EUROPEAN UNION AGENCY
FOR CYBERSECURITY

MSS MARKET ANALYSIS

An Analysis of the Managed Security Service Market

JUNE 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 information and communication technology products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

To contact the authors, use market@enisa.europa.eu.
For media enquiries about this paper, use press@enisa.europa.eu.

AUTHORS (IN ALPHABETICAL ORDER)

Sofia Roxana Banica (ENISA), Benedetta Burston (Università Bocconi), Lisa Fontanella (Università Bocconi), Louis Marinos (ENISA), Greta Nasi (Università Bocconi), Silvia Portesi (ENISA), Leonardo Saveri (Università Bocconi).

ACKNOWLEDGEMENTS

We would like to thank the respondents to the survey for providing the data, along with the national liaison officers' representatives, the ENISA Advisory Group members, Aljosa Pasic, and the ENISA colleagues who reviewed drafts of this deliverable and provided their feedback.

LEGAL NOTICE

Luxembourg: Publications Office of the European Union, 2025

COPYRIGHT NOTICE

ISBN 978-92-9204-702-3, doi:10.2824/7566738

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Managed security services (MSS) are continuing to gain in importance in relation to enhancing cybersecurity levels for almost all types of customers, from small to large organisations and from the public to the private sector, and for all types of infrastructure, from commercial to critical. The MSS market is important for the internal market of the European Union (EU), as shown by a dedicated amendment to the Cybersecurity Act (CSA) ([1]) to clarify the definition and an ongoing request to develop a candidate certification scheme. MSS are a focus of the European Commission and the Member States. In a situation of increasing infrastructure complexity, MSS are seen as an important tool in mastering cybersecurity challenges and enhancing cybersecurity cyber resilience in the EU.

This report addresses the market for MSS on both the demand and the supply side. It addresses MSS usage patterns, compliance and skills certification, threats, requirements, incidents and challenges relating to MSS, along with MSS market and research trends.

The aim of this analysis is to assess the characteristics of the MSS market to the benefit of various stakeholders who will find this information useful for their plans. At the same time, its aim is to deliver market-related data in support of other activities within the EU, such as the CSA amendment and the EU Cybersecurity Reserve provided for in the Cyber Solidarity Act ([2]), within the scope of the European Union Agency for Cybersecurity's (ENISA) role therein. For the purpose of this work, internal and external synergies were established.

For this analysis, ENISA performed primary research, i.e. a survey involving the main stakeholder types in the MSS ecosystem by means of dedicated questionnaires. The survey was disseminated via ENISA's social media channels and the ENISA website to all related European Commission and Member State groups, and also via direct emails. A number of replies were collected via the survey. However, as the data collected, especially from the demand side, are limited in comparison to the entire existing demand and supply of MSS, it is not possible to provide complete assurance that the dataset used for the analysis is representative of the MSS needs of all Member State organisations.

Qualitative checks of the data collected from the survey and validation of the findings were carried out via desk research.

Although international organisations participated in the ENISA survey, the main geographical focus of the report remains the EU.

Among the conclusions drawn from this market analysis, the following can be highlighted.

- Investment trends from the demand side reveal that most entities allocate less than 10 % of their budget to MSS.

([1]) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15, https://eur-lex.europa.eu/eli/reg/2019/881/oj.

([2]) Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act), OJ L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj.

- The preference for hybrid solutions on the demand side and periodic procurement reviews suggests a balance between stability and adaptability, ensuring security investments align with long-term operational needs.
- The main barriers to MSS adoption include cost concerns, a lack of internal expertise, provider-related issues regarding the customisation of service level agreements (SLAs) and challenges with technical and process integration.
- Regulatory adoption remains supplier driven, with service providers investing more in frameworks such as information security management systems and quality systems. The demand side exhibits stronger engagement in specific areas such as information security management system auditing and supplier relationship management, reflecting a targeted regulatory approach.
- The perception of cyber threats varies among stakeholders, leading to gaps in the adoption and implementation of MSS. This creates blind spots in threat management strategies, ultimately affecting overall resilience.
- Current MSS-applicable regulatory frameworks emphasise technical controls, such as detection and response mechanisms, with a secondary emphasis on governance issues. However, there is a gap in the adoption of operational processes between demand and supply. This may generate imbalances between technical implementation and operations security governance, the latter of which is often necessary for long-term resilience and service performance.

1. INTRODUCTION

This European Union Agency for Cybersecurity (ENISA) report presents an analysis of the managed security services (MSS) market covering the various services included in MSS offerings. It highlights cybersecurity-related characteristics of the services offered for all types of organisations. Based on this analysis, some observations have been made and conclusions drawn on the structure, dynamics and development of the MSS market.

ENISA mainly collected the data for this report via an online survey. The MSS market data collected have also been used, among other purposes, for an analysis conducted by ENISA to assess potential MSS certification needs ([3]).

1.1 AIM OF THE REPORT

This report addresses the market for MSS on both the demand (need for MSS) and the supply (offering of MSS) side.

Regulation (EU) 2025/37 ([4]) adds the following definition of MSS to the Cybersecurity Act (CSA):

> *a service provided to a third party consisting of carrying out, or providing assistance for, activities relating to cybersecurity risk management, such as incident handling, penetration testing, security audits and consulting, including expert advice, related to technical support*.

The information collected for this analysis includes all cybersecurity-related characteristics of services, cybersecurity requirements, threat exposure and market trends, but also demographic information on the main market stakeholders.

The geographical scope of the analysis mainly covers the European Union (EU).

Its aim is to understand the MSS market in the EU and, at the same time, to deliver market-related data in support of other activities within the EU, such as the CSA amendment and the Cyber Solidarity Act, within the scope of ENISA's role therein.

1.2 LEGAL AND POLICY CONTEXT

Article 8(7) of the CSA states that:

> *ENISA shall perform and disseminate regular analyses of the main trends in the cybersecurity market on both the demand and supply sides, with a view to fostering the cybersecurity market in the Union*.

Furthermore, recital 42 states that:

> *ENISA should develop and maintain a 'market observatory' by performing regular analyses and disseminating information on the main trends in the cybersecurity market, on both the demand and supply sides*.

This analysis of MSS has been conducted in implementation of Output 7.1, 'Market analysis on the main trends in the cybersecurity market on both the demand and the supply side, and

([3]) See ENISA, *Feasibility Study on EU Cybersecurity Certification For Managed Security Services*, that aims at supporting the future Ad-Hoc Working Group in drafting the candidate scheme for the EU cybersecurity certification for MSS.

([4]) Regulation (EU) 2025/37 of the European Parliament and of the Council of 19 December 2024 amending Regulation (EU) 2019/881 as regards managed security services, OJ L, 2025/37, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/37/oj.

evaluation of certified products, services and processes', under Activity 7, 'Supporting the European cybersecurity market and industry', of the 2024 ENISA work programme ([5]). Elaborations on the market uptake of cybersecurity products, services and processes contribute to ENISA's strategic objectives of a 'high level of trust in secure digital solutions' and 'empowered and engaged communities across the cybersecurity ecosystem'.

Recital 3 of Regulation (EU) 2025/37 states that MSS 'have gained increasing importance in the prevention and mitigation of incidents. Accordingly, the providers of those services are considered to be essential or important entities belonging to a sector of high criticality' pursuant to the **NIS 2 Directive** ([6]).

The MSS market is important for the EU's internal market, as shown by a dedicated amendment to the CSA to clarify the definition of MSS and an ongoing request to develop a candidate certification scheme.

As stated in a recent European Parliamentary Research Service breifing on MSS, although MSS are key for the prevention and mitigation of cybersecurity incidents:

> *they were not included in the scope of the EU cybersecurity certification framework in the 2019 Cybersecurity Act. As some Member States have begun adopting certification schemes for managed security services that are divergent or inconsistent, there is a need to avoid fragmentation in the internal market. The present proposal therefore includes targeted amendments to the scope of the Cybersecurity Act, seeking to enable managed security services schemes by means of Commission implementing acts* ([7]).

These amendments to the CSA were recently adopted under Regulation (EU) 2025/37, and entered into force on 4 February 2025. Through them, among other things, MSS will fall under the framework for the establishment of European cybersecurity certification schemes.

With these recent amendments the CSA intends:

> *to complement the horizontal regulatory framework establishing comprehensive cybersecurity requirements for products with digital elements pursuant to [the Cyber Resilience Act ([8])] by providing for security objectives for managed security services as well as the application and trustworthiness of those services* ([9]).

Furthermore:

> *Managed security service providers can also play an important role in relation to Union actions supporting response and initial recovery in cases of significant incidents and large-scale cybersecurity incidents, relying on services from trusted private providers and on testing of critical entities for potential vulnerabilities based on Union level coordinated security risk assessments. The certification of managed security services could play a role in the selection of trusted managed security service providers as defined in [the Cyber Solidarity Act]* ([10]).

([5]) ENISA, *ENISA Single Programming Document 2024–2026*, Publications Office of the European Union, Luxembourg, 2024, https://data.europa.eu/doi/10.2824/010827, pp. 74 ff.
([6]) 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 (NIS 2 Directive), OJ L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.
([7]) European Parliament: European Parliamentary Research Service, Negreiro Achiaga, M. D. M., 'Managed security services', PE 754.556, 25 October 2024, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)754556.
([8]) Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), OJ L, 2024/2847, 20.11.2024, ELI: https://eur-lex.europa.eu/eli/reg/2024/2847/oj.
([9]) Recital 2 of Regulation (EU) 2025/37.
([10]) Recital 5 of Regulation (EU) 2025/37.

1.3 SCOPING MSS

In accordance with the ENISA cybersecurity market analysis framework ([11]), we performed a breakdown analysis of the services offered in the market segment/area of MSS. Under the framework, this breakdown is referred to as a 'value stack', and is defined as a collection of services contributing to the value proposition of an organisation. The breakdown of services offered is derived from an analysis of three different types of source: supply-side portfolios, demand-side usage patterns and other market analyst reports.

As regards the MSS, the following services have been identified, consolidating offerings found in the relevant market. They are grouped together in generic categories characterising individual segments of MSS offered.

Security solution and technical services:

- identity and access management, including privilege management;
- managed data security, including data loss prevention, managed backup and business continuity management;
- endpoint security management, including antivirus, update/patch management and other endpoint protection measures (e.g. end-device encryption);
- network perimeter and infrastructure security, including intrusion detection systems, intrusion prevention systems, firewalls and secure access service edge;
- managed detection and response, including managed security information and event management, threat hunting and reverse engineering;
- technical assessment services, including vulnerability scanning and penetration testing;
- threat management services, including cyber threat intelligence sharing;
- managed cloud security.

Consulting and deployment services:

- compliance assessment;
- audit and reporting;
- risk management;
- development of simulations/exercises, including building, testing and improving exercises for incident detection and incident response;
- maturity and policy assessments;
- deployment/integration;

Training services:

- simulation/exercises, including through the participation of staff in exercises;
- employee security training/awareness.

In the absence of a relevant standard breakdown of MSS, the assumed set of MSS services in this report has been generated by compiling vendor offerings and collecting good practices and the opinions of field experts.

These services constitute the basis for the present MSS market analysis, i.e. they are used to assess service offerings and service needs, but also standardisation needs, requirements, purchasing criteria, etc.

The abovementioned services can be implemented and delivered to customers (i.e. the demand side) through a variety of delivery models, depending on the kind of infrastructure used to host the service. In this analysis, we discriminate among the following four infrastructure delivery models for hosting MSS.

([11]) ENISA, Wright, D., Tomić, N., Portesi, S. and Marinos, L., *ENISA Cybersecurity Market Analysis Framework V2.0 (ECSMAF)*, 2023, https://data.europa.eu/doi/10.2824/96301.

- **On-site.** The delivered service is hosted entirely within the infrastructure of the customer.
- **Remote.** The delivered service is hosted entirely within the infrastructure of the supplier (e.g. dedicated/shared security operations centre).
- **Cybersecurity as a service.** The delivery is implemented through a subscription. The service can be integrated into the corporate infrastructure of the customer.
- **Hybrid.** This delivery model consists of a mix of the abovementioned delivery models.

Both MSS service breakdowns and delivery models are important for understanding the market. They are used throughout the present analysis to assess the current status of supply and demand, but also future development and implementation plans.

1.4 ENISA SURVEY ON MSS

When conducting a market survey, ENISA typically mobilises a portion of its stakeholders by means of a survey. The survey is used in part fulfilment of the input requirements that precede data analysis and a desk study. To a great extent, the observations and conclusions in this report are the outcome of expert analysis, in which the survey results play a role. By the same token, the survey results do not constitute the exclusive input, and the collective knowledge and expertise of the market team play the key role. It is important to highlight the profile of the respondents, because many or all of them represent expert organisations in the field. In addition, a fair number of responses originated from public authorities across the Member States, which in the light of varying maturity levels across the Member States can be deemed as being largely sufficient.

ENISA carried out a survey to collect information on MSS, with a focus on:

- MSS stakeholder demographics;
- MSS adoption and use;
- MSS needs and capabilities;
- MSS offerings;
- MSS-related threats;
- MSS requirements and challenges;
- MSS-related research; and
- regulatory practices for MSS.

Through the survey, ENISA collected data from the following stakeholder types:

- **supply side** (i.e. vendors/providers of MSS);
- **demand side** (i.e. users of MSS, from both the public and the private sector);
- **research organisations** (i.e. members of organisations conducting research on MSS), also referred to in this report as ‘R & D’.
- **bodies involved in regulatory activities** (i.e. competent national regulatory bodies active in MSS regulatory activities), also referred to in this report as ‘regulators’.

The survey underwent a process that included various phases, namely dissemination, pre-registration and collection of responses. The table below provides information on these phases.

Table 1: Overview of survey phases and data collection

Survey phase	Recipients/respondents	Comment
Dissemination	Around 800 organisations worldwide	Via the ENISA website and social media to all ENISA groups and professional associations, and via direct email messages to potential participants
Pre-registration	Around **170**	Worldwide coverage

Survey responses received	**83** (49 % of those who had pre-registered) *Balance of responding stakeholders*: supply: 38 (46 % of total) demand: 30 (36 % of total) regulators: 13 (16 % of total) R & D: 2 (2 % of total)	Worldwide coverage

The dataset of the present analysis consists of around 3 700 data points with the following features:

- a balanced sample of demand and supply organisations;
- a mix of large and smaller organisations, on both the demand and the supply side;
- suitable coverage of the EU geographical space; and
- sufficient coverage of EU regulatory bodies, as the interest, availability and appetite vary across the Member States.

The survey was disseminated via ENISA's social media channels and the ENISA website to all related European Commission and Member State groups, and also via direct emails. Given the typical outreach of ENISA activities, it can be argued that the responses are representative of EU entities and international entities with an EU presence. However, as the data collected, especially from the demand side, are limited in comparison to the entire existing demand and supply of MSS, it is not possible to provide complete assurance that the dataset used for the analysis is representative of the MSS needs of all Member State organisations.

In terms of the validation of the results, the analysis and the final conclusions have been reviewed by various subject-matter experts, such as ENISA experts, members of the ENISA Advisory Group and the ENISA National Liaison Officers Network.

1.5 TARGET AUDIENCE OF THE REPORT

The target groups that may benefit from the results of the analysis are listed below, together with short explanations of the information included in the report that may be useful to the different target groups.

Demand-side organisations.

- The ENISA MSS market analysis will deliver information on common MSS user requirements, threat exposure, perceived market barriers, common models of MSS usage, etc. As such, this report will be useful for end users of MSS, as it provides a variety of data about the perceptions and experiences of the MSS users that participated in the survey (i.e. demand-side organisations).

Supply-side organisations.

The ENISA MSS market analysis will be useful for understanding demand requirements, perceived threat exposure, trends in models of MSS usage, etc. Standardisation and certification requirements will lay the foundations for forthcoming activities in the areas of skills development and certification.

European Commission, Member State organisations and regulatory bodies.

- Assessed MSS requirements are provided as input within the Cybersecurity Reserve provided for in the Cyber Solidarity Act.

- Member States' MSS standardisation and certification needs serve as input into the CSA amendment.

Research organisations.

- The ENISA MSS market analysis will be useful for understanding supply and demand requirements, perceived threat exposure, market trends and trends in models of MSS usage, market barriers, and innovation and research needs.

Industry and cross-sectoral associations.

- The MSS analysis report may help in the analysis of requirements, challenges, market opportunities, trends, etc. Moreover, it provides related standards and certifications for the design, implementation, deployment and operation of MSS.

1.6 STRUCTURE OF THE REPORT

The structure of this report is as follows.

- **Section 1.** Introduction.
- **Section 2.** Demographics of the stakeholders involved.
- **Section 3.** MSS usage patterns.
- **Section 4.** Compliance and skills certifications.
- **Section 5.** Threats, requirements, incidents and challenges.
- **Section 6.** MSS market and research trends.
- **Section 7.** Concluding remarks.

2. DEMOGRAPHICS OF THE STAKEHOLDERS INVOLVED

This section provides a comprehensive analysis of the demographics of the entities that participated in the survey, namely participating users (demand side), suppliers and regulatory bodies. Due to the limited number of replies received from R & D organisations, the R & D sample was considered too small to be used for the demographic analysis below. However, in the rest of the report, input received from R & D has been taken into account, for example where the data from R & D could be consolidated with relevant data from the other stakeholder types, such as in the case of market and research trends (see Section 6).

2.1 OVERVIEW OF DEMOGRAPHICS FOR DEMAND, SUPPLY AND REGULATORS

Figure 1: Overview of geography across participating organisations

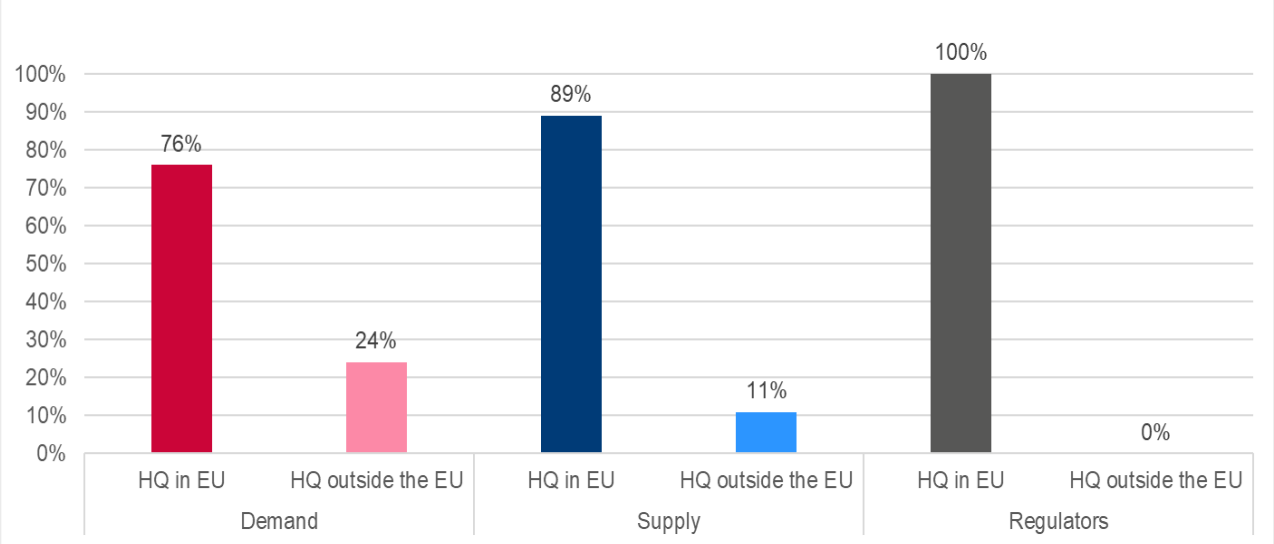


Figure 2: Organisation size by type of respondent – number of employees

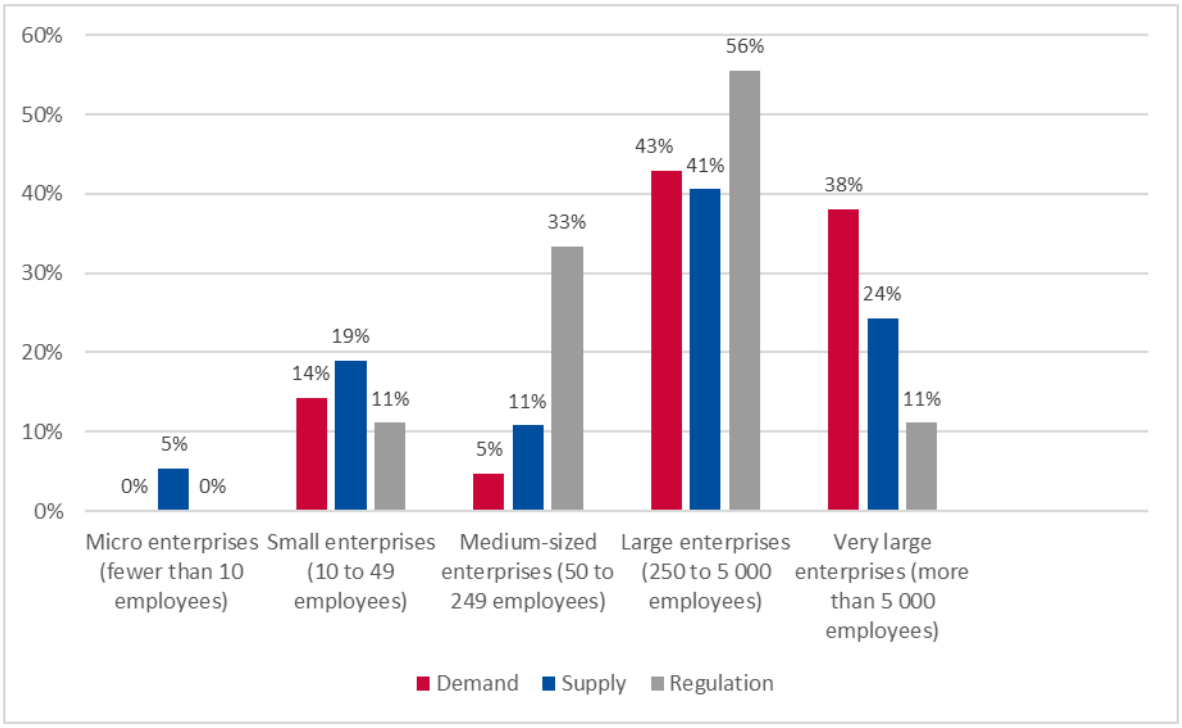
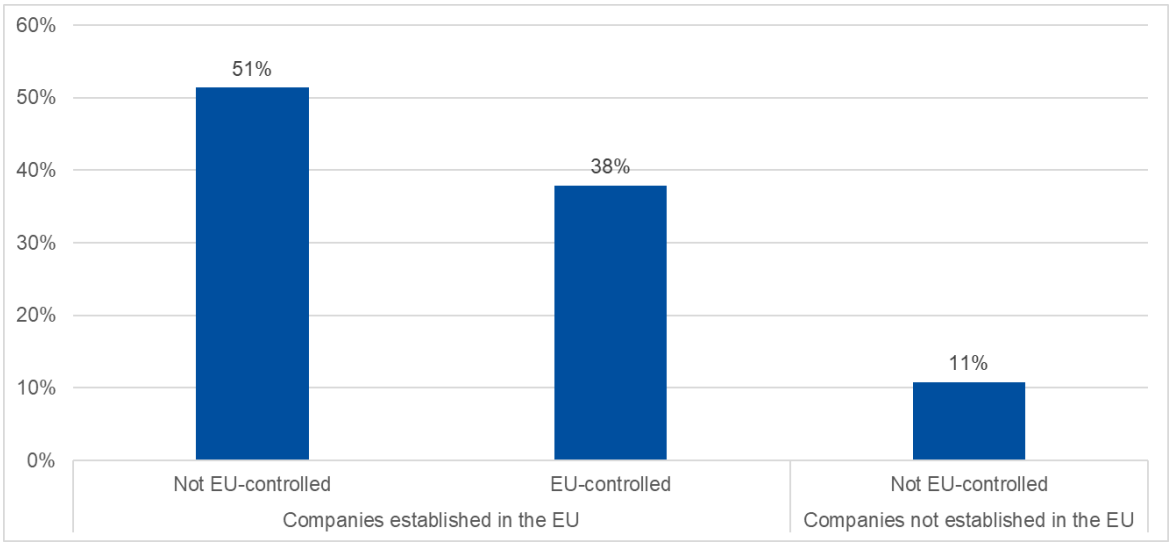
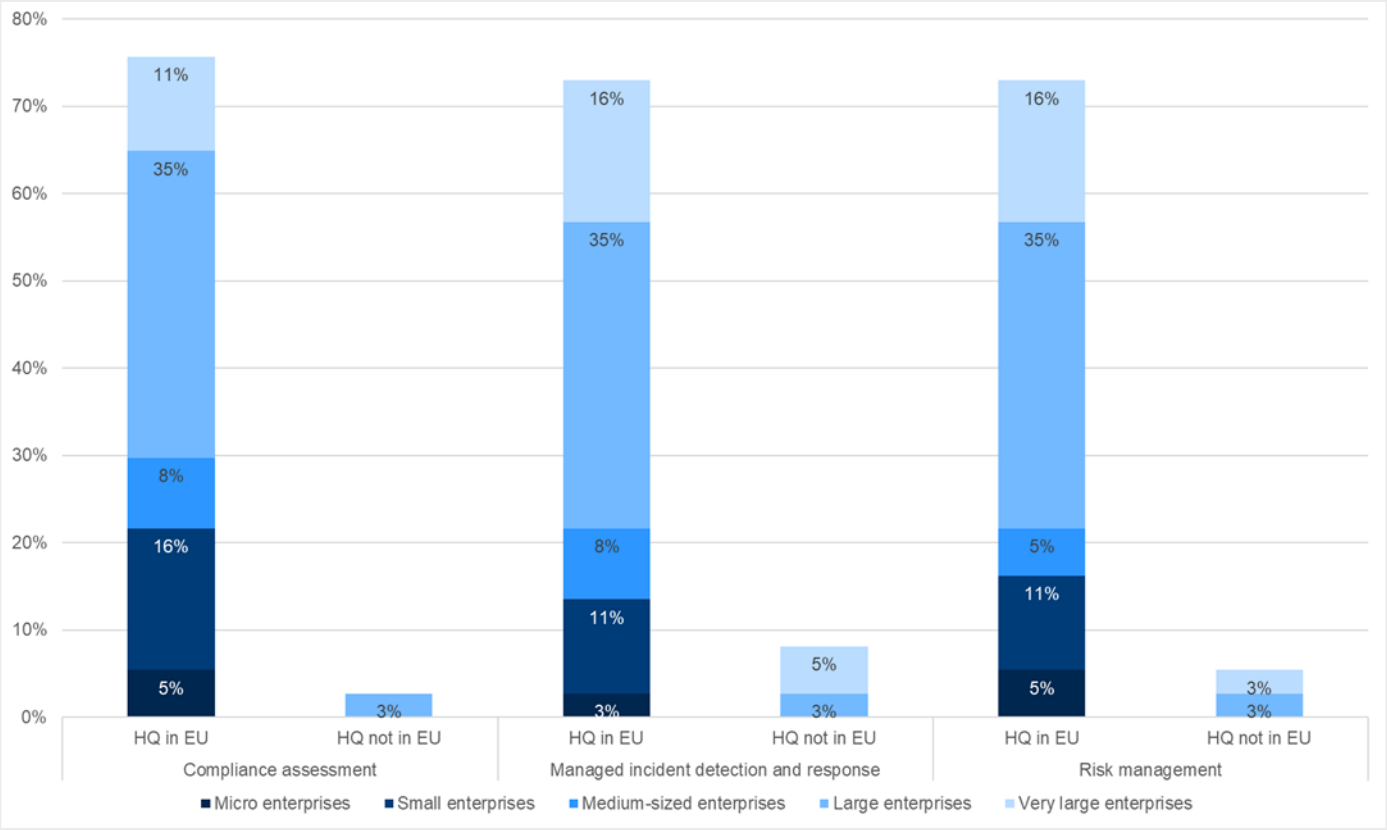


Figure 3: Organisations controlled ([12]) in EU (supply)



([12]) 'Control' should be understood as the possibility to exercise decisive influence – directly or indirectly, through one or more intermediate entities, *de jure* or de facto – on strategic business decisions (the appointment and removal of senior management, the budget, investments and business plans, market-specific decisions, etc). The fact that no influence is actually exercised is not relevant as long as the possibility exists. Please note that international companies with an office in the EU or the European Economic Area are not considered to be EU controlled.

Figure 4: Overview of the top-three managed services by geography and size of organisation (supply)



Observations drawn from overall demographics.

These observations are based on the data collected and may not be representative of the entire population.

- The majority of the organisations that participated in the survey were from the supply side, with fewer from the demand-side category and the smallest – though a representative – sample from the regulation category, representing around 45 % of EU Member States.
- Looking at **Figure 1**, geographically speaking, EU-based participants predominate across suppliers (89 %), demand-side entities (76 %) and bodies involved in regulatory activities (100 %), emphasising the survey's focus on the EU MSS ecosystem. This distribution reflects the EU's significant role in fostering a local supply chain, addressing regional demand and maintaining regulatory oversight. The presence of non-EU participants, particularly on the demand side (24 %), suggests both opportunities for international collaboration and the global appeal of EU-based MSS solutions, and a market that is potentially underserved by EU suppliers. However, it may be that non-EU entities are under-represented in this survey, indicating that its dissemination mainly triggered the interest of EU-based MSS market actors.
- In **Figure 2**, the distribution of survey participants by organisation size shows that, for demand-side and supply-side entities, it was mainly larger enterprises (large and very large) that participated in the survey. In contrast, there was limited representation of smaller enterprises (micro, small and medium-sized), highlighting the dominance in the market of large entities. The relatively low rate of representation of small enterprises implies a potential gap between the security needs of smaller companies and what is

available on the market. Regulators are represented mainly by large organisations, as they are usually the main regulating body in their country.

- In terms of survey representation, shown in **Figure 3**, the supply side of the survey is primarily represented by organisations established in the EU. The majority are non-EU-controlled companies (51 %), with only 38 % being EU controlled. Organisations not established in the EU make up a smaller portion (11 %). This highlights the significant presence in the MSS market of non-EU-controlled entities with a base in the EU, suggesting a diverse supplier base in which EU-based organisations hold a substantial, but not dominant, share of the MSS market. Moreover, given the complexity of MSS, one can correctly assume that non-EU actors play a role in the MSS supply chain, such as the provision of infrastructure components/software/tools used by EU-controlled entities in their service provisioning. Supply-chain dependencies have not been investigated in the present analysis. However, both the relatively low percentage of EU-controlled MSS suppliers and supply-chain dependencies may be worthy of further discussion in the context of digital sovereignty.
- The top three MSS selected by respondents showcased in **Figure** 4 – compliance assessment, managed incident detection and response, and risk management – are predominantly delivered by enterprises headquartered in the EU, with very large enterprises playing a leading role across all services. Smaller enterprises contribute significantly but remain secondary to larger entities. Non-EU enterprises have a limited presence, particularly in compliance assessment and risk management, highlighting the dominance of EU-based organisations in these critical MSS.

2.2 FINANCIAL DEMOGRAPHICS

Figure 5: Turnover by organisation size

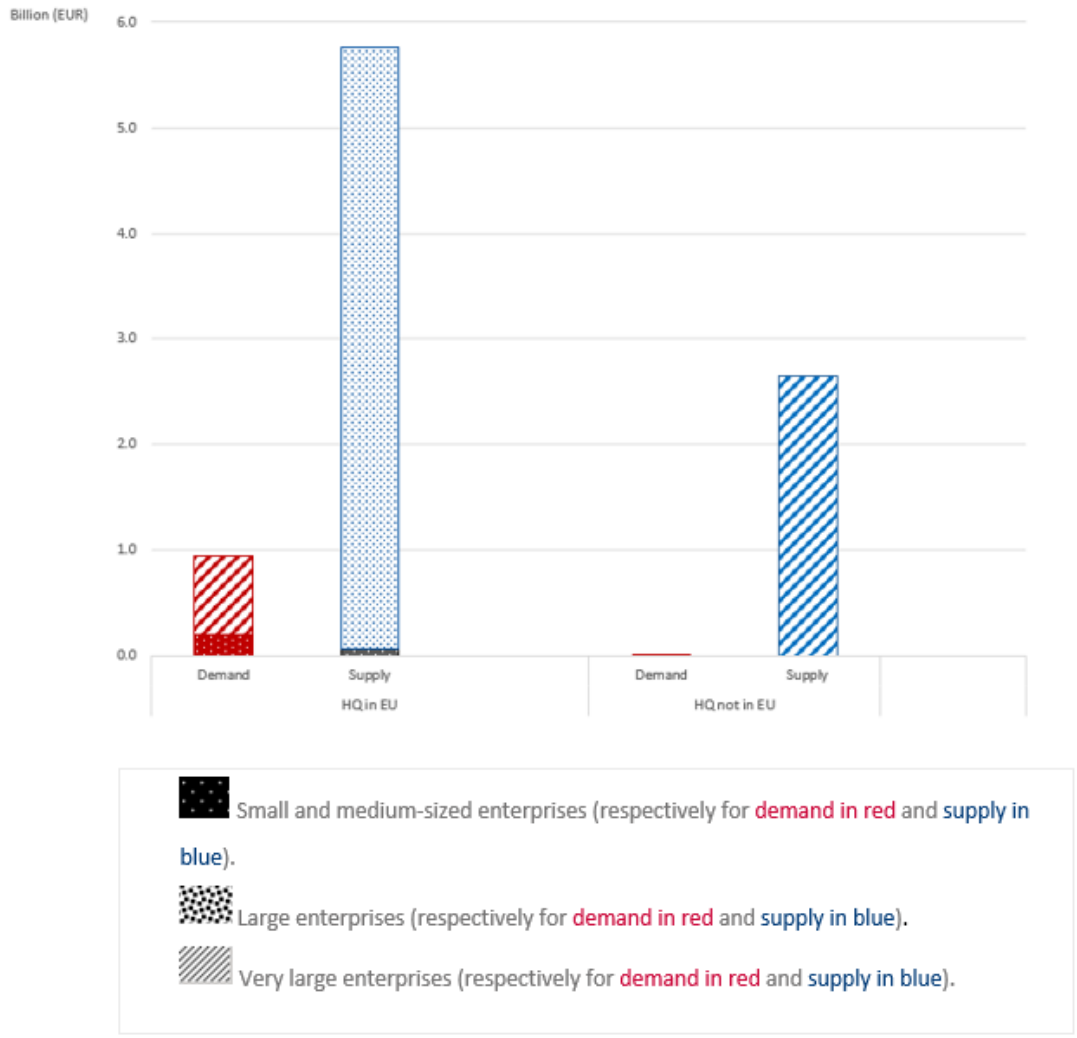
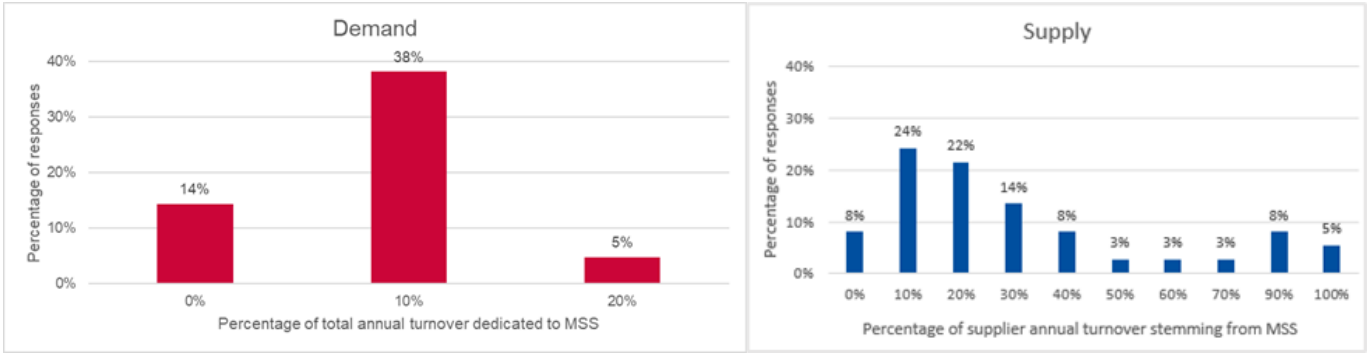


Figure 6: Percentage of budget spent on MSS (demand side) and of turnover from MSS (supply side)



Observations drawn from financial demographics.

- Looking at **Figure 5**, it appears that large and very large organisations hold the largest share of the MSS market on the supply side, while very large organisations are the main consumers of MSS.
- As shown in **Figure** 6, the entities on the demand side invest on average less than 10 % of their total turnover in MSS. This number is on a par with the findings of ENISA's *NIS Investments 2024* study, which assessed it at around 7 % ([13]). On the supply side, most earnings from MSS – as a percentage of total annual turnover – fall within the 10 % to 30 % range, indicating a moderate level of income from MSS offerings by most entities. However, given the size of the majority of supplier organisations that participated in the survey (large or very large), the moderate percentage of investment in MSS development can be explained by the complexity/size of their product portfolio, in which MSS is just one of many products offered. On the other hand, approximately 20 % of the suppliers that participated have a stronger MSS focus (i.e. 60–100 % of their income is through MSS).

([13]) ENISA, Drougkas, A., Komzaite, U., Philippou, E., Abel, P. et al., *NIS investments 2024 – Cybersecurity policy assessment,* 2024, https://data.europa.eu/doi/10.2824/5220134.

3. MSS USAGE PATTERNS

3.1 USAGE PATTERNS OF SUPPLY AND DEMAND

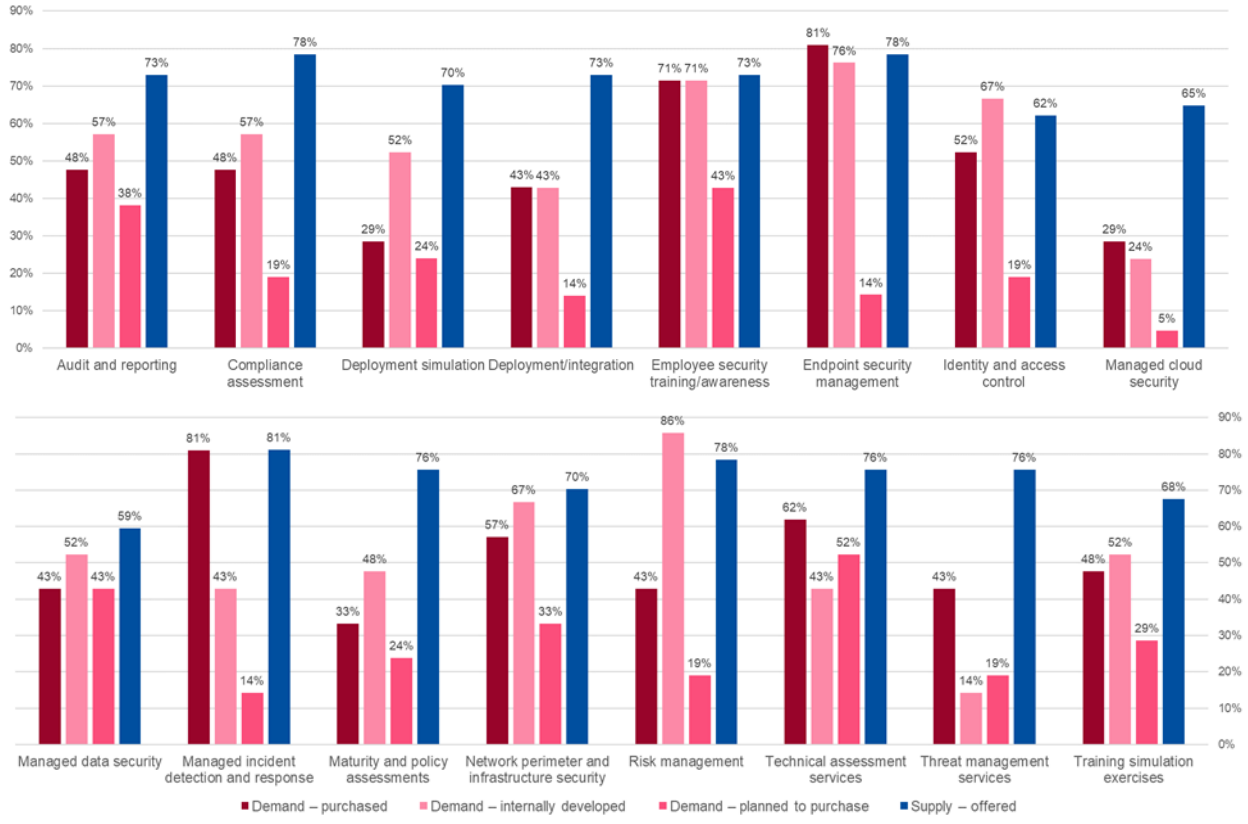
In this section we present our findings regarding MSS implementation preferences by demand. This has been achieved by assessing implementation options for MSS, in particular the purchase of products, own implementation of MSS functions and plans to purchase MSS solutions. Suppliers were asked which MSS services they offer in their portfolios (see **Figure 7**).

Figure 8 presents the planning horizon of demand reflected in their plans to purchase MSS solutions, and **Figure 9** presents the MSS demand and supply delivery options of choice.

The MSS usage analysis concludes with a graph showing the business objectives to be covered by the use of MSS, as proposed by demand-side organisations. In the same graph, suppliers provide their view of the demand objectives the use of their MSS is designed to cover (see

Figure 10**)**. This graph provides an interesting comparison of the demand and supply perspectives.

Figure 7: MSS purchased, internally developed and planned to be purchased by the demand side, and offered by the supply side ([14])



([14]) The data were collected by asking the demand side which services had already been purchased, which had been internally implemented and which are planned. From suppliers, we collected data about their available MSS offerings.

Figure 8: Planning horizon of MSS purchases

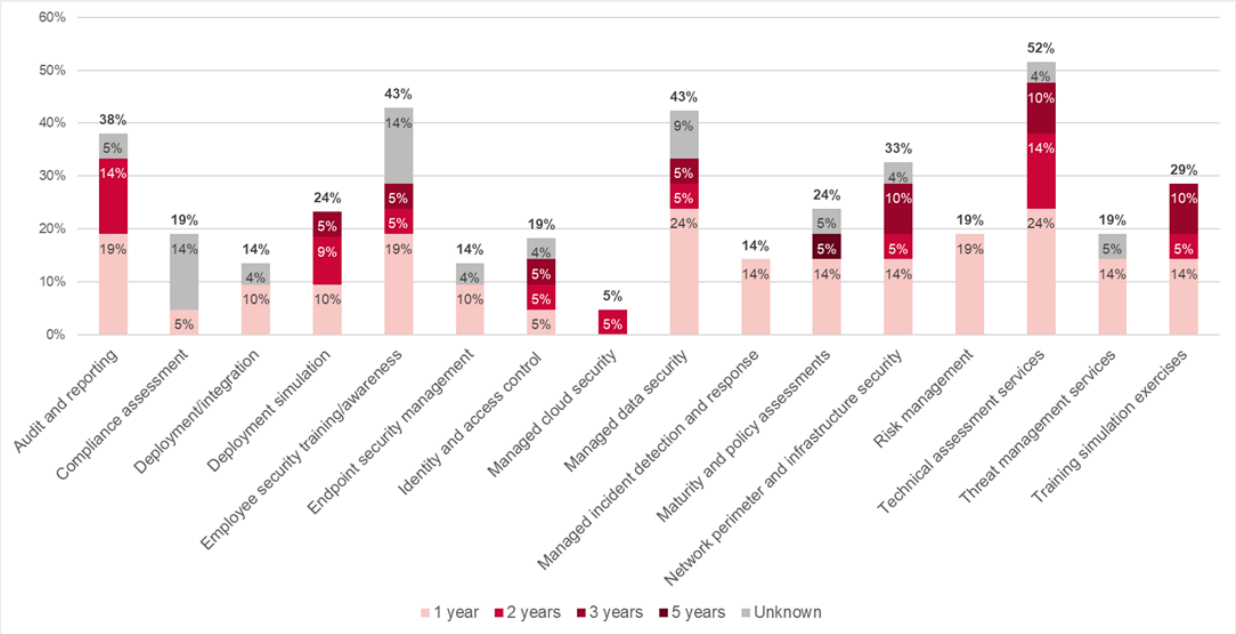


Figure 9: MSS delivery options

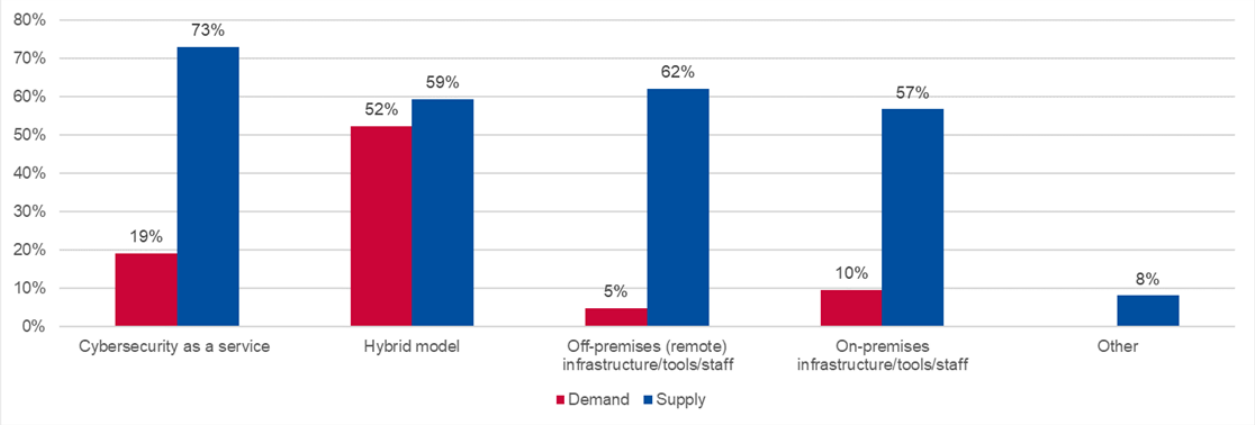
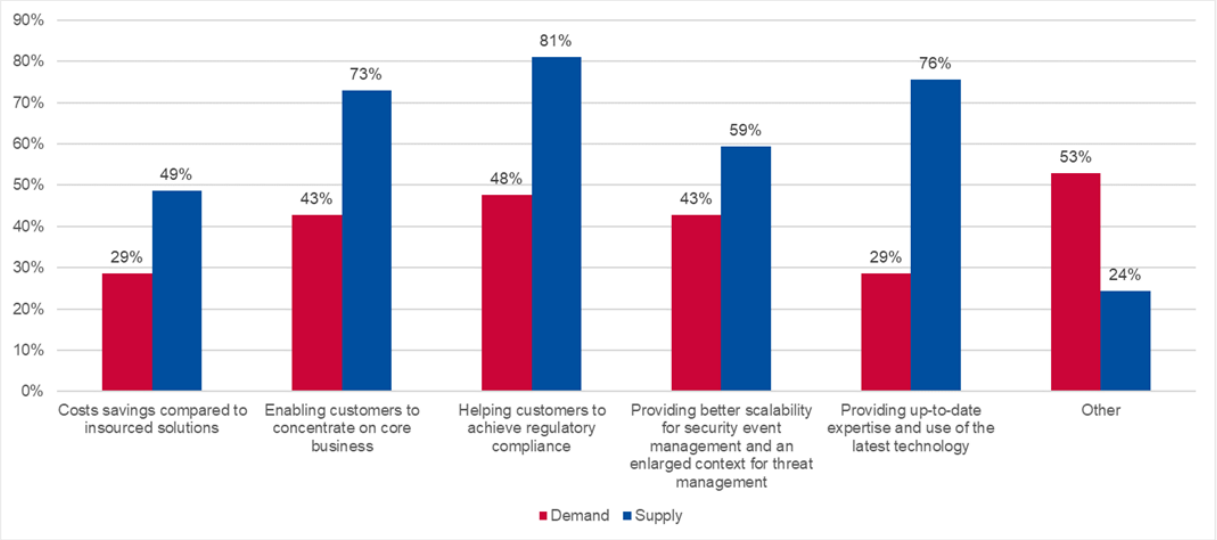


Figure 10: Business objectives on the demand side and on the supply side



Observations drawn from usage and capabilities.

- Figure 7 highlights an apparent imbalance between supply and demand across various cybersecurity service categories, with supply often exceeding purchased or planned-to-purchase demand. However, closer examination reveals that, for certain key services, the combined purchased and planned-to-purchase demand surpasses the available supply, indicating strong market interest. Moreover, the fact that supply is higher than demand may also indicate that the MSS suppliers/providers within the scope of the analysis are also selling their services in markets other than the EU.
- Figure 7 also shows that 86 % of demand-side respondents replied that risk management is not outsourced. This is indicative of the availability of business and information security risk management skills in most of the responding organisations. This reflects the broader trend of organisations typically retaining foundational security capabilities in-house. The graph also shows that 67 % of demand-side respondents have deployed network infrastructure as part of their normal business and operate their own infrastructure. This can be seen as being related to their business continuity management, their business continuity strategy and their risk appetite: many organisations prefer to build security functions in-house rather than rely entirely on external providers, particularly for services deemed critical or requiring bespoke implementation, underscoring the strategic importance of these functions.
- Identity and access control shows an already established market where solutions have already been purchased or internally developed, while managed cloud security shows a lower level of solutions planned for purchase, already purchased and internally developed, suggesting a lower priority for investment. Meanwhile technical assessment services (52 %), employee security training/awareness (43 %), managed data security (43 %) and audit and reporting (38 %) demonstrate significant planned purchases, highlighting areas in which demand is still evolving and organisations are carefully assessing their options before committing to external solutions.
- When planning their purchases (Figure 8), enterprises mostly plan in the short term (one year), with very few planning for the longer term (five years). Technical assessment services, already well adopted, show the most planned purchases, along with managed data security, employee security training/awareness, and audit and reporting.

- **Figure 9** highlights a significant gap between supply and demand for MSS delivery options, with cybersecurity as a service showing the second-largest disparity (73 % supply versus 19 % demand), reflecting an imbalance between demand and supply in terms of need versus offerings. The low level of interest in managed cloud security contradicts general cloud adoption trends and deserves further investigation.
  The hybrid model has the closest alignment (59 % supply versus 52 % demand), indicating that its market is in a state of equilibrium (supply and demand are in balance, or almost are). Off-premises and on-premises solutions show a high level of supply (respectively 62 % and 57 %) but minimal demand (respectively 5 % and 10 %). This could be interpreted as MSS providers being in a position to deliver their services both on-site and remotely, while the demand side is either unable to afford them or not in favour of such solutions.
  The 'Other' category includes hardware security module as a service and key management as a service in compliant dedicated data centres in the EU and globally, anti-fraud, fully managed security operations centre and customised security solutions. shows that MSS providers focus heavily on helping customers meet regulations (81 %) and offering the latest expertise (76 %).
  The high demand in the 'Other' category (53 %), linked mainly to timely advantage, shows that businesses want faster and more responsive solutions, which may not yet be fully available.
- According to the data collected in the survey about desirable MSS criteria/characteristics, we can observe that organisations seem to focus heavily on compliance with regulatory requirements and the flexibility of pricing models (both 81 %), clear communication (76 %) and expertise tailored to their industry (71 %), reflecting a strong need for trust, alignment with regulations and cost-effectiveness. Less emphasis on criteria such as the use of the latest technologies (29 %) and references from others (38 %) suggests businesses prioritise proven capabilities and operational factors over innovation and external validation.
- Moreover, when it comes to re-evaluating these criteria after procurement, according to the data collected via the ENISA survey on MSS, the majority favour a cautious, long-term approach, with only 5 % conducting annual reviews and 19 % opting for a three-year cycle. This indicates that businesses aim for stability while ensuring periodic updates to adapt to changing needs and market dynamics. Together, these insights suggest a balance between reliability, cost and adaptability, with periodic checks ensuring alignment without overburdening operations. All in all, trust in external MSS providers is gradually increasing, mainly based on credible, proven capabilities and pricing models that fit budgets.

4. COMPLIANCE AND SKILLS CERTIFICATIONS

Compliance is a strong market driver for the adoption of products, and so also for MSS. In this section, an of overview regulations, standards and good-practice frameworks as compliance targets is presented, covering compliance requirements from both the demand and the supply side. This information presents the expectations of demand and supply regarding compliance. Moreover, skills certifications fulfilling the skill profile required by MSS operation and development are also taken into account. The latter reflects the urgent need for MSS-related skills, as expressed by survey participants, for both the demand and the supply side.

Concerning the certification needs of MSS by means of compliance with technical cybersecurity requirements, ENISA prepared the *Feasibility Study on EU Cybersecurity Certification For Managed Security Services*, that aims at supporting the future Ad-Hoc Working Group in drafting the candidate scheme for the EU cybersecurity certification for MSS.

4.1 RELEVANT REQUIREMENTS, REGULATIONS, STANDARDS AND FRAMEWORKS

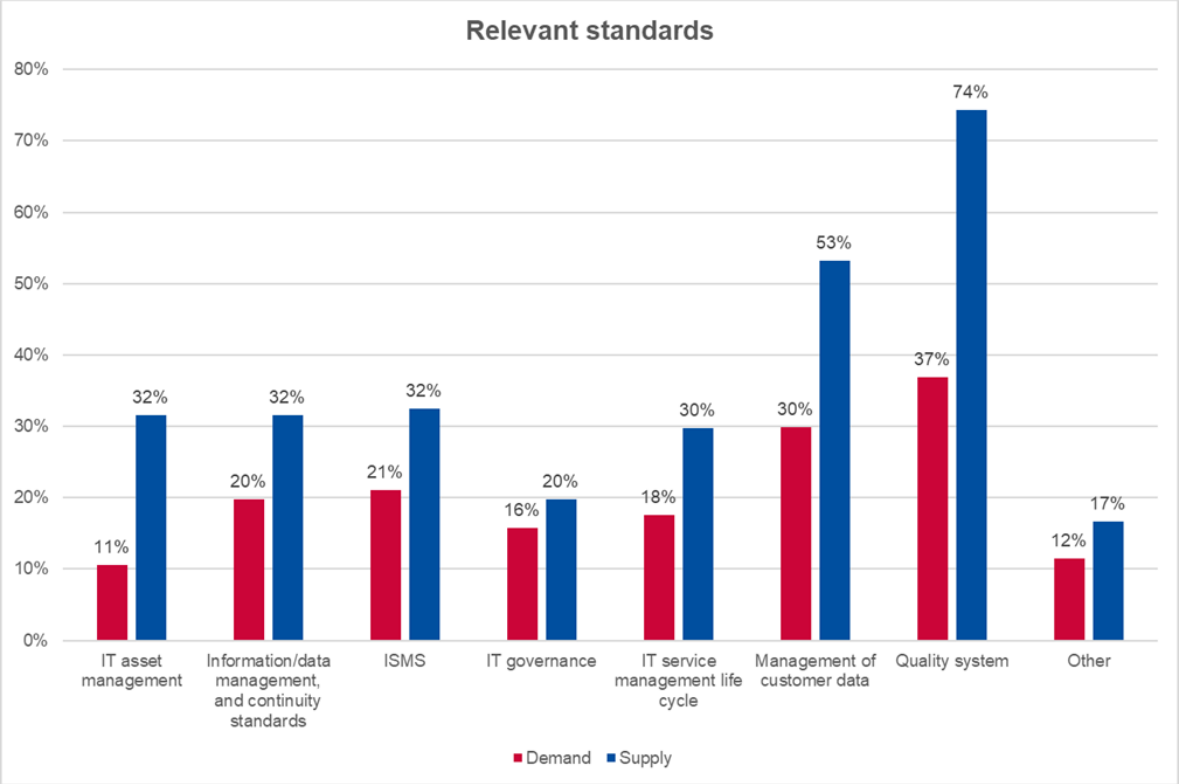
Table 2: Relevant regulations, standards and frameworks for MSS compliance/certifications, highlighting deviating demand and supply perspectives ([15])

MSS-related regulations/standards/frameworks	Demand	Supply
Information security management system (ISMS)	**21 % (average)**	**32 % (average)**
ISO/IEC 27001 on ISMS, ISO/IEC TS 27022 on information management system processes, ISO/IEC 27002 on information security controls, ISO/IEC 27003 on ISMS guidance, ISO/IEC 27004 on monitoring, measurement and evaluation	53 %	92 %
Quality management system	**37 % (average)**	**74 % (average)**
ISO 9001 – Quality management systems – Requirements	37 %	74 %
Information technology (IT) governance	**16 % (average)**	**20 % (average)**

([15]) This table shows the frequency of reference to regulations/standards/frameworks that are considered relevant for MSS compliance/certification, as assessed by demand and supply organisations. The full table of requirements regarding the use of regulation/standards/frameworks can be found in Annex B. This excerpt shows those cases in which perceptions between demand and supply deviate by more than 10 %.

MSS-related regulations/standards/frameworks	Demand	Supply
ISO/IEC 38500 – Information technology – Governance of IT for the organization	13 %	24 %
IT service management life cycle	**18 % (average)**	**30 % (average)**
ISO/IEC 20000 – Information technology – Service management	16 %	24 %
Information Technology Infrastructure Library	26 %	55 %
Information/data management and continuity standards	**20 % (average)**	**32 % (average)**
Business continuity management, e.g. ISO 22301, ISO/IEC 27031	39 %	50 %
Communication security, ISO/IEC 27010 – Information security management for inter-sector and inter-organisational communications	13 %	24 %
ISO/IEC 27701 on privacy management	18 %	37 %
Management of customer data	**30 % (average)**	**53 % (average)**
General Data Protection Regulation (GDPR)	50 %	76 %
Payment Card Industry Data Security Standard	11 %	39 %
System and Organization Controls 2	29 %	45 %
IT asset management	**11 % (average)**	**32 % (average)**
ISO/IEC 19770 – Information technology – IT asset management	11 %	32 %
Other	**12 %(average)**	**17 % (average)**
ISO 31000 – Risk management	18 %	32 %
ISO/IEC 27017 on cloud security	16 %	29 %
Other	18 %	39 %

Figure 11: Overview of the most important areas of compliance on the demand and supply sides



Observations drawn from the relevance of standards as perceived by demand and supply.

- Based on the data we collected, in **Figure 11**, the importance of IT asset management is given as 32 % on the supply side and 11 % on the demand side. **Table 2** and **Table 8** in Annex A show that this category only includes ISO/IEC 19770, which accounts for the entirety of the data and reflects a limited emphasis on formalised asset management frameworks on the demand side. This gap represents a point of concern, given its importance for the assessment of asset protection needs.
- As shown in **Figure 11**, the importance of information/data management and continuity standards is 32 % for the supply side and 20 % for the demand side. This disparity suggests suppliers' greater focus on standards for system-wide integration and communication security. **Table 2** and **Table 8** in Annex A show that the supply side is influenced by the high incidence of business continuity management standards (50 %), while hardware-related standards (8 %) lower the overall demand score, indicating less robust adoption of these specialised frameworks by client organisations.
- In **Figure 11**, ISMS importance scores 32 % for the supply side and 21 % for the demand side. This moderate alignment reflects shared importance between suppliers and clients, but with a stronger emphasis from the supply side. From data provided in **Table 2** and **Table 8** in Annex A, it is evident that ISO/IEC 27001 influences these figures, with 92 % importance indicated by suppliers and 53 % on the demand side. This can be interpreted as ISO/IEC 27000 being a de facto industry standard for MSS suppliers and a popular compliance target on the demand side. ISO/IEC 27000 compliance on the part of MSS suppliers may significantly facilitate the achievement of demand-side compliance.
- In **Figure 11**, IT governance importance is shown at 20 % for the supply side and 16 % for the demand side. This indicates moderate alignment, but with slightly more

emphasis from suppliers. **Table 1** shows that the results are moderately spread across the category's components.

- In **Figure 11**, the importance of the IT service management life cycle is considered to be 30 % on the supply side and 18 % on the demand side. The higher supply-side figure highlights MSS providers' emphasis on IT service management frameworks. **Table 2** shows that this is primarily driven by the Information Technology Infrastructure Library, with 55 % adoption by suppliers compared to 26 % on the demand side. The rest of the cluster is poorly populated. This is an indication that the Information Technology Infrastructure Library is the framework of choice MSS providers use to design and implement the MSS service management life cycle.
- In **Figure 11**, management of customer data scores 53 % on the supply side and 30 % on the demand side. This shows strong alignment between suppliers and clients, reflecting a shared priority on privacy and data protection. **Table 2** shows that the GDPR is a significant driver, with 76 % supplier adoption compared to 50 % on the demand side. ISO/IEC 27701 on privacy management also contributes, with suppliers adopting it at 37 % compared to 18 % on the demand side.
- In **Figure 11**, the importance of quality systems is shown to be 74 % for the supply side and 37 % for the demand side, demonstrating that this is an area of substantial focus for suppliers. **Table 2** shows that ISO 9001 is the only driver of these figures, suggesting that while suppliers invest heavily in quality frameworks, client organisations may view them as being less critical. The fact that demand-side entities have not listed quality management system requirements as a must could also be interpreted as showing that a culture of having ISO 9001 by default is already present.
- In **Figure 11**, the importance of 'Other' is shown to be 17 % for the supply side and 12 % for the demand side. This broad category reflects supplementary compliance areas and standards, with the main references being ISO/IEC 27017 on cloud security and ISO 31000 on risk management (see also **Table 2**).

4.2 SKILLS AND COMPETENCES

The areas of the most requested skills certifications for the staff of MSS providers include general cybersecurity, offensive security and forensics, penetration testing and threat intelligence. Some further areas of interest regarding skills certifications can be found in **Table 3**.

Table 3: Areas of most requested skills certifications/diplomas for the staff of MSS – supply side

Area
General cybersecurity
Offensive security
Forensics, penetration testing and threat intelligence
Vendor specific
ISO and process oriented
Specialised certifications
Additional skills and requirements

Table 4: Relevance of future skills and competences for MSS, as considered by demand and supply

Skills	Percentage
Managed incident detection and response	39 %
Technical assessment services	26 %
Managed cloud security	21 %
Employee security training/awareness	16 %
Threat management services	13 %

Observations drawn from the certified solutions and certification priorities as exposed by suppliers.

- Based on the data we collected, general cybersecurity certifications dominate the landscape, reflecting their foundational role in equipping professionals with a broad understanding of security frameworks.
- In offensive security, the results testify to the growing demand for proactive defence strategies (**Table 3**).
- The high prioritisation of skills certifications from forensic analysis and penetration testing is a sign of suppliers' commitment to specialised and advanced skills tailored to dynamic threat landscapes. Moreover, the high rates of certification in areas such as incident response and security monitoring indicate an industry shift towards proactive defence mechanisms in the face of increasingly sophisticated cyber threats (**Table 3**).
- Vendor-specific certifications demonstrate the integration of platform-based expertise into supplier offerings (**Table 3**).
- ISO and process-oriented certifications such as ISO/IEC 27001 lead auditor/implementer reflect a strong focus on compliance with ISMS, reinforcing the importance of compliance in operational integrity (**Table 3**).
- Specialised certifications and emerging qualifications indicate suppliers' investment in niche, high-demand skill sets (**Table 3**).
- The relevance of certifications relating to forensics, penetration testing, threat intelligence and offensive security signals the importance of aligning MSS practices with regulatory requirements and ensuring operational accountability. This aligns with the broader industry trend of integrating offensive and defensive strategies to achieve comprehensive security (**Table 3**).
- On the other hand, **Table 4** highlights an interest in emerging areas, and the top five priorities to be implemented are represented. The top skills suggest organisations are heavily focused on immediate threat detection and response capabilities.
- In **Table 4**, the relatively lesser focus on awareness and preventive measures suggests either a gap in addressing the human factor in cybersecurity or an already developed skill set. This stands in contrast to the higher prioritisation of technical solutions. These results resonate with the findings from the previous section.

5. THREATS, REQUIREMENTS, INCIDENTS AND CHALLENGES

5.1 MARKET THREATS, CHALLENGES AND REQUIREMENTS FOR MSS

Figure 12: Most relevant threats reduced through MSS (according to demand-side, supply-side and regulators' survey respondents)

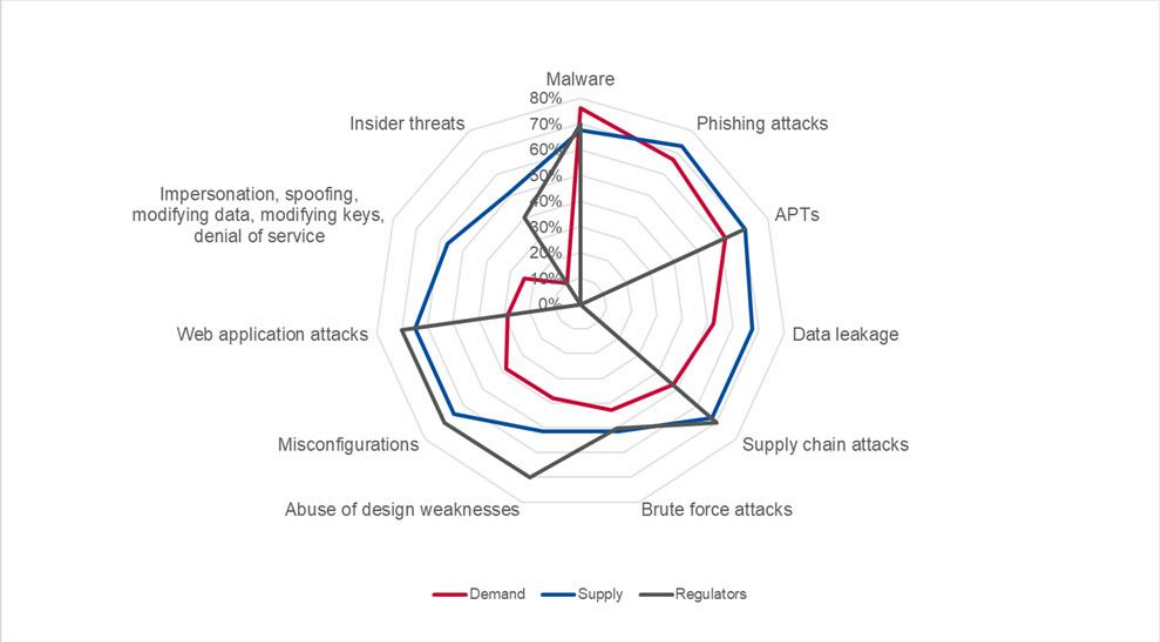


Table 5: Requirements for MSS – deviating views between the demand and supply sides

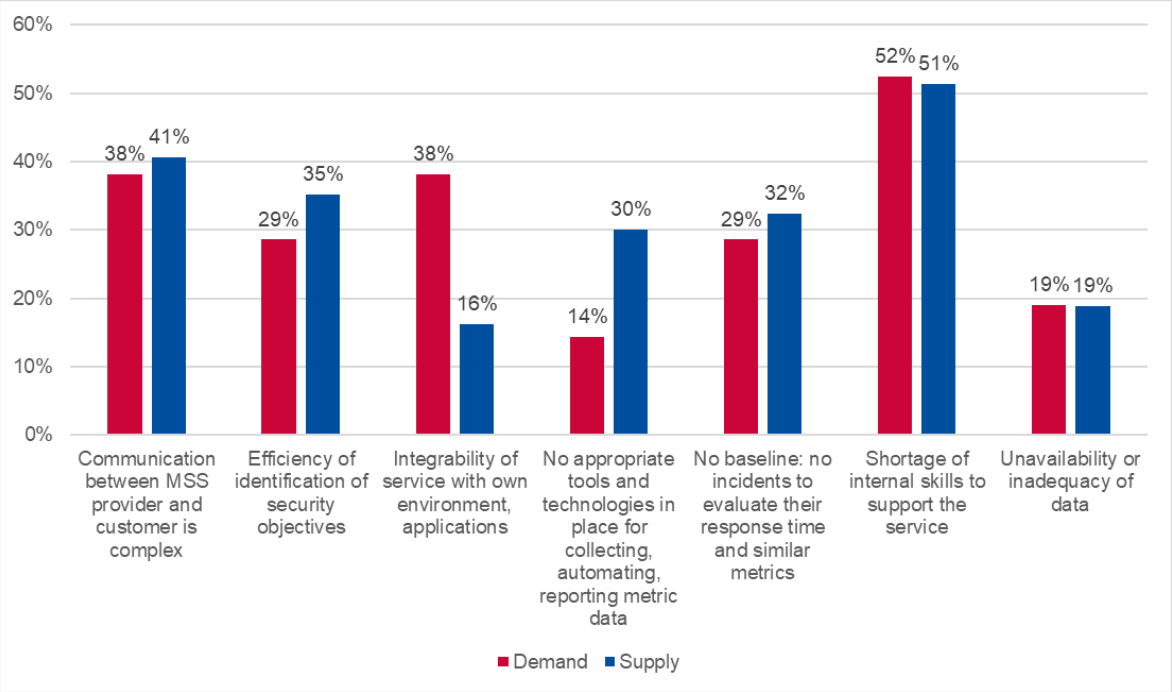
Relevant requirements	Demand	Supply
Technical	**43 % (average)**	**48 % (average)**
Data protection tools and techniques	38 %	54 %
Methods of data analytics that are necessary for service provisioning	19 %	30 %
Multi-platform/multi-device coverage	29 %	49 %
Preparedness and prevention requirements	86 %	62 %
Restore and recovery tools and techniques	76 %	51 %
Use of technical standards and good practices	29 %	54 %
Vulnerability and update management tools and techniques	52 %	68 %
Processes and procedures	**52 % (average)**	**61 % (average)**

Relevant requirements	Demand	Supply
Data protection and privacy control and compliance requirements	43 %	54 %
The service provider can advise on and support security service coordination by means of dedicated processes, whereas coordination may be provided on demand, end to end and either remotely or on-site	38 %	51 %
Use of procedural standards and good practices	38 %	65 %
Requirements relating to digital sovereignty	**76 % (average)**	**78 % (average)**
Business requirements	**57 % (average)**	**34 % (average)**
Proof of concept before contracting	67 %	0 %
SLA and metrics requirements	**55 % (average)**	**30 % (average)**
Customisation of SLAs according to operational needs	86 %	59 %
Selection and parametrisation of metrics for defined SLAs	24 %	0 %
Workforce-related requirements	**55 % (average)**	**30 % (average)**
Available workforce certifications and experience levels	38 %	49 %
The service provider has the capacity to support the management and coordination of multiple requests/incidents simultaneously, including large-scale ones	33 %	49 %
Provider organisational-level requirements (average of requirements in category)	**51 % (average)**	**55 % (average)**

Table 6: Requirements to be fulfilled through MSS (regulatory side)

Requirement	Regulators
Data protection requirements	70 %
Digital sovereignty requirements	10 %
Monitoring and detection requirements	90 %
Network measures requirements	70 %
Other requirements	10 %
Policy, procedure and strategy requirements	40 %
Preparedness and prevention requirements	70 %
Restore and recovery requirements	0 %
Security governance, risk and control requirements	60 %
Vulnerability and update management requirements	90 %

Figure 13: Most relevant technological challenges relating to MSS delivery on the demand and supply sides



Observations drawn from threats, requirements and challenges.

- Based on the data we collected, **Figure 12** reveals a significant reliance on MSS to mitigate a wide range of cyber threats, including phishing attacks, malware and advanced persistent threats (APTs). Among these, phishing and malware appear to be the most frequently addressed. This relevance is highlighted by all three stakeholder categories actively mitigating such threats, indicating the ability of MSS market to evolve in a rapidly changing threat landscape. What is shown in **Figure 12** is in alignment with the threats identified in the *ENISA Threat Landscape 2024* ([16]) (supply-chain attacks, phishing (as part of social engineering), malware (including ransomware) and data leakage (as a special case of threats against data)). Some additional threats, such as misconfigurations, insider threats, impersonation/spoofing and brute force attacks, can be considered that target information and functionality relating to MSS.
- It is notable that insider threats score very low in the perception of the demand side, though the demand side is the most appropriate actor to defend against such threats. In particular, exposure to such threats can be reduced through available tools that are specifically designed to address insider threats, such as managed detection and response, and data loss prevention. This disconnect between the demand-side viewpoint and actual MSS capabilities is an element of concern that deserves a more detailed analysis.
- In **Figure 12**, the demand side's relatively lesser emphasis on risks such as impersonation and data leakage highlights potential underpreparedness, which may lead to blind spots in threat management strategies.
- The technical requirements category reveals the most widely deviating perspectives between demand and supply (see **Table 5**). Preparedness and prevention tools are a high priority on the demand side (86 %) but comparatively less so on the supply side (62 %), suggesting suppliers may not be fully aligned with customer expectations.

([16]) ENISA, Lella, I., Theocharidou, M., Magonara, E., Malatras, A. et al., *ENISA Threat Landscape 2024 – July 2023 to June 2024*, 2024, https://data.europa.eu/doi/10.2824/0710888.

- The demand-side requirements on SLAs and SLA metrics are significantly higher than those of supply. Suppliers may need to add additional flexibility in their SLA policies (see **Table 5**).
- Moreover, the significant gap in restore and recovery tools (76 % demand versus 51 % supply – see **Table 5**) indicates a potentially critical mismatch between customer needs for post-incident support and the services offered by suppliers.
- It is also notable that supply significantly exceeds demand expectations for a number of requirements relating to data protection, use of standards and multi-platform/multi-device coverage (see **Table 5**).
- Additional insights on requirements can be gained from the full table of requirements (**Table 9** in Annex B). Both the demand and the supply side may draw further interesting conclusions on MSS from this material.
- In **Table 6**, regulatory frameworks strongly prioritise monitoring and prevention (70 %) but neglect restore and recovery (0 %), leading to an oversight in relation to post-incident resilience.
- Requirements relating to monitoring and detection tools and techniques, prioritised by 76 % of the supply side and 67 % of the demand side, align with the high level of regulatory emphasis (90 %), showing strong industry alignment for proactive threat identification (see **Table 9** in Annex B).
- The shortage of internal skills (52 % demand, 51 % supply) reflects a shared challenge, potentially hampering both service delivery and effective collaboration between stakeholders (see **Figure 13**). For more information on skills and competences, see related articles available on the ENISA website ([17]).
- In **Figure 13**, integration with existing environments poses significantly more difficulty for demand (38 %) than for supply (16 %), while at the same time indicating the important role of service integrability in MSS adoption on the demand side. This difference may be because the demand side – being the owner of the IT infrastructure – has a better view of the caveats relating to the technical integration of MSS in their IT environment.
- In **Figure 13**, the lack of appropriate tools and technologies for collecting, automating, visualising and reporting metric data seems to be a bigger challenge on the supply side (30 %) than on the demand side (14 %). This difference may be because the supply side experiences these shortcomings in delivering their services in their attempt to fulfil related demand-side requirements (e.g. monitoring service performance, SLA metrics, etc.).

([17]) ENISA, 'Skills and competences' (https://www.enisa.europa.eu/topics/skills-and-competences), 'Skills and competences (for companies)' (https://www.enisa.europa.eu/topics/skills-and-competences-for-companies) and 'Education and career path' (https://www.enisa.europa.eu/topics/education-and-career-path), ENISA website, accessed February 2025.

5.2 INCIDENTS AND INCIDENT REPORTING

Figure 14: Awareness of the occurrence of significant incidents within the organisation

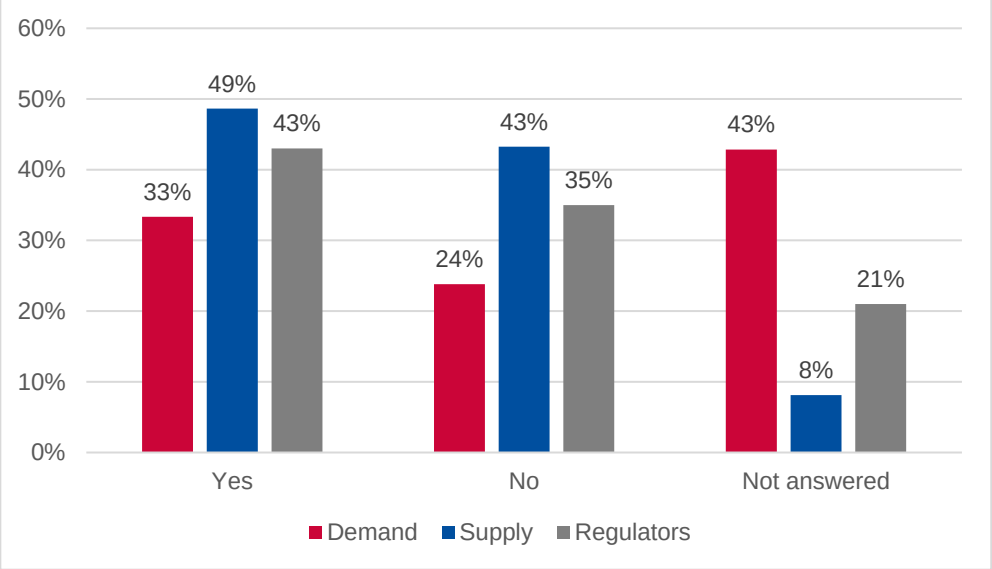
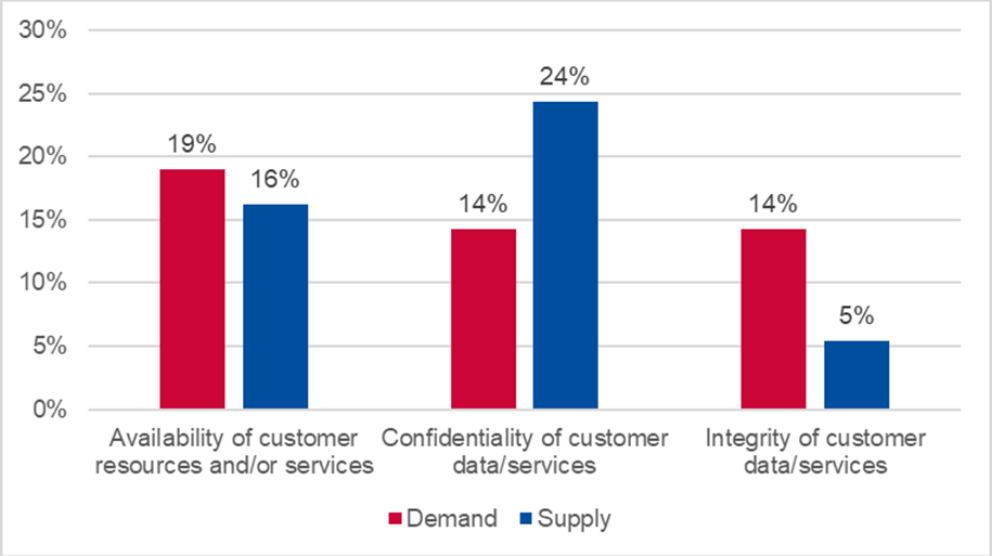


Figure 15: Impact of the abovementioned incidents on the demand and supply sides



Observations drawn from the reporting of incidents ([18])**.**

- Based on the data we collected, **Figure 14** highlights a notable imbalance among the participating stakeholders with regard to significant incidents. The following can be noted in particular.
- It seems that around 56 % (35 % + 21 %) of regulators either have not registered significant incidents or did not answer the question. A figure of more than half of regulators having no awareness of such incidents appears to be rather high. The grounds for this may need further elaboration.

([18]) The ENISA survey on MSS mainly referred to significant incidents relating to services used (in any part of the supply chain, e.g. in tools, infrastructure or staff participating in service provisioning) as defined by the NIS 2 Directive. On reporting obligations, see Article 23 of the NIS 2 Directive.

- The majority of demand-side organisations (67 %) that participated in the survey have either never managed a significant incident or did not respond. Given that the majority of participating demand-side organisations are either large or very large organisations, it is rather unlikely that only 33 % have managed a significant incident. The grounds for this finding may need further elaboration.
- Given that significant incidents are mainly reported by the demand side, the percentage gap shown in the figure for reported incidents is unexpected. The grounds for this finding may need further elaboration.
- **Figure 15** indicates that the impact of incidents may vary widely within the three main cybersecurity dimensions (confidentiality, integrity and availability). An interesting observation in this regard is that the supply side reports a greater impact on the confidentiality of customer data. Equally interesting is the fact that the integrity of data/services has more of an impact on the demand side. The grounds for these findings may need further elaboration.
- Overall, the data indicate a growing need for incident transparency, driven by demand, supply and regulators alike. Minor sector-specific nuances could be further explored, such as under-reporting, which could hinder joint mitigation and defence measures.
- Though existing roles in the national/sectoral context are not missing, a better alignment with real-world set-ups could help overcome incident reporting and management inefficiencies. Aligned roles (e.g. sector-tailored security operations centres) may warrant coordinated action in specific industries. Where relevant, additional compliance or capability requirements could be defined to address specialised threats (e.g. operational technology (OT) in energy, the internet of things (IoT) in healthcare, etc.).

6. MSS MARKET AND RESEARCH TRENDS

6.1 MSS MARKET EVOLUTION

Figure 16: Main technology drivers for the use of MSS by the demand and supply sides

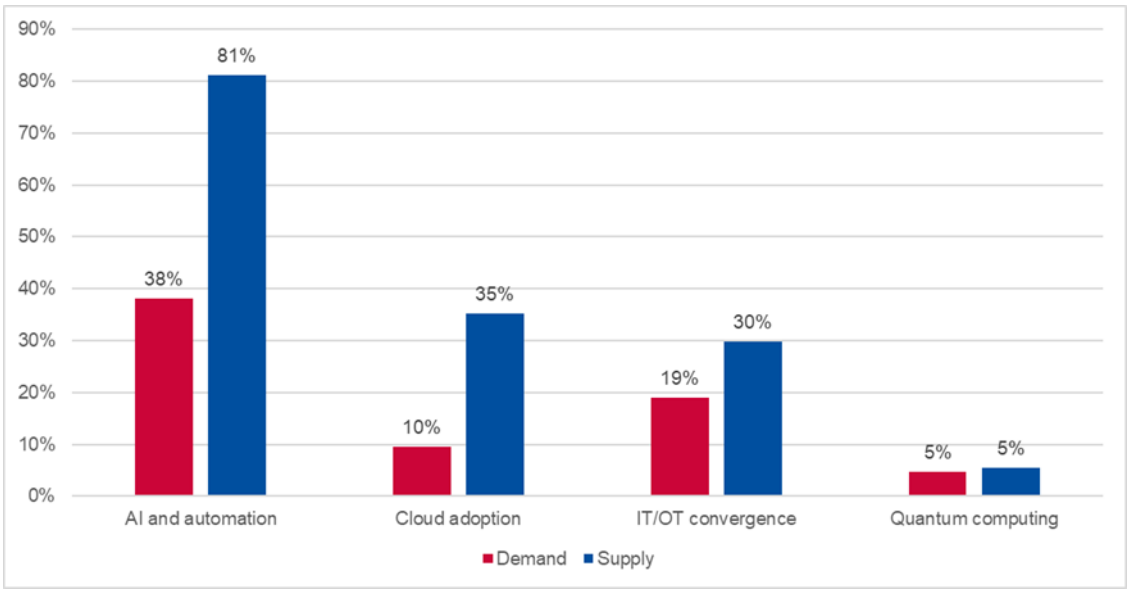


Figure 17: Main business drivers for the use of MSS by the demand and supply sides

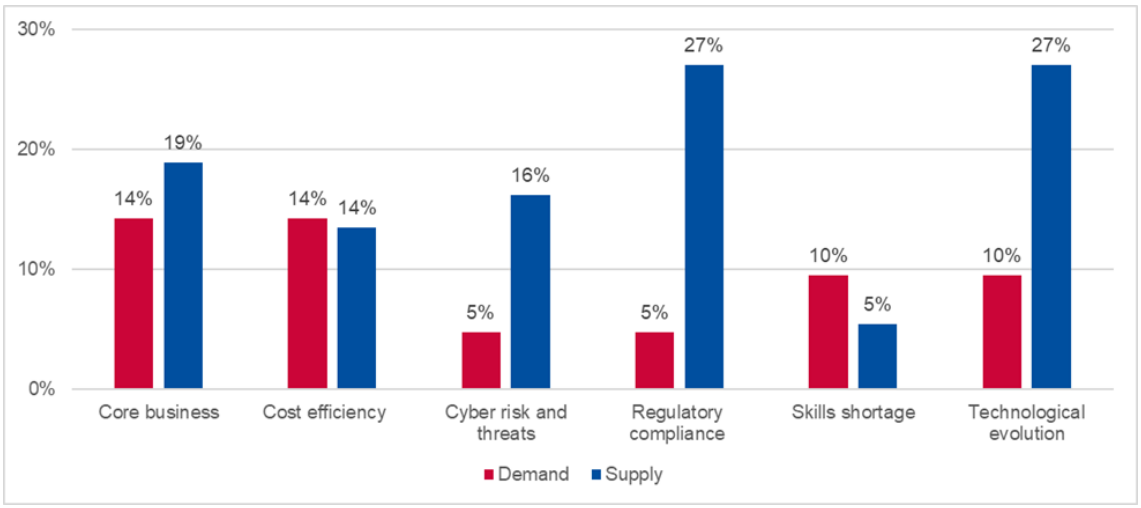
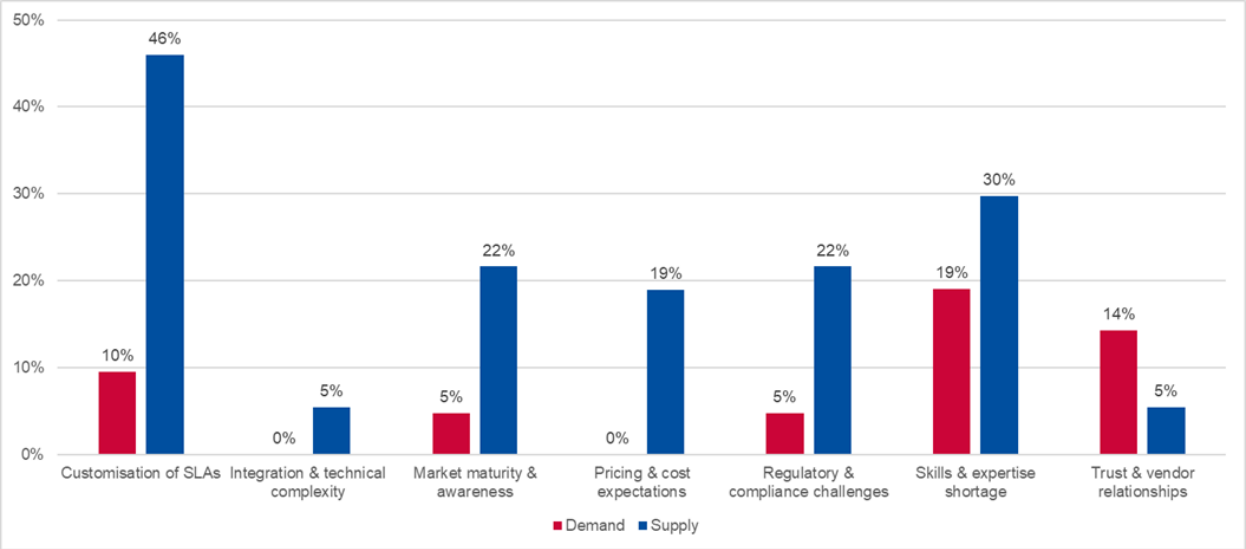


Figure 18: Gaps between demand and supply, identified through activities of the organisation



Observation drawn from market evolution.

- **Figure 16** shows that the key technology drivers both the demand and the supply side consider important include 'AI and automation' and 'IT/OT convergence', signalling a balanced perception on both sides in acknowledging the growing challenges in MSS. It is interesting that the demand side does not consider cloud adoption to be a technology driver for MSS. This trend is in line with the findings on preferred usage patterns, where managed cloud security scores low in users' plans (see **Figure 8**), and on delivery options (see **Figure 9**).
- **Figure 17** shows an alignment between demand and supply in relation to cost-efficiency, emphasising that both organisations and providers see MSS as a way to optimise costs. In addition, a core business focus is a commonly chosen driver, indicating that organisations seek to offload security management to concentrate on their primary operations, while providers slightly overestimate this need.
  However, there are differences in the domain of regulatory compliance (5 % demand, 27 % supply), suggesting that providers see compliance with (upcoming) regulations as a major market driver, while organisations may prioritise it as a technical driver (see **Figure 1**)
- .**Figure** 18**,** the gap most identified by both the demand and the supply side is skills and expertise shortage, reflecting a shared concern about the lack of qualified cybersecurity professionals. The most significant discrepancy appears in the customisation of service agreements, where providers see this as a major challenge (likely because customisation requires more resources), indicating a potential mismatch in perceived service needs.
- A significant gap between demand and supply appears with regard to trust and vendor relationships. It seems that the demand side rates vendor trust and vendor relationships much more highly than the supply side. Given the currently emerging geopolitical transformation, market players may need to keep an eye on the dynamics of this gap and work on viable alternatives to close it.

6.2 MSS MARKET BARRIERS

Figure 19: Potential barriers to adoption and/or upgrading of MSS by the demand and supply sides

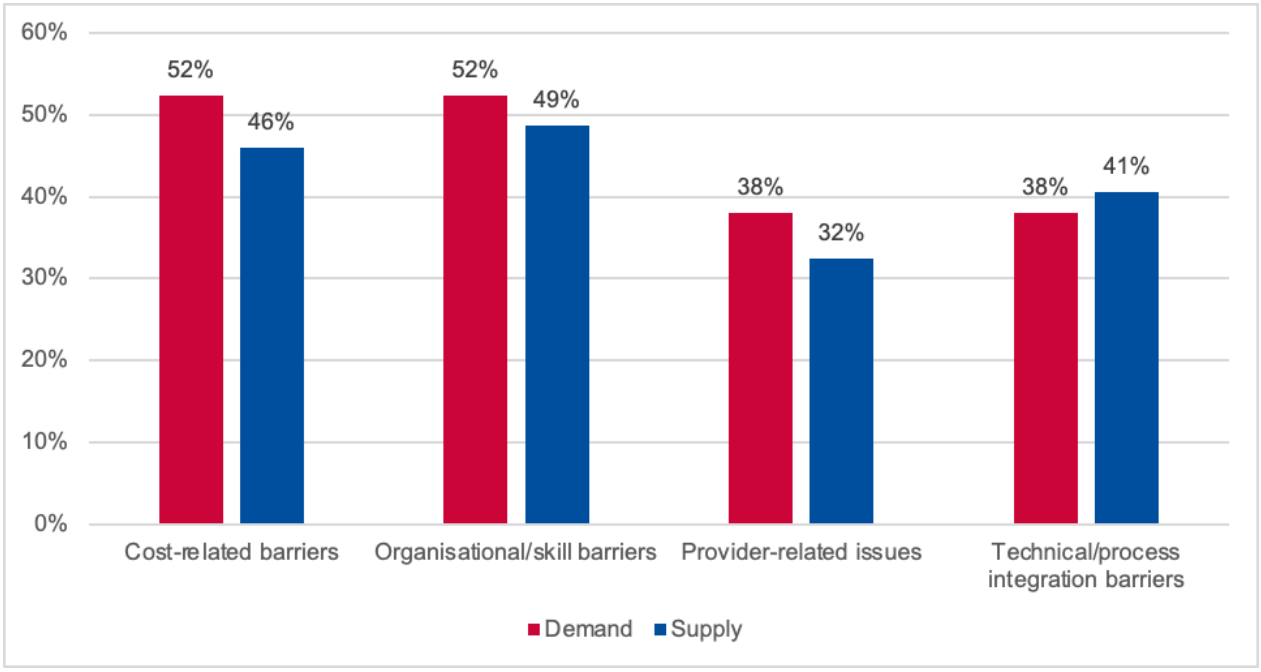
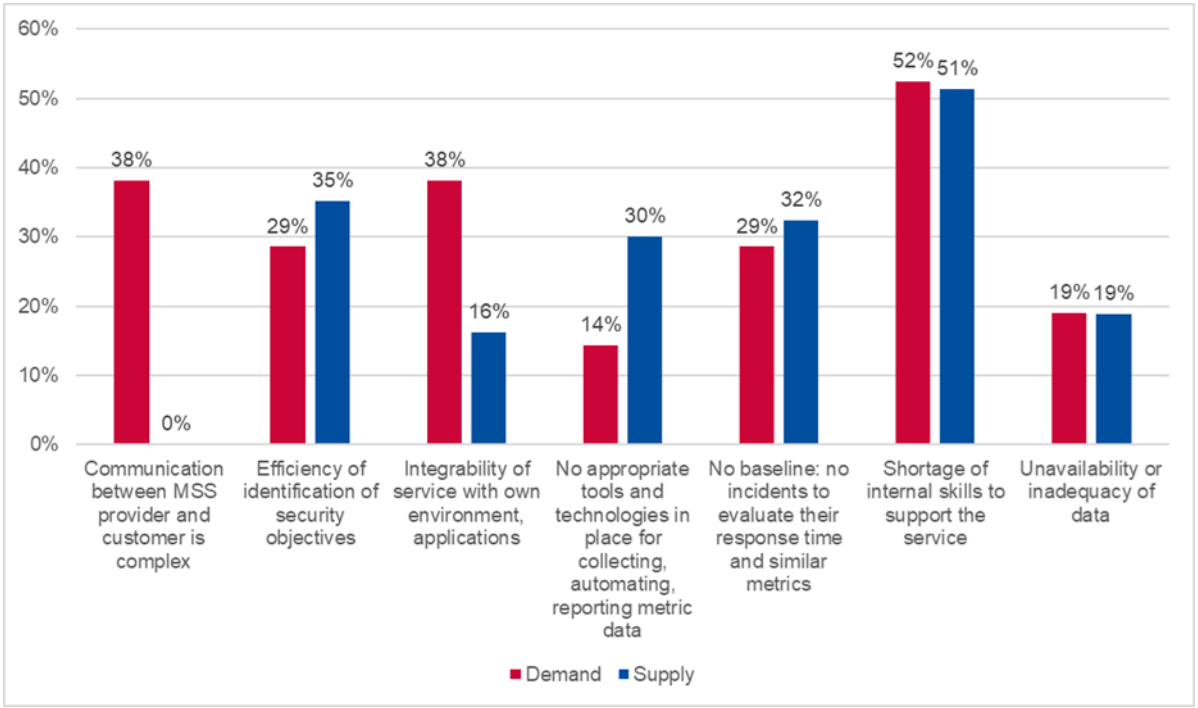


Figure 20: Most relevant technological challenges relating to MSS delivery on the demand and supply sides



Observations drawn from market barriers.

- Figure 19 depicts a situation in which the barriers to adopting or upgrading MSS are remarkably similar across both demand and supply, with only slight variations in

percentage points. All categories show high levels of respondents, and this alignment suggests that both sides have a shared understanding of the key challenges in MSS adoption. Organisations recognise these barriers as being real obstacles, while providers are aware of them, likely from customer feedback and industry experience.

- While **Figure 20** has been taken into account in Section 5 'Threats, requirements, incidents and challenges', it provides a valuable source regarding the difficulties of service delivery for the demand and supply sides. In relation to barriers, they provide evidence of the assessed skill shortage, the complexity of communication between demand and supply and the absence of baselines and of automation tools and technologies. Though these challenges may appear interdependent, they can also be considered as barriers to MSS adoption, efficiency of use and operation.

6.3 MSS INNOVATION IDEAS

Table 7: Top-five most important cybersecurity services and MSS research topics ([19])

MSS research topics
Digital supply chains
Application of AI for cybersecurity services
Developing more effective methods for detecting and responding to cyberattacks
Automation of a plan to mitigate threats (e.g. course of action)
Advanced analysis of security threats and vulnerabilities

Observations drawn from innovation ideas.

- **Table 7** highlights that the most critical cybersecurity services and MSS research topics for clients are 'digital supply chains' (67 %) and the 'application of AI for cybersecurity services' (62 %), highlighting a strong focus on securing interconnected ecosystems and leveraging artificial intelligence (AI) for threat detection and response. On the other hand, 'economic issues' (14 %) and 'developing cybersecurity policies, standards and certifications' (10 %) are the least prioritised (see **Table 10** in Annex C), suggesting that respondents are more concerned with technological advancements and operational challenges than with regulatory and cost-related aspects.
- Moreover, key IT developments impacting cybersecurity R & D include the application of AI, the use of the IoT, and advanced cyberattack detection and response methods, according to respondents. While AI enhances automation and efficiency, and the IoT expands monitoring capabilities, both also introduce new challenges, requiring stronger security frameworks and proactive threat mitigation strategies.

([19]) Indicated by the demand side as 'EU-based organisations with innovation potential'. A complete list of the topics and companies identified can be found in **Table 10** in Annex C.

7. CONCLUDING REMARKS

This section summarises the findings of the present market analysis. The aim of this summary is to highlight the most important issues identified in the MSS market. The findings combine various interrelated MSS topics covered in this analysis to express:

- trends (T);
- gaps (G);
- barriers (B);
- regulatory-related topics (R); and
- research topics (R & D).

For each of the findings, a practical proposal is provided to address the issues identified.

It should be noted that these points represent the main findings: in the analysis and observations made in the previous sections, additional detailed MSS market facts and issues can be found that may be of interest to readers with a special interest in the topics covered.

7.1 MAIN MARKET FEATURES AND TRENDS

T1 – Overview of MSS organisations and market dynamics. The assessed market for MSS in the EU shows a large number of suppliers and demand-side entities with their headquarters in the EU, along with a smaller percentage of non-EU participants. However, only a small percentage of suppliers are EU controlled, highlighting a diverse supply chain in which non-EU-controlled entities operate within the EU. Large and very large enterprises dominate both the supply and the demand side of this market analysis, while smaller enterprises play a secondary role. Investment trends reveal a moderate commitment to MSS, with most entities allocating significantly less than 10 % of their turnover to security services. Regarding regulatory bodies, this market analysis provides insights from across the EU, maintaining a balance between the different geographical areas.

Proposed action. *Increase the number of EU-controlled entities with market incentives at both the national and the EU level, especially regarding emerging MSS players with innovative, niche offerings who could influence market dynamics.*

T2 – Balancing supply and demand in cybersecurity services. The cybersecurity market reveals an interesting interplay between supply and demand. Some critical services, such as risk management and network perimeter and infrastructure security are developed in-house rather than being fully outsourced, emphasising their strategic importance for the demand side. While some areas such as technical assessment services and employee security training/awareness show a balance between demand and supply, others reflect a significant demand for external expertise, which has already been purchased or is planned to be purchased, particularly in compliance-driven and technologically evolving security domains. The evolving demand for technical assessments, data security and employee awareness training suggests a growing focus on proactive security measures and regulatory alignment.

Proposed action. *Establish targeted market surveillance (beyond products with digital elements) and market quality metrics to respond to current and emerging MSS customer needs.*

T3 – Cautious approach to managed security services adoption. While MSS providers prioritise regulatory compliance and industry-specific expertise, businesses remain cautious in

adopting new service models. This indicates a potential misalignment between MSS suppliers and users. The preference for hybrid solutions on the demand side and periodic procurement reviews suggests a balance between stability and adaptability, ensuring security investments align with long-term operational needs. The lesser emphasis on cutting-edge technologies in procurement decisions indicates a focus on proven reliability and cost-effectiveness over rapid innovation.

Proposed action. *Develop MSS good practices according to a variety of demand-side needs.*

T4 – Vendor trust and relationships in the light of geopolitical developments. The balance of vendor–customer trust will potentially be affected by current geopolitical developments. As requirements relating to European autonomy and digital sovereignty increase, MSS will play a central role in European strategic autonomy and will probably undergo a transformation. These developments could be an important driver for European MSS market development and growth. Moreover, both the relatively low percentage of EU-controlled MSS suppliers and supply-chain dependencies may be worthy of further discussion in the context of digital sovereignty.

Proposed action. *Investigate the level of dependencies in MSS and implement planned initiatives, such as the Cybersecurity Reserve provided for in the Cyber Solidarity Act. Action under T2 and T3 above contributes to this objective.*

7.2 MAIN GAPS

G1 – Inconsistent threat prioritisation across stakeholders and awareness gaps. The perception of cyber threats varies among stakeholders, leading to gaps in the adoption and implementation of MSS. While some threats, such as phishing, malware, APTs and supply-chain attacks (see Section 5.1), are comprehensively addressed, others receive far less attention and are handled inconsistently across stakeholders, particularly by regulators, as in the case of data leakages and impersonation attacks. This creates blind spots in threat management strategies, ultimately affecting overall resilience. Conversely, the expectations of demand-side and supply-side stakeholders are relatively coordinated regarding MSS, unlike those of regulators. To bridge this gap, industry-wide initiatives should focus on raising awareness of under-represented threats, especially on the regulatory side, to ensure robust frameworks for addressing emerging threats.

Proposed action. *Generate awareness among all relevant MSS stakeholders regarding the importance of threat analysis in various MSS activities.*

G2 – General cybersecurity market maturity observation. There seems to be a generic lack of market maturity assessment in the EU cybersecurity market landscape. This can be seen by the absence of continuous cybersecurity market surveillance that goes beyond products with digital elements (as in the Cyber Resilience Act) and covers cybersecurity-related services and infrastructure, including data residency and data operations aspects. Moreover, the lack of a significant demand- and supply-side focus on application security, despite its critical role in cybersecurity, could be covered by this kind of assessment. Sovereignty matters and supply-chain dependencies should constitute the main elements of such a cybersecurity market maturity assessment.

Proposed action. *Develop MSS market maturity criteria and implement them within market surveillance activities and resulting policy initiatives to increase EU MSS market maturity.*

7.3 MAIN BARRIERS

B1 – Diverging perspectives between customers and providers. The main barriers to MSS adoption include cost concerns, a lack of internal expertise, provider-related issues and challenges with technical and process integration. Both the demand and the supply side

recognise these obstacles. However, key differences arise in relation to how these barriers are perceived: the supply side places more emphasis on issues relating to customisation, service-level alignment and communication with customers; the demand side is more focused on trust, vendor relationships and the capability to integrate services into their existing environments. These differences highlight the contrasting priorities and expectations between MSS providers and their customers. Market consolidation could provide a means to reduce the variance in the delivery of MSS services; by the same token, the significant demand for these services across the Member States will likely lead to reduced variance and improved performance. It is also likely that service providers would keep the same stance in relation to mechanisms and funding schemes that allow them to benefit from government business and public tenders. In the light of this, while the market remains open for specific and clearly defined services, service provision can be entrusted to providers who meet strict(er) criteria that appeal more to Member States' public authorities and better serve the interests of the Member States.

Proposed action. *Monitor diverging perspectives with the aim of establishing equilibrium between demand expectations and supply-deployment plans, with an emphasis on service level alignments/customisations. This could have a catalytic role in increasing market maturity (see G2 above).*

B2 – Barriers regarding reporting incidents. The analysis of incidents is important in enhancing impact assessment and understanding the effect of cyber threats. Many organisations, however, may be concerned about disclosing incidents due to potential reputational damage, other legal repercussions, the perception of unclear obligations or insufficient monitoring capabilities. In a similar manner, a significant challenge in cybersecurity management is the risk of incidents – including significant ones – remaining unnoticed or unreported. This may happen due to the distributed responsibilities in the MSS service provisioning chain and the level of capabilities on the demand side. Regulatory stakeholders could strengthen frameworks for incident disclosure policies, while MSS suppliers should develop reporting tools to facilitate compliance with these frameworks and disseminate supported reporting practices to the demand side.

Proposed action. *Make incident management processes a component of regulatory compliance guidelines and have them implemented via MSS deployment plans.*

7.4 MAIN POINTS WITH REGULATORY RELEVANCE

R1 – Regulatory asymmetry in compliance adoption. Regulators populated the compliance frameworks landscape through certifications and mandated security policies, shaping expectations for both suppliers and demand-side organisations. However, regulatory adoption remains supplier driven, with service providers investing more in frameworks such as ISMS and in quality systems, while demand-side organisations implement them reactively to meet legal requirements rather than as part of a structured risk management strategy. Despite this, the demand side exhibits stronger engagement in specific areas such as ISMS auditing and supplier relationship management, reflecting a targeted regulatory approach. By providing ample guidance to their stakeholders, regulatory bodies can facilitate their efforts on the road to compliance. Cooperating and relying on the analytical competence of ENISA is a way to find commonalities across jurisdictions in the Member States, while weeding out obstacles that prevent stakeholders from complying. An additional area of concern for public authorities is the technical specification and service requirements in MSS. It follows that coordination with other, similar services already procured in public administration will be necessary to prevent overlaps. In specific terms, and with an eye to digital transformation, tenders for cloud services would be a sound area to coordinate with MSS in an effort to improve complementarity.

Proposed action. *Develop guidance to facilitate compliance processes by leveraging existing MSS approaches. Try to coordinate the adoption of transformative technologies (e.g. cloud services) in a homogeneous manner with regard to MSS-related services.*

R2 – Market mobilisation through regulation. Current regulatory frameworks primarily emphasise technical controls, such as detection and response mechanisms. Less emphasis is put on governance issues. While regulations ensure compliance with standards like the GDPR, leading to high supplier adoption rates, governance standards, security awareness courses and specialised training remain underdeveloped, especially on the demand side. This may generate imbalances between technical implementation and operations security governance, the latter of which is often necessary for long-term resilience and service performance. Regulators could address this imbalance by expanding enforcement beyond procedural compliance to ensure a sustainable and effective cybersecurity posture. While seeking to mobilise the market through regulation, public authorities should remain vigilant on the procedural cybersecurity requirements. It follows that to prevent service providers from being impacted by regulation, any regulatory requirements should remain reasonably balanced and should stimulate holistic service resilience, both technically and operationally.

Proposed action. *Include operational security in regulatory frameworks and support MSS market stakeholders in developing a sustainable long-term cybersecurity posture.*

R3 – Regulatory considerations in cybersecurity service adoption. The cybersecurity market demonstrates a strong regulatory influence on purchasing decisions, with businesses prioritising compliance with standards and industry-specific requirements. MSS providers emphasise regulatory alignment, yet demand remains selective, favouring stability and proven solutions over rapid technological adoption. Additionally, the cautious approach to re-evaluating service providers highlights the importance of long-term regulatory consistency and trust in cybersecurity procurement. Certification plays a key role, as a significant proportion of available solutions meet formal compliance criteria. Certification in MSS has a dual purpose: on the one hand it concerns aspects of service provisioning and delivery; on the other it contains a component about skills. Consequently, skills may eventually become part of MSS cybersecurity certification. A likely future direction for MSS certification is that it will take into account potential overlaps with certified cloud services, as they may embrace security management functions within the cloud functionalities offered.

Proposed action. *Promote MSS certifications, based on either existing standards or certification schemes, that provide long-term regulatory consistency, by also maintaining consistency in relation to the requirements of overlapping security management functions (e.g. cloud computing).*

7.5 MAIN RESEARCH TRENDS

R & D1 – Innovations and key focus areas. Current research trends in cybersecurity emphasise the need for innovation in digital supply chains, the application of AI for cybersecurity services, and enhanced detection and response mechanisms for cyberattacks. For the R & D community, the most pressing concerns revolve around web application attacks and APTs, both of which present significant risks for organisations. Supply-chain attacks and misconfigurations further compound these challenges, emphasising the critical need for advanced research on detecting and mitigating these threats. Until now, research on APTs and misconfigurations has been reserved for highly specialised entities such as large IT market players and small companies. Through the application of AI techniques, research around APTs, supply chains and misconfigurations may be facilitated and may become more suitable for academic institutions or most small and medium-sized enterprises in the cybersecurity space. In the wake of the war on the European continent and the cybersecurity support action it has resulted in as a means of response, EU and industry responses to such challenges can be further studied and analysed ([20]).

([20]) Cyber Solidarity Act.

Proposed action. *In order to create competitive advantages in the EU MSS market, promote technological approaches (AI) that can enable EU research in high-profile areas in the context of MSS, such as the identification of supply-chain dependencies, APTs and misconfiguration threats.*

R & D2 – Key IT developments in cybersecurity services research. Emerging IT developments are set to significantly shape cybersecurity services research, with both positive advancements and potential challenges. The application of AI for cybersecurity services stands out as a key enabler, as it will enhance threat detection, automate response mechanisms and improve overall efficiency in handling cyber incidents, the automation of penetration testing, anomaly detection, identity management, attack simulation, etc. However, AI also presents new threats by lowering the barrier for attacks. In addition, AI systems are an attractive cybersecurity target. Similarly, the use of the IoT / OT within a more efficient MSS presents both a positive impact (i.e. by means of a facilitating finer-grained security management) and a threat (i.e. due to the exposure of IoT components). Another critical development is the focus on developing more effective methods for detecting and responding to cyberattacks, a fundamental area of research that aligns with both AI innovations and the growing complexity of cyber threats.

Proposed action. *Promote the incorporation of emerging technologies (AI, IoT) to increase the overall efficiency of MSS functions and remove possible gaps and barriers (see also G1, G2, B1 and B2 above).*

ANNEX A: COMPLIANCE AND SKILLS

Table 8: Relevance of requirements, regulation, standards and frameworks for MSS – demand and supply perspectives

Requirements, regulations/standards/frameworks	Demand	Supply
Information security management system (ISMS)	**21 % (average)**	**32 % (average)**
ISO/IEC 27001 on ISMS, ISO/IEC TS 27022 on information management system processes, ISO/IEC 27002 on information security controls, ISO/IEC 27003 on ISMS guidance, ISO/IEC 27004 on monitoring, measurement and evaluation	**53 %**	**92 %**
ISO/IEC 27006 – Requirements for auditing ISMS	**8 %**	**3 %**
ISO/IEC 27007 – Guidelines for ISMS auditing	**3 %**	**3 %**
Quality management system	**37 % (average)**	**74 % (average)**
ISO 9001 – Quality management systems – Requirements	**37 %**	**74 %**
IT governance	**16 % (average)**	**20 % (average)**
Control Objectives for Information and Related Technology	**18 %**	**16 %**
ISO/IEC 38500 – Information technology – Governance of IT for the organization	**13 %**	**24 %**
IT service management life cycle	**18 % (average)**	**30 % (average)**
Information Technology Infrastructure Library	**26 %**	**55 %**
ISO/IEC 20000 – Information technology – Service management	**16 %**	**24 %**
ISO/IEC 27013 – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	**11 %**	**11 %**

Information/data management and continuity standards	**20 % (average)**	**32 % (average)**
Business continuity management, e.g. ISO 22301, ISO/IEC 27031	**39 %**	**50 %**
Communication security, ISO/IEC 27010 – Information security management for inter-sector and inter-organisational communications	**13 %**	**24 %**
Hardware-related standards	**8 %**	**16 %**
ISO/IEC 27701 on privacy management	**18 %**	**37 %**
Management of customer data	**30 % (average)**	**53 % (average)**
GDPR	**50 %**	**76 %**
Payment Card Industry Data Security Standard	**11 %**	**39 %**
System and Organization Controls 2	**29 %**	**45 %**
IT asset management	**11 % (average)**	**32 % (average)**
ISO/IEC 19770 – Information technology – IT asset management	**11 %**	**32 %**
Other	**12 % (average)**	**17 % (average)**
ISO 31000 – Risk management	**18 %**	**32 %**
ISO/IEC 27017 on cloud security	**16 %**	**29 %**
ISO/IEC 27021 – Competence requirements for information security management systems professionals	**5 %**	**3 %**
ISO/IEC 27035 on incident management, ISO/IEC 27041 on incident investigative method, ISO/IEC 27043 on incident investigation principles	**16 %**	**21 %**
ISO/IEC 27036 on supplier relationships (includes service providers)	**11 %**	**3 %**
ISO/IEC 27037 on collection of digital evidence, ISO/IEC 27042 on interpretation of digital evidence (under 'management of customer data' or 'Other'), ISO/IEC 27050 on electronic discovery	**3 %**	**8 %**

ISO/IEC 27039 – Selection, deployment and operations of intrusion detection and prevention systems	**5 %**	**0 %**
Other	**18 %**	**39 %**

ANNEX B: REQUIREMENTS

Table 9: Relevance of requirements from the demand and supply sides

Relevant requirements	Demand	Supply
Technical	**43 %** (average)	**48 %** (average)
Data analytics can be applied on large amounts of data/logs	29 %	32 %
Data protection tools and techniques	38 %	54 %
Methods of data analytics that are necessary for service provisioning	19 %	30 %
Monitoring and detection tools and techniques	67 %	76 %
Multi-platform/multi-device coverage	29 %	49 %
Preparedness and prevention requirements	86 %	62 %
Restore and recovery tools and techniques	76 %	51 %
Size of the customer infrastructure	0 %	0 %
The service provider can provide analysis of artefacts and forensic evidence, compliant with international standards and best practices	43 %	43 %
The service provider can provide support in triage, information collection, root-cause analysis and co-relation of cybersecurity incidents affecting the protected assets	48 %	59 %
Use of technical standards and good practices	29 %	54 %
Vulnerability and update management tools and techniques	52 %	68 %
Processes and procedures	**52 %** (average)	**61 %** (average)
Cybersecurity governance, risk and control requirement	76 %	76 %
Cybersecurity policy, procedures and strategy	67 %	68 %
Data protection and privacy control and compliance requirements	43 %	54 %
End-to-end coordination of action relating to emergencies	52 %	54 %
The service provider can advise on and support security service coordination by means of dedicated processes, whereas coordination may be provided on demand, end to end and either remotely or on-site	38 %	51 %
Use of procedural standards and good practices	38 %	65 %
Requirements relating to digital sovereignty	**76 % (average)**	**78 % (average)**

Location of data storage	76 %	78 %
Business requirements	**57 % (average)**	**34 % (average)**
Flexible pricing schemes	48 %	51 %
Proof of concept before contracting	67 %	0 %
Support for multi-vendor inclusion capabilities	57 %	51 %
SLA and metrics requirements	**55 % (average)**	**30 % (average)**
Customisation of SLAs according to operational needs	86 %	59 %
Selection and parametrisation of metrics for defined SLAs	24 %	0 %
Workforce-related requirements	**55 % (average)**	**30 % (average)**
Available workforce certifications and experience levels	38 %	49 %
The service provider has the capacity to support the management and coordination of multiple requests/incidents simultaneously, including large-scale ones	33 %	49 %
Training of own personnel	48 %	46 %
Workforce availability	62 %	62 %
Workforce knowledge/expertise	76 %	70 %
Provider organisational-level requirements	**51 % (average)**	**55 % (average)**
Geographical presence, allowing ad hoc on-site engagement of provider personnel	62 %	70 %
Levels of capacity	76 %	62 %
National certification of accreditation of service provider in cybersecurity field	38 %	46 %
Communication offered in official languages of EU Member States	48 %	57 %

ANNEX C: MARKET RESEARCH AND INNOVATION

Table 10: Most important cybersecurity services and MSS research topics (demand)

MSS research topics	Percentage of responses
Digital supply chains	67 %
Application of AI for cybersecurity services	62 %
Developing more effective methods for detecting and responding to cyberattacks	52 %
Automation of a plan to mitigate threats (e.g. course of action)	48 %
Advanced analysis of security threats and vulnerabilities	48 %
Dealing with new cybersecurity threats and vulnerabilities	43 %
Role of cloud computing in cybersecurity services	38 %
Convergence of OT/IT	38 %
Data exchange and ingestion to improve analysis of the threat level and vulnerability risk	33 %
Cybersecurity indicators, metrics, SLAs	29 %
Legal issues	29 %
Use of the IoT and its impact on cybersecurity services	29 %
Impact of remote working (e.g. zero trust)	19 %
Economic issues	14 %
Developing cybersecurity policies, standards and certifications that consider MSS	10 %

ANNEX D: ABBREVIATIONS

Abbreviation	Description
APTs	advanced persistent threats
AI	artificial intelligence
B	barrier
CSA	Cybersecurity Act
ENISA	European Union Agency for Cybersecurity
EU	European Union
G	gap
GDPR	General Data Protection Regulation
IEC	International Electrotechnical Commission
IoT	internet of things
ISMS	information security management system
ISO	International Organization for Standardization
IT	information technology
MSS	managed security services
OT	operational technology
R	regulatory-related topics
R & D	research and development / research topics
SLA	service level agreement
T	trend

TP-01-25-010-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 978-92-9204-702-3
doi:10.2824/7566738