANCE SECTOR

D.3.1 Sector scope

The EU finance sector includes entities responsible for managing financial transactions, providing credit, and maintaining the stability of the European financial system. For the purposes of this study, we look at this sector in the context of two subsectors:

- **banking**, which includes credit institutions (banks) and
- **Financial Market Infrastructures** (FMIs) limited to central counterparties and trading venues

D.3.2 Maturity

Maturity in the sector remains high or moderate high, with an outlook to become very high. This is due to the implementation of Regulation EU 2022/2554 (DORA)[51], which affects all entities in the financial sector, not only the entities included in the NIS scope.

Policy framework and guidance:

- The EU finance sector is one of the most regulated, with NIS2 setting out baseline requirements and DORA introducing sector-specific rules that will apply from 17 January 2025. Cybersecurity maturity is enhanced by the efforts of the European Supervisory Authorities (ESAs)[52] and the European Central Bank (ECB), who work at EU level to support the various entities in the financial ecosystem increase their maturity. In 2024, regulatory and implementing technical standards[53] were issued under DORA, expanding the existing body of guidance from the ESAs and ECB to strengthen sector-wide cyber resilience.

Risk management and good practices:

- Across the finance sector, many surveyed entities have implemented robust cyber risk management practices, such as securing leadership approval for risk controls, adopting supply chain cybersecurity policies, and deploying measures to foster trust within the supply chain, adopting advanced security measures, including real-time threat detection, multi-factor authentication, and zero-trust models to better safeguard their services.
- **Banking** institutions perceive themselves to have a higher level of cyber risk management maturity compared to **FMIs**, and also report stronger network and information systems maturity—a view that is also reflected by surveyed national and sector-specific authorities.

The sector's maturity is further supported by EU-level initiatives designed to help the sector better understand and manage cyber risks. This includes standards and guidance issued by the ESAs before DORA's applicability, such as EBA Guidelines on ICT and security risk

[51] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554&from=FR
[52] The European Supervisory Authorities are the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA)
[53] https://www.eba.europa.eu/publications-and-media/press-releases/esas-published-second-batch-policy-products-under-dora

management[54], EIOPA Guidelines on ICT security and governance[55], the Cyber resilience oversight expectations for financial market infrastructures[56] etc.

Collaboration and information sharing:

- Across the finance sector, several entities, actively participate in information-sharing and collaboration initiatives. This happens primarily through EU-ISACs, industry associations, and national ISACs, with all surveyed entities from the banking sector and almost all from the FMIs sector suggesting they engage with their national competent authorities.
- National-level supervisory authorities also take part in such initiatives at both national and EU levels, though dedicated working groups exist predominantly for **banking**.
- The banking sector benefits from two very active ISACs that both include a large number of banking institutions as members (FI-ISAC and FS-ISAC). **FMIs** do not benefit from the same level of organisation. That said, to some extent, the CIISI-EU addresses this for the systemic players within the financial ecosystem.

Operational preparedness:

- Across the finance sector, surveyed entities report engaging in preparedness-building activities, primarily within their organisations and, to a lesser extent, at the EU level. Surveyed entities in the **banking** sector view their detection and response capabilities as mature, allowing them to manage sophisticated attacks across most parts of their infrastructure. In contrast, **FMIs** report lower levels of capability, mainly able to detect simpler attacks. National authorities seem to corroborate this, noting that banking entities are better prepared overall, with FMIs often having plans in place but not consistently testing them.
- In 2024, the ECB conducted a cyber resilience stress test[57] for banks further contributing to the development of their operational resilience.
- Furthermore, the existing European framework for threat intelligence-based ethical red teaming – the TIBER-EU framework[58] – helps competent authorities and financial entities fulfil the requirements for threat- led penetration testing.
- Finally, the Systemic Cyber Incident Coordination Framework (EU-SCICF) has been established to support communication and coordination during systemic cyber crises among EU authorities, while also engaging with key international stakeholders.

D.3.3 Criticality

The EU finance sector is heavily reliant on digital technologies to support its core operations, from real-time transactions and data management to risk analysis and fraud detection. These advancements drive the efficiency and accuracy of essential services, including online banking, trading platforms, and payment systems. However, the sector's high level of digitalisation, combined with its critical role in the economy and the sensitive, high-value information it processes, makes it an attractive target for cybercriminals.

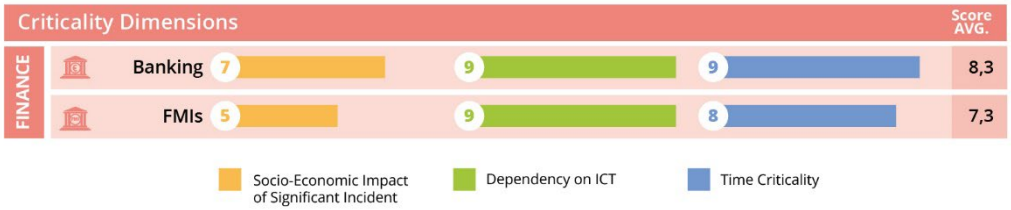
As one of the primary targets for cyberattacks, the sector faces persistent threats like phishing, ransomware, and data breaches. According to ENISA's 2024 Threat Landscape report[59], the sector accounted for 9% of all recorded events during the reporting period, with DDoS and data

[54] https://www.eba.europa.eu/guidelines-ict-and-security-risk-management
[55] https://www.eiopa.europa.eu/publications/guidelines-information-and-communication-technology-security-and-governance_en
[56] https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf
[57] https://www.bankingsupervision.europa.eu/press/pr/date/2024/html/ssm.pr240726~06d5776a02.en.html
[58] What is TIBER-EU?
[59] ENISA THREAT LANDSCAPE 2024

related threats emerging as the most common against the sector. On the CIRAS[60] platform, the sector reported 12% of all incidents in 2023, 27% of which were attributed to malicious activities.

Financial institutions deploy advanced technologies such as encryption, multi-factor authentication, and AI-driven threat detection to safeguard data and comply with regulations. Still, not all entities within the ecosystem meet the same cybersecurity standards. Strengthening cybersecurity across the sector is vital to ensuring trust, resilience, and stability in the EU's financial system.

The criticality of the overall finance sector is at High level.



Socio-economic impact:

- Cyber incidents affecting the EU **banking** sector generally have a greater socio-economic impact than those targeting the in-scope portion of the **FMI** sector. A successful cyberattack on **banks** can lead to widespread disruptions, affecting millions of customers, businesses, and the broader economy. It can result in financial losses, erode public trust, and potentially cause liquidity issues. In contrast, while cyberattacks on in-scope **FMIs** can still be severe, their impact is anticipated to be more contained within the financial system itself and less visible to the general public. With that said, widespread attacks against the EU financial system, could potentially undermine confidence in it and hinder economic activity, especially in MS heavily reliant on digital transactions.

Dependency on ICT:

- The finance sector heavily relies on ICT for its core operations, including transactions, data management, and risk analysis. ICT enables real-time processing of vast amounts of financial data, ensuring accuracy and efficiency in services like online banking, trading, and payment systems. It also underpins cybersecurity measures, protecting sensitive financial data from threats.

Time criticality:

- Cyber incidents in the EU finance sector have a high time criticality due to the sector's interconnected nature. An attack on a major **bank** or an **FMI** could quickly spread across member states, and affect other sectors directly and indirectly. The reliance on third-party service providers and shared cloud platforms increases the risk of rapid, widespread disruptions. The banking subsector faces high time criticality, as any incident directly impacts citizens' day-to-day activities, such as access to banking services, while FMIs directly affect the financial sector.

D.3.4 Areas for improvement

Based on the above, the following areas of improvement/interventions are proposed to help the sector further develop its cyber maturity:

- Conduct **sector-specific exercises**, including tabletop simulations, to improve FMI resilience and detection response.

[60] Incident reporting — CIRAS

- Facilitate greater **collaboration and information sharing** particularly among FMIs, but also between the financial sector and public institutions that work with the sector at EU level.

D.4 HEALTH SECTOR

D.4.1 Sector scope

The NIS 2 Directive significantly expands the scope of entities classified as critical for EU's healthcare ecosystem. Under NIS 2 Annex I, the health sector includes:

- **healthcare providers**—such as hospitals and other legal entities delivering healthcare within Member States[61]
- EU reference **laboratories**,
- **research and development** entities for **medicinal products**,
- **pharmaceutical manufacturers**,
- **manufacturers of medical devices** that are critical during public health emergencies.

D.4.2 Maturity

ENISA has observed a positive shift in the health sector's cybersecurity maturity, increasing from a low level in 2023 to a moderate level in 2024. This shift is likely influenced by the fact that the majority of ENISA's respondents are large enterprises, rather than a change across the entire sector.

Policy framework and guidance:

- The NIS Directive serves as the primary framework for the sector, but its implementation varies widely across Member States due to the significant diversity of health entities. This framework is further complemented by several other regulations and proposals that address more specific aspects of the sector's needs (e.g., Medical Device Regulation[62], European Health Data Space[63], Cyber Resilience Act, AI Act[64]). Although national authorities play a crucial role in supporting and supervising cybersecurity, entities within the sector perceive the support as basic, since not all authorities provide the full range of services (such as high-level guidance, audits, security scans, and ex-ante and ex-post supervision). While the resources, personnel, and operational capacity of these authorities are expected to grow, their current limitations highlight the need for more comprehensive and consistent support across the sector.

Risk management and good practices:

- In over 80% of the surveyed health entities, leaders approve cyber-risk management controls, and policies for supply chain risk management are also in place. However, there is limited guidance on how to effectively manage these risks. Although entities may conduct risk assessments and implement good practices, these efforts are inconsistent across the sector. Many organisations lack a clear understanding of their critical assets, the related cyber risks, and effective strategies for mitigation. At the EU level, there is no comprehensive understanding of sector-wide risks, nor a unified approach to addressing them. To date, no

[61] these were the sole focus of NIS1
[62] https://eur-lex.europa.eu/eli/reg/2017/745/oj/eng
[63] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0197
[64] https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

EU-wide risk assessment has been conducted for the health sector, highlighting a gap in coordinated risk management.

Collaboration and information sharing:

- The health sector benefits from several well-established collaboration platforms, including an EU-level ISAC, a dedicated NIS Cooperation Group workstream on Health, and an annual health cybersecurity conference organised by ENISA. While national authorities cooperate effectively, there is a need for stronger collaboration between private entities. Participation in information-sharing and collaboration initiatives could be further improved within the sector.

Operational preparedness:

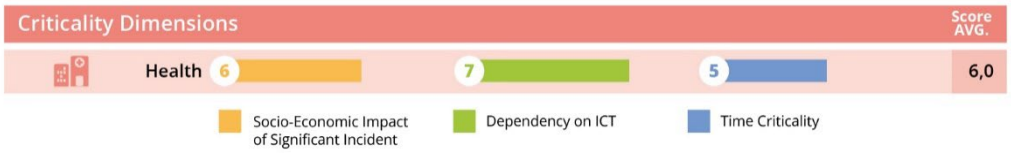
- The operational preparedness of the EU health sector presents a mixed picture. On one hand, entities surveyed—mostly larger organisations—report stronger operational positions, suggesting significant progress in their individual preparedness efforts. On the other hand, national and sector-specific authorities provide a different view, indicating that the sector as a whole still faces considerable gaps in its readiness to handle cybersecurity threats, incidents, and crises. This discrepancy is primarily due to the sector's heterogeneous nature, encompassing a wide variety of entities, devices, and products. Many health entities continue to rely on legacy or outdated systems, which hinder the adoption and implementation of effective cybersecurity measures. The Cyber Europe 2022 exercise[65], which focused on the health sector, uncovered significant weaknesses in its operational preparedness. Despite the insights gained and the roadmap for improvement that emerged from this exercise—representing a step forward—the sector remains inadequately prepared on a broader scale. Notably, there's limited evidence of the sector's ability to respond effectively to large-scale cyberattacks. Substantial work is still needed to achieve consistent, sector-wide operational readiness and address the existing vulnerabilities.

D.4.3 Criticality

Digitalisation in the EU **health sector** is progressing steadily, with advancements improving the efficiency, accessibility and quality of healthcare across Member States. However, this growing reliance on digital systems also introduces new cybersecurity challenges, exposing the sector to various threats and risks.

According to the 2023 ENISA Threat Landscape for Health, EU healthcare providers and especially hospitals (42%) were particularly affected by incidents during the period from January 2021 to March 2023 covered by the report. At the same time, incidents targeted health authorities, bodies and agencies (14%) and the pharmaceutical industry (9%).[66] The same report identified ransomware as the prime threat against health sector entities (54%), both in terms of number of incidents but also in terms of impact and often coupled with a data breach. Additionally, almost half of the total incidents analysed to produce the report (46%) took the form of a threat against the data of health organisations (data breaches, data leaks). Data related threats continue to be one of the main threats in the sector, not only for Europe but also globally. On CIRAS, in 2023, the sector reported 24% of all incidents, the highest volume amongst all sectors reporting to the platform.

[65] Cyber Europe 2022: After Action Report | ENISA
[66] Health Threat Landscape — ENISA



Socio-economic impact:

- The socio-economic impact of a significant incident in the health sector is relatively limited despite its leading role in employment among NIS2-mapped sectors in 2022 and its 6.2% contribution to total value added. While ransomware attacks in this sector can cause substantial financial losses, these are primarily confined to the national level with minimal broader economic effects. As a result, cyber incidents in the health sector typically register a moderate impact, scoring 6/10, due to minor disruptions like temporary service suspensions, with effects largely limited to the sector itself. Unlike incidents in critical sectors such as electricity, disruptions in the health sector are unlikely to significantly affect the overall economy.

Dependency on ICT:

- **The** health sector scores 7/10, reflecting its high dependence on ICT systems. Most core processes rely heavily on ICT tools, with minimal manual backup options available, such as sensors, monitoring devices, AI solutions, and electronic health records, making it challenging to function effectively without them. This reliance is expected to grow further due to the sector's unique role in processing highly sensitive and personal information.

Time criticality:

- The impact of incidents in health is typically felt within a few hours, but the sector has a relatively high tolerance before an outage escalates into a crisis. Critical functions, such as data exchange, can often be postponed or managed through alternative methods, giving the sector a moderate level of time-criticality. However, significant incidents, while not posing an immediate threat, still require proactive attention to prevent disruptions, safeguard the sector's security, and address its limited potential for maturity growth.

D.4.4 Areas for improvement

Based on the above, the following areas of improvement/interventions are proposed to help the sector further develop its cyber maturity:

- **Clarify the interplay and synergies** between NIS2 and the Medical Device Regulation, alongside other policy initiatives such as the AI Act, Cyber Resilience Act, Cyber Solidarity Act, and the EU Health Data Space. Leverage the forthcoming regulatory mapping by NISCG and ENISA (expected in 2025) to guide this effort.
- **Develop and disseminate online toolkits**, including guidelines for the procurement of services, products and infrastructure.
- **Establish tailored methodologies to help entities better understand and manage cybersecurity risks** in their environments. Maintain relevant resources such as ENISA's taxonomy of threats and assets in smart health services and infrastructure as a foundation.
- **Conduct sector-specific exercises, including tabletop simulations, to improve response capabilities at the national level.** Supplement EU-level planned exercises with more frequent localised testing, incorporating guidance on operational technology (OT) security measures.
- **Expand participation in information-sharing and collaboration initiatives**, and launch targeted awareness campaigns to foster a stronger cybersecurity culture across the sector.

D.5 DRINKING & WASTE WATER SECTORS

D.5.1 Sector scope

The **drinking water** and **waste water** sectors include a range of entities critical to maintaining essential services across the EU. In particular:

- **suppliers** and **distributors** responsible for providing water for human consumption[67]
- organisations involved in the **collection**, **disposal**, or **treatment** of urban, domestic, or industrial wastewater[68].

D.5.2 Maturity

The **drinking water sector** has a moderate level of maturity, while the **waste water sector** has a low level of maturity.

Policy framework ang guidance:

- Both the **drinking water** and **waste water** sectors are subject to the NIS2 Directive, which sets baseline cybersecurity objectives for these sectors. While other sector-specific directives exist, such as the EU Drinking Water Directive and the EU Urban Waste Water Treatment Directive, they do not directly address cybersecurity concerns.
- Neither sector benefits from dedicated EU-level authorities or bodies specifically tasked with supporting cybersecurity objectives. As a result, there is greater reliance on national authorities for support and guidance in meeting these objectives. The drinking water sector benefits from national authorities with more experience in supervising the sector, largely due to its earlier inclusion under the NIS Directive. Entities in this sector report receiving some support from national authorities, primarily in the form of general guidance. In contrast, entities in the waste water sector report receiving less significant support, highlighting a disparity in the level of assistance provided.
- Both sectors have access to guidance to support compliance with cybersecurity requirements, though the timeliness and comprehensiveness of this guidance vary.

Risk management and good practices:

- Entities in the **drinking water** sector report higher rates of leadership approval for cyber risk management controls and the adoption of supply chain cybersecurity policies compared to those in the **waste water** sector. On average, **drinking water** entities implement more controls to build trust within their supply chains than their **waste water** counterparts. These entities indicate they are making progress towards developing a solid understanding of cyber risks, enhancing the effectiveness of their risk mitigation measures, strengthening vulnerability management, and keeping up with legacy systems in both IT and OT. In contrast, waste water entities suggest they are still in the process of building their understanding of cyber risks and management practices. While they are making progress in vulnerability management, they continue to struggle with legacy systems and balancing IT/OT security.

[67] excluding those for whom water distribution is only a small part of their broader activities, such as companies primarily focused on other goods.
[68] with exceptions for entities where these activities are only a minor aspect of their main operations.

- National and sector-relevant supervisory authorities report that entities in both the **drinking water** and **waste water** sectors are implementing NIS2-aligned measures to some extent, with **drinking water** entities generally showing more progress in areas such as identifying, protecting against, detecting, responding to, and recovering from cyber threats. Authorities also note that both sectors tend to perform better in post-incident than in pre-incident ones, which may indicate a more reactive risk management culture.

Collaboration and information sharing:

- Entities within the **waste water** sector report minimal participation in information-sharing and collaboration initiatives, whereas entities in the **drinking water** sector report higher levels of participation, primarily through EU-level associations and national ISACs. National-level supervisory authorities for both **drinking** and **waste water** sector entities also engage in such initiatives at the national and EU levels, although their participation is less extensive compared to other sectors (and at the EU level, this may not necessarily be in the context of the two sectors in particular, but rather the other sectors the authorities supervise).
- At the EU level, platforms for collaboration and information-sharing among sector entities are limited, with no dedicated EU-level ISACs, cybersecurity conferences, workstreams, or expert groups. The **drinking water** sector benefits from somewhat more established information-sharing mechanisms than the **waste water** sector, most likely due to its longer experience with cybersecurity requirements relevant to this area, under NIS.

Operational preparedness:

- Across the **drinking water** sector, entities engage in preparedness-building activities, most commonly within their own organisations, and to a lesser extent via national exercises. **Drinking water** sector entities generally report that their current detection and response capabilities enable them to detect and respond mostly to simple attacks on most parts of their infrastructure. **Waste water** sector entities, on the other hand, suggest they are able to detect or respond to only some simple attacks on most parts of their infrastructure.
- From a supervisory authority standpoint, both sectors are seen as requiring more work to develop their preparedness, with the **drinking water** sector so far focusing predominantly on documenting processes and procedures to deal with cyber crises and less so on testing those, while efforts in the **waste water** sector remain modest, again focusing more on documentation of plans rather than testing.
- From an EU-level standpoint, neither of the sectors has ever been engaged in an EU-level sector-relevant cyber drill.

D.5.3 Criticality

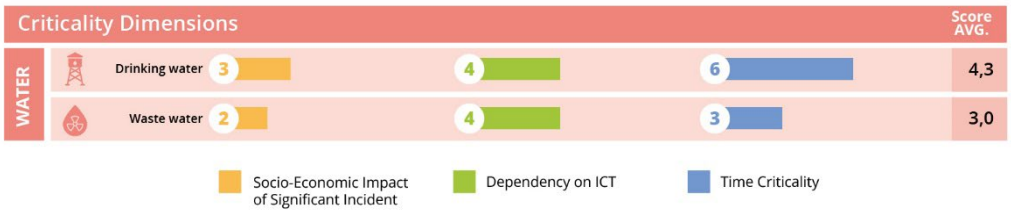
Digitalisation across both water sectors is gaining momentum, with **drinking water** utilities generally ahead due to the critical need for water quality monitoring, which has driven historically higher investment and earlier adoption of remote management, IoT, and cloud technologies to optimise maintenance and efficiency. While **waste water** utilities are also adopting digital solutions, their progress is slower, influenced by the complexity of their systems and historical underinvestment. Currently, both sectors are increasingly leveraging cloud and IoT for better data management, predictive maintenance, and addressing issues like obsolescence and budget constraints.

With their digitalisation advancing steadily, both sectors are starting to experience cyberattacks. According to ENISA's 2024 Threat Landscape report[69], the **drinking and waste water sectors** accounted for 0.64% of events recorded during the reporting period. On CIRAS[70], the drinking water sector represented 1% of all incidents reported in 2023, 44% of which were attributed to

[69] ENISA THREAT LANDSCAPE 2024
[70] Incident reporting — CIRAS

malicious actions. While these numbers are modest for now, the growing adoption of interconnected technologies increases both the exposure to cyber risks and the likelihood of more frequent and impactful cyberattacks in the future.

Despite some shared challenges, the EU water sectors have different levels of criticality, shaped by the socio-economic impact of incidents, their reliance of ICT, and their time-criticality.



Socio-economic impact:

- For **drinking water**, the socio-economic impact of a significant cyber incident is assessed as minimal, likely resulting in minor disruptions with effects largely confined to the sector. **Waste water** shows an even lower level of impact, deemed negligible, with limited disruption or societal consequence expected. This assessment reflects the fact that the core services of both sectors are not yet fully reliant on digital systems, with many processes still supported by traditional, non-digital methods that reduce the immediate vulnerability to cyber threats.

  This assessment also takes into account the economic contribution of these sectors within the EU's business economy which is low across all dimensions considered (i.e., number of enterprises, value added and employment). These figures underscore the sectors' relatively limited economic footprint, supporting their low assessed socio-economic criticality in the event of a cyber incident.

Dependency on ICT:

- Both the **drinking water** and **waste water** sectors rely on digital tools to support core processes, but their dependency on ICT remains limited compared to other sectors. While digital technologies are increasingly used for tasks such as monitoring and managing systems, the pace of digital transformation of both sectors is slower than that of others, with traditional, non-digital methods continuing to play a significant role.

Time criticality:

- The **drinking water** sector demonstrates higher time criticality compared to the **waste water** sector due to the relatively faster onset of societal impact of significant incidents against it. A cyber incident impacting the systems supporting the core functions of the drinking water sector could lead to supply interruptions or compromised water quality, with noticeable effects within a few hours, given its crucial role in public health and daily life. In contrast, the waste water sector has lower time criticality, as disruptions generally result in more localised impacts that may take longer to manifest and affect broader societal functions (e.g., environmental contamination).

D.5.4 Areas for improvement

Based on the above, the following areas of improvement/interventions are proposed to help the sector further develop its cyber maturity:

- **Enhance understanding of cybersecurity challenges relevant to the sectors** – Support national authorities in developing a better understanding of the cybersecurity maturity and unique challenges of both the drinking water and waste water sector entities, so they can provide more effective support to them.

- **Raise awareness around sector-relevant cyber risks** – Increase awareness among sector entities, particularly in the waste water sector, about the evolving cyber risks they face, including supply chain and third-party risks.
- **Promote collaboration and information sharing –** Encourage greater collaboration and information sharing among sector entities in the drinking water sector and promote the adoption of collaboration and information sharing practices among waste water sector stakeholders**.**
- **Support efforts to develop operational preparedness of both sectors** via guidance on how to create effective incident and crisis management plans and support on how to ensure those are actionable.

D.6 DIGITAL INFRASTRUCTURE SECTOR

D.6.1 Sector scope

The digital infrastructure sector consists of entities that are critical to the operation of digital and communication services across the EU. It includes:

- **core internet service providers**, such as Internet Exchange Point (IXP) providers, Domain Name System (DNS) service providers[71] top-level domain (TLD) name registries, and content delivery network (CDN) providers.
- **cloud computing service providers**,
- **data centre service providers**,
- **trust service providers** that deliver essential services such as electronic signatures, electronic seals, electronic time stamps, electronic registered delivery services, and digital certificates, while excluding eID systems, frameworks, and digital identity wallets,
- **telecoms providers**, namely public electronic communications network operators and providers of publicly available electronic communication services.

D.6.2 Maturity

The digital infrastructure sector consists of subsectors with varying levels of maturity. The telecoms sector exhibits a high level of maturity, while the other subsectors fall within the moderate-high maturity range.

Policy framework ang guidance:

- **Telecoms** ranks highest among all digital infrastructure subsectors in this dimension. Although the sector is a recent addition to the scope of the NIS2 Directive, it was covered by cybersecurity provisions within the European Electronic Communications Code (EECC) adopted in 2018. At the EU level, the sector is supported by BEREC (the Body of European Regulators for Electronic Communications) and its Cybersecurity Working Group. Nationally,

[71] excluding operators of root name servers

the sector receives oversight and guidance from experienced national or sector-specific authorities. At the EU level, ENISA has developed common technical guidelines for the sector's security measures and incident reporting in collaboration with ECASEC expert group[72], which is used by about half of EU countries for supervision in line with the EECC.

- **Trust Services** closely follows with comparable scores. In addition to the NIS2 Directive, the sector has been supported by the eIDAS regulation since 2014, with the European Digital Identity (EUDI) regulation[73] building upon eIDAS, having come into force on May 20, 2024. EUDI covers both electronic identification (eID) and trust services for electronic transactions, while NIS2 sets out security requirements for trust service providers. These requirements are not new, as they were previously part of the eIDAS regulation. The Implementing Regulation (EU) 2024/2690 further specifies the technical and the methodological risk—management measures required under NIS2.There are dedicated sector-specific authorities in EU member states that provide detailed cybersecurity guidance for the sector. Overall, the level of supervision under this policy framework is high, but it applies primarily to qualified trust service providers (QTSPs).
- **Core Internet, cloud, and data centre services** rank lower in this dimension. While these sectors are also covered under NIS2, coordinated efforts to ensure better alignment with NIS2 requirements are still in the early stages. However, the Commission's issuing of the Implementing Regulation (EU) 2024/2690 on October 17, 2024, which sets out technical and methodological requirements for cybersecurity risk management and incident notification, is a positive step forward[74]. National authorities provide supervision and support at the national level but may lack the technical expertise required to effectively oversee the sector. While oversight from national authorities is generally viewed positively, sector entities believe there are additional opportunities to enhance the level of support provided. At the same time, both entities within the sector and national authorities see opportunities for enhanced support at the EU level, including ENISA guidance[75] to better meet their needs.

Risk management and good practices:

- Across the **digital infrastructure** sector, many entities report the implementation of robust cyber risk management practices. These include securing leadership approval for cyber risk management controls, adopting cybersecurity policies for the supply chain, and deploying measures to enhance trust within it. Sector entities surveyed also report a solid understanding of cyber risks, alongside effective mitigation measures and security practices for managing vulnerabilities and legacy systems in both IT and OT environments. For **telecoms**, this is corroborated by national and/or sector-specific supervisory authorities, who suggest that the sector is already on track with implementing NIS2-aligned security measures.
- In contrast, a discrepancy is observed between the perceived maturity of sector entities, as assessed by the entities themselves and as assessed by the authorities overseeing or supporting them, across all other digital infrastructure subsectors. Authorities provide a much more modest assessment of the sectors' progress towards implementing NIS2-aligned measures for identifying, protecting against, and detecting cyber threats. This disparity may in part be attributed to the fact that authorities may not yet have a comprehensive enough view of these sectors (some were previously within NIS scope), or they may lack the capacity to supervise them effectively given how diverse they are[76].

[72] https://www.enisa.europa.eu/publications/guideline-on-security-measures-under-the-eecc and https://www.enisa.europa.eu/publications/enisa-technical-guideline-on-incident-reporting-under-the-eecc
[73] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1183
[74] It is noted that IXPs are not in scope of this Implementing Regulation.
[75] ENISA Implementation guidance on security measures under the NIS2 Implementing Regulation 2024/2690
[76] Whenever we identified discrepancies between how authorities and sector entities assessed maturity, we conducted further analysis to understand the reasons behind the disparity. In this case, we examined why authorities perceived the sector as less mature, considering factors such as their level of visibility and supervisory capacity. At the same time, we investigated why entities viewed themselves as more mature, assessing whether this was due to overestimation. By comparing their self-assessments with responses from other entities, we found that entities within this sector were generally more self-critical than those in less digitally mature sectors—likely a manifestation of the Dunning-Kruger effect.

- From an EU-level perspective, the higher score for **telecoms** in this dimension is further supported by EU-wide initiatives that help the sector better understand the cyber risks it faces. These include the 2024 EU-wide risk assessment conducted by NISCG including the sector in its scope[77], the 2024 risk assessment conducted by MS on Europe's communications infrastructures and networks following up on the Nevers call of 9 March 2022[78] the recommendations of which are actively being followed up, but also older work such as the 2019 EU-wide coordinated risk assessment of 5G network security[79] that culminated in the EU 5G Toolbox – a set of risk alleviating measures towards addressing the risks identified that are also being actively followed up by the sector.

Collaboration and information sharing:

- Within the **digital infrastructure** sector, **telecoms** and **core internet services** demonstrate the highest levels of collaboration and information sharing. **Telecoms** benefit from EU-level initiatives such as the ECASEC expert group, the NISCG 5G workstream, and industry-led ISACs like the European Telco ISAC and GSMA's T-ISAC, which effectively bring together national authorities and industry stakeholders. Similarly, national authorities and entities within **core internet services** come together at supranational level via a dedicated NIS Cooperation Group workstream for digital infrastructures, TLD ISAC, CENTR, and Euro-IX, fostering equivalent collaborative efforts.
- The **trust services** sector follows, with EU-level collaboration primarily occurring through the ECATS expert group, which facilitates coordination and information exchange specific to this subsector.
- **Cloud and data centre services**, in contrast, exhibit lower levels of collaboration in this area as no dedicated initiatives exist at EU-level bringing national supervisory authorities and/or industry entities together.
- 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. These annual gatherings provide vital opportunities to strengthen cooperation and address shared challenges across the digital infrastructure sector. At the same time, sector-focused situational awareness reports are produced and disseminated with the sector by ENISA on a bimonthly basis.

Operational preparedness:

- Across the digital infrastructure sector, entities engage in preparedness-building activities, though not to the extent observed in other sectors. Most commonly, entities do so within their own organisations, with fewer participating in community-driven workshops and training sessions. Sector-wide entities surveyed, report that their current detection and response capabilities enable them to manage most simple attacks across most of their infrastructure.
- From a supervisory authority standpoint, **telecoms** sector entities are regarded as the most operationally prepared for incidents or crises within the digital infrastructure domain, with many having documented and tested plans and processes through cyber exercises. **Entities within the remaining sectors** are viewed as less prepared.

  The perception that entities in sectors other than telecoms are less prepared may stem from several factors. It could indicate that these sectors are indeed less prepared, but it is also possible that authorities lack the necessary technical expertise or resources to effectively supervise them. This latter effect could also be compounded by the fact that the digital infrastructure sector is very broad and some of the types of entities within its scope are new to

[77] Risk assessment report on cyber resilience on EU's telecommunications and electricity sectors | Shaping Europe's digital future
[78] Report on the cybersecurity and resiliency of the EU communications infrastructures and networks | Shaping Europe's digital future
[79] EU-wide coordinated risk assessment of 5G networks security | Shaping Europe's digital future

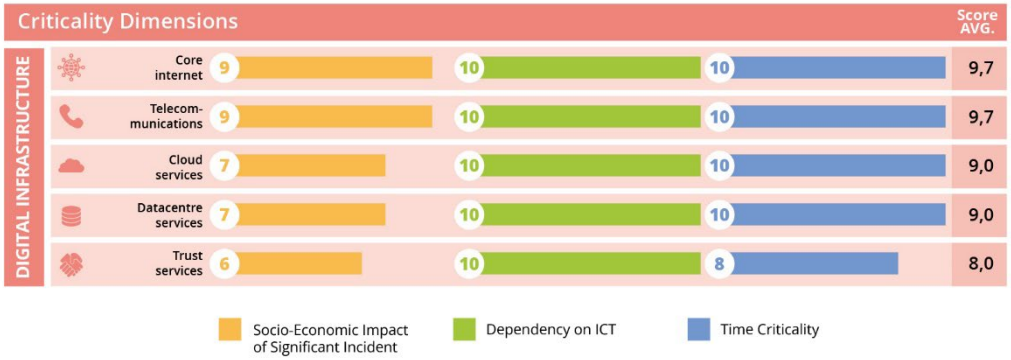
NIS. Therefore, the perceived preparedness levels may reflect a combination of genuine preparedness gaps and limitations in regulatory oversight.

D.6.3 Criticality

The digital infrastructure sector stands as one of the most digitally advanced and rapidly evolving in the EU, serving as the backbone for communication, connectivity, and data services. Through continuous innovation, it has adopted cutting-edge technologies, enhancing both efficiency and scalability. As digital transformation accelerates, the sector plays a critical role in driving the EU's broader digitalisation efforts, while also navigating emerging challenges related to resilience, cybersecurity, and cross-border interoperability.

According to ENISA's 2024 Threat Landscape report[80], the digital infrastructure sector, accounted for 8.16% of all recorded events during the reporting period, with DDoS and data-related threats being most common. On CIRAS[81], the sector reported 29% of incidents reported in 2023, 23% of which were due to malicious actions. Vulnerabilities across sector entities include DDoS attacks on telecoms and core internet infrastructure, exploitation of weak security controls in trust services, data breaches in cloud environments, and physical security risks at data centres. The sector's reliance on complex, interconnected systems and legacy technologies and protocols further increases its exposure to cyber threats.

The digital infrastructure sector comprises subsectors with High levels of criticality.



Socio-economic impact:

- Cyber incidents affecting **core internet services** and **telecoms** networks have the highest socio-economic impact among all digital infrastructure sectors, due to their essential role in facilitating communication and connectivity across all sectors. These incidents can result in widespread service outages, disrupting business operations, emergency services, and public access to critical services. The impact may cascade across various sectors, with knock-on effects to economy. For instance, telecoms outages can cripple e-commerce, banking systems, and key communication channels for both citizens and businesses, resulting in substantial revenue loss and long-term operational disruptions.
- **Data centres** and **cloud services** also have a high socio-economic impact, albeit lower than that of core internet and telecoms as they support a wide array of business applications, services, and digital platforms. Significant incidents impacting the services provided by these sectors can result in service downtime for a range of other sectors, potentially causing delays in service delivery and financial losses, especially for organisations reliant on cloud-based infrastructure for daily operations.
- While the socio-economic impact of cyber incidents in **trust services** is notable, it tends to be lower than that of core internet services, telecoms, data centres, and cloud platforms. Trust

[80] ENISA THREAT LANDSCAPE 2024
[81] Incident reporting — CIRAS – Sum of Communications, Digital Infrastructure and Trust Services figures.

services, such as digital certificates and e-signatures, are integral to secure online transactions and identification processes. Disruptions in these services can delay e-commerce transactions, government services, and financial operations. However, their impact is typically more confined, with the effects often concentrated in sectors that depend heavily on secure digital transactions, such as finance and e-commerce. In these sectors, trust issues can cause reputational damage and delays, but the broader economic repercussions are less severe compared to disruptions in other digital infrastructure sectors.

Dependency on ICT:

- The **digital infrastructure** sector is fundamentally reliant on ICT due to its fully digital nature, forming the backbone of the EU's digital economy and society.
- **Core Internet services** rely entirely on digital systems to support critical functions. IXPs manage digital routing and traffic flow, DNS providers enable internet navigation, CDN providers use cloud-native tools for content delivery, and TLD name registries operate fully digitalised systems to manage domains and provide access to registration data.
- **Cloud service providers** depend on advanced digital infrastructures built on technologies like virtualisation and automation, enabling scalable, efficient, and secure service delivery.
- **Data centre providers** operate fully digital environments to store, process, and manage data, using ICT systems to ensure reliability, security, and operational continuity.
- **Trust service providers** deliver essential digital certification services that underpin secure electronic transactions, authentication, and encryption, ensuring trust in digital ecosystems.
- **Telecommunication network and service providers** include fixed-line operators offering increasingly digitalised fibre-optic networks, Mobile Network Operators (MNOs) managing advanced digital infrastructures such as 4G and 5G networks, and Internet Service Providers (ISPs). These entities leverage technologies like software-defined networking (SDN) and network function virtualisation (NFV) to optimise and enhance digital service delivery and management.

Time Criticality:

- **Core internet services** are highly time-critical, with the impact of significant incidents often being felt almost immediately, typically within a few minutes, due to their foundational role in enabling digital connectivity and communication. For example, routing failures at IXPs can block data traffic regionally or globally, while DNS and TLD outages can disrupt specific TLD zones and DNS resolver services critical for domain resolution. Similarly, CDN failures can degrade access to essential online content and services. Temporary mitigations, such as DNS caching, rerouting, or fallback to origin servers, offer limited resilience but are inadequate for sustained incidents that could severely impact operations across sectors reliant on internet connectivity.
- Similarly, **telecoms** are highly time-critical. Significant cyber incidents affecting telecoms networks, including mobile (4G/5G) and fixed-line providers, can have effects within minutes to a few hours. These networks are foundational, supporting internet access, emergency communication services, IoT systems, and business continuity. Mobile networks are particularly time critical, with impacts felt within minutes, while fixed-line networks may show slightly more resilience. The cascading effects of disruptions within the telecoms sector are severe, as it underpins nearly all digital and communication services. Prolonged outages may disrupt critical services such as emergency calls, online transactions, and remote work. While alternatives like satellite internet or fallback systems exist, they lack the scalability to address the effects of large-scale disruptions effectively.
- Likewise**, cloud computing services** are highly time-critical, with significant cyber incidents often having an impact within hours. Such incidents can disrupt the availability of cloud platforms, leading to severe consequences for dependent sectors. Businesses may lose access to critical applications, platforms may become inaccessible, and services relying on the cloud may face significant delays. While alternative providers, local backups, on-prem systems or offline modes may restore functionality in the short term, migration or recovery processes are often time-consuming and resource-intensive.

- Equally, **data centre services** are highly time-critical, with the impacts of a significant cyber incident potentially manifesting within minutes to hours. The extent of the disruption depends on the redundancy and failover mechanisms in place. Their high time criticality stems from their role in underpinning almost all digital services, including cloud platforms, e-commerce, content delivery, storing and processing of data. While many data centres have robust recovery plans, prolonged outages can spill over and affect dependent sectors severely. Migration to alternative data centres is possible but complex and often takes days to execute effectively.
- The time criticality of the **trust services sector** is also high, though slightly lower than that of the other digital infrastructure sectors. Prolonged outages can affect sectors reliant on secure authentication, such as e-commerce, finance, and digital government services. For example, the inability to verify digital signatures could delay or cancel critical transactions. Although caching mechanisms and alternative validation methods offer temporary buffers, they are insufficient to mitigate the impacts of extended outages.

D.6.4 Areas for improvement

Based on the above, the following areas of improvement/interventions are proposed to help the sector further develop its cyber maturity:

- **Help national authorities deepen their understanding of the Digital Infrastructure sector's composition and unique challenges** to ensure more effective support and supervision of entities within it, particularly in the core internet, cloud and data centre service provision space but also when it comes to infrastructure such as subsea cables where it is not clear at national level who has the responsibility and mandate for their protection and security.
- **Equip national authorities to effectively support entities implement and harmonise security measures and incident reporting requirements outlined in NIS2 and relevant implementing acts**, ensuring consistent support for entities across Member States.
- **Build on recommendations from EU-level risk assessments to address remaining gaps** in telecoms and core internet services, embracing an all-hazards approach that **also takes into account hybrid and emerging threats** such as the implications of post-quantum cryptography. Support national authorities and entities, particularly in the trust services sector, in adapting to emerging technologies to strengthen long-term resilience.
- **Strengthen information sharing and collaboration** among sector entities – particularly for cloud, data centre and trust service providers – and between these entities and national authorities. The sector could also benefit for stronger collaboration between national and/or sector-specific authorities and national and/or sector-specific CSIRTs where those are not under one roof.
- **Support sector entities particularly those with multi-MS presence by harmonising compliance requirements and ensuring a more streamlined cross-border supervision and cross-border crisis management regime** -via clear protocols for interaction among national authorities and access to tools.
- **Strengthen the capacity of national authorities to respond to cross-border incidents** by improving their understanding of available tools and mechanisms (e.g., EU CyCLONE) and validating their application through practical exercises.

D.7 ICT SERVICE MANAGEMENT SECTOR

D.7.1 Sector scope

In the NIS2 Directive, critical entities within the "**ICT services management** (business-to-business)" sector are defined as **managed service providers (MSPs)** and **managed security service providers (MSSPs).** Those providers are usually employed as third parties to support an entity in one or several aspects of its business's technology needs and cyber risk management.

- **MSPs** typically undertake activities like setting up, running, and maintaining ICT products (e.g., desktops, laptops, servers, routers, switchers, firewalls), networks (e.g., LAN, WAN Cloud-based networks), infrastructure (e.g., data centre, storage system, cloud infrastructure) and applications (e.g., CRM, MySQL, Outlook, antivirus, intrusion detection system). MSPs handle the tech side of things by providing services such as installing software, fixing issues, updating systems, and offering ongoing support, either on-site or remotely.
- MSS providers operate as trusted partners to organisations, offering continuous support in addressing cyber risks and enhancing their security posture MSS typically span the monitoring and management of security systems and functions. Services offered by **MSS providers** cover a wide range of activities including threat monitoring, vulnerability assessments (audits, pentesting, etc.), incident response, and overall security architecture management. It is important to note that many sectors depend on ICT service management providers, which is why several sector-specific initiatives, such as DORA, also contain provisions related to MSPs and MSS providers as third-party service providers.

D.7.2 Maturity

The maturity of the ICT service management sector is at Moderate level.

Policy framework and guidance:

- The NIS2 Directive serves as the main cybersecurity framework for the ICT service management sector, providing sector-specific guidelines on implementing cybersecurity measures and reporting incidents to enhance harmonisation across the EU. This framework is supported by additional regulations that address the roles and responsibilities of MSS and MSP providers as third-party service entities, and Implementing Regulation (EU) 2024/2690. While many national authorities established under the NIS1 Directive are prepared to support the sector, entities have yet to experience this support fully, as the sector is newly regulated under the expanded scope of NIS2.

Risk management and good practices:

- In 96% of the ICT service management sector, leaders actively approve cyber-risk management controls, and 70% of entities have established policies for managing supply chain risks. However, when it comes to self-assessing cybersecurity maturity, there is a noticeable gap between entities' perceptions (rating themselves 7/10) and authorities' assessments (1/10). This disparity arises from authorities' limited familiarity with the sector, as it has not yet been formally assessed. At the EU level, a comprehensive understanding of sector-wide risks is lacking, and no unified approach exists to address them. Additionally, the absence of an EU-wide risk assessment for the ICT service management sector highlights the need for improved coordination in risk management.

Collaboration and information sharing:

- In the ICT service management sector, national authorities collaborate effectively; however, stronger cooperation among private entities is needed. Notably, 74% of ICT service management entities reported that they do not participate in collaboration or information-sharing initiatives, highlighting a significant gap in sector-wide engagement.

Operational preparedness:

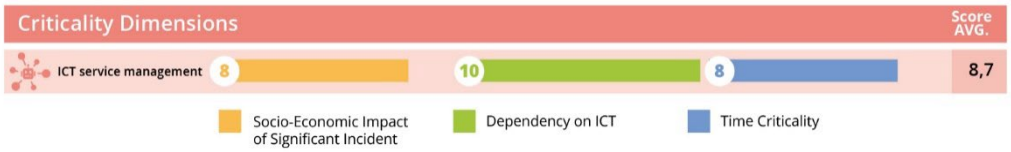
- In their self-assessment of capabilities to detect and respond to sophisticated cyber threats, the ICT service management sector scored an average of 6.8, which is consistent with the overall average performance of other NIS2 sectors. Despite 74% of entities anticipating an increased volume of cyberattacks, participation of this sector in cybersecurity preparedness initiatives remains limited. As a newly regulated sector, ICT service management shows minimal involvement in national-level cyber exercises.

D.7.3 Criticality

The ICT Services Management sector across the EU is characterised by a high level of digitalisation, as it includes managed service providers (MSPs) and managed security service providers (MSSPs), who are integral in supporting organisations with various aspects of technology management and cyber risk mitigation.

According to ENISA's 2024 Threat Landscape (ETL) report, the ICT service management sector accounted for 3.2% of all events recorded during the reporting period from July 2023 to June 2024[82]. The prime threats against the sector were ransomware attacks and data-related threats. In fact, according to the ETL's ransomware strains breakdown, Cl0p ransomware group predominantly targeted entities in this sector, with a 19,5% of events linked to the group, being associated with attacks against ICT service management entities.

The criticality of the ICT service management sector is at High level.



Socio-economic impact:

- The ICT service management sector has a significant socio-economic impact despite ranking 8th in terms of employment among NIS2-mapped sectors in 2022. This high impact stems from the critical dependencies of numerous other sectors on ICT service management for their operations. A disruption in this sector—such as service delays, degradation, or inaccessibility—can lead to widespread noticeable effects and potential spill-over impacts, highlighting its pivotal role in maintaining the functionality and security of interconnected industries.

Dependency on ICT:

- The ICT service management sector is one of the 'digital by default' sectors. ICT service management revolves around managing and optimising IT infrastructures, systems, and services that are entirely digital. Services like monitoring, incident response, software updates, and system maintenance are conducted using specialised digital tools and platforms. Overall,

[82] ENISA THREAT LANDSCAPE 2024

this sector is built around the use, support, and advancement of digital technologies and infrastructures, making it indispensable for the smooth operation of the digital economy.

Time criticality:

- The ICT service management sector's high time criticality stems from the immediate and widespread consequences of any disruption[83], affecting dependent sectors and society within hours and amplifying the urgency for rapid response and recovery. ICT service management supports essential operations in sectors like healthcare, finance, energy, transportation, and government. These sectors rely on ICT services for core functions such as communication, data management, and system operations.

D.7.4 Areas for improvement

Based on the above, the following areas of improvement/interventions are proposed to help the sector further develop its cyber maturity:

- **Promote Collaboration Among National Regulatory Authorities (NRAs):** given the dependency of other sectors on ICT service management sector, encourage continued efforts to bring NRAs together to ensure consistent and unified cybersecurity practices across the EU, fostering greater alignment in regulatory approaches. Once developed, a European certification scheme for managed security services could prove valuable in this context.
- **Centralised, EU-wide information-sharing platform** could enable real-time exchange of threat intelligence, best practices, and incident reports among authorities. This would ensure swift reactions to cybersecurity threats across borders.
- **Strengthen Cross-Border Supervision**: develop a harmonised supervision of cross-border entities, facilitating the sharing of best practices and supporting the effective implementation of NIS2 requirements.
- **Participation in information-sharing and collaboration initiatives** within the sector can be significantly enhanced. Establishing a dedicated information-sharing platform could streamline collaboration and ensure secure and efficient data exchange among stakeholders.

[83] As manifested also during the widespread IT outage of July 2024 - https://www.crowdstrike.com/en-us/blog/falcon-content-update-preliminary-post-incident-report/

D.8 PUBLIC ADMINISTRATION SECTOR

D.8.1 Sector scope

Under the NIS2 Directive, the **public administration sector** includes:

- **public administration** entities at the **central government level**, as defined by each Member State.
- **public administration entities** at the **regional level**, as defined by each Member State based on risk assessments, provided the services they offer are critical to societal or economic stability
- **local public administration entities**, which Member States may choose to include within the Directive's scope.

The identification of entities falling under the NIS2 scope is still underway, which may explain why only 27% of public administrations surveyed as part of our industry survey are currently aware of the Directive's general scope and provisions. Member States have considerable flexibility in determining which organisations qualify as public administrations under NIS2. Consequently, the sector is expected to display significant diversity, reflecting the varied constitutional frameworks and governmental structures across Member States.

D.8.2 Maturity

The maturity of the public administration sector is at Moderate level.

Policy framework and guidance:

- The public administration sector is newly covered by the NIS2 Directive, which introduces a range of cybersecurity requirements. The sector is still in the early stages of implementing these new obligations. While many national authorities have already been established to support entities, the sector has yet to fully experience the benefits of this support, as it is newly regulated under the expanded scope of NIS2. As a result, the sector's engagement with the Directive's requirements is still in the early stages.

Risk management and good practices:

- In 80% of the public administration sector, leaders approve cyber-risk management controls, and 60% have supply chain risk policies in place, the lowest across sectors.
- There's a significant gap between entities' self-assessments (6/10) and authorities' assessments (3/10) of risk management capabilities, reflecting limited familiarity with the sector.
- At the EU level, there's a lack of comprehensive sector-wide risk understanding, highlighting the need for better coordination.

Collaboration and information sharing:

- In the public administration sector, national supervisory authorities work effectively both domestically and with their EU counterparts, engaging in initiatives such as workgroups and expert groups. However, 76% of critical entities within the sector report not participating in collaboration or information-sharing initiatives, indicating a significant gap in sector-wide engagement. Most cooperation is limited to information sharing with national competent authorities, with only 3% of entities being members of national ISACs and 7% of the EU-ISACs, such as ISAC4Cities.

Operational preparedness:

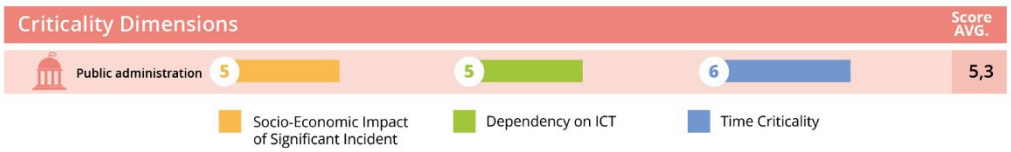
- In self-assessments of their ability to detect and respond to sophisticated cyber threats, public administrations scored an average of 6.7, aligning with the overall performance of other NIS2 sectors. Although the public administration sector ranks third in terms of information security expenditure, with an average of €7.6 million, only one-third of surveyed public administrations are actively enhancing their preparedness through the development of plans, policies, procedures, and training. As a newly regulated sector, however, their participation in national-level cyber exercises remains very low, highlighting a gap in operational readiness despite financial investment in security.

D.8.3 Criticality

In recent years, EU MS have made significant strides in digitalising public administration, focusing on IT-based services and improved efficiency. Despite the many benefits that digitalisation has brought forward however, it has also made the sector a more attractive target for cybercriminals, with public administrations facing a rise in cyberattacks in recent years.

According to ENISA's 2024 Threat Landscape report, cyber incidents targeting the public administration sector, accounted for 19% of all events recorded during the reporting period from July 2023 to June 2024[84], making it the most affected sector. DDoS attacks were the primary threat, impacting a wide range of sectors, with public administration being the most targeted, accounting for 33% of DDoS incidents. At the same time, **public administration** also emerged as a key target for data-related threats, accounting for 12% of incidents and ranking as the second most affected sector. Malware attacks impacted 11% of **public administration**, while social engineering attacks targeted 10%. On CIRAS[85], the sector reported 3% of all incidents in 2023, 81% of which were attributed to malicious actions.

The criticality for the public administration sector is at Moderate level.



Socio-economic impact:

- The public administration sector ranks lower than energy sector in terms of employment among NIS2-mapped sectors in 2022 and constitutes 0.8% share in business economy. However, this sector is vital to the functioning of society, with 48% of people relying on digital public services. Although the socio-economic impact of a significant incident in this sector may be moderate, it can still cause noticeable disruptions. The effects may manifest in temporary suspensions of services, potentially affecting a wide range of critical functions. These incidents may not cause long-term damage but could disrupt essential services that the public relies on.

Dependency on ICT:

- The public administration sector in the EU demonstrates a medium level of digitalisation. Over recent years, many Member States have initiated significant reforms to enhance service delivery and drive digital transformation within public administration. These reforms focus on the development of IT-based public services, consolidating data centres, streamlining operations, and improving overall efficiency. As a result, digital tools now support several core administrative processes, leading to greater productivity and service delivery. However,

[84] ENISA THREAT LANDSCAPE 2024
[85] Incident reporting — CIRAS

manual and analogue methods are still in use, indicating that while digitalisation is progressing, it has not yet fully replaced traditional methods across all public administration functions.

Time criticality:

- Cyber-attacks on public administration often cause disruptions in the availability of public services or delays in administrative processes. However, because many public services can be handled manually in cases of system failure, the overall societal impact is typically moderate in the short term, with minimal direct consequences for critical infrastructure.

D.8.4 Areas for improvement

Based on the above, the following areas of improvement/interventions are proposed to help the sector further develop its cyber maturity:

- **Enhanced preparedness and response**: facilitate access to simulation environments where public administration entities can test their incident response capabilities in a risk-free setting.
- **Awareness raising**: conduct campaigns to raise awareness of the NIS2 Directive's provisions, targeting both public administration leadership and operational staff to ensure they understand compliance requirements.
- **Strengthen sectorial threat awareness:** to enhance the sector’s understanding of the threats it faces.
- **Collaborative engagement**: organise regular workshops and collaborative sessions to improve cross-sectoral engagement and foster partnerships between public administration entities and private stakeholders.

D.9 SPACE SECTOR

D.9.1 Sector scope

The NIS2 Directive applies to **operators of ground-based infrastructure** supporting space-related activities, *excluding providers of public electronic communications networks*. These operators are usually organisations or entities responsible for running facilities and equipment on the ground essential for supporting space-related activities and services. Examples of the ground assets encompass transportation, launch, and operations, with a focus on secure practices, critical infrastructure, and the management of control centres, monitoring stations, and ground stations.

In addition, the NIS2 Directive (Annex II) **also covers the manufacturing sector** engaged in the **production**[86] **of satellites and equipment crucial for supporting space activities** such as computer, electronic, optical products and transport equipment[87].

The NIS2 Directive primarily focuses on infrastructures owned, managed, and operated by Member States or private entities, excluding those operated by or on behalf of the Union under its space program (i.e., Galileo, EGNOS). This scope includes Low Earth Orbit (LEO) satellite communication (SatCom) systems, Geostationary Orbit (GEO) and Medium Earth Orbit (MEO) satellite systems. LEO systems enable a broad range of essential services, including broadband internet, IoT connectivity, emergency response, and secure government communications. While satellite technologies enhance 5G connectivity by extending coverage to remote and underserved areas, they also improve network reliability.

GEO are predominantly used for television broadcasting, weather forecasting, and military communications. MEO satellites are commonly employed in navigation, remote sensing, and communication services, bridging the gap between LEO and GEO in terms of both latency and coverage.

The NIS2 Directive doesn't cover the space segment which involves satellites orbiting Earth, and can be divided into two main categories: **Satellite operations**, or the 'platform', which includes all assets necessary to operate and maintain a satellite in orbit, and **Mission execution (satellite payload)**, which includes the assets required to carry out the mission.

D.9.2 Maturity

The maturity of the space sector is at Moderate level.

Policy framework and guidance:

- The NIS2 Directive serves as the primary cybersecurity framework for the space sector. Alongside this directive, the sector relies on non-binding standards and guidance from international organisations, national space agencies, and standardisation bodies. The European agency EUSPA also plays a key role in supporting the industry. While many national authorities are already in place to assist entities, the space sector is newly regulated

[86] Production includes assets needed for satellite planning, design, development, cryptography, testing, and simulations.
[87] This includes semiconductors, microprocessors, and circuit boards, which are vital for satellite systems, signal processing, and telemetry.

under the expanded scope of NIS2. Consequently, the sector is still in the early stages of aligning with the Directive's requirements and realising the benefits of this support.

Risk management and good practices:

- In the space sector, 80% of leaders approve cyber-risk management controls, and 66% have supply chain risk policies. However, given the sector's heavy reliance on supply chains, this is insufficient. While traditional security practices are central, the adoption of emerging technologies like zero-trust and Post-Quantum Cryptography remains minimal (2%), highlighting room for improvement. Finally, the space sector received one of the lowest perceived maturity scores, with entities rating themselves 5/10 and authorities scoring them 1/10, the latter reflecting also a limited understanding of the sector.

Collaboration and information sharing:

- In the space sector, national supervisory authorities collaborate effectively both domestically and with their EU counterparts through initiatives like workgroups and expert groups. However, the majority of entities report limited participation in collaboration or information-sharing initiatives, with most cooperation restricted to sharing information with national authorities and involvement in associations. Established in 2024, the EU Space ISAC is expected to promote more proactive sharing of security-related information, incidents, cyber trends, vulnerabilities, and threats among commercial space operators.

Operational preparedness:

- In self-assessments of their ability to detect and respond to sophisticated cyber threats, the space sector scored below the average performance of other NIS2 sectors. This may be attributed to the remote nature of space systems complicating the detection and response to incidents, and the design of many space-based assets, which often lack modern security considerations, leaving them particularly vulnerable to contemporary cyber threats. The space is also one of sectors with the lowest investment in information security. Entities in space industry are developing their preparedness via plans, policies, procedures and training, however their participation in national-level cyber exercises remains very low.

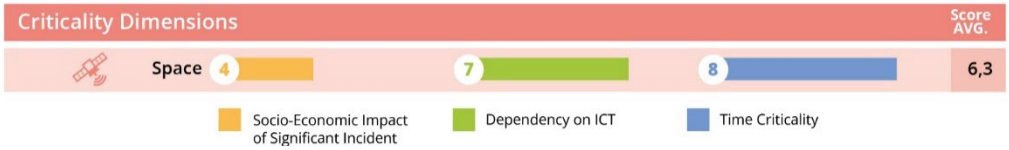
D.9.3 Criticality

The EU space sector is highly digitalised, relying heavily on ICT for crucial operations like satellite communications, data processing, and control functions. This sector uses advanced technology, real-time analysis, and depends on supply chains for off-the-shelf components, all of which increase its vulnerability to cyberattacks.

While the list of cyber incidents affecting LEO, GEO and MEO systems remains relatively short, attacks predominantly fall into two categories: data theft—often achieved through reverse engineering of user link transmission techniques—and denial of service (DoS) attacks targeting either the ground or space segments. Such disruptions can result in degraded performance or complete service outages, posing significant risks not only to the space sector but also to dependent industries and services reliant on satellite-based connectivity[88]. As reliance on LEO, GEO and MEO systems grows, ensuring their cybersecurity is essential to safeguarding critical infrastructure and minimising potential cascading impacts across the EU economy.

The criticality of the space sector is at Moderate level.

[88] LEO SATCOM Cybersecurity Assessment



Socio-economic impact:

- The socio-economic impact of a significant incident in the space sector cause temporary disruptions with manageable socio-economic impact, having minimal impact on operations in maritime and aviation due to the low frequency of attacks. However, as reliance on satellite systems increases and cyber threats grow more sophisticated, the potential impact is expected to rise significantly. Future attacks could result in prolonged outages, costly delays, and widespread inefficiencies. As a result of these factors, the sector's criticality is expected to grow in the future.

Dependency on ICT:

- The space sector is highly dependent on ICT due to its reliance on digital systems for mission-critical operations, including satellite communications, data processing, telemetry, and control functions. Advanced technologies such as satellite management software, ground station communication systems, and real-time data analytics require seamless integration and robust ICT infrastructure to ensure operational efficiency and reliability. Additionally, the sector's reliance on global supply chains, particularly Commercial Off-The-Shelf (COTS) components, for communication, launch, data reception, and control facilities further underscore the importance of ICT. These off-the-shelf components, while cost-effective, can introduce vulnerabilities if not properly secured, as they often lack industry-specific customisation or hardened security measures, increasing the exposure of space operations to cybersecurity risks.

Time criticality:

- Recovery from cyberattacks is time-critical in the space sector because disruptions can rapidly cascade across multiple dependent sectors, causing significant societal and economic impacts. Satellite-based systems provide essential services such as global navigation, communication, weather forecasting, and critical infrastructure management. A cyberattack compromising these systems can immediately affect industries like aviation, shipping, and emergency services, where timing and precision are crucial.

D.9.4 Areas for improvement

Based on the above, the following areas of improvement/interventions are proposed to help the sector further develop its cyber maturity:

- **Encourage Workshops and Training Programs**: Organise workshops, webinars, and training sessions to increase awareness and improve cybersecurity skills in the sector, focusing on practical scenarios and the latest cybersecurity challenges.
- **Enhance preparedness and response:** Facilitate access to simulation environments and exercises where public and private space operators can test their incident response capabilities in a risk-free setting.
- **Develop guidelines and best practices to** support the implementation of thorough security analysis and testing of components before deployment. Such guidelines could encourage stakeholders within the space and satellite technical community, along with other industry players involved in the development, manufacturing, or testing of satellite systems, to conduct comprehensive security evaluations. Currently, just nearly half of organisations (49%) that use COTS in the space sector perform security testing on products before integration.
- **Foster collaboration and information exchange** on threats, vulnerabilities, and incidents, recognising that the space sector is inherently cross-border and requires coordinated international efforts. Collaboration and information exchange should be pursued both within the sector, across other sectors, and with international partners.

ANNEX E SURVEY PARTICIPATION

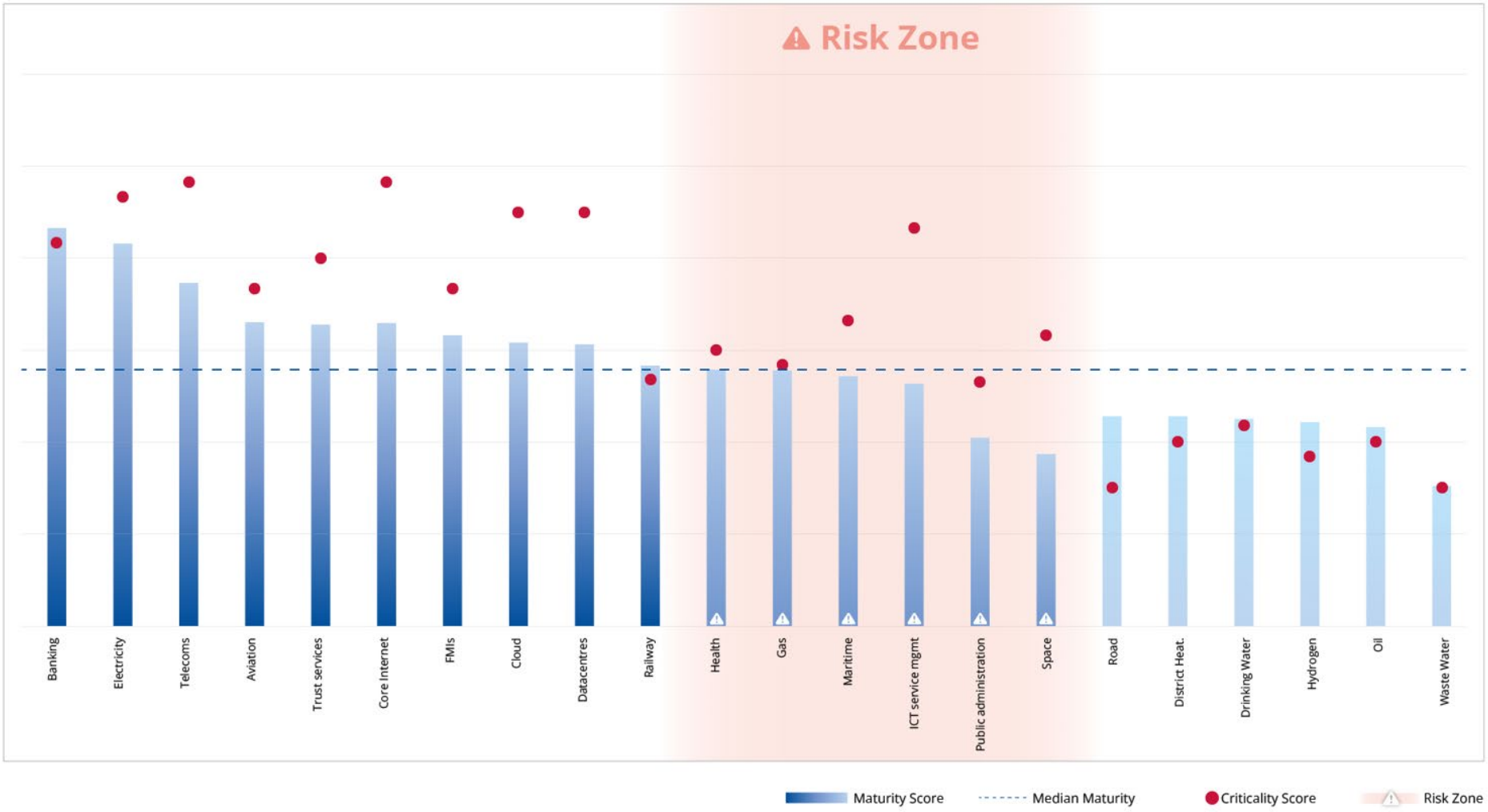
Below we provide a breakdown of responses processed per sector, per survey:

In-scope sector	Responses received from industry[89]	Responses received from authorities[90]
Energy - Electricity	180	22
Energy - District Heating and Cooling		22
Energy - Oil		21
Energy - Gas		22
Energy - Hydrogen		22
Transport - Aviation	175	23
Transport - Railway		23
Transport - Maritime		21
Transport - Road		21
Banking	130	22
FMIs	40	34
Health	150	22
Drinking water	45	16
Waste water	25	16
Digital Infra - Core internet	261	21
Digital Infra - Cloud		21
Digital Infra – Data centres		21
Digital Infra - Telecoms		21
Digital Infra - Trust		22
ICT service management	100	18
Public Admins	150	16
Space	44	18
TOTAL	1350	465

[89] A total of 1350 entities responded to our industry survey. The survey was run in the context of a broader study focused on understanding how cybersecurity policy impacts entity decisions across the Union. The primary goal of that study is to ensure representation from all EU Member States, rather than sector-specific focus. As such, information gathered is at the sector level, rather than delving into subsectors. This was accounted for in our study.

[90] A total of 59 sector-specific or sector-agnostic national authorities across Europe replied to our authorities' survey. Authorities were asked to provide insights only for the sectors they support or supervise from a cybersecurity perspective, with some national authorities overseeing multiple sectors. Responses were received from all but four EU Member States.

ANNEX F RISK ZONE



TP-01-25-002-EN-N

ABOUT ENISA

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

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

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

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

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