EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CLOUD CYBERSECURITY MARKET ANALYSIS

VERSION 1.0

MARCH 2023

ABOUT ENISA

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

CONTACT

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

AUTHORS [1]

Andrea Ganzaroli, Louis Marinos, Greta Nasi, Aljosa Pasic, Silvia Portesi

ACKNOWLEDGEMENTS

ENISA would like to thank the following persons.

- The members and observers of the ENISA Ad Hoc Working Group on EU Cybersecurity Market Analysis for their guidance and feedback during the various phases of this work and review of this document.
- The ENISA National Liaison Officers Network, the ENISA Advisory Group, the European Cybersecurity Certification Group and Stakeholder Cybersecurity Certification Group for their input during the scoping phase and for their feedback during the validation phase of this report.
- All ENISA colleagues who provided input during various phases of this report and/or reviewed this report.

[1] The authors are listed in alphabetical order by surname.

LEGAL NOTICE

COPYRIGHT NOTICE

978-92-9204-623-1, 10.2824/050402

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The present European Union Agency for Cybersecurity (ENISA) report is an analysis of the cloud cybersecurity market, planned for in ENISA's *Work Programme 2022* ([2]) under activity O.7.1., 'Market analysis on the main trends in the cybersecurity market on both the demand side and the supply side'. The selection of this segment for this year's cybersecurity market analysis is the result of a poll carried out with the involvement of multiple stakeholders, both outside and within ENISA. The criteria used for the prioritisation of the collected proposals were the size of the relevant market, the importance and criticality of the market for businesses of all sizes, relevance of the sector to EU policy, relevance to research and relevance to regulatory activities.

For this analysis, ENISA has performed primary research, that is, a survey involving the main stakeholder types of the cloud computing ecosystem by means of dedicated questionnaires. The quantitative information from the survey has been validated via qualitative information obtained through open-source information, as well as by means of quality assurance by various external experts, including the members of the ENISA Ad Hoc Working Group on Cybersecurity Market Analysis.

By collecting information from various stakeholder types of the cloud ecosystem, we were in the position to assess stakeholder-specific perspectives on cloud cybersecurity. Differences among stakeholder perspectives are key to understand differences in viewpoints, requirements, capability levels, perceptions about threats and challenges, compliance, etc. These variating views are – in many cases – indicative of potential market trends, market barriers, market and research gaps, skill shortages, the existence of market niches, etc. The conclusions of this report capture many of these topics, in particular the following ones.

- **Market characteristics and market trends.** A variety of cybersecurity market characteristics and market trends are presented, including manageability of offered cybersecurity functions, technical integration options for various cybersecurity functions, the role of data privacy, consolidation of on-premises and off-premises security (see Section 8.1).
- **Market barriers.** Factors leading to difficulties in the market adoption of cloud computing services have been identified, in particular variating perceptions about the level of threat management by various cybersecurity functions, lack of cybersecurity skills in most of the stakeholders of the cloud ecosystem, the reduced level of adoption of cybersecurity-related certifications, low availability of standards and intellectual property rights (IPRs), as well as distortions in the flow of vulnerability and incident information among the cloud stakeholders (see Section 8.3).
- **Market gaps.** Various gaps in the cloud cybersecurity market emerge through mismatches in deployment of cybersecurity functions between the demand side and supply side. The market gaps are rooted in concerns about the management of various threats and unclear distributions responsibilities about the implementation and maintenance of cloud cybersecurity functions (see Section 8.2).
- **Research and innovation.** Some clear indications about the importance of zero-trust architectures, the use of privacy enhancing technologies and the impact of cloud technology in artificial intelligence, 5G and quantum computing make these topics excellent candidates for research and deployment actions (see Section 8.4).

([2]) https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-document-2022-2024, accessed November 2022.

- **Future market projections.** A number of reflections regarding the future paths for the development of the supply of cloud cybersecurity services have been formulated. These are mainly attempts to properly orchestrate cybersecurity services, where different approaches will be implemented, depending on the nature of cloud suppliers (for example hyperscalers and cloud enablers) (see Section 8.5).

Besides the analyses and conclusions presented in this document, there is some additional material in this work that may be interesting for a number of stakeholders. This includes collected raw data, developed questionnaires, details of the various stakeholder perceptions, scoping information, as well as the tools and processes used. ENISA is open to share any kind of information resulting from this cybersecurity market analysis with interested stakeholders.

1. INTRODUCTION

The present report on cloud cybersecurity market analysis is the result of an activity planned in the European Union Agency for Cybersecurity (ENISA)'s *Work Programme 2022* ([3]), under activity O.7.1.: 'Market analysis on the main trends in the cybersecurity market on both the demand side and the supply side'. Elaborations on the market uptake of cybersecurity products, services and processes contribute toward the ENISA strategic objective of 'A high level of trust in secure digital solutions'.

Market analysis at ENISA is performed on an annual basis, delivering each year an analysis of a market sector that has been selected by several of ENISA's stakeholders. For 2022, the area of cloud cybersecurity market analysis has been selected. Various factors have contributed to this selection, namely: the activities in the area of cybersecurity certification through the European Union Cybersecurity Certification Scheme for Cloud Services (EUCS), the emergence of various technological factors that will influence this important market segment (e.g. artificial intelligence (AI), 5G), the wish to foster EU innovation based on research results in this area, ongoing/emerging regulatory actions both at EU and Member-State level. With this work, ENISA seeks to provide market intelligence in this domain, in order to facilitate all these activities.

With this objective in mind, primary research has been performed on the basis of a survey that was developed and conducted by ENISA with the support of the ENISA Ad Hoc Working Group on Cybersecurity Market Analysis ([4]) and some external experts. The entire work has been conducted via processes and activities as described in the ENISA Cybersecurity Market Analysis Framework (ECSMAF). What is more, this year's work has served as a thorough test of ECSMAF; the experience gained has been fed back to the ENISA framework and has led to an updated version of ECSMAF V.2 ([5]).

This report is the outcome of this ENISA analysis. It contains the most important findings from the survey, which are oriented towards the various target groups of this report, these being the following.

- **EU institutions, bodies and agencies**. Market analyses are important to help policymakers understand trends and related supply and demand issues.
- **National public authorities, in particular bodies involved in regulation.** Market surveillance is the main instrument for efficient regulatory policies.
- **ENISA stakeholder groups** (e.g. the European Cybersecurity Certification Group, Stakeholder Cybersecurity Certification Group, and ENISA Advisory Group). Market intelligence may support decision-making for prioritising various cybersecurity efforts and spotting market gaps.
- **Industry and cross-sectoral associations.** Market analyses allow them to analyse market opportunities, trends, challenges and vulnerabilities and allow for the creation of competitive advantages for EU industry players.
- **Consumer organisations and associations.** Market analyses allow them to comprehend the needs and requirements of consumers for cybersecurity products, services and processes, and their prospects in the European cybersecurity market.

([3]) https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-document-2022-2024, accessed November 2022.
([4]) https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf-v2.0

- **Research and development (R & D) organisations.** They can use the proposed methodology to assess the maturity of existing products and markets and guide the development of new technologies and services.

As a final note, one should underline that this activity has value that goes beyond the content of this report, which lies mainly in the fact that an entire market analysis life-cycle process was performed. Numerous other side products of this life cycle may also be useful to a variety of stakeholders: scoping information, generated questionnaires, threat assessments, raw data collected, etc. This material bears a high potential for reuse, re-scoping and adaptation to other purposes, among other things. Last but not least, by performing a complete market analysis life cycle, ENISA is in the position to transfer this knowledge to interested parties and/or elaborate on integration and use-cases with relevant cybersecurity disciplines, thereby creating a win-win situation.

1.1. SCOPING OF THE CLOUD CYBERSECURITY ANALYSIS

Performed in accordance with the ECSMAF ([5]), the present analysis of the cloud cybersecurity market has been initiated through a scoping activity. The objective of scoping is manifold.

- To agree on the depth and breadth of the analysis, by focusing on the relevant cybersecurity market elements according to their importance (i.e. role for the supplier, role for the demand side, level of exposure to threats). The agreement for the current analysis included the members of the ENISA Ad Hoc Working Group on Cybersecurity Market Analysis, stakeholders of ENISA (ENISA Advisory Group and National Liaison Officers Network), as well as ENISA internal groups.
- To make sure that the analysis effort can be performed with the available resources (human and monetary) within the available time.
- To identify the data collection method (primary, secondary).
- To identify the groups participating in the validation of the intermediate and final results of the analysis.

As proposed in the ECSMAF, the focus of the current cybersecurity market analysis has been set in such a way as to cover the important concerns and perceptions of the various stakeholders of the cloud computing ecosystem:

- **the demand side**, which includes the end users of cloud services;
- **the supply side**, which includes cloud service providers (CSPs) and cloud enablers;
- **organisations conducting R & D in cloud computing**;
- **bodies involved in regulation**, covering regulatory activities in could computing.

Detailed descriptions and profiles of these stakeholders can be found in Section 2.1.1.

The focus of the present cloud cybersecurity market analysis is summarised in Table 1. The detailed scoping of the analysis can be found in Annex B.

Table 1: Scoping overview of current market analysis

Scoping criteria categories	Scoping criteria		
Demand side	• Assessment of generic company data for the demand side		

([5]) https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf-v2.0

Scoping criteria categories	Scoping criteria		
	• Role of procured service for the business • Required demand-side capability or maturity for deploying the procured product • Role of the product in risk mitigation • Demand-side presence in various geographies • Demand-side requirements to be met by the procured product • Identification of gaps in products available to meet demand-side requirements • Investment plan for financing procurement of the product • Market barriers towards deployment of the service		
Supply side	• Supplier financial figures • Assessment of supply-side company data • Presence in different geographic spaces of the supplier who delivers the product • Business role of the product in the supply chain of the supplier • Capabilities required to deploy the product • Role of the product in threat reduction • Assessment of product requirements • Gaps and emerging requirements • Investment strategies to finance the development of the product • Market trends and barriers.		
R & D	• R & D financial figures • R & D organisational details • Assessment of relevant contemporary research activities in the market area; • Assessment of efficient funding instruments • Market drivers in the related market area • Market trends barriers • Importance of skills • Innovative research topics in related technology areas		
Bodies involved in regulation	• Type, size and areas of influence of the organisation		

Scoping criteria categories	Scoping criteria		
	• Market segments/areas/sectors under regulatory supervision; • Regulatory instruments used • Cybersecurity threats whose exposure will be reduced via regulatory activities • Assessment of transition plans to new regulatory instruments; • Market drivers for regulatory compliance • Market barriers for regulatory compliance • Planned incentives to support transition by market players		

The selection of the scope for the cloud cybersecurity market analysis has significantly influenced the content of the survey. The consequences of the above scoping decision for the collected and analysed information are discussed below.

Focus, content and structure of the collected market information

The current analysis aims at highlighting the **cybersecurity-related properties** of cloud offerings. Moreover, it embraces the perceptions of the stakeholders of the cloud ecosystem, by analysing their cybersecurity and business requirements, their needs and the impact of service deployment towards reduced exposure to cyberthreats. The following elements are taking into consideration in the market analysis:

- **Collection of stakeholder perspectives on equal or similar issues.** By asking questions about various cybersecurity-related matters of cloud services to a variety of stakeholder types, their viewpoints can be compared and various interesting points can be identified (i.e. similarities and gaps in perception, differentiated requirements, various views of relevant threats, etc.). Most of the sections of this analysis present such views in a comparative manner.
- **Emphasis on the cybersecurity details of the offerings.** Instead of looking at generic market figures, the cybersecurity analysis conducted concentrates on the cybersecurity-related properties of the service. This creates a specific angle of analysis that is merely based on the conception and consumption of the cybersecurity characteristics of the service.
- **Emphasis on cybersecurity threats and challenges.** A basic element in the conducted analysis is the ability of a service to reduce exposure to cyberthreats and to help master cybersecurity challenges. By taking into account data on cyberthreat exposure and cybersecurity challenges for cloud services, we generate a multi-stakeholder perception of the central cybersecurity properties of the analysed service.
- **Assessment of necessary capabilities, market drivers and barriers.** A number of important market success parameters are also taken into account. Adequate demand-side capabilities to efficiently deploy the service is an important adoption criterion. Similarly, market divers (and its antipode, market barriers) are decisive factors towards achieving market vitalisation and the successful launch of a product/service.

Market information that is outside the focus of the analysis

Given the selected scope of the cloud cybersecurity analysis, we have neither collected economic/financial figures regarding supply and demand in cloud computing nor assessed any of the long-term financial figures and statistics of the relevant market. This is particularly the case for financial data on supplier and end-user market activities and market development statistics; such data include past, present and forthcoming market-value information on suppliers and end users. The collection of such economic figures is a long-term activity, requiring qualitative, long-term data collection. Such activities go beyond our scope, resource availability and planning horizon. There are certainly other activities/organisations that are better suited to perform such long-term tasks, both outside ([6]) ([7]) and within ENISA ([8]).

1.2. INFORMATION ON PERFORMED DATA COLLECTION

Through ENISA stakeholder consultations and past experience with market analysis, it has been decided to perform primary research for the cloud cybersecurity market analysis. For this purpose, a survey has been generated, supported by the ENISA Ad Hoc Working Group on Cybersecurity Market Analysis and external experts. The survey was divided in questions targeting the various stakeholders of the cloud ecosystem. The survey consisted of around 100 in questions total, for all cloud stakeholder types (i.e. supply, demand, R & D and bodies involved in regulation). As survey tool, the EUSurvey ([9]) platform has been used. The survey is anonymous. No data about the responders has been collected, therefore tracing back the responders is impossible.

Through an ENISA announcement, 230 stakeholders interested in participating in the survey have been identified (pre-registered). Among those, there were also associations of cloud suppliers and cloud users, but also cloud computing consortia. While the pre-registered individuals came from all over the world, the majority were located or active in the EU. Around 60 responses were submitted via the online survey.

Table 2 provides an overview of the data collection process.

Table 2: Overview of survey phases and data collection

Survey phase	Responders	Comment
Announcement of survey		Via the ENISA website, social media and email messages to potential participants
Pre-registration	Ca. 230	Worldwide coverage
Number of responders to survey	Ca. 60 (26 %)	Worldwide coverage
Balance among targeted stakeholder types	Supply: 25 % (15) Demand: 35 % (21)	

([6]) https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Cloud_computing_-_statistics_on_the_use_by_enterprises#Use_of_cloud_computing:_highlights, accessed November 2022.
([7]) https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html?gclid=Cj0KCQjwmouZBhDSARIsALYcouoE5lzylvOuu6pgJA3ZcVr5TYESo_H1GEciWISu5uf4HnOeNJlW7F0aAhTvEALw_wcB, accessed November 2022.
([8]) https://www.enisa.europa.eu/news/enisa-news/cybersecurity-spending-an-analysis-of-investment-dynamics-within-the-eu, accessed November 2022.
([9]) https://ec.europa.eu/eusurvey/home/welcome, accessed November 2022.

	R & D: Regulators:	20 % (12) 20 % (12)	

After reception of the submitted answers, a quality analysis of the received data was performed. This included mainly data sanity checks, such as plausibility and data consistency checks. The data set that went into the analysis is considered as a whole to be representative thanks to:

- a good mix of large and smaller organisations, both on the supply and demand sides;
- good coverage of EU Member States;
- good coverage of R & D organisations conducting cloud-related research; and
- good coverage of EU regulatory bodies engaging in cloud regulation.

The quantitative data obtained through the survey have been validated by means of additional qualitative data obtained through desktop research: the analysed results and conclusions made were compared with findings from publicly available information to examine in more depth their validity. As an additional validation step, the analysis and the final conclusion was reviewed by various subject-matter experts, such as contracted external experts and members of the ENISA Ad Hoc Working Group on Cybersecurity Market Analysis.

All in all, the survey had a positive outcome for ENISA, in particular to gain further experience in terms of scoping and structuring a cyber security market survey, market stakeholder mobilisation and data sanity and data validation.

The second deliverable in 2 years' time, this analysis helped ENISA to increase its maturity level in the performance of cybersecurity market analysis tasks, with the advantage of being in the position to transfer collected knowledge to external and internal ENISA stakeholders alike.

1.3. STRUCTURE OF THIS REPORT

The report has been structured so as to contain the highlights of the performed cloud cybersecurity market analysis. Its sections contain the most important findings from the performed survey and comprise a synthetic view based on the collected evidence. With the presented material, we seek to cover the information needs of the main target group of the report, this being all stakeholder types of the cloud ecosystem (see also Section 2.1.1), thus covering the information needs of supply, demand, regulatory bodies and R & D organisations. It is assumed that with this information at hand, the needs of Member States, the European Commission and EU institutions, bodies and agencies will also be covered, as they will be in the position to satisfy their information needs by taking into account the presented results in all kinds of oversight, guidance and regulatory activities. Should some of these external stakeholders wish to have access to the anonymous raw data collected, they can contact ENISA to submit their request (see contact information at the beginning of this report).

Moreover, the generated results will be of value to ENISA's internal stakeholders. For example, various ENISA activities in the areas of certification, cybersecurity index, research and innovation, cybersecurity investments, cyberthreat analysis, vulnerability management, etc., may use both these results, but also raw data of the performed survey for their own purposes.

It is worth mentioning that the structure of this report has already been validated by ENISA stakeholders, such as the ENISA Advisory Group and the National Liaison Officers Network, and ENISA-internal groups working in areas overlapping with the contents addressed in this analysis.

The structure of this report is as follows.

- **Chapter 2** 'Characteristics of the cloud cybersecurity ecosystem', builds the basis for the entire analysis. It provides all items that are considered to be relevant for cloud cybersecurity. This content had the main role in the formulation of the survey questions, and consequently for the entire set of findings.
- **Chapter 3** 'Demographics of involved stakeholder types', presents the findings related to structural, geographical and organisational details of the surveyed companies and organisations.
- **Chapter 4** 'Cloud usage patterns and requirements', presents in detail the usage patterns of the cloud, both from the supply and demand sides, and the cybersecurity requirements as they are fulfilled within cloud offerings, but also as they are anticipated by the demand side.
- **Chapter 5** 'Threats, challenges and capabilities', provides valuable information from all involved stakeholder types about their perceptions of assessed cyberthreats, cybersecurity challenges encountered and levels of capability to mitigate these threats and face these challenges.
- **Chapter 6** 'Role of regulation and certification', is dedicated to regulatory activities in cloud cybersecurity, highlighting the role of certification in this regard.
- **Chapter 7** 'Cloud cybersecurity market trends', provides the analysis results regarding market evolution, market drivers and barriers, and market innovation areas.
- **Chapter 8** 'Concluding remarks', provides a summary of the conclusions drawn from the current cloud cybersecurity analysis.

2. CHARACTERISTICS OF THE CLOUD CYBERSECURITY ECOSYSTEM

When analysing the cloud computing cybersecurity market, it is necessary to envisage/assess various building blocks of cloud computing, such as infrastructure components, models, activities, characteristics, capabilities and service architecture. These cloud computing elements ([10]) will be impacted by any materialised threat, deliberate or accidental, causing potential damage to hosted data and services.

In this section, we present all relevant elements of cloud computing that are considered as the main assets of cloud computing infrastructure. Existing standards regarding the cloud computing infrastructure components, cloud models and service provisioning have been considered for this discussion ([11]). Moreover, numerous publications do exist, consolidating cybersecurity issues in cloud computing environments. Based on this material, a summary of various cloud computing assets is provided in the discussion below. Related threat-assessment reports/documents indicate methods on how they can be targeted and which cybersecurity issues have been encountered.

In the context of a cybersecurity market analysis, the role of the presented material is to set the scene for the relationship between cybersecurity and cloud computing.

Companies in cybersecurity market segments, for example, relate to cloud computing in several ways, such as by providing security from the cloud (the 'security as a service' (SECaaS) business model), providing security for the cloud computing infrastructure (e.g. secure stack components) or providing security in the cloud (e.g. confidentiality of data in the cloud).

Similarly, companies from the cloud computing market segment, which could be hyperscalers offering public cloud services, independent software vendors or even other enablers (managed cloud, brokers etc.), increasingly offer various cybersecurity security products and services as well.

This makes market segmentation and value-chain issues in cloud computing security highly dynamic and volatile, with convergence and interference of cybersecurity and cloud computing elements being an important part of the context for this report.

With this material in mind, survey questions were formulated to cover both demand and supply perceptions on:

- the overall structure of cloud computing infrastructure, related ecosystem and elements, including service provisioning and relevant cloud computing stakeholders;
- available cloud and cybersecurity services,
- common cloud computing and service threats;
- cybersecurity challenges in the cloud computing ecosystem; and

([10]) The word 'elements' is used as a synonym of 'cloud computing building blocks'. Moreover, assets are considered cloud elements that are critical for the user of the service and/or for the operator of the cloud computing infrastructure, thus being valuable for the end-to-end service provisioning and/or for the business process they implement.
([11]) E.g. https://www.iso.org/committee/601355.html#, accessed April 2022.

- cybersecurity controls, technologies and solutions, deployed to deal with threats and challenges in cloud computing.

It must also be noted that most of the collected material reflect the status of cloud computing as it has evolved in the last years, but it is limited in that it has to present a rather a static view on cloud computing.

The development and adoption of emerging technologies, such as the Internet of Things (IoT), 5G and AI, but also the pace of digital transformation, has contributed to an even faster evolution and adoption of cloud computing technology. Edge computing ([12]) / fog computing ([13]) and cloud continuum ([14]), are examples of the transformation of cloud computing. Within this analysis, the dynamic part is captured by means of an assessment of cloud innovation trends.

The analysis targets ecosystem perspectives through a number of stakeholder views (see also Section 2.1.1). On the demand side, these are mainly stakeholders who already have (or wish to establish) a contractual relationship with a CSP and use cloud security products or services, either from the same CSP or from another supply-side stakeholder (cloud enabler, independent software vendor, etc.). Regarding the supply side, these are either stakeholders directly providing cloud computing and cloud security services or enablers adding some value to the cloud service provided by the CSP (i.e. cybersecurity product or services, managed detection and response, consulting, etc.).

2.1. CLOUD ECOSYSTEM

The cloud ecosystem is understood as mix of technology, operational and organisational entities that make up the entire service provisioning chain and cover both supply and demand. The cloud ecosystem consists of different cloud service categories, cloud deployment models, cloud capability types and cybersecurity-related services, functions and capabilities. Roles and relationships between stakeholders on the supply and demand sides are the most important part to define an ecosystem, together with specific resources, requirements and issues for certain organisations or users. While cloud computing roles and associated activities and responsibilities are standardised ([15]) ([16]), the relationship with cybersecurity might not clearly taken into account in these definitions. To give an example, a managed cybersecurity service operator (e.g. managed detection and response) might need access to cloud computing network traffic or log files on behalf of its client, but it might not be considered as a 'cloud service partner' as defined by ISO ([17]).

In this section, the various cloud ecosystem elements that are important for this analysis are briefly presented. They make up the basis of this analysis and were an integral part of the survey.

As regards the cloud infrastructure, four infrastructure levels are considered. The cloud infrastructure levels are related to cybersecurity, both within cybersecurity products and services (see Section 2.3) and by means of threats targeting those infrastructure levels (see Section 2.5). These levels are:

- the **data level**, representing the data household of cloud computing, with both stored data and data in transit;
- the **application level**, representing installed applications using the cloud computing resources (hardware and software);

([12]) https://en.wikipedia.org/wiki/Edge_computing, accessed May 2022.
([13]) https://en.wikipedia.org/wiki/Fog_computing, accessed May 2022.
([14]) https://www.veritis.com/blog/what-is-cloud-continuum-and-how-businesses-can-leverage-it/, accessed May 2022.
([15]) https://www.iso.org/standard/60544.html, accessed November 2022.
([16]) https://www.iso.org/standard/60545.html, accessed November 2022.
([17]) https://www.iso.org/standard/60544.html, accessed November 2022.

- the **network level**, representing the network elements/service used by the cloud computing node, including security elements responsible for the network protection; and
- the **host level**, representing all elements supporting the virtualisation functions, such as the virtual server, virtual machines and the hypervisor.

2.1.1. Cloud Computing Stakeholder Types

While multiple stakeholders may be part of the cloud computing ecosystem, for the sake of this market analysis, we will only consider the main stakeholder types described below (see Table 3). It is worth mentioning that organisations may play multiple roles in the cloud ecosystems. For example, a research institution can concurrently act as a cloud user, an enabler can consume cloud services for its own need, and a regulator can subscribe to a cloud service.

The roles presented below are the main ones mentioned in various publications on cloud computing. Nonetheless, they present a rather static view, as opposed to the dynamic nature of the cloud ecosystem, where various other roles may emerge and existing ones may overlap or evolve. The choice of this rather static approach is due to the purpose of grouping questions of this survey accordingly.

In the survey underlying this analysis, stakeholders invited to participate in the survey may refer to the various roles they may hold in the cloud ecosystem. For each role, they will be asked to answer the corresponding survey questions dedicated to that role. In this way, we aim at covering the maximum scope of their activities in the cloud ecosystem.

Table 3: Main cloud stakeholder types considered for the purpose of the present market analysis

Stakeholder type	Description	Examples
Supply side: CSPs	Owners and operators of cloud computing systems offering public, private, hybrid and community cloud services. They are responsible for end-to-end service provisioning, including maintenance, protection and infrastructure upgrades. They may include various service providers in their service provisioning supply chain.	Microsoft, Google, Amazon (all models: software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS), Oracle, SAP, Salesforce (for SaaS, PaaS).
Supply side: enablers	Enablers are intermediates between end users and public-service platform providers and/or private cloud computing. They facilitate the adoption of cloud services by, for example: • packaging services; • providing added-value services on top of services offered by service platform providers; • operating the private cloud for customers; • providing multi-cloud solutions. Enabler examples include cloud brokers, integrators, consultants, developers, outsourcers, application hosting, etc. Their offerings add value to CSPs (see above) and/or operators/managers of private cloud platforms.	ATOS, Cap Gemini, Accenture, Deloitte, PwC, KPMG etc.

Stakeholder type	Description	Examples
Demand side: end users, consumers	Both current and prospective subscribers of cloud computing services, at all levels of their business processes (including infrastructure providers integrating cloud services within their infrastructure, e.g. 5G operators, financial institutions, IoT service providers, etc.).	All kinds of subscribers – both private and commercial – irrespectively of size and business needs.
Entities involved in regulatory work	National or international entities / public authorities / institutions that – directly or indirectly – exert regulatory influence on cloud services.	European Commission, regulators of Member States, data protection authorities, associations, etc.
R & D	Public and private organisations performing research on cloud technology, cloud services, cloud operations, cloud functions, usage models, etc.	Universities, research institutions.

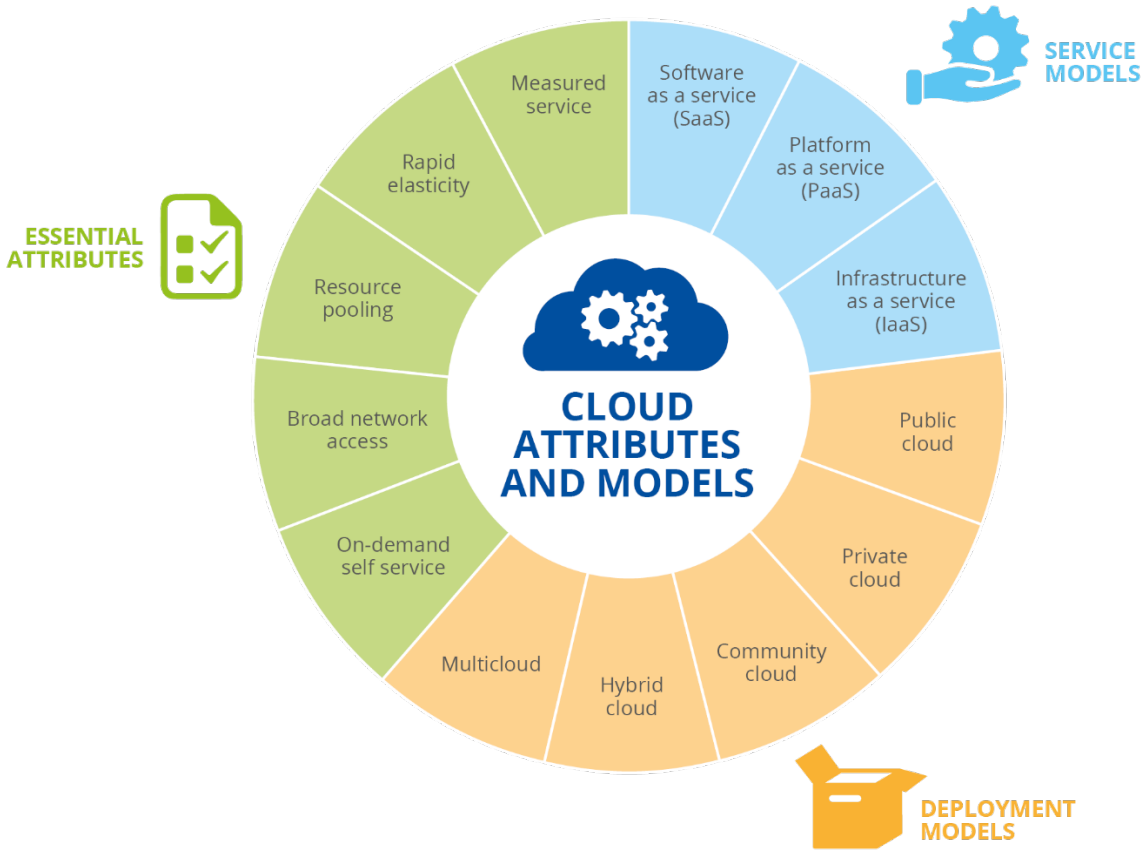
Note: Throughout this cloud cybersecurity market analysis, we have not discriminated between cloud service providers and enablers. Instead, we have merged these two types under the stakeholder type 'supply side'. Although this differentiation would be significant to capture the market role of these two stakeholder types, there is still a certain 'blurriness' in the market regarding these types. In many cases, cybersecurity services are integrated in typical CSP offerings. On the other hand, enablers often act as resellers of typical cloud services, while providing value-added cybersecurity services. This fact introduces a certain 'blurriness' in the market. Besides this, the merge was also done in order to simplify the dissemination to organisations that are active in supplying cloud services and in order to avoid confusion on the part of the participating organisations.

2.2. CLOUD MODELS AND ATTRIBUTES

As defined in relevant standards ([18]), the cloud paradigm consists of five essential attributes, three service delivery models and four deployment models. Their relationship with cybersecurity is documented in different standards ([19]) ([20]) and other reports. Understanding the ecosystem and division of responsibility is essential in order to understand the market context, with so many vendors, platforms, tools and services that fall under the IaaS, PaaS and SaaS categories, sometimes overlapping, as well as the fast evolution of deployment models. While responsibility used to be more statically assigned in the past, these days it is more appropriate to talk about the sliding scale of security responsibilities in the cloud. Figure 1 provides an overview of this.

([18]) https://www.mdpi.com/2076-3417/11/19/9005/pdf, accessed April 2022.
([19]) https://www.iso.org/standard/67545.html, accessed November 2022.
([20]) https://www.iso.org/standard/43757.html, accessed November 2022.

Figure 1: Cloud computing attributes and models



The contents of the cloud computing models and attributes are described in the following sections.

2.2.1. Service Models

The service models consist three main use-cases of cloud infrastructures. Depending on the service model used, the responsibilities for the operation and maintenance of the corresponding computing layers/functions are attributed either to the service provider or the end user. The following computing functions are considered: application, data, runtime, middleware, operating system, virtualisation and hardware.

- **'Software as a service' (SaaS) model.** The user of the service can access applications hosted by a service provider on a network. Users of this service can directly use the desired application. I many cases, this model is associated with a pay-as-you-go policy, and easy access to the application via a browser is often implemented. In this service model, the provider is responsible for maintaining all hosted computing functions: applications, data, runtime, middleware, operating system, virtualisation and hardware. In this model, the provider is responsible for the cybersecurity of the entire service, covering the entire set of hosted components.
- **'Platform as a service' (PaaS) model.** While the user of an application is responsible for its installation, maintenance and data management, the provider delivers all other computing functions, such as runtime, middleware, operating system, virtualisation and hardware. PaaS often delivers software-development tools and various programming languages, allowing users to develop their own software.
- **'Infrastructure as a service' (IaaS) model.** In this model, the service provider delivers resources to the user hardware as a single tenant, often on the basis of a pay-per-use policy. This allows users of the service to minimise high initial hardware investments.

Moreover, service providers are in the position to respond to changing performance requirements in a quick and cost-effective manner.

2.2.2. Deployment Models

Deployment models are the initial choice of cloud users regarding the desired model for sharing, access and ownership of the available computing resources. Deployment models determine the number and nature of tenants using a shared cloud computing resource. Deployment models include the public cloud, private cloud, community cloud and hybrid cloud.

- **Public cloud.** This deployment model – often referred to as an external cloud – is open to a large number of users who can access it via the internet. The access to the cloud resources is managed by the CSP, who also carries the responsibility of maintaining the operation of the service, according to the selected service model.
- **Private cloud**. This deployment model is dedicated to the use of the available cloud computing resources by a single tenant (i.e. by a user, group or institution). This deployment model is a more secure but more expensive option. It can be operated either by the CSP or by any other third party, both on-site and off-site.
- **Community cloud.** This deployment model is dedicated to groups of users/communities that share the same type of requirements (i.e. security, privacy, compliance, policies, etc.). It can be managed by members of the community or any other third party, including the CSP.
- **Hybrid cloud.** This deployment model represents a mix of two or more of the above deployment models. By mixing these deployment models, users might aim at having a more restrictive policy for parts of their infrastructure (e.g. data management), while other parts (e.g. applications) may be used by means of a shared model.
- **Multi-cloud.** Multi-cloud is a cloud environment that integrates various deployment models (just as the hybrid cloud does). The difference with the hybrid cloud is that a mixed cloud also integrates various instances of the same deployment model types into a single logical cloud infrastructure. Issues of compatibility of data and applications are essential in this regard.

Although multi-cloud is considered as a distinct deployment model ([21]) ([22]), within this analysis it is not considered as an additional option, as it is considered to be covered by the abovementioned 'hybrid cloud' option.

2.2.3. Cloud Essential Attributes

Cloud essential attributes represent the means for provisioning the various cloud computing models mentioned above, with the aim to offer users differentiated pricing methods. These attributes apply to each of the above models and provide various means of flexibility for the pricing options of the used services.

- **On-demand self-service (pay-as-you-use).** The user will be in the position to pay per usage, thus reducing costs according to their needs. This pricing model is imposed automatically by the service provider, without any human intervention.
- **Broad network access.** Available cloud services can be offered via the network through (thick) client platforms and through a number of devices, such as laptops, workstations and mobile devices.
- **Resource pooling (multi-tenant).** Multiple users participating in a multi-tenant model can use pooled resources – both physical and virtual – according to their demand.
- **Rapid elasticity.** Available cloud resources can be released in a rapid manner, scaled according to user requests/requirements. Requested resources can be allocated at any time and in any quantity.

([21]) https://www.veritis.com/infographics/hybrid-cloud-vs-multi-cloud-whats-the-difference/, accessed May 2022.
([22]) https://www.cloudflare.com/learning/cloud/multicloud-vs-hybrid-cloud/, accessed May 2022.

- **Measured service.** Cloud services can automatically control resource utilisation by automatically measuring the level of usage (e.g. number of users, amount of processing, network bandwidth). This is done for optimisation purposes and also increases transparency of usage for both users and providers.

2.3. CYBERSECURITY PRODUCTS AND SERVICES RELATED TO CLOUD COMPUTING

Consolidating the information on the cloud computing ecosystem, models and attributes mentioned so far, but also that on other existing information on cloud based service offerings, this section provides a non-exhaustive list of products and services developed to cover cybersecurity requirements and the needs of both supply and demand – from the cloud, in the cloud and for the cloud. This information is presented in a tabular form, breaking down the various cybersecurity services and functions (considered as value-added services on top of those cybersecurity features and services already available or provided by CSPs), in a similar manner as the ECSMAF ([23]) (see Table 4).

Table 4: Various cybersecurity-related value-added services of cloud computing

Value-added service group	Value-added functions	Comments
Cloud software security	Cloud testing tools and services	
	Secure web gateways	
	Virtual machine backup and recovery	
	Cloud application discovery	
	Cloud security posture assessment	
	Cloud management platforms	
	Cloud workload protection	
	Cloud data backup	
	Cloud data protection gateways	
	SaaS	
	Software-defined perimeter	
	Container security	
	Micro-segmentation (software defined segmentation)	
	Secure software development tools and practices	
	Secure access service edge (SASE)	
	Application audit/logging	
	Security orchestration, automation and response	
Data security	Data loss prevention	

([23]) https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf/@@download/fullReport, accessed April 2022.

Value-added service group	Value-added functions	Comments
	Data encryption	
	Disaster recovery as a service	
	(IaaS) container encryption	
	Data audit/logging	
Identity Management	Identity as a service, identity and access management (IAS)	
	User awareness	
	Multi-factor authentication	
	Password policy	
	Key management as a service	
	Identity proofing services	
	Role- and attribute-based access and control	
	Audit/logging	
Operational cybersecurity	Cloud security assessments	
	Security rating service	
	Penetration testing	
	Security information and event management	
	Cyberthreat intelligence and threat hunting	
	Cloud monitors / continuous monitoring	
	Forensics	
	Vulnerability management	
Network security	Virtual private network – network encryption	
	Firewall as a service	
	Demilitarised zone	
	Intrusion detection	
	Network logging	
Cloud hardware security	Secure tokens	
	Hardware availability/ recovery	
	Hardware redundancy	
	Hardware security policy (e.g. testing)	

2.4. CLOUD COMPUTING CYBERSECURITY CHALLENGES

In this section, some security challenges are presented. They constitute a list of cybersecurity concerns that are relevant for the majority of cloud computing stakeholder types (i.e. supply, demand and regulatory bodies). Though not completely overlap-free, these challenges are indicative of the necessity to protect cloud resources on the basis of the assumption that cloud computing is – now and within the foreseeable future – a growing industry and a central facility for the processing of company data. Cybersecurity challenges will be used within the present analysis to capture the concerns of demand, supply and regulatory bodies. The cybersecurity challenges summarised below (in alphabetical order) have been found in various publications related to cybersecurity in cloud computing ([24]) ([25]).

- **Access control.** Access-control challenges emerge through the difficulty of implementing a distributed access-control architecture embracing all distributed access of the – eventually distributed – organisation. The need for asynchronous interactions in a decentralised, distributed environment may pose additional challenges to the technical implementation of a coherent access-control policy.
- **Audit.** Such challenges emerge from the complexity of audit actions aiming to regularly monitor performance and compliance within end-to-end cloud service delivery.
- **Authorisation.** These challenges emerge through errors/misconfigurations in tools for authorisation management and for accessibility of cloud computing resources (i.e. applications, data and network).
- **Availability.** Availability challenges emerge for users and service providers alike. Users need to develop proper strategies ([26]) by properly configuring available cloud resources to obtain application and data availability. On the other hand, availability offered by CSPs has been traditionally limited to local installations of hardware and software resources. With the inclusion of multiple players in the cloud computing infrastructures and supply chain, the achievement of an overall end-to-end availability of services requires large orchestration across a number of organisations and infrastructures.
- **Chain of trust / chain of responsibility.** These are challenges related to the maintenance of coherent account control and accountability control throughout an organisation (i.e. multi-cloud and local processing) in accordance with enterprise policies.
- **Compliance.** These challenges are related to the compliance of cloud services regarding international, national and sectorial requirements, especially regarding the confidentiality and privacy of processed information, but also the governance of services. Depending on geographies of business activities, for a single organisation, multiple compliance requirements may be applicable. This adds an additional level of complexity in mastering compliance challenges.
- **Confidentiality.** Confidentiality challenges emerge in the cloud mainly at the data and network levels. At the data level, confidentiality challenges are related to the disclosure of user data to unauthorised entities, which is mainly an effect of misconfiguration, malfunctioning or discoordination of access rights. At the network level, confidentiality breaches occur when network content is captured by attackers, particularly in multi-tenant environments.
- **Cybersecurity incident management.** These challenges are related to the ability to recognise, analyse and respond to incidents related to various valuable assets offered to users via a cloud service (i.e. applications, data and cloud infrastructure elements).
- **Identification and authentication.** Identification and authentication challenges may emerge through difficulties in the coordination of identity managements in both cloud and internal systems. The introduction of the necessary cloud credentials and their

([24]) https://www.sans.org/white-papers/40225/, accessed May 2022.
([25]) https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8485370/, accessed May 2022.
([26]) https://www.techtarget.com/searchcloudcomputing/feature/3-best-practices-to-achieve-high-availability-in-cloud-computing, accessed May 2022.

management needs to be coherent with the identity management policies applied in the internal IT (see also threat 4 in Section 2.5).

- **Integrity.** Integrity challenges in the cloud environment may emerge regarding data, network and insecure application programming interfaces (APIs). Data integrity challenges exist due to data storage in multiple locations. Network integrity challenges are due to the reuse of IP addresses and the corruption of routing information, both leading to information leakages. At the level of insecure APIs, integrity challenges emerge through violations of access control and authentication, leading to loss of data.
- **Multi-tenancy.** These challenges emerge from multi-tenancy, especially regarding data loss, loss of confidentiality and availability. Such challenges may arise when virtual machines / hypervisors are successfully attacked and the adversary gets access to all available tenants.
- **Network security.** Challenges in network security emerge through the complexity of network connections to be managed in a distributed virtualised environment. In contrast to traditional networks where the entry and exit points are fixed, in cloud a number of dynamically configured network access points need to be managed (e.g. network traffic analysis). Managing the network in a virtualised environment is a far more complex, leaving space for misconfigurations that offer attack surface.
- **Privacy.** Privacy challenges emerge from the necessity to impose an organisation-wide privacy policy in a highly distributed, decentralised and virtualised environment. Diversity of privacy regulations in various geographies adds an additional level of difficulty to master privacy challenges.
- **Storage.** These challenges are related to secure storage, compatibility of data among various platforms, potential data losses, assurance of physical location of stored data in virtual environments (i.e. within the various deployment models).
- **Transparency/visibility/nonrepudiation.** These are challenges stemming from the absence of visibility and transparency in the use of cloud services (applications, data, APIs, etc. – see also threats 10 and 11 in Section 2.5).

2.5. THREAT EXPOSURE OF CLOUD COMPUTING

Cloud infrastructures and cloud services are exposed to a number of cyberthreats. For the current analysis, we will consider the threats assessed through Cloud Security Alliance ([27]) (i.e. the 'Egregious Eleven') ([28]). These threats represent the exposure of cloud computing infrastructure levels and functions. Ideally, existing cybersecurity measures will reduce the attack surface, thus reducing exposure to these threats.

1. **Data breaches ([29]) ([30]).** Through unauthorised access, protected information can be manipulated, deleted, released or stolen. The reasons of such an incident can be manifold, including human error, misconfiguration, malicious attack, negligence, etc. Mostly, a data breach is a consequence of a successful attack from inside or outside the organisation.
2. **Abuse of misconfigurations and inadequate change control.** Errors in the configuration of IT components and/or inadequate management of software is a weakness that can be abused by adversaries. Such weaknesses may be detected by attackers and can be exploited through attacks to related IT components.
3. **Lack of cloud security architecture and strategy.** A smooth transition to cloud based services needs to go hand in hand with a plan for the expansion of the cybersecurity

([27]) https://cloudsecurityalliance.org/artifacts/top-threats-egregious-11-deep-dive, accessed February 2023.
([28]) Some of the egregious eleven are rather weaknesses/vulnerabilities, for example insecure interfaces and APIs. In order to overcome this, for the sake of this analysis some modifications have been made in the titles of these threats. These additions are annotated through italics. Moreover, some of the egregious eleven indicated as 'security issues' are rather 'actions on objectives' (according to the cyber kill chain), for example the nefarious use of cloud services.
([29]) https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach, accessed April 2022.
([30]) https://en.wikipedia.org/wiki/Data_breach, accessed May 2022.

perimeter. Uncoordinated/unplanned adoption of cloud services may otherwise create gaps in cybersecurity protection and thus increase exposure to cyberthreats.

4. **Abuse of insufficient identity, credential, access and key management.** The deployment of cloud services brings new IAM challenges. The introduction of the necessary cloud credentials and their management needs to be coherent with the identity management policies applied in the internal IT. The coordination of both access managements (cloud and internal) has to be planned (see previous threat), configured and managed (see also threat 2). This will reduce exposure to the threat of abuse of (weak) cloud identification and access management functions.

5. **Account hijacking ([31]).** This threat indicates the effect of threat materialisation leading to the take-over of an account (e-mail, computer, web, etc.) by an adversary. An account hijacking is the entry point of a series of abuses and attacks related to confidential user data and available functions. Examples of attacks following an account hijacking are phishing, fraud, exploitation of available functions and abuse of vulnerabilities.

6. **Insider threat ([32]).** An insider threat is an action that may result in an incident, performed by someone or a group of people affiliated with or working for the potential victim. There are several patterns associated with threats from the inside. A well-known insider threat pattern (also known as 'privilege misuse') occurs when outsiders collaborate with internal actors to gain unapproved access to assets. Moreover, insiders may cause harm unintentionally through carelessness or because of a lack of knowledge.

7. **Abuse of insecure interfaces and APIs.** Cloud services are offered to consumers via a series of APIs. Moreover, APIs are used within components of the cloud to enable functions among all layers of the cloud infrastructure. When adversaries gain access to these APIs, they can cause significant damage, to both cloud users and CSPs (e.g. manipulations, eavesdropping, data exfiltration).

8. **Abuse of weak control plane.** Being the main control tool for data management (e.g. data storage, data migration, data duplication), the control plane plays an important role in maintaining data security in the cloud. Given the complexity of configuring cloud services, especially multi-cloud environments, a control plane that lacks coherence with overall security policy and IT architecture may introduce cybersecurity weaknesses. When abused, such weaknesses may lead to massive data losses.

9. **Metastructure and applistructure failures.** For the managing of cloud services through customers, a series of interfaces (user interfaces and APIs) are offered by the CSP. These interfaces offer security and protection functions with the aim to be used by cloud users (i.e. user applications and user control plane). These interfaces reveal important information about security and protective measures to users of the service. Failures, weakness, improper use or misuse of these interfaces may introduce significant risks to the entire infrastructure.

10. **Abuse of limited cloud usage visibility.** Organisations may not be in the position to fully track the use of cloud applications and services, irrespectively of the origin of the user (internal or external). Due to a potentially low visibility of the use of cloud applications, attackers may gain malicious access to available application interfaces and unnoticeably use computing resources, manipulate data and perform data exfiltration.

11. **Abuse and nefarious use of cloud services.** As a result of a successful attack, adversaries may be in the position to gain access to cloud resources and use them for malicious activities requiring significant resources, such as denial-of-service attacks, cryptomining, brute force attacks and massive phishing attacks. Moreover, cloud resources may be used to hide/store malicious content such as malware and stolen data.

([31]) https://www.techopedia.com/definition/24632/account-hijacking, accessed May 2022.
([32]) https://www.enisa.europa.eu/publications/insider-threat, accessed May 2022.

3. DEMOGRAPHICS OF INVOLVED STAKEHOLDER TYPES

In accordance with the identified cloud stakeholder types, the analysis of the cloud security market focuses on cloud security users (i.e. demand) and CSPs. The assessment of the cloud security ecosystem to advance our understanding of the state of play, trends, threats and opportunities for future secure development requires a complete understanding of all the key stakeholder types that may influence these elements, including regulatory bodies intervening in shaping the market and the R & D initiatives on cloud security.

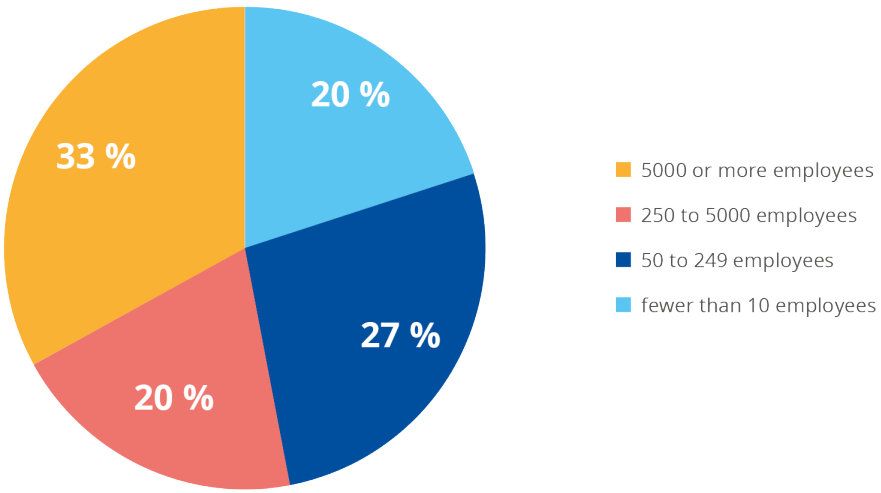
In this chapter, the general characteristics of the surveyed organisations are presented. They mainly consist of information on sizes, geographies covered by the surveyed organisations and the sectors of their activities.

3.1. DEMAND SIDE: THE PROFILE OF CLOUD USERS

To analyse the profile of organisations that have adopted cloud systems, the report sorts the respondents by size (see Figure 2). Large multinational companies (5 000 employees or more) represent 33 % of the sample, followed by medium-sized enterprises (50 to 249 employees, 27 % of the sample). Large enterprises (250 to 5 000 employees) and micro companies (less than 10 employees) each represents 20 % of the sample, making up 40 % of the sample.

As regards the cloud usage of the demand side, our hypothesis is that smaller organisations will make more use of SECaaS providers, while large organisations will have more complex deployment and cloud usage patterns, which in turn will reveal more demand for innovative cybersecurity products and services from this customer segment.

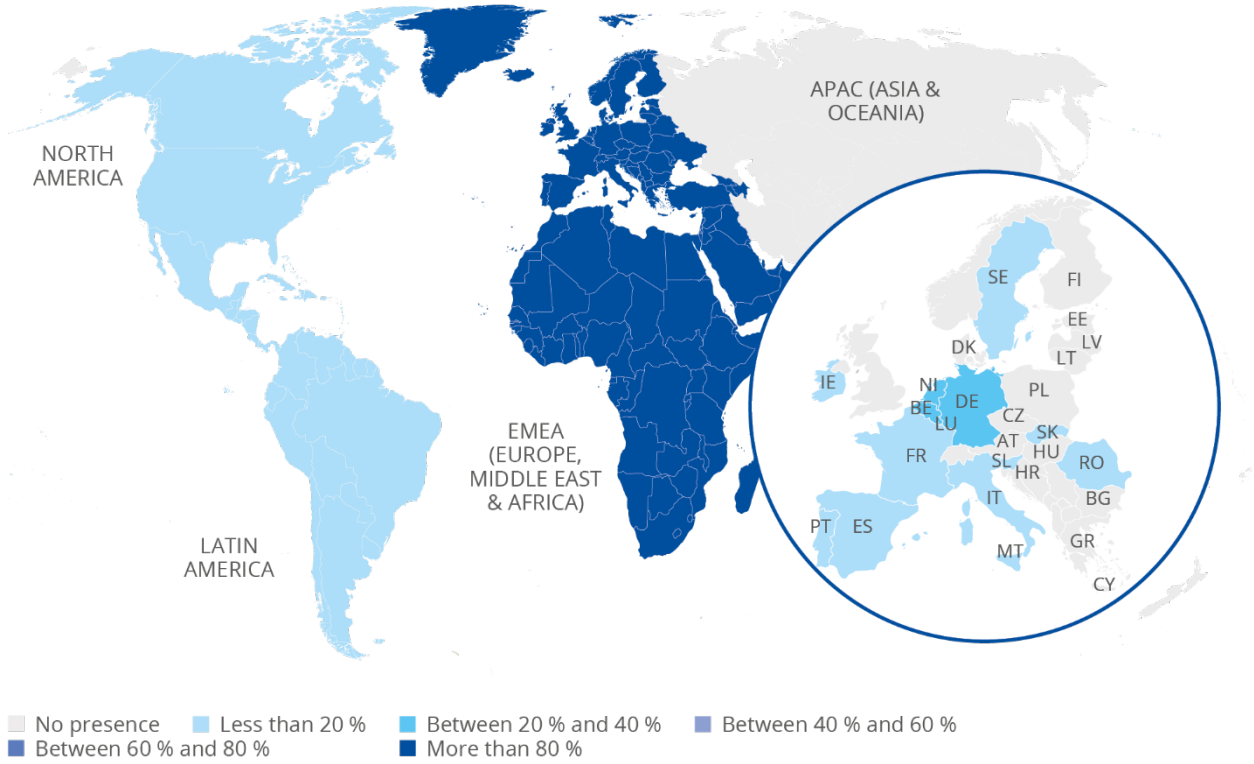
Figure 2: Size of demand-side organisations (based on number of employees)



As we can see in Figure 3, which depicts the geographical distribution of survey responders, most of the respondents are located in the Europe, Middle East and Africa region (the EMEA region), while the remaining 20 % are divided between North and Latin America.

Within the EMEA region, there are no respondents based in Africa. In contrast, several operate in EU Member States (Figure 3), mainly in Belgium, Germany and the Netherlands, followed by the Czechia, Ireland, France, Italy, Portugal, Romania, Slovenia, Slovakia, and Sweden.

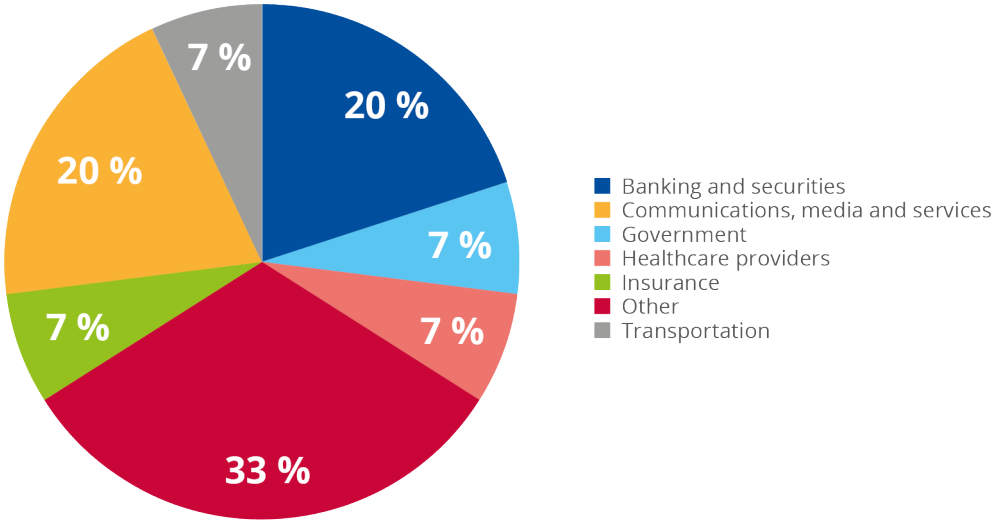
Figure 3: Geographical distribution of surveyed demand-side organisations



As we can see in Figure 4, , which depicts the engagement of the demand-side in various sectors, about 40 % of cloud security users are involved in two industries: in banking and securities and in communications, media and services ([33]) (each representing 20 % of the sample). In addition, the government, healthcare, insurance and transportation industries each represent 7 % of the mapped market. 33 % of user companies operate in other sectors, such as cybersecurity consulting, technology consulting, ICT, food and beverages, and services industries.

([33]) It is worth noting that the communication and media industry embraces Telecommunications. reason why this group is so prominent among survey responders.

Figure 4: Sectors of activity of the surveyed demand-side organisations



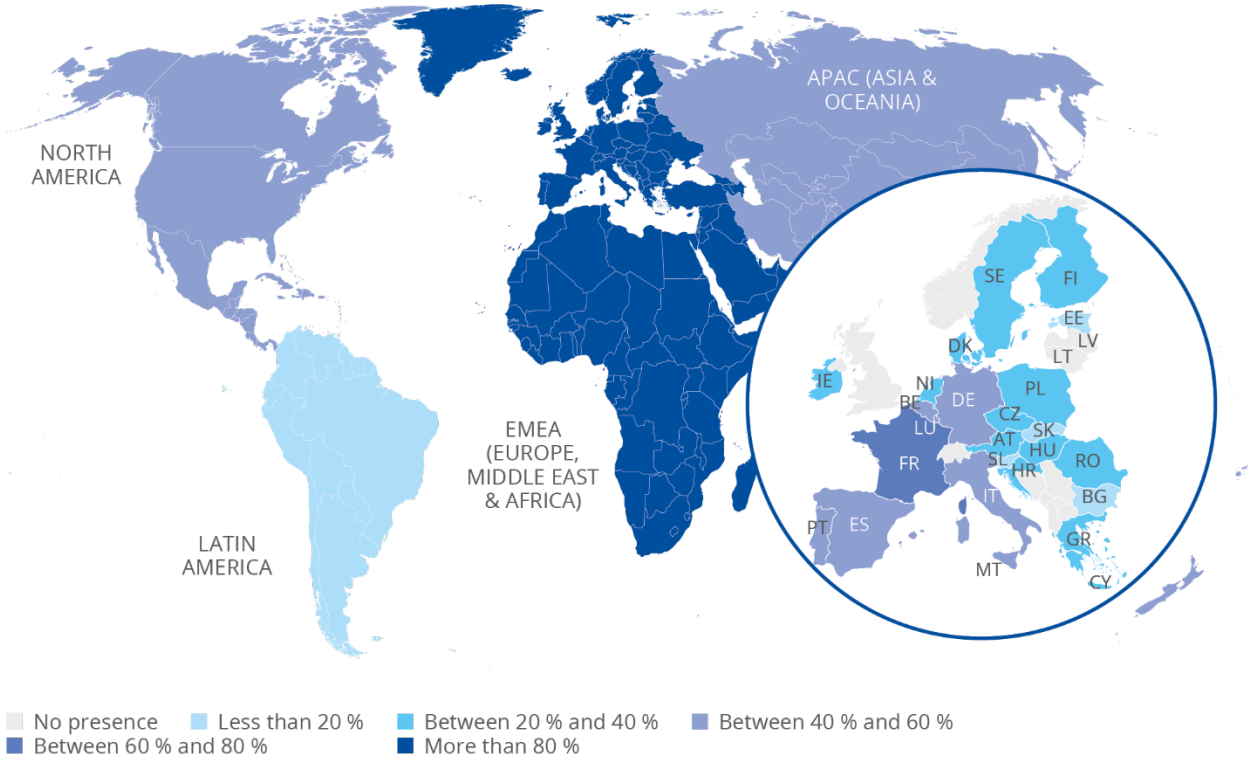
3.2. SUPPLY SIDE: THE PROFILE OF CLOUD PROVIDERS

The cloud-security providers that responded to the survey are mainly multinational companies (5 000 employees or more, 36 % of the total), followed by medium-sized enterprises (50 to 249 employees, 27 %). Large enterprises (250 to 5 000 employees) and micro companies (less than ten employees) comprise 18 % of the sample ([34]). Most of them are located in several geographical areas besides the EU.

More than 80 % have a physical presence in the EMEA region, 60–80 % are also in the Asia–Pacific region (APAC) or North America, and 20–40 % also have an office in Latin America (Figure 5). If we focus only on the EU Member States (Figure 5), 60–80 % of interviewed companies are present in France, while 40–60 % have offices in Germany, Spain, Italy, Portugal and the Netherlands. Between 20 % and 40 % of companies are in Czechia, Denmark, Ireland, Greece, Croatia, Hungary the Netherlands, Austria, Poland, Romania, Finland and Sweden. Less than 20 % also have offices in Bulgaria, Estonia, Cyprus, Slovenia and Slovakia. Figure 5 shows the geographical distribution of the surveyed cloud suppliers.

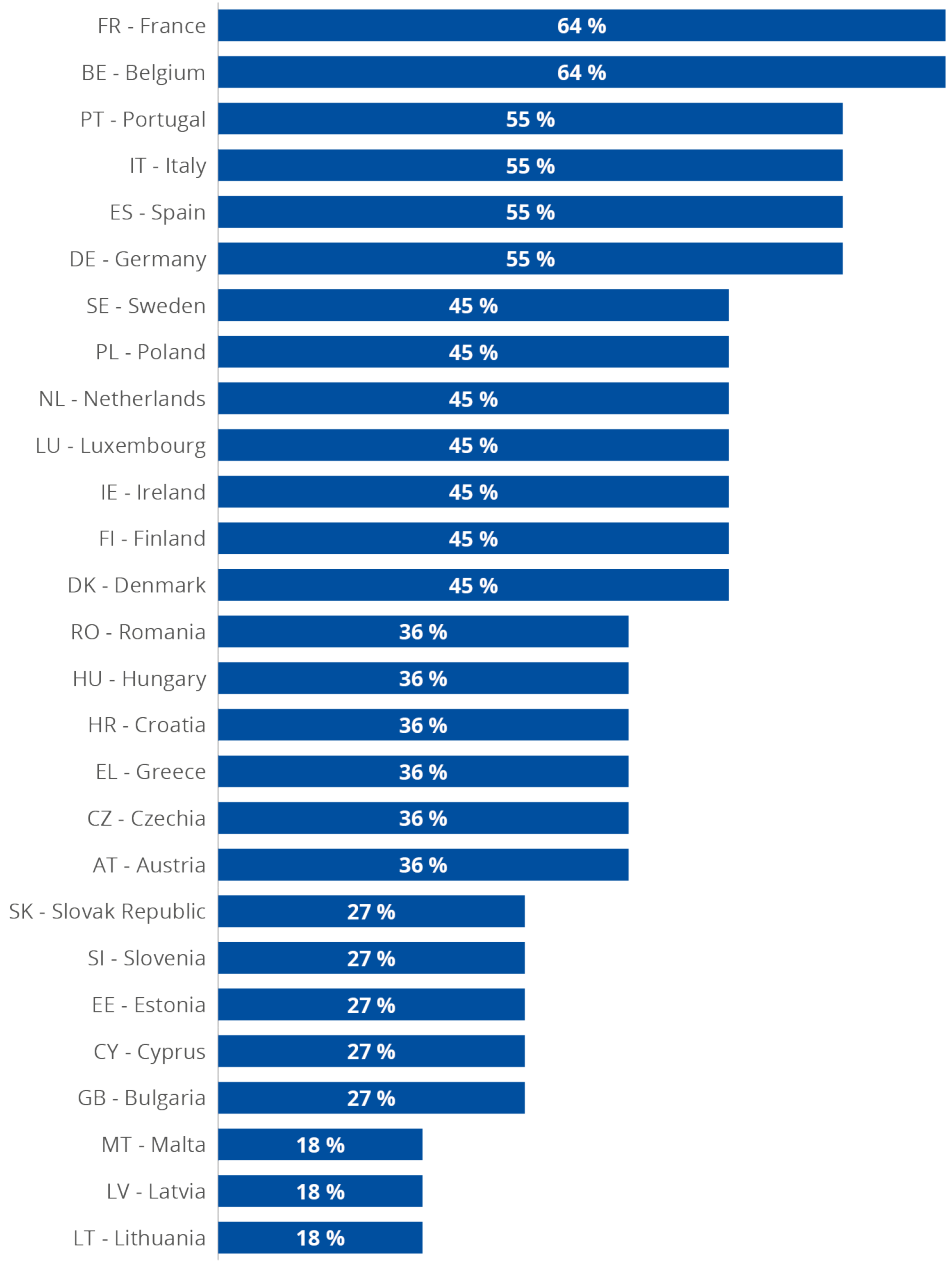
([34]) It should be noted that the definitions of company sizes comply with the EU definitions (see https://single-market-economy.ec.europa.eu/smes/sme-definition_en).

Figure 5: Physical presence of cloud service suppliers



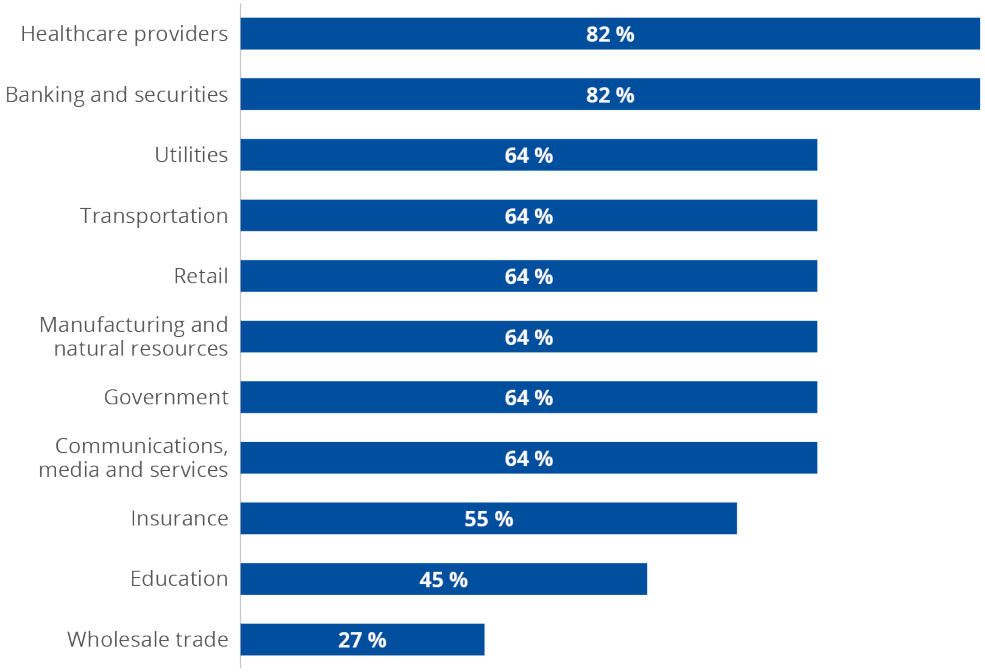
A large percentage (55 %) of the suppliers that responded to the survey only serve EMEA clients; within the EU Member States, suppliers report serving customers mainly in France, Belgium (64 %), Germany, Spain, Italy, and Portugal (55 %) (Figure 6). However, 36 % of suppliers count clients not only in EMEA but also in Latin America, North America and notably APAC; the remaining 9 % focuses only on the EMEA and APAC markets. The collected data about the geographical presence of cloud customers in the EU can be found in Figure 6.

Figure 6: Countries of origin of cloud customers of the surveyed cloud suppliers



Their customers operate in the healthcare and banking and securities industries (82 % of suppliers work for them), followed by utilities, transportation, retail, manufacturing and natural resources, government and communication, media and services (64 % of suppliers), insurance (55 %) and education (45 %). Only (27 %) have customers in the wholesale trade sector (see Figure 7).

Figure 7: Sectors of activity of cloud-supplier customers

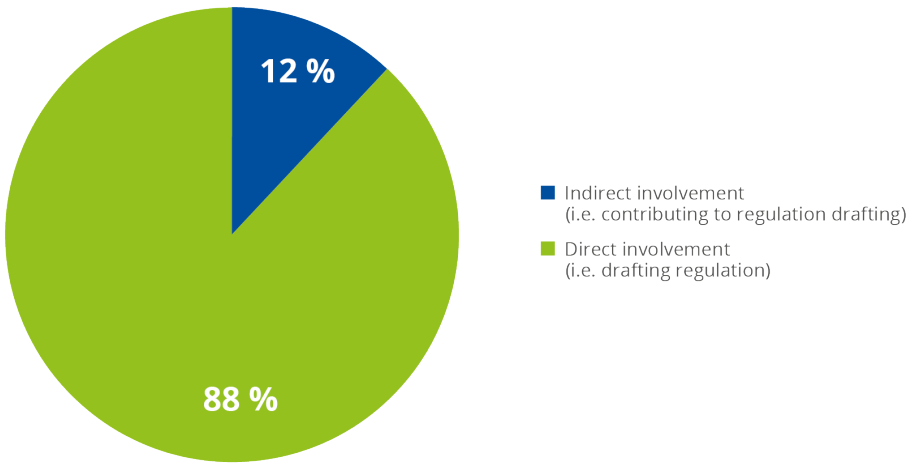


3.3. REGULATORY BODIES

The appreciation of the role regulatory bodies as an important stakeholder type in the cloud ecosystem is an important element of this analysis. It complements the existing analyses by assessing the actors' role and positioning in shaping the context of the cloud security market and its evolution.

Most of the respondents of this survey (88 % of the sample organisations) take a direct approach by actively/directly participating in the development, enforcing and promoting of new regulations in cloud cybersecurity, by paying particular attention to the core sectors of this market (see Figure 8 and Figure 9).

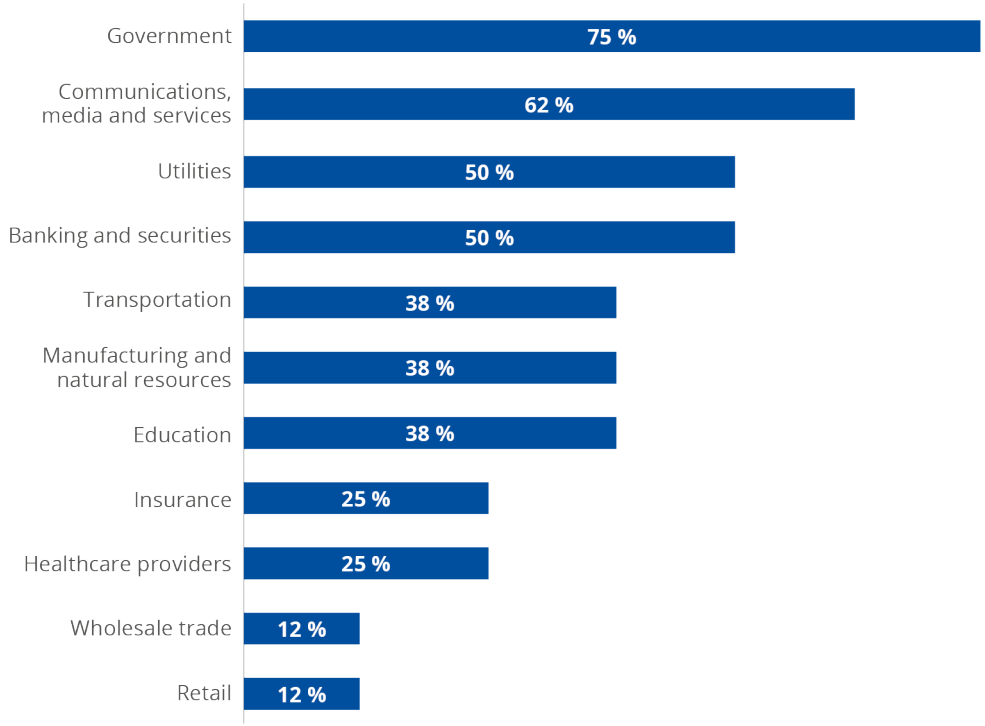
Figure 8: Role of regulatory bodies in cloud-related regulation



Regulatory activities mainly target the public sector, highly regulated industries and critical infrastructure-related industries (see Figure 9). The significant majority of regulators focus on government (targeted by 75 % of the involved organisations); communication, media and

services (62 %); banking and security and utilities (50 %); education, manufacturing and natural resources; transportation (38 %); insurance and healthcare providers (25 %); and lastly retail and wholesale trade (12 %).

Figure 9: Sectors targeted by regulatory activities



3.4. RESEARCH AND DEVELOPMENT ORGANISATIONS

Understanding the focus of investments in R & D is essential to foresee the trajectory of cloud cybersecurity as R & D may shape the market evolution and its potential opportunities and threats. The respondents of the survey state that their R & D initiatives mainly focus on the following sectors: banking and securities; education; government; wholesale trade; transportation and other sectors, such as technology services, aerospace and military implications.

A smaller percentage of initiatives (17 %) focuses on utilities, retail, manufacturing and natural resources; insurance; healthcare providers; and communication, media and services (a sector including telecommunications).

3.5. INTERESTING OBSERVATIONS: CLOUD DEMOGRAPHICS

1. Regulated sectors assessed do not comply to most frequent sectors of cloud supply and demand. Although this may be due to the forward-looking nature of regulation, it might be interesting to investigate how regulators interact with existing cloud use-cases in various sectors and how this shapes their regulatory activities.
2. Data about providers' location and customers' location may suggest implications for policymakers – i.e. capacity to interpret privacy/security regulation, etc.
3. It seems as though R & D is not taking care of sectors that use cloud services the most. This either means that there are limited research needs in those sectors, or that R & D tends to conduct research on special requirements in a sector-independent manner.
4. Stakeholders that have been involved in this survey are engaged in cloud computing cybersecurity in several ways, such as: i) providing security from the cloud (SECaaS business model), ii) providing security for the cloud computing infrastructure e.g. secure

stack components, and iii) providing security in the cloud, for example confidentiality of data in the cloud. We have a well-balanced split between different types and sizes of demand-side stakeholders (users). Smaller demand-side organisations use SECaaS providers, a sub-segment of SaaS model, more frequently. Large organisations have more complex cloud usage patterns, which in turn reveals more demand for innovative cybersecurity products and services from this customer segments.

5. Many CSPs are also cloud security providers (for example, SECaaS is frequently considered as a sub-segment of the SaaS market) and a portion of supply-side stakeholders only provides cybersecurity products and services (see also 'Supply-side enablers' in the definitions of cloud stakeholder types in Section 2.1.1).

4. CLOUD USAGE PATTERNS AND REQUIREMENTS

4.1. CLOUD USAGE PATTERNS

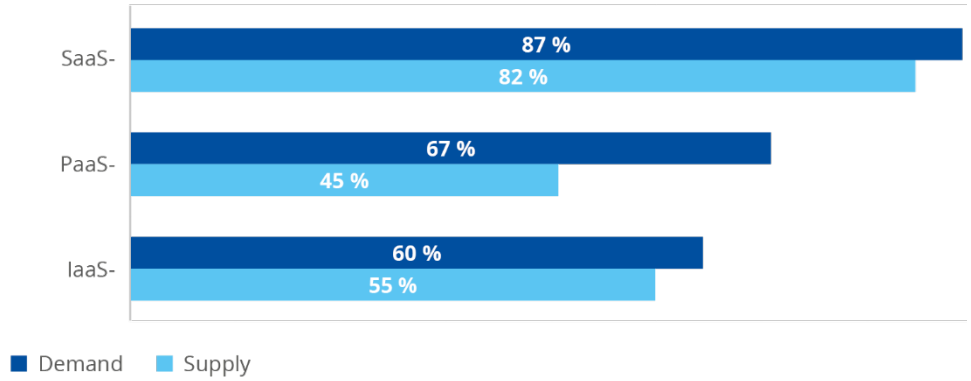
The characterisation of cloud adoption and cloud usage depends on the following elements (see also Section 2.1.1):

- the service model used (IaaS, PaaS, SaaS);
- the deployment model (public cloud, private cloud, multi-cloud, community cloud or hybrid cloud) indicating the preferred access model of the provided services; and
- the cloud attributes indicating the most appropriate/efficient provisioning model to use the cloud services.

In terms of the most widely used cloud service model (see Figure 10), according to both the demand (87 % of sampled companies) and supply (82 %) sides, there is a clear preference for the SaaS cloud service model. However, interestingly, 67 % of customers also use cloud through the use the PaaS model, which is offered by only 45 % of providers. These results may therefore be indicative of a potential market niche, as demand seems to show a preference for the PaaS cloud service model. We also note that there is a higher concentration of suppliers (limited supply) in the PaaS cloud service model segment. On the supply side, PaaS is mainly used by application developers, for which PaaS helps to simplify development and deployment. It was traditionally also the least important service model in terms of revenue, as not every organisation has internal developers.

However, PaaS offerings became more widely adopted with the support of micro-service architectures. Advanced application functionalities, supporting big data, AI, machine-learning capabilities or the IoT may further drive adoption of PaaS services, and this segment could be an opportunity for the emerging cloud providers.

Figure 10: Cloud service model, a comparison of perceptions of supply and demand sides

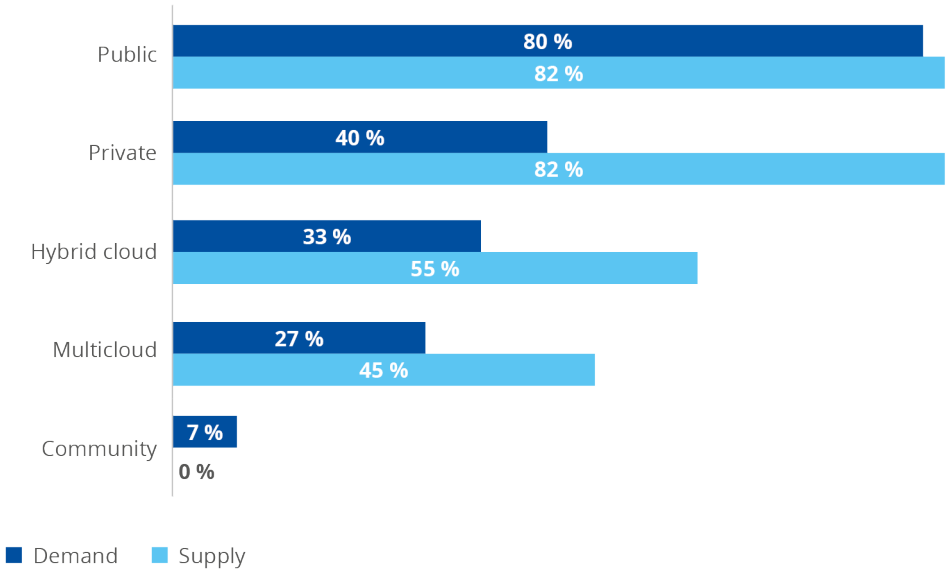


A market imbalance is also clearly visible in terms of deployment models (see Figure 11). Indeed, even though supply and demand are aligned on the preference for public services (used by 80 % of customers and offered by 82 % of sellers), the demand for the other services is much lower than the reported offer, with the highest gap between private cloud demand (40 %) and supply (82 %). This imbalance may suggest that providers are already building capacity

in preparation for a future differentiation in the market or that customers prefer these deployment models in areas not included in the demand sample (e.g. APAC).

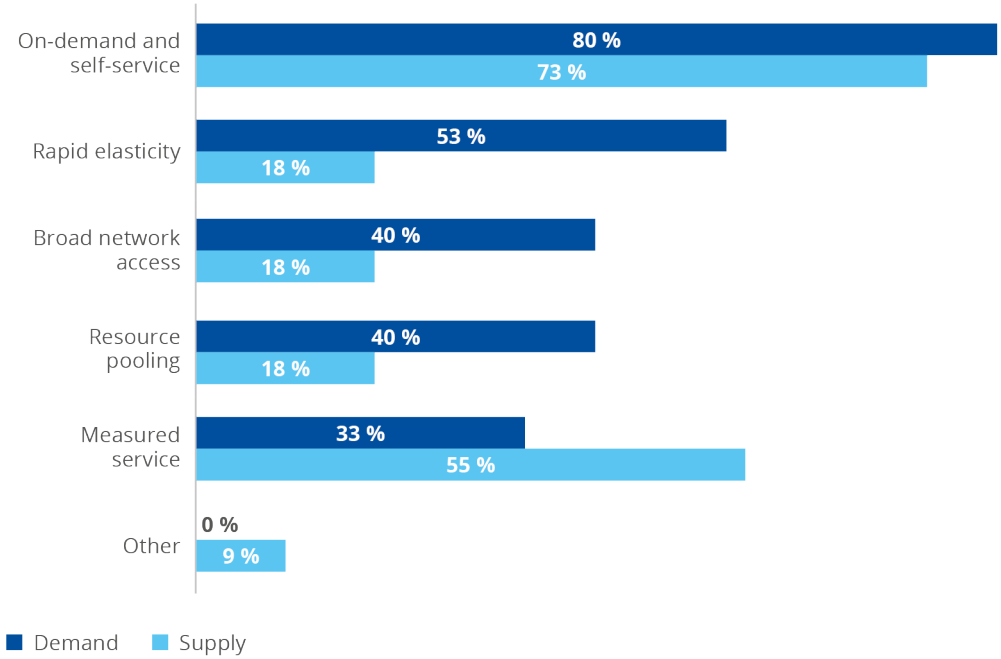
In regards to private cloud services, an adoption of 40 % is in line with the type of demand-side respondents: private cloud services are usually contracted by larger users, which form about 50 % of the respondents of this study (see Figure 2).

Figure 11: Cloud deployment model, a comparison of perceptions of supply and demand



Results on main cloud attributes confirm a somewhat misaligned situation between demand-reported use and supply offering (Figure 12). Indeed, both parties agree that on-demand self-service (pay-as-you-use) is the most critical characteristic of a successful cloud service. However, suppliers' evaluation does not match the relevance that customers given to other attributes, such as rapid elasticity, broad network access and resource pooling. The opposite is true regarding measured service and other attributes, such as specialised compliance services.

Figure 12: Cloud attributes, a comparison of perceptions of supply and demand



In the context of cloud security, the relationship and shared responsibility between customer and CSP is essential. The customer is responsible for securing how they use the cloud services, including proper configuration. This is another reason why customers contract cloud 'enablers' to configure the cloud on their behalf, i.e. by adapting some of the default settings that CSPs provide. While CSPs provide some tools or mechanisms for self-service (e.g. AWS provides many related services, such as GuardDuty ([35]), CloudTrail ([36]), CloudHSM ([37]) and CloudWatch ([38])), this makes things more complex. Also, customers might not be able to manage it by themselves.

This is where the 'dichotomy of control' challenge arises: while customers want more control through self-service and customisation, these can also open new threat vectors.

For example, the on-demand self-service provisioning features enable 'shadow IT' ([39]) ([40]), which may lead to the use of cloud services without the consent of an IT department. The result may be unauthorised use of cloud services, which in turn results in increased risk of malware infections or data exfiltration/loss.

Another challenge related to on-demand self-service provisioning is APIs, which customers use to manage and interact with cloud services, and which can contain vulnerabilities.

Resource pooling in another attribute in high demand, where the risks can outweigh the benefits for the demand side. While the benefits for public cloud providers are clear, security risks for the supply side include the reuse of resources by different tenant applications, placing services that belong to different tenants on the same server or automated processes that handle the allocation and de-allocation of resources at the CSP level. Even in the private cloud, where a

([35]) https://aws.amazon.com/guardduty/, accessed November 2022.
([36]) https://aws.amazon.com/cloudtrail/, accessed November 2022.
([37]) https://aws.amazon.com/cloudhsm/, accessed November 2022.
([38]) https://aws.amazon.com/cloudwatch/, accessed November 2022.
([39]) https://www.everestgrp.com/2019-04-why-shadow-it-is-the-next-looming-cybersecurity-threat-in-the-news-49881.html/, accessed December 2022.
([40]) https://www.crowdstrike.com/cybersecurity-101/cloud-security/shadow-it/, accessed December 2022.

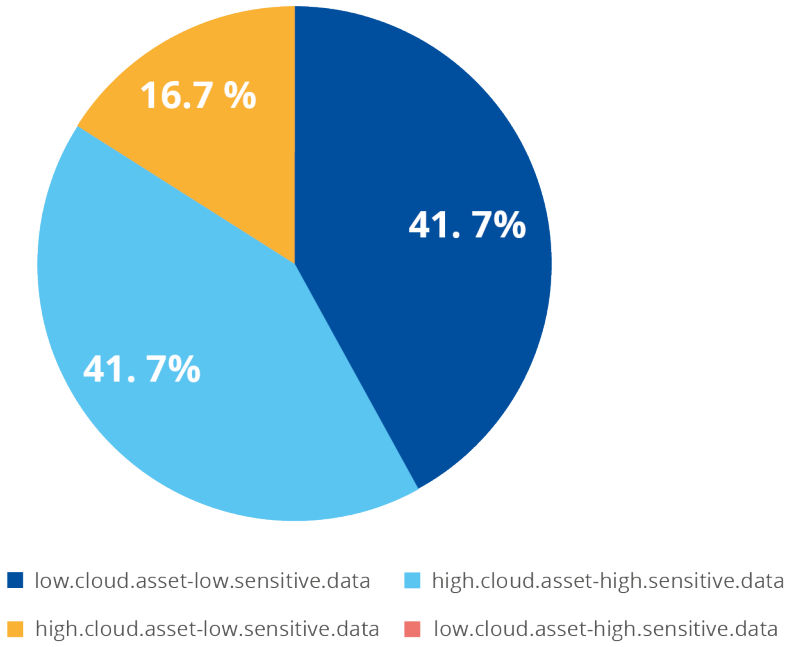
virtual machine could be hosted on any of the servers in the private cloud, there is a risk that the server might host applications and services that belong to different security zones, with different authentication and authorisation needs.

The assessment also focuses on the respondents' perceived relevance of cloud services and the relevance given to cloud cybersecurity regarding the amount of company digital assets and sensitive data stored in the cloud. Indeed, when combining these last two pieces of information (percentage of digital assets in the cloud and percentage of sensitive data stored in cloud services (Figure 13)), the following observations can be made.

- 42 % of companies have a low cloud asset usage and low share of sensitive data storage online;
- Another 42 % of companies have the opposite tendency, high cloud asset usage and high share of sensitive data in the cloud;
- The remaining 17 % uses a high percentage of cloud assets but only stores a small portion of sensitive data online.

These results reveal a divided market, with an almost perfect balance between two opposite approaches (high and low overall cloud usage, in terms of assets and sensitive data) and a smaller share of realities opting for a combination of the two.

Figure 13: Percentages of digital assets stored in the cloud



It is indicative that the ENISA cloud certification proposal ([41]) (EUCS) covers three assurance levels: 'Basic', 'Substantial' and 'High'. These assurance levels can be considered as overlapping with the three demand-side clusters mentioned above. For example, a high assurance level would be appropriate to cover cybersecurity requirements for users who have highly sensitive data stored in the cloud and a heavy usage of cloud services.

4.2. CLOUD CYBERSECURITY REQUIREMENTS

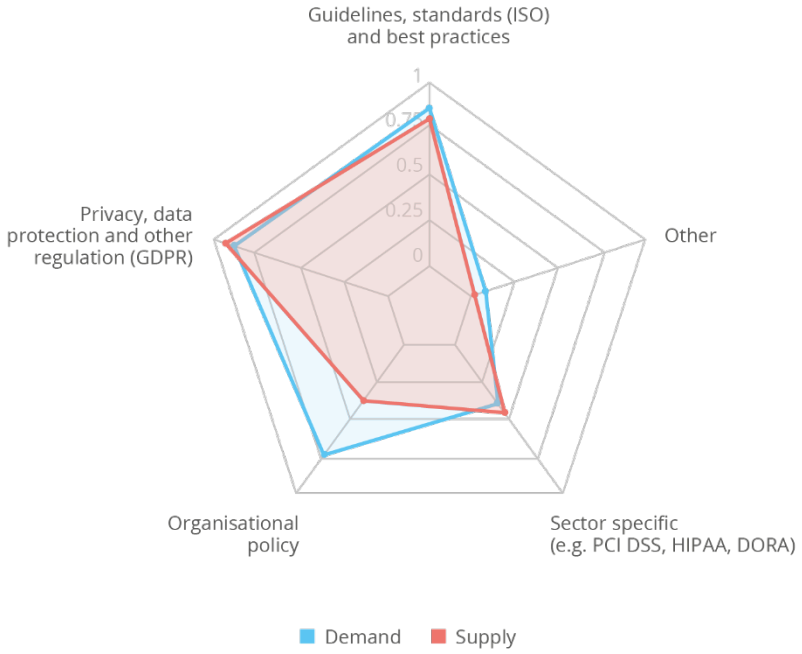
This section covers the most relevant requirements for cloud security services in terms of compliance (general data protection regulation, sector-specific or organisational policies, etc.) and business (availability and resilience, flexibility, business continuity, etc.). They concern three main service aspects: compliance with regulation, guidelines and best practices; business

([41]) https://www.enisa.europa.eu/news/enisa-news/cloud-certification-scheme, accessed November 2022.

requirements; and other relevant requirements (i.e. geopolitical requirements, supply chain or procurement rules, etc.).

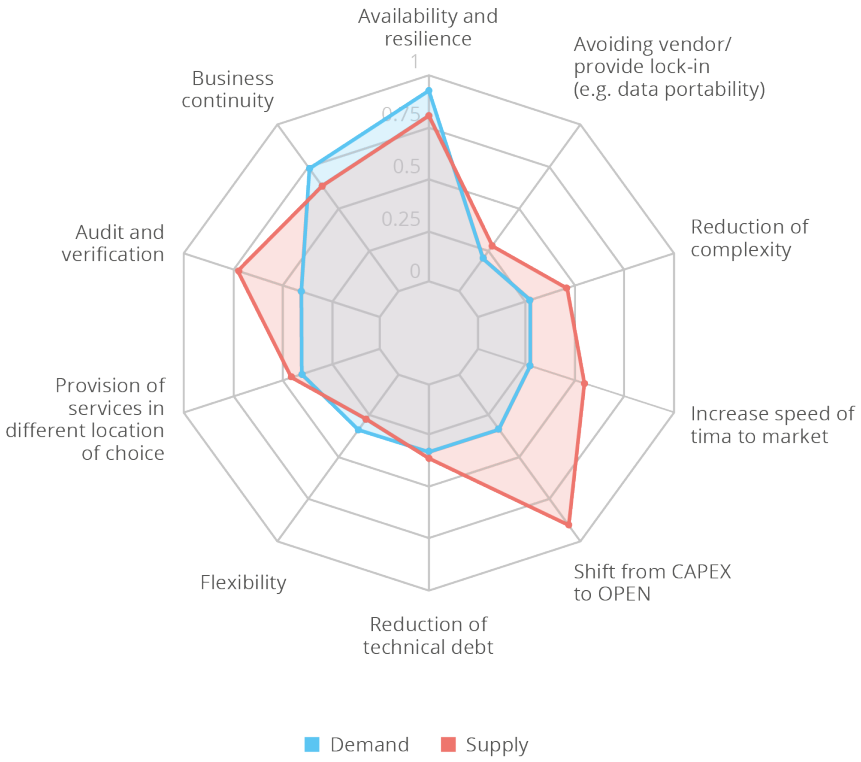
Regarding compliance requirements (Figure 14), the perceptions of the supply and demand sides are almost completely aligned, with a focus on enforcing privacy and data protection, respecting guidelines, standards and best practices (e.g. ISO27001) and achieving compliance with sector-specific standards (e.g. PCI DSS). The users (demand side) also highlight the relevance of organisational policies.

Figure 14: Most relevant compliance requirements, supply vs demand perceptions



On the contrary, the relevance given to the different business requirements (see Figure 15) varies: while demand companies mainly focus on the availability and resilience of services– and, in a lower regard, on business continuity – suppliers assign a higher relevance to the shift from Capital Expenditures (CAPEX) to Operational Expenditures (OPEX). Moreover, they give more importance to requirements such as shorter time to market, the reduction of complexity, audit and verification.

Figure 15: Most relevant business requirements, supply vs demand perceptions

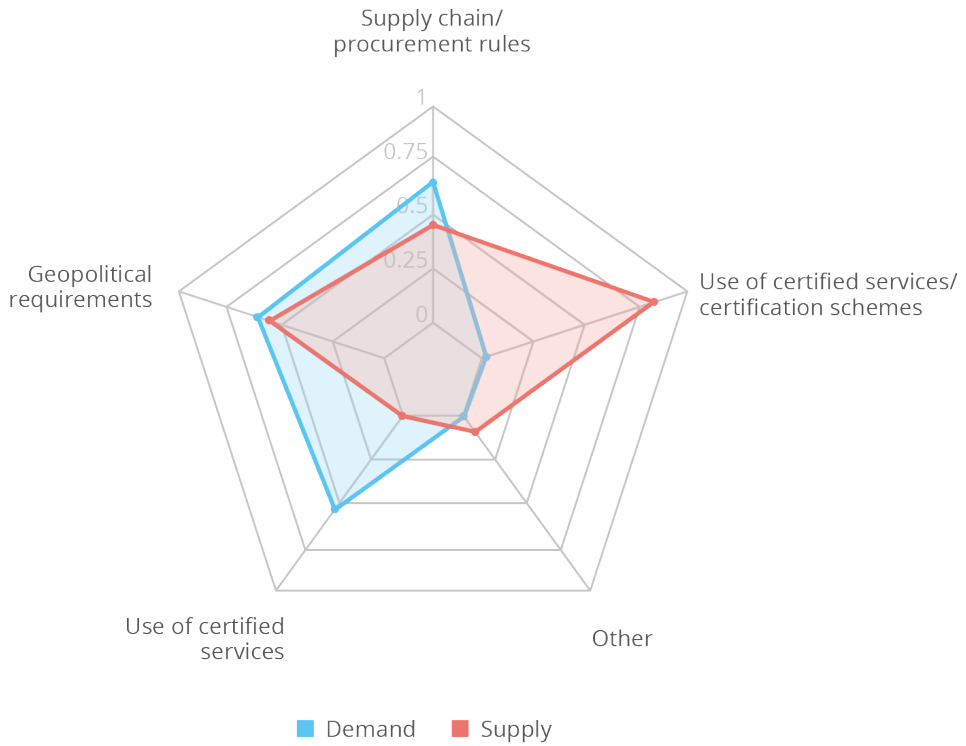


Other requirements (Figure 16) perceived as relevant by cloud service users (demand side) are the use of certified services, compliance with geopolitical requirements and compliance with supply chain/procurement rules. Suppliers agree on the crucial role of geopolitical obligations but focus more on using certified services and certification schemes.

The shift from CAPEX to OPEX has been used for many years as the main argument to move to the cloud, as businesses do not need high up-front investment in IT and can only pay for the computing services they need. when they need them (OPEX model). However, in reality it seems that this is not so important for the demand side, as opposed to the argument used by the supply side.

One explanation could be that transition from one model to another proved to be challenging for organisations with processes in place. While new start-ups do not have this problem, some organisations that rely on the CAPEX model may be reluctant to shift to the cloud and relinquish full control of their IT environment. In PaaS environments, for example, the developer often decides what infrastructure or cloud services to use. This decision is based on performance or technical concerns, without the cost being the main element for this decision. Losing oversight or fear of decentralisation are probably the main reasons behind the small number of demand-side respondents supporting the 'Shift from CAPEX to OPEX' argument.

Figure 16: Other relevant requirements



4.3. INTERESTING OBSERVATIONS: CLOUD USAGE PATTERNS AND REQUIREMENTS

1. Given that half of the demand-side respondents are smaller organisations, they are less likely to use PaaS model; this was also confirmed by the survey. Application developers interested in simplifying development and deployment mainly use PaaS. While PaaS offerings were traditionally the least important service model in terms of revenue, they recently became more widely adopted through the increased use of micro-service architectures. Advanced application functionalities, supporting big data, AI and machine-learning capabilities, or the IoT might further drive the adoption of PaaS services, and this segment could be an opportunity for the emerging cloud providers.
2. Similar conclusions hold for the adoption of private cloud services, where 40 % of the adoption is in line with the type and size of demand-side respondents. Private cloud services are usually contracted by larger users, which form about 50 % of respondents of this study (see Figure 2).
3. The shift from CAPEX to OPEX has been used for many years as the main arguments to move to the cloud, as businesses do not need high up-front investment in IT. They can pay only for the computing services they need, and only when they use them (OPEX model). However, it seems as this is not so important for the demand side, as opposed to the argument used by the supply side.

The next bullet points set new hypotheses for later conclusions about threat perception.

4. Shared responsibility and 'dichotomy of control' in cloud computing usage patterns are challenges where stakeholder perspectives might differ. While the demand side wants more control through self-service and customisation, these options may also open new threat vectors. The on-demand self-service provisioning features, for example, enable 'shadow IT', which is the use of cloud services without an IT department's consent. This can result in unauthorised use of cloud services that in its turn may lead to an increase of malware infections or data exfiltration incidents.

5. Another related challenge is linked to the use of APIs to manage and interact with cloud services. Such APIs may contain vulnerabilities, thus leading to a compromise of these management services. These are a security responsibility of the supply side. This situation may lead to diverging perceptions on related threat exposure between the supply and demand sides.
6. Resource pooling in another attribute in high demand, where risks can outweigh benefits for the demand side. While the benefits for public cloud providers are clear, security risks for the supply side include reuse of resources by different tenant applications, the positioning of services that belong to different tenants on the same server, and automated processes that handle the allocation and de-allocation of resources at CSP level. Even in the private cloud, where a virtual machine could be hosted on any of the servers in the private cloud, there is a risk that the server might host applications and services that belong to different security zones, with different authentication and authorisation needs.

5. THREATS, CHALLENGES AND CAPABILITIES

5.1. CLOUD CYBERSECURITY: THREATS, CHALLENGES AND CAPABILITIES

The cloud has many benefits and the potential to transform many businesses, but it has also introduced new cybersecurity challenges and threats. One of the main differences with 'traditional' cybersecurity is that cloud security is a shared responsibility model, with some challenges and threats originating from its own nature as a cloud, such as we have seen in Section 2.2.

Cybersecurity threats, challenges and capabilities constitute one of the focuses of this market analysis. Cybersecurity threats are the reason why cloud services are being enhanced with cybersecurity features, while cybersecurity challenges emerge from the necessity to reduce threat exposure or the need to integrate cloud security with the existing security policies on the customer side. The ability to implement necessary cybersecurity controls reflects the capability levels on both the demand side and the supply side and is indicative of the level of management of these threats.

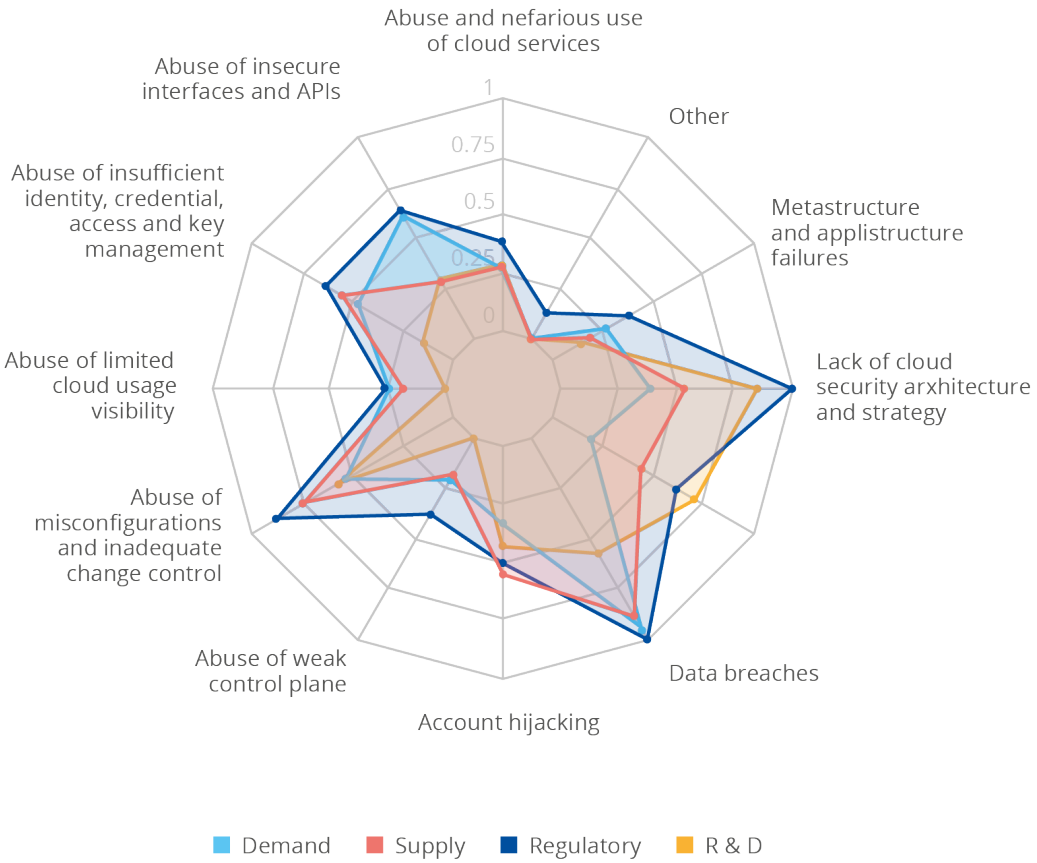
Cloud cybersecurity threats, challenges and capabilities are a common subject of interest for all the stakeholder types involved in this analysis. The information collected in this regard constitutes a very good basis to compare views on threats and challenges, but also to assess the perceived level of threat management.

5.1.1. Cloud Cybersecurity Threats: Multiplicity of Perception within All Stakeholder Types

The stakeholders' perception of the most relevant cybersecurity threats (Figure 17) appears to be generally aligned among the various stakeholder types, with particular attention given to the lack of cloud security architecture and strategy, data breaches and abuse of misconfiguration and inadequate change control. However, some differences are evident, namely the following.

- **Demand and supply.** Their perception is similar, as both dedicate particular attention to data breaches and abuse of misconfiguration and inadequate change control. The only evident difference concerns the abuse of insecure interfaces and APIs, which is not very relevant for suppliers, while customers are far more worried by this threat. Moreover, suppliers focus more on the abuse of misconfigurations and inadequate change control or identity credentials, on the general lack of cloud security architecture and strategy and on account hijacking.
- **Regulatory bodies.** Their perception of all threats is heightened compared to the other actors. The only exceptions are insider threats and account hijacking, by a small margin;
- **R & D.** Contrary to regulatory bodies, research organisations give less importance than other actors do to most cybersecurity threats, especially to abuse of insufficient identity, credential access and key management, abuse of weak control planes and data breaches. The only exception is insider threats, to which R & D bodies give particular importance.

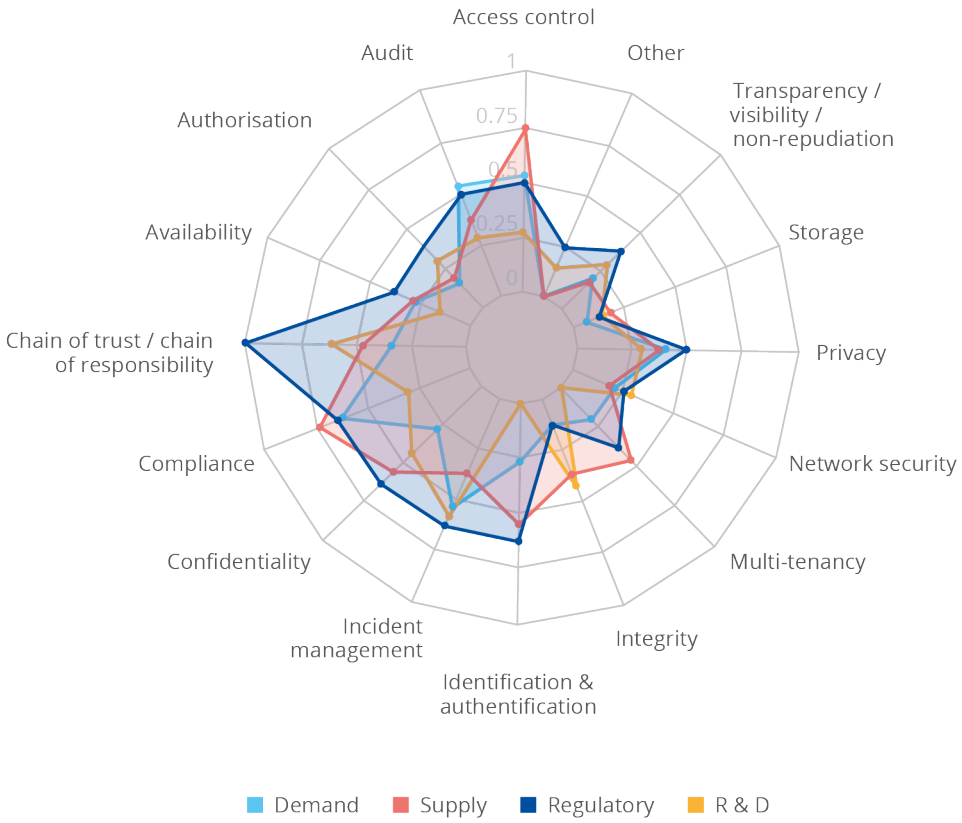
Figure 17: Cloud cybersecurity threats, overview of perceptions from all stakeholder types



5.1.2. Cybersecurity Challenges and Level of Implementations

As mentioned in Section 2.4, cybersecurity challenges capture concerns which relate to both demand and supply regarding the materialisation of a threat. In the current analysis, cybersecurity challenges were used as a basis to firstly capture the concerns of surveyed stakeholders; at the same time, cybersecurity challenges were used as an index to measure implementation efforts to master those challenges. The summary of perceived cybersecurity challenges provides a comprehensive overview of perceived challenges among all involved stakeholder types (see Figure 18).

Figure 18: Cloud cybersecurity challenges, overview of all involved stakeholder types



The fact that the list of cybersecurity challenges resembles cybersecurity control groups has helped survey participants to express the level of implementation within their organisation. Therefore, based on the collected data, the mastering of cybersecurity challenges is considered within this analysis as indicative for the cybersecurity capability/maturity level of surveyed organisations.

This section presents a series of complementary views on threats and challenges: firstly, participating stakeholders were asked about their perceived level of management of cloud cybersecurity threats. Secondly, the implementation status of countermeasures to master the challenges was assessed. Both views are presented in the analysis below.

To reduce threat exposure– and consequently master cybersecurity challenges – organisations are implementing several cybersecurity measures (Figure 19 and Figure 20): incident detection and response, IAM, hardware and data security, cloud-native and application security, cloud infrastructure security and policy enforcement, and antivirus and malware protection. Most companies have already started to introduce all of the measures mentioned above or expect to do so in the next 1–2 years, with the only relevant exception of value-added security services, which 40 % of the supply-side sample companies expect to implement at a later stage (2–5 years); however, the other 60 % of companies have already implemented these services. Overall, these results confirm the active approach both customers and suppliers have adopted in enforcing cloud cybersecurity.

Figure 19: Time range of implementation, demand side

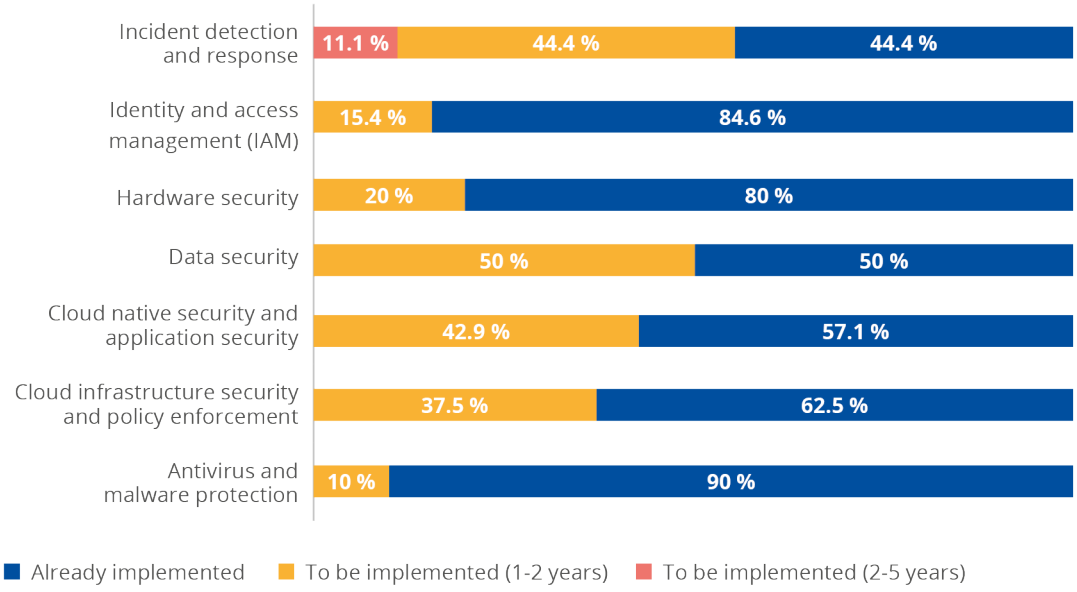
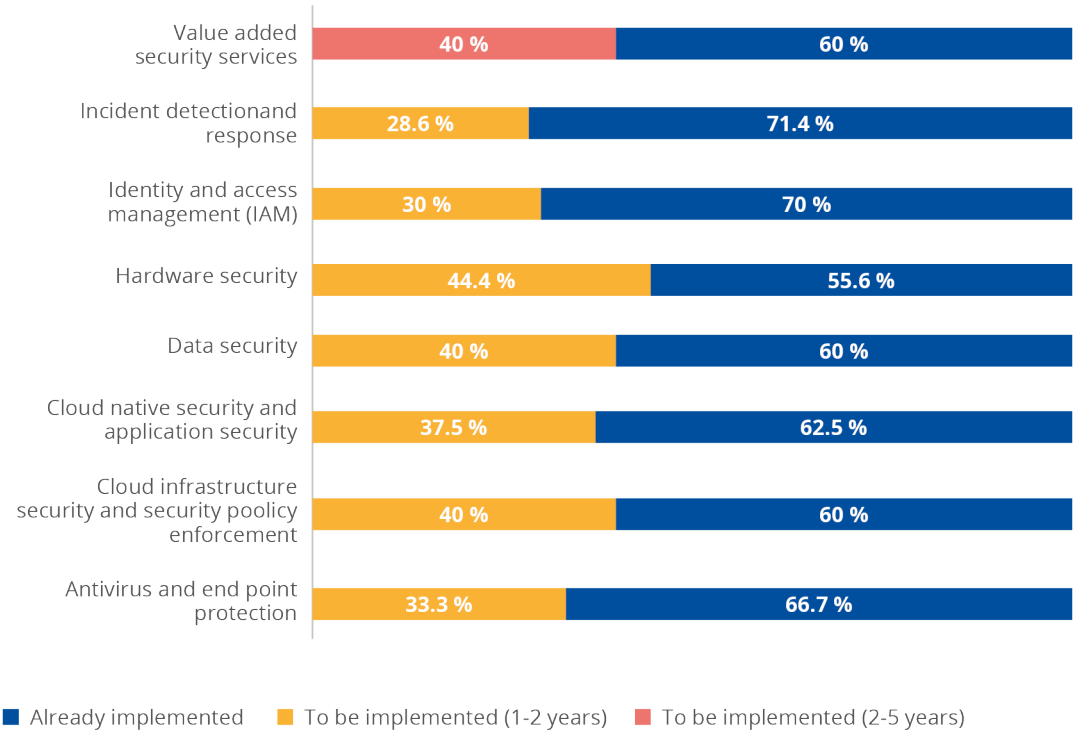


Figure 20: Time range of implementation, supply side



Nonetheless, a lot remains to be done. Figure 21 depicts how the general perception on the demand side is that a significant gap remains between the threats perceived and those effectively managed, especially regarding the abuse of insecure interfaces and APIs and data breaches.

A similar gap is registered when comparing perceived and managed cybersecurity threats for supply companies (Figure 21B): indeed, the lack of incident management is evident, especially concerning data breaches and abuse of misconfigurations and inadequate change control, two of the most worrisome threats for all actors, as previously highlighted. However, on a more

positive note, companies' management of the abuse of insecure interfaces and APIs appears to be particularly effective.

Results for R & D organisations (Figure 21D) are the most encouraging ones. Indeed, the management of the following cybersecurity threats goes beyond the perceived threats:

- abuse of limited cloud usage visibility;
- abuse of insufficient identity, credentials, access and key management;
- abuse of insecure interfaces and APIs;
- meta-structure and appli-structure failures; and
- lack of cloud security architecture and strategy.

However, management of data breaches, account hijacking, abuse of weak control planes, abuse of misconfigurations and inadequate change control and abuse of the nefarious use of cloud services is still lacking.

Focusing on each stakeholder group, regulatory bodies assign the highest level of importance to the chain of trust / chain of responsibility, while suppliers deem access control to be a bigger challenge. Demand-side organisations focus more on audit and access control, and R & D bodies give the most importance to incident management.

Shifting the focus on regulatory bodies (Figure 21C), once again, an important gap between perceived threats and their management is evident, especially concerning the three most relevant cybersecurity menaces (lack of cloud security architecture and strategy, data breaches and abuse of misconfigurations and inadequate change control). Notably, reported perceived and managed threats coincide with the abuse of insecure interfaces and APIs; abuse of insufficient identity, credential access and key management; abuse of weak control planes; insider threats and other (for example, data extraction for future decrypting); these results suggest that current strategies in place are deemed adequate for these threats.

Figure 21: Most relevant managed threats – (from top left to bottom right)
A. Demand side, B. Supply side, C. Regulatory bodies side, D. R & D side

5.2. INCIDENTS AND VULNERABILITIES

In this section we provide an overview of the most impactful security incidents experienced lately (in the last 12 months) by the cloud cybersecurity market and the cloud infrastructure vulnerabilities registered, analysing the type and level of consequences they caused and the relationship with the regulatory bodies in their management.

Before going into the analysis of the survey result, it is important to provide some statistics related to cloud incidents and cloud vulnerabilities. The statistics below have been assessed via available open-source publications.

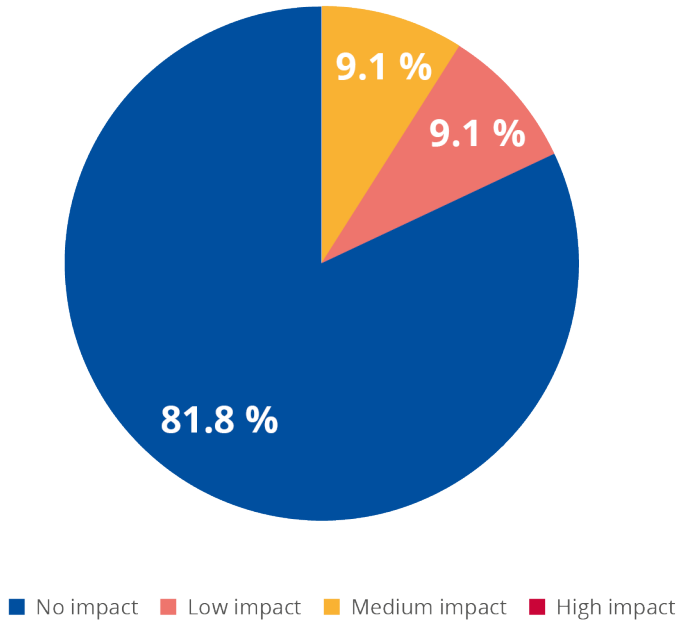
- **Number of cloud incidents in 2022.** With some 53 % of cloud users suffering an incident (attack) between 2020 and 2022 ([42]), there is a significant increase in the detection of incidents, most commonly caused by phishing (73 %), account compromise (31 %), ransomware and targeted attacks (29 %) and accidental data leakage (25 %). Remarkably, incidents caused by these threats have doubled within this period. Consequently, the percentage of targeted users is expected to continue growing over time.

([42]) https://www.netwrix.com/download/collaterals/Netwrix_Cloud_Data_Security_Report_2022.pdf, accessed November 2022.

- **Number of cloud vulnerabilities in 2022.** Though the total number of cloud vulnerabilities is difficult to assess, vulnerability statistics from a single cloud provider indicate that around 50 vulnerabilities were detected in 2021, around 13 % of them being critical ([43]). By extrapolating this number to other major CSPs by analogy, one can easily equate this to around a few hundred vulnerabilities on a yearly basis.

The **impact of incidents** reported by demand-side organisations (Figure 22) highlights that **the majority of reported cybersecurity incidents had low (73 %) or no impact (13 %)**. Only a **small portion (13 %)** had a **medium impact**, and none caused high-level consequences. These results suggest that even though great attention is devoted towards cybersecurity threats and an overall sense that more could be done to reduce threat exposure, measures in place are quite effective, at least in preventing incidents leading to serious consequences.

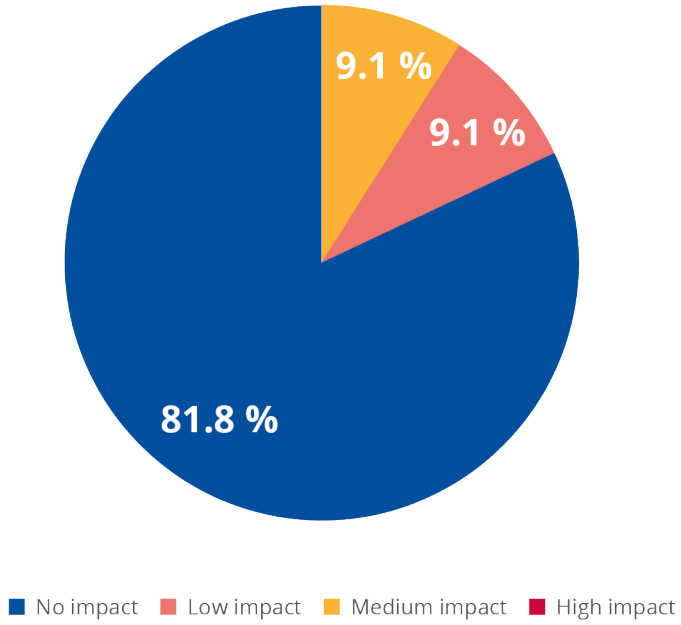
Figure 22: Demand-side experience with impactful incidents



When looking at the suppliers (Figure 23), the results confirm the effectiveness of the defensive measures in place, which appear to be even more effective than in demand-side companies. Indeed, in this case, the majority of causalities had no impact at all on the company (82 %), while only a small portion had a low (9 %) or medium impact (9 %).

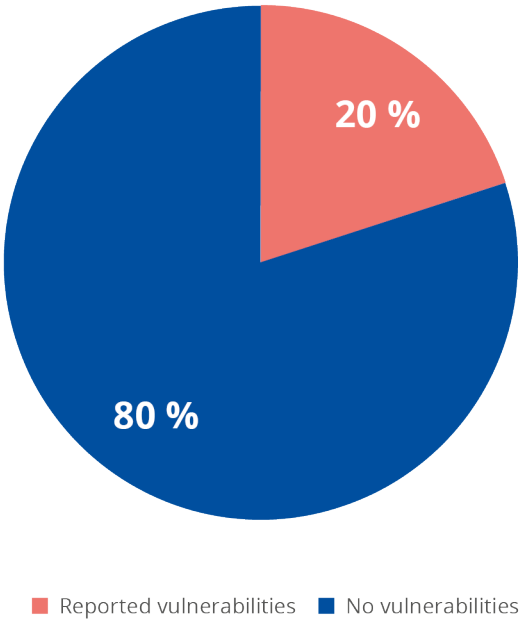
([43]) https://www.beyondtrust.com/resources/whitepapers/microsoft-vulnerability-report, accessed November 2022.

Figure 23: Impact of incidents, supply side



On the other hand, the demand side reported a low number of vulnerabilities communicated by CSPs (see Figure 24). Given the number of cloud vulnerabilities registered in 2021 and the high percentage of incidents (i.e. abused vulnerabilities), it is rather unlikely that used cloud services were not affected by vulnerabilities.

Figure 24: Percentage of the demand -side that received vulnerability report



5.3. INTERESTING OBSERVATIONS: THREATS, CHALLENGES AND CAPABILITIES

1. Insider threats are also the most difficult threats to address. It is common concern for both the demand-side and supply-side perspectives, but modelling of these threats (that include human factors) is very difficult.

2. Lack of visibility and transparency of cyberthreat management seems to be a topic that needs to be considered, as it influences market adoption.
3. Differences in threat perception reveal some doubts about 'shared model responsibility' in cloud security: the supply-side might minimise the probability of vulnerabilities in their APIs, while the demand side would do the same for their misconfigurations.
4. Regulatory stakeholders give more importance to the chain of trust, as they take a more holistic approach and deal with IT supply-chain security in general.
5. Incident management and audit scores are low on the supply side, which can be explained by the fact that many CSPs are reluctant to share logs and give access to their cloud for incident-management services.
6. When seen purely from a cybersecurity perspective, it seems that multi-tenancy is mainly beneficial for the supply side, as it brings risks for the demand side. However, according to the data collected, the perception is different.
7. Segments of cloud-native, application and cloud infrastructure cybersecurity and policy enforcement show a high level of adoption, which is indicative of good cybersecurity awareness from demand-side stakeholders.
8. Suppliers feel like they are 'in control' of API vulnerabilities, while considering 'customer-side' threats, such as misconfigurations, as a source of higher risk.
9. Given the relatively low level of vulnerability information communicated to the demand side, it seems necessary to raise awareness and intensify notification on vulnerabilities both via the cloud services and the applications used by all users of the cloud services. Eventually, Service Level Agreements (SLAs) would need to be checked and potentially updated to include vulnerability notifications to users of the service. New or emerging EU regulations see vulnerability management as a central part of incident notification; such SLA updates will hence be mandatory for a variety of products and services, especially the ones used in critical sectors. If such a change is not made, it could turn into a barrier for market adoption.

6. ROLE OF REGULATION AND CERTIFICATION

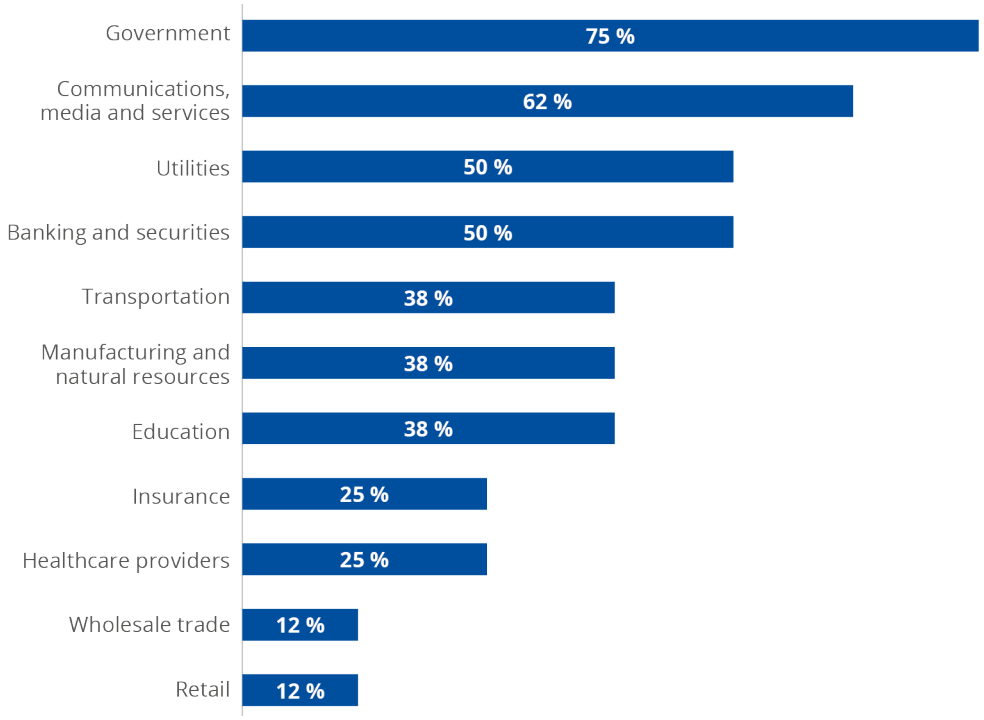
The inclusion of regulatory bodies as a stakeholder type in this analysis has provided a complementary perspective with regard to their scope, the regulatory instruments used and the plans for their implementation. This section outlines the regulatory bodies' influence on the cloud cybersecurity market. Use of standards and certification constitutes the main instrument for the fulfilment of cybersecurity requirements. As regards the use of certification, the survey addresses intentions for the introduction of the EUCS. In addition, an analysis of the plan developed by various regulatory bodies for its implementation (degree of penetration, timeline of introduction, funds allocated) has been performed. This includes the EUCS' impact on the reduction of cybersecurity threats.

6.1. TYPES OF REGULATORY ACTIVITIES IN CLOUD CYBERSECURITY

The regulatory supervision of the participated regulatory bodies concentrates on the following core sectors: government (targeted by 75 % of the involved organisations), communications, media and services (62 %), banking and security, utilities (50 %), education, manufacturing and natural resources, transportation (38 %), insurance, healthcare providers (25 %), retail and wholesale trade (12 %) (see Figure 25).

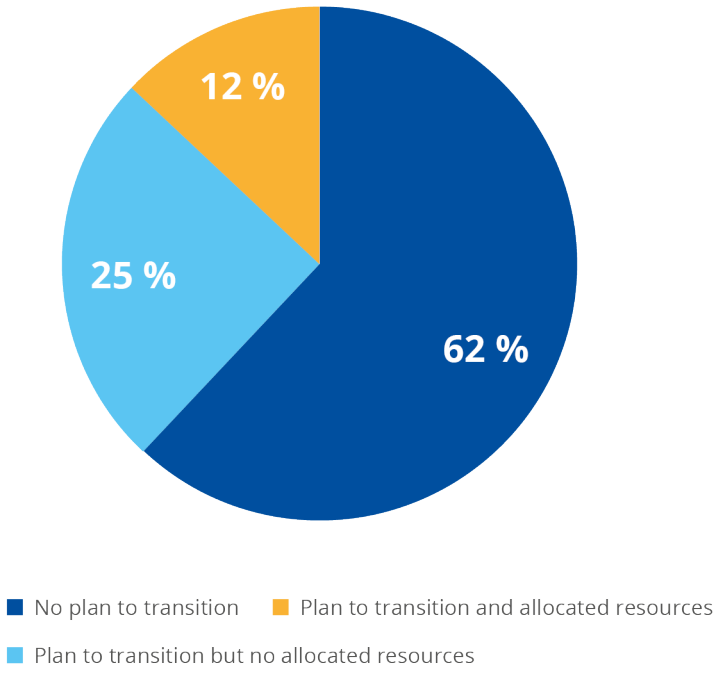
To quote one of the survey's participants, 'a cloud certification scheme is necessary to support a secure digital single market, the digitalisation and competitiveness of European businesses and the security of our citizens, businesses, and public administrations'.

Figure 25: Sectors falling into regulatory supervision



However, this does not imply that the adoption of the EUCS will happen in the near future (Figure 26). Indeed, 62 % of the interviewed regulatory bodies have no plan to transition to this framework, and 25 % plan to transition, but likely not in the immediate future, as no resources have been allocated to this intent. Only 12 % of the organisations have planned the transition and allocated funds for it.

Figure 26: EUCS, an important emerging regulatory instrument

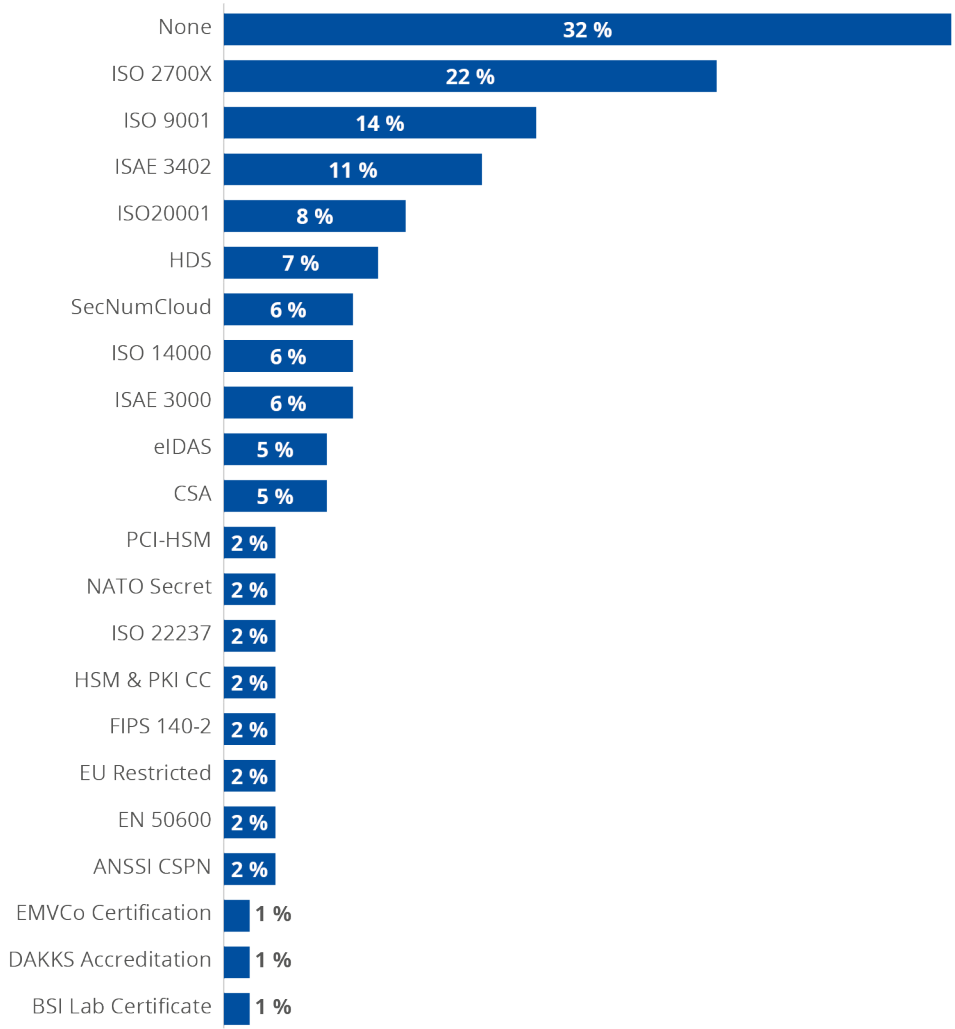


6.2. THE ROLE OF CERTIFICATION IN CLOUD CYBERSECURITY

The scope of this section is to investigate certifications' relevance for cloud cybersecurity providers and the relative instruments used by regulatory bodies. The role of certification has been assessed for the supply side, demand-side and bodies involved in regulation stakeholder types. The details of the analysis are presented in the discussion below.

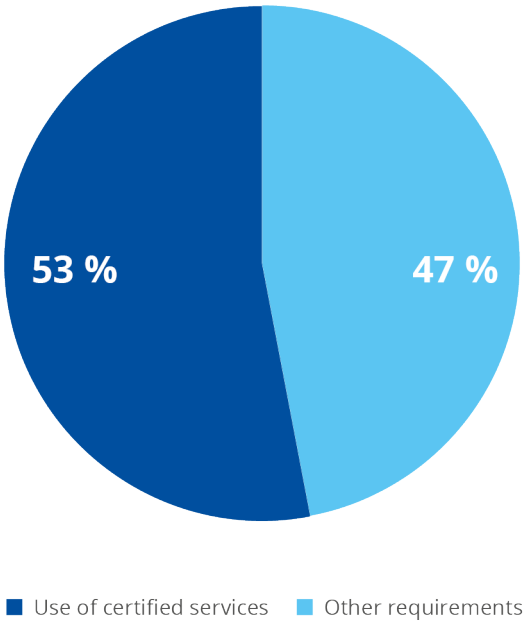
Supply side. Suppliers of cloud services were surveyed about the certifications they use for their offerings, including about their service and deployment models and cloud attributes. The certifications used cover both cybersecurity properties, but also process security and quality. Figure 27 shows the used certifications and standards.

Figure 27: Supply-side certification (standards, attestations, schemes, etc.)



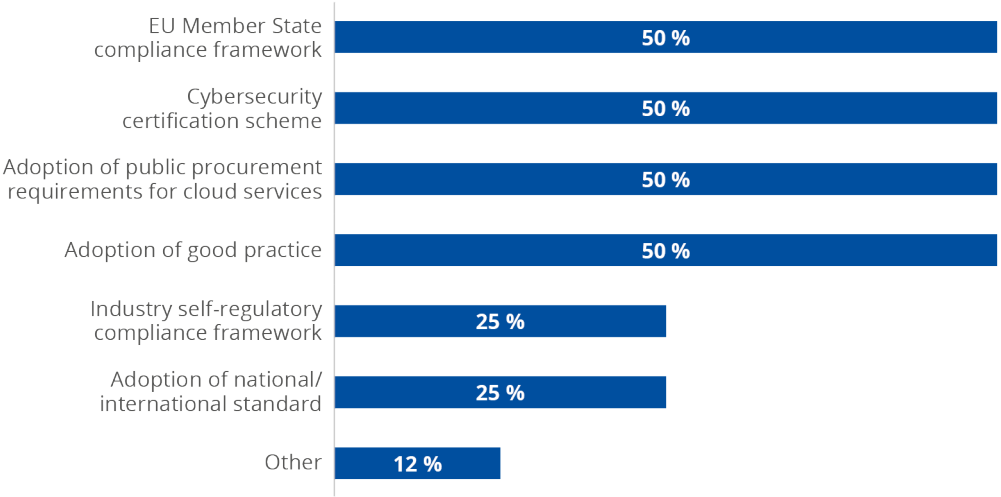
Demand side. Cloud users were surveyed to assess their requirements in terms of certification and standardisation and expectations regarding the used services. These requirements meet both their compliance and cybersecurity protection needs. The assessed requirements reflect the generic intention/desire to use certified services, rather than mentioning specific ones. Figure 28 shows the percentage of demand-side organisations that use certified cloud services.

Figure 28: Demand-side certification requirements



Regulatory bodies. Bodies involved in regulation consider cloud certification as an important element for the implementation of cybersecurity protection, coming second among all available regulatory instruments. It should be mentioned, however, that cybersecurity certification is part of the EU Member States' cloud compliance framework ([44]). Hence, cloud certification has a potentially higher ranking, as indicated in Figure 31. Taking into consideration the plan to transition to the EUCS, cloud certification seems to be one of the most important emerging methods within EU regulatory bodies to achieve proper cybersecurity protection in the cloud ecosystem (see Figure 26 and Figure 29).

Figure 29: Regulatory instruments



([44]) https://digital-strategy.ec.europa.eu/en/policies/cloud-computing, accessed November 2022.

6.3. INTERESTING OBSERVATIONS: ROLE OF REGULATION AND CERTIFICATION

1. It is worth noting that a significant number of suppliers still do not use any certifications for the offered services. It seems that the higher risk appetite of the demand side can be explained either by the lack of cybersecurity awareness or by a higher prioritisation of cost/performance issues. Nonetheless, the desire of the demand side to use certified services (ca. 50 %) does not fully resonate with the supplier side, when considering the level of supported certifications of offered cloud services.
2. Although the EUCS seems to have become an important EU instrument to achieve better cybersecurity protection levels, it has not been sufficiently envisaged yet within implementations in available cloud offerings. This is expected to change when regulators make their transition to the EUCS in the future (see Figure 26).

.

7. CLOUD CYBERSECURITY MARKET TRENDS

7.1. CLOUD CYBERSECURITY MARKET EVOLUTION

Analysis of the collected evidence indicates that cloud cybersecurity is an expanding market, and most market actors agree that significant market gaps remain. According to demand-side and supply-side companies and R & D organisations, these uncovered areas mainly concern three cybersecurity areas/issues: i) privacy and data protection, ii) security-enhancing technologies and regulation, and iii) the absence of a unified certification method.

The state of cloud cybersecurity and the quality of cloud regulation are perceived as the two most impactful aspects for market development. This can be attested by the preference of survey participants for multi-cloud cybersecurity strategies and SaaS solutions. In both cases, regulatory activities and orchestrated cybersecurity controls are especially crucial. Survey participants have indicated that deficiencies in this regard may significantly increase exposure to cyberwarfare and cyberterrorism threats. Although the emergence of these threats has also been assessed in this year's *ENISA Threat Landscape* ([45]), these survey findings are mainly motivated by the impressions of cloud stakeholders regarding current geopolitical developments.

Demand-side companies are also particularly attentive to signs of instability in the market, paying particular attention to the monopolistic position assumed by hyperscalers. As a matter of fact, even though the drive to innovate in the field of cybersecurity is lacking momentum, solutions and cybersecurity controls are gradually being adopted on an individual level. Concerning cybersecurity drivers, the focus of customers and suppliers is on building a resilient, trustworthy and highly available cloud environment, incorporating new elements such as deep integration, IoT, zero-trust security, cloud automation, quantum computing, 5G and the adoption of AI in cloud services.

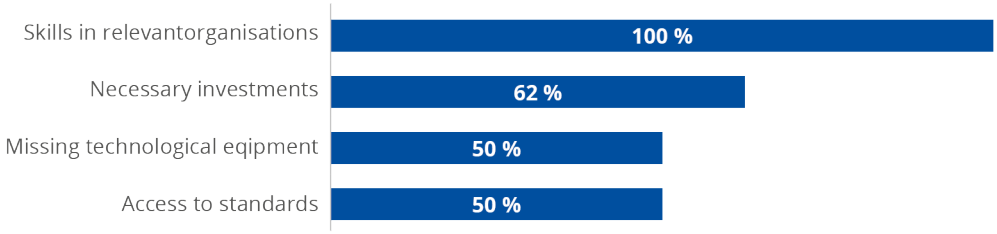
7.2. CLOUD CYBERSECURITY DRIVERS AND BARRIERS

The aim of this section is to investigate the technological and business drivers for the cloud cybersecurity ecosystem and the relative barriers encountered. In particular, the analysis shifts beyond cloud cybersecurity-market stakeholder types, investigating the drivers and barriers of regulatory bodies and R & D initiatives in promoting regulatory compliance and research uptake. In addition, we analyse the main instruments for research and innovation funding and the implementation issues (such as lack of skills) encountered in R & D projects.

The technological barriers reported by regulatory bodies (Figure 30) mainly concern four aspects: access to standards, missing technological equipment (both encountered by 50 % of interviewed organisations), lack of technological investments (62 % of organisations) and lack of skills. The latter emerges as the most relevant barrier, as all organisations face it.

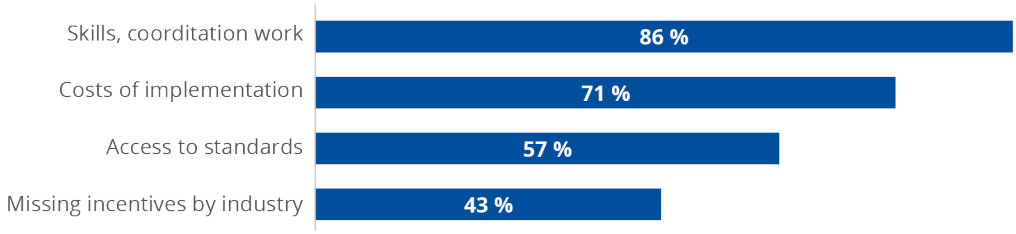
([45]) https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022, accessed December 2022.

Figure 30: Technological barriers according to regulatory bodies



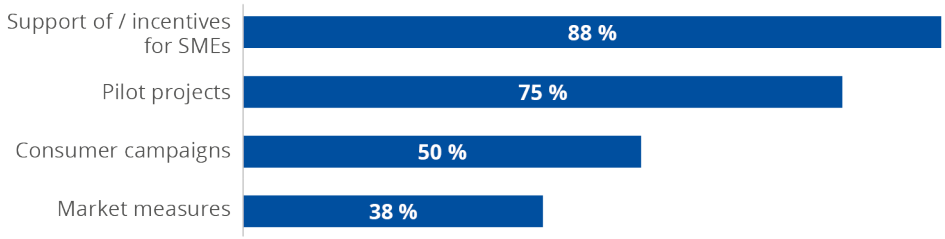
Concerning regulatory barriers (Figure 31), the main limitations registered are a lack of incentives on the industry side (reported by 43 % of organisations), the already mentioned low access to standards (57 %), the high implementation costs (71 %) and the lack of skills (86 %). Analysing these answers and comparing them against the ones concerning technological barriers, it is possible to conclude that the most critical barriers encountered by regulators are the lack of resources, the low access to generalised standards and the lack of skills in relevant organisations, with a significant impact on the ecosystem of cloud cybersecurity.

Figure 31: Main regulatory compliance barriers according to regulatory bodies



Shifting our focus from barriers to drivers for promoting regulatory compliance (Figure 32), according to regulatory bodies, the most relevant ones are market measures (for 38 % of interviewed organisations), consumer campaigns (50 %), pilot projects (75 %) and support for SMEs, namely in the form of monetary incentives (88 %).

Figure 32: Drivers for promoting regulatory compliance according to Regulatory Bodies

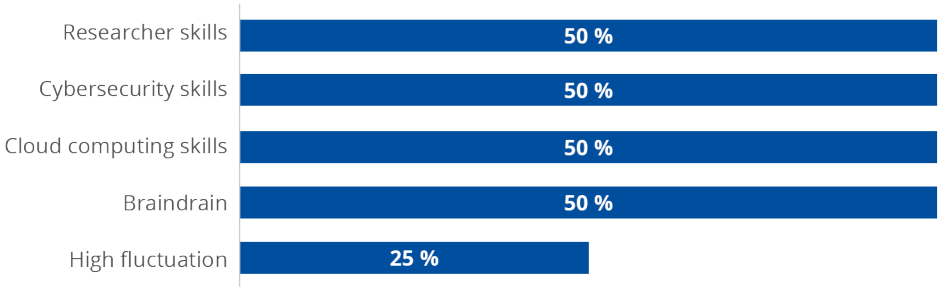


Regarding R & D organisations, the surveyed organisations highlighted three main technological barriers: lack of technological equipment (20 % of R & D bodies); missing access to product IPRs (40 %) and missing access to standards (40 %) (see also Figure 33).

Figure 33: Technological barriers encountered by R & D organisations

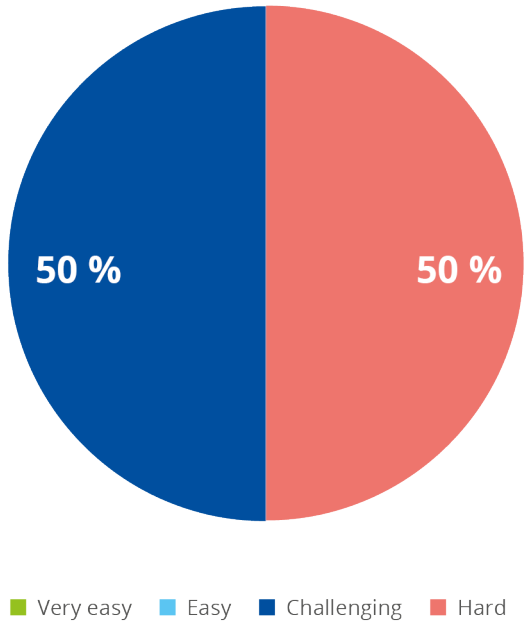
The lack of skills, a barrier already highlighted by regulatory bodies, is also relevant in R & D organisations (Figure 34). Indeed, half of the interviewed organisations denote a lack of researcher skills, cybersecurity skills and cloud computing skills, and brain drain; a smaller proportion (25 %) also report a high fluctuation of skilled personnel.

Figure 34: Lack of skills in research and development organisations



Another relevant barrier for R & D in cloud cybersecurity is the accessibility to research funding (Figure 35): all organisations state that they face problems in procuring financial resources, with difficulty levels ranging from 'challenging' to 'hard'.

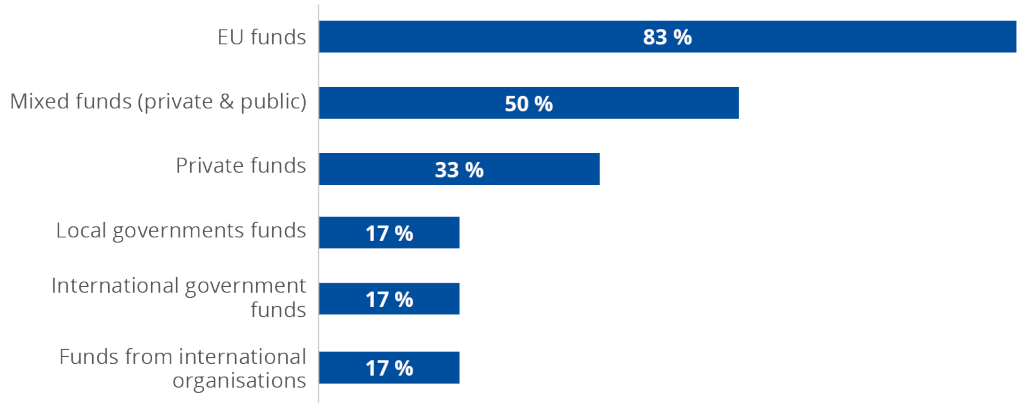
Figure 35: Accessibility of research funding for research and development organisations



Concerning research funding instruments (Figure 36), R & D organisations rely on EU funds (83 %), mixed funds (private and public) (50 %) or private financing only (33 %). A smaller

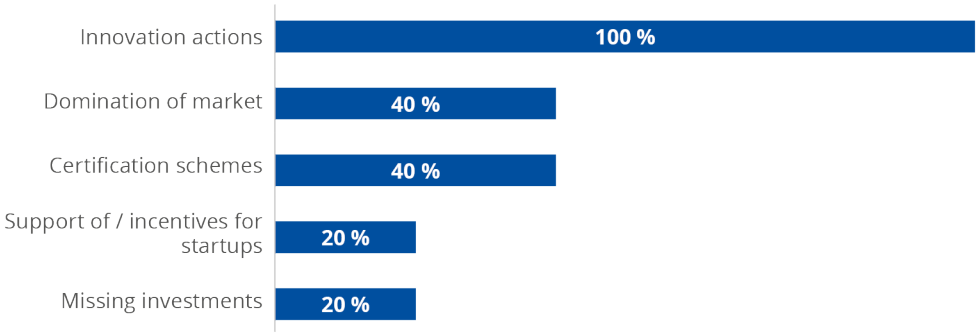
proportion (17 % of organisations) also receives funds from local governments, international governments or international organisations.

Figure 36: Most important instruments for research funding according to R & D organisations



All R & D organisations agree that innovation actions are a core driver in promoting research and innovation (Figure 37). Moreover, 40 % of the interviewed realities also highlight the importance of market domination and certification schemes. A smaller percentage (20 %) indicate missing investments and support for start-ups (namely through incentives) as relevant drivers for cloud cybersecurity research.

Figure 37: Market/financial/economic/societal drivers according to R & D organisations

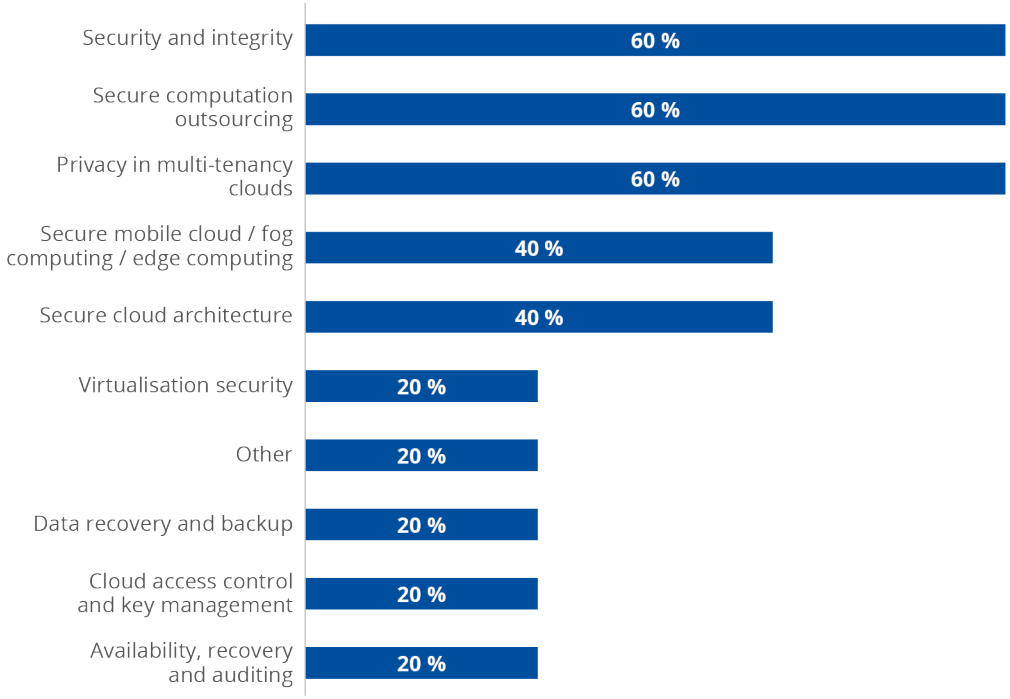


7.3. Cloud cybersecurity innovation areas

This section provides an overview of the trending topics in cybersecurity research, identifying the market's research and innovation priorities. Current research could develop into future technology trends, which may one day influence the market; it is therefore crucial to determine which research topics are considered particularly relevant in the market (supply and demand) and compare this information with current R & D activity, assessing the state of play in research. This allows us to estimate the readiness of available technology research results for market deployment, the impact of adopting new technologies in the market and the time horizons for technology adoption.

According to the surveyed R & D organisations, the most relevant research topics in cloud computing related to cybersecurity (Figure 38) are security and integrity; secure computation outsourcing and privacy in multi-tenancy clouds (all mentioned by 60 % of the involved organisations); secure mobile cloud computing / fog computing / edge computing and secure cloud architecture (both at 40 %); virtualisation security; data recovery and backup; cloud access control and key management; availability; recovery and auditing and other topics (such as cybersecurity certification and automation) (all at 20 %).

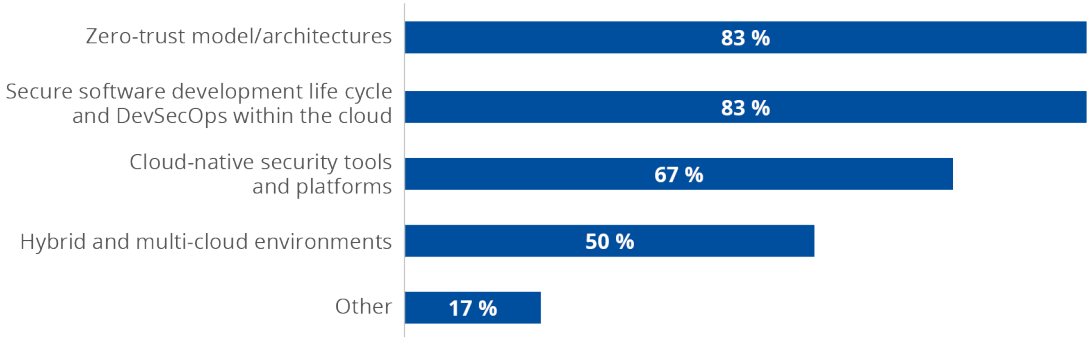
Figure 38: Important researched cybersecurity topics according to R & D organisations



Considering instead cloud computing developments that are already in place and used beyond research, according to R & D organisations, the most impactful ones (Figure 39) are:

- zero-trust models/architectures (according to 83 % of organisations);
- secure software-development life cycle (SDLC) and DevSecOps for the cloud (83 %);
- cloud-native security tools and platforms (67 %);
- hybrid and multi-cloud environments (50 %);
- other developments, such as automation and AI (17 %).

Figure 39: Impactful cloud computing developments for cybersecurity according to R & D organisations



7.4. INTERESTING OBSERVATIONS: CLOUD CYBERSECURITY MARKET TRENDS

1. The comparison between these results and the research priorities for market actors (supply and demand companies) leads to some interesting insights. Indeed, their interests are mainly focused on two research streams: privacy and security for the cloud (privacy-enhancing technologies, double encryption, etc.), and innovative technologies (AI, 5G,

quantum computing, superconducting microchips, etc.). While the first research priority coincides with the information reported by R & D companies, the second stream of activities does not seem to be a current focus area for cloud cybersecurity R & D organisations.

2. Availability of standards seems to be a significant barrier for both regulatory bodies and R & D. Although this barrier is well known, no significant corrective measures have been implemented so far in the EU.
3. Skill shortage seems to be another common barrier. As it is obvious that available skilled personnel will switch to better paid jobs in the industry, it might be necessary to achieve better remunerations and/or to 'pool' skills by means of public institutions. At the same time, it is important to foster the creation of corresponding curricula at universities.
4. Innovation areas identified may be an important stepping stone for short-term research, but also market drivers and market trends.

8. CONCLUDING REMARKS

In this chapter, conclusions are drawn on the basis of the findings of this cybersecurity market analysis. The conclusions of this section constitute a synthesis of interesting observations made in the different Chapters (Chapters 1 to 7) of this analysis, while comparing this against evidence found in available cloud computing studies. In doing so we:

- use the evidence presented so far by means of findings from the survey, interesting observations and identified cross-cutting issues;
- seek to validate conclusions by comparing findings to existing cloud reports, obtained through open-source research (corresponding references can be found in each conclusion by means of footnotes); and
- highlight the different stakeholder types concerned by each conclusion.

The above elements are included in each conclusion by means of references to interesting points and similar conclusions found in open-source reports and /references to the concerned cloud stakeholder types. Within each section, the conclusions drawn are enumerated to facilitate identification and referencing.

It should be noted that the conclusions drawn do not exhaust all interesting observations of each of the Chapters 1 to 7. We recommend that interested readers visit this material in order to gain a better understanding – on a second level of detail – all the interesting topics identified in this analysis.

Another important note to be made is that the content of these conclusions is not overlap-free: some of the conclusions below might touch upon issues mentioned in another conclusion category (sub-section). For example, a conclusion on market trends may affect research issues and vice-versa. When possible, we have indicated where the content overlaps.

8.1. CONCLUSIONS ON MARKET CHARACTERISTICS AND TRENDS

1. Many demand-side stakeholders are using security services from the same companies that also provide cloud services, as a kind of 'bundled offering', but it is in reality very difficult to establish market patterns when it comes to security products and services, whether these are offered directly by the CSPs themselves, by enablers or partners of CSPs, or by independent suppliers contracted by cloud service consumers (CSCs). In this respect, the market can be said to be 'blurred', as security products/services are bundled with all-inclusive services in such a way as to dilute their distinguishable features.

   Evidence from observations: Observations 4 and 5 in Section 3.5, Observation 5 in Section 4.3.
   Relevant stakeholder types: supply side, demand side.

2. About 40 % of respondents consider secure mobile cloud computing /fog computing / edge computing and secure cloud architectures to be the most relevant research topics (see Figure 38), which echoes the opportunities outlined in the EU report elaborated following the CEO roundtable 'Shaping the next generation cloud supply for Europe' and addressed to Thierry Breton, European Commissioner for the Internal Market ([46]). This report identified

([46]) European industrial technology roadmap for the next generation cloud-edge offering May 2021, https://ec.europa.eu/newsroom/repository/document/2021-

[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

opportunities such as cloud edge continuum (e.g. innovative hardware encryption for the edge), energy-efficient cloud, cloud-native 5G, EU open ecosystem of applications and toolkits for cloud, as well as convergence information technology (IT) and operational technology (OT). Secure access service edge (SASE) is presented as an opportunity for EU players, including a new network security model that combines multiple controls such as zero-trust network access, a Cloud Access Security Broker (CASB), firewall as a service and data loss protection. Secure Access in 5G Mobile Networks will lead to the integration of end-to-end service orchestration of SD-WAN, SASE and mobile networks across the entire solution.

Evidence from observations: Observations 4 and 5 in Section 3.5, Observation 5 in Section 4.3.
Relevant stakeholder types: supply side, R & D, demand side.

3. While some SASE solutions include the CASB functionality as part of their offering, these two solutions/functionalities are likely to co-exist, a least for some time. In addition, SASE looks more like a framework that combines network security and wide-area networking than a concrete security solution. Its vendors follow an 'all in one' approach, as opposed to security-solution integration or 'chaining' done by customers or system integrators on their behalf. While further service and product consolidation is desirable and expected, in Gartner's hype cycle for cloud security for 2021 ([47]), SASE is at the peak of inflated expectations.

   Evidence from observations: NA (derived as a cross-cutting analysis conclusion).
   Relevant stakeholder types: supply side, demand side, R & D.

4. About 60 % of respondents find secure computation outsourcing and privacy in multi-tenancy cloud systems to be the important challenge ([48]) (see also Figure 38), while 50 % are planning to implement data-security solutions, which reveals opportunities in emerging sub-segments such as confidential computing, a technology that mentioned in Gartner's hype cycle for cloud security in 2020 and 2021 ([49]). Confidential computing is a mechanism that protects sensitive code and data from third parties, including the CSP. Indeed, confidential computing protects data while it is 'in use', or as it is being processed, thus bridging a gap in common encryption protection that focuses on data at rest or in transit. Confidential computing is particularly relevant in the context of in-cloud use of data. Confidential computing also makes it easier to move between different cloud environments without exposing any sensitive data and is adequate for the scenarios where there is no mutual trust. In the EU there are already several companies, mainly start-ups, working on this technology, as well as some mature research on trusted execution environments, multi-party computation and other related topics, which could be an opportunity for EU suppliers. Ensuring that start-ups working on these technologies receive adequate funding to grow and become pervasive in cloud computing environments is paramount to ensuring that security concerns about cloud services are addressed. Furthermore, given the importance that these market actors have and the protection that they afford users, a certification scheme laying down qualitative expectations for these organisations' products might prove useful.

   Evidence from observations: Observation 4 in Section 7.4.
   Relevant stakeholder types: R & D, supply side, demand side.

18/European_CloudEdge_Technology_Investment_Roadmap_for_publication_pMdz85DSw6nqPppq8hE9S9RbB8_76223.pdf, accessed November 2022.

([47]) https://www.gartner.com/en/documents/4004061, accessed November 2022.

([48]) Note: Although the identification of this conclusion has its roots in Innovation areas, it is considered as relevant to market trends, as many of the referenced technologies do exist and adaptation of existing offerings seem to be feasible.

([49]) https://www.gartner.com/en/documents/4004061, accessed November 2022.

5. SDLC and DevSecOps for the cloud were considered as impactful developments by 83 % of R & D respondents (Figure 39). In addition, 43 % of customers and 62 % of suppliers plan to implement some solutions related to cloud-native and application security (Figure 19 and Figure 20, respectively). Similar to the intersection of networking and security, in this area there is a consolidation of features and capabilities provided by previously separated tools. A cloud-native application protection platform is a segment addressing both SDLC and the traditional gap between security and DevOps teams, while its focus is on the cloud-native ecosystem. This segment is also halfway between evolution and convergence of cloud security posture management and cloud workload protection platforms, and is also expected to consolidate cloud service network security, which in turn has replaced mechanisms such as a web application firewalls or web application and API protection.

   Evidence from observations: Observation 4, Section 7.4.
   Relevant stakeholder types: R & D, supply side, demand side.

6. Among cloud security product companies, there are those that address the same security concerns as 'on-premises IT' but adapted to the cloud, while others address security concerns unique to the cloud. Emerging consolidation is also visible in this area, which makes procurement very difficult. Some cloud-security segments overlap, while other raise doubts regarding different alternatives: should customers choose one single vendor that unifies many different cloud security controls (integration), or should they opt for separated solutions ('chaining' of controls)? This is a question that needs to be further researched and which may lead to some added-value offerings from suppliers (especially enablers).

   Evidence from observations: NA (derived as a cross-cutting analysis conclusion).
   Relevant stakeholder types: supply side, demand side.

8.2. CONCLUSIONS EMERGING FROM VARIATING PERCEPTIONS AND POTENTIAL GAPS

1. The *2021 AWS Cloud Security Report* ([50]), based on a comprehensive survey of 316 cybersecurity professionals and focused on responses to new security threats, noted that configuration is the top concern (71 %), exfiltration of sensitive data comes second (59 %), and insecure APIs comes third (54 %). In our survey, misconfigurations scored high as a threat with supply-side respondents (75 %, see Figure 21), with the highest gap between perceived and managed threats. On the demand side, this gap is not as big for this specific threat, but becomes significant when it comes to insecure APIs, which are perceived as a threat by 60 % of demand-side respondents (see Figure 21).

   Evidence from observations: Observations 3 and 8 in Section 5.3 and Observation 5 in Section 4.3.
   Relevant stakeholder types: supply side, demand side.

2. Misconfigurations scored high as a threat with supply-side respondents (around 75 %, see Figure 21), with the highest gap between perceived and managed threats. However, there are different kinds of misconfigurations in the cloud, related to the different responsibilities of CSPs and CSCs, and different tools and controls that deal with this threat. Infrastructure-as-code scanning, for example, is a form of automation to minimise cloud misconfiguration risks, as it ensures code quality of the cloud infrastructure configuration files. Cloud infrastructure entitlements management – which appeared as a separated cloud security segment very recently –deals, among other things, with IAM misconfigurations. Both solutions are increasingly being seen as yet another feature of the cloud-native application protection platform. Furthermore, customers said they require some (53 %) or extensive (20

([50]) https://www.cybersecurity-insiders.com/portfolio/2021-aws-cloud-security-report-cloudpassage/, accessed November 2022.

%) help with the customisation of cloud applications, including security configurations ([51]). This also shows that beyond specific cloud-service solutions, there is still a large demand for cloud security enablers, i.e. companies that act on behalf of the customer, implement, integrate or deploy different cloud security solutions.

Evidence from observations: Observation 3 and 8 in Section 5.3.
Relevant stakeholder types: supply side, demand side.

3. CSPs prioritised 'security of the cloud', in other words keeping their cloud infrastructure and stack secure, which is not always their responsibility. They also offer some security services – such as monitoring, detection, and security management services – to their clients, which can be bundled together with cloud services or provided separately. A CSC cannot presume that the vendor of their cloud environment will be entirely responsible for security; they need to look for the best solution through additional investment in products and services. The absence of clearly delimited responsibilities leads to both uncertainties, the risk of over - or underlaps and increased resources requirements. Making CSPs fully responsible may solve this problem. The key consideration is currently the 'shared responsibility model', often linked to a service-level agreement.

   Evidence from observations: Observation 9 in Section 5.3.
   Relevant stakeholder types: supply side, demand side.

4. Threats such as abuse of insufficient or inappropriate identity, credentials, access and key management are perceived as important both by suppliers (over 50 %, see Figure 21) and by demand-side respondents (around 50 %, see Figure 21). While cloud IAM solutions exist and are used (implemented by 84 % of demand-side respondents according to the survey, see Figure 19), they have limitations in the multi-cloud environment. Each CSP has its own policies, and mapping permissions across different platforms at scale is a challenge; for this reason, organisations also use Cloud Infrastructure Entitlements Management (CIEM). This is a topic that needs further elaboration in order to obtain a more efficient deployment and use of available controls on both sides (supply and demand). Eventual involvement of R & D might facilitate the identification of possible solutions in this regard ([52]).

   Evidence from observations: NA (derived as a cross-cutting analysis conclusion).
   Relevant stakeholder types: supply side, demand side, R & D.

8.3. CONCLUSIONS ON MARKET BARRIERS

1. Lack of visibility and transparency and related threats are perceived very differently in our survey by suppliers (around 25 %, see Figure 21) and demand-side respondents (almost 25 %, see Figure 21). This observation is confirmed in the *2022 Fortinet Cloud Security Report* (by 49 % of respondents) ([53]). As differences in perceptions are important barriers for market adoption, one can argue that the entire conclusions of Section 8.2 can be considered as issues to be addressed for a better adoption of cloud cybersecurity throughout the market both within the EU and internationally.

   Evidence from observations: Observation 2 in Section 5.3.
   Relevant stakeholder types: supply side, demand side.

2. Lack of skills also emerges as the most relevant barrier for adoption, as perceived by all stakeholders (around 78 % of all respondents on average, see Figure 30, Figure 31, Figure 34). In (ISC)²'s *2022 Cloud Security Report* ([54]), 78 % of respondents claimed that

([51]) https://tbri.com/tbr-insight-center/cloud-and-software-competitive-intelligence/customer-research/cloud-applications/, accessed November 2022.
([52]) Note: to this extent, this conclusion introduces an overlap with Section 8.3.
([53]) https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-2022-cloud-security.pdf, accessed November 2022.
([54]) https://www.isc2.org/-/media/5E48A83950264AB1B265B1F073F5C9FB.ashx, accessed November 2022.

traditional security solutions do not work or have limited functionality in cloud environments, while lack of expertise (40 %) was perceived as the main barrier for adoption.

Evidence from observations: Observation 3 in Section 7.4.
Relevant stakeholder types: supply side, regulatory bodies, R & D.

3. It bears noting that a significant amount of supplier still do not hold any certifications for the offered services. On the other hand, it seems that the higher risk appetite of the demand side can be explained either by the lack of cybersecurity awareness or by a higher prioritisation of cost/performance issues. Nonetheless, the desire of the demand side to use certified services (around 50 %), does not fully resonate with the supply side, when considering the adoption level of the existing cloud service certifications. This may be considered as another barrier for the adoption of cloud services, especially when compliance requirements on the demand side do matter (e.g. financial sector, other critical sectors).

   Evidence from observations: Observation 9 in Section 6.3 (almost as is).
   Relevant stakeholder types: supply side, demand side, regulatory bodies.

4. Availability of standards and necessary IPRs seems to be a significant barrier for both regulatory bodies and R & D. Although this barrier is well-known in almost all domains, no significant corrective measures have been implemented so far in the EU.

   Evidence from observations: Observation 2 in Section 6.3 (almost as is).
   Relevant stakeholder types: supply side, regulatory bodies, R & D.

5. Given the relatively low level of vulnerability information communicated to the demand side, it seems necessary to raise awareness and intensify notification on existing vulnerabilities both in the cloud services and the used applications for all users of the cloud services. Eventually, SLAs would need to be checked and potentially updated to include vulnerability notification to users of the service. New or emerging EU regulations see vulnerability management as a central part of incident notification, therefore such SLA updates will be mandatory for a variety of products and services, especially the ones used in critical sectors. If such a change is not made, it could turn into a barrier for market adoption.

   Evidence from observations: Observation 2 in Section 5.3 (as is).
   Relevant stakeholder types: supply side, demand side, regulatory bodies.

8.4. CONCLUSIONS ON RESEARCH AND INNOVATION TOPICS

1. Zero-trust model/architectures also confirmed in our survey as one of the main developments in cloud computing that may be impactful for cybersecurity, according to 83 % of organisations (Figure 39). This is confirmed by market trends ([55]), where SASE vendors are already incorporating functionalities or capabilities of zero trust, while replacing or converging with other cybersecurity capabilities and tools such as the virtual private network (VPN) or even capabilities of more recent solutions such as the (CASB) functionality. Cloud infrastructure security and policy enforcement was considered to be implemented by around 37 % of the respondents in our study, which shows how important this area is (Figure 19).

   Evidence from observations: Observation 4 in Section 7.4.
   Relevant stakeholder types: R & D, supply side, demand side.

([55]) https://ec.europa.eu/newsroom/repository/document/2021-18/European_CloudEdge_Technology_Investment_Roadmap_for_publication_pMdz85DSw6nqPppq8hE9S9RbB8_76223.pdf, accessed November 2022.

2. The comparison between the analysis results of the chapter on cybersecurity market trends (see Chapter 7) and the research priorities for market actors (demand-side and supply-side organisations) leads to some interesting insights. Indeed, assessed demand-side and supply-side trends mainly focus on two research streams: privacy and security for the cloud (privacy-enhancing technologies, double encryption, etc.) and innovative technologies (AI, 5G, quantum computing, superconducting microchips, etc.). While the first research priority coincides with the information reported by R & D companies, the second stream of activities does not seem to be a current focus of R & D organisations. Hence, these areas might be excellent candidates for a deployment action, given the fact that the underlying technologies have matured and that corresponding products do exist (e.g. AI, 5G), while other technologies are in the advanced prototype phase (e.g. quantum computing and supercomputing).

   Evidence from observations: Observation 1 in Section 7.4 (almost as is).
   Relevant stakeholder types: R & D, supply side, demand side.

8.5. FURTHER CONSIDERATIONS AND PROJECTIONS

Beyond the conclusion formulated above, both this analysis and the open-source research performed have revealed some additional points that are worth analysing, in order to gain valuable insights into future market developments. They mainly concern possible paths through which vendors might evolve their market strategies in order to use emerging market opportunities. One of the main dilemmas on the demand side is related to the strategy regarding the so-called 'cloud ecosystem' around hyperscalers (mainly Google Cloud, Microsoft Azure and AWS).

There are important trends in these strategies. The Microsoft Partner Network (with 400 000 member organisations) became the Microsoft Cloud Partner Program in October 2022, targeting all partners in the ecosystem, for companies selling services, software solutions or devices. Six solution areas are aligned to Microsoft market strategy: Data & AI (Azure), Infrastructure (Azure), Digital & App Innovation (Azure), Business Applications, Modern Work and Security. Microsoft will divide partners into 'peers', according to their capability score.

In this ecosystem, we include all types of 'vendors': there are smaller CSPs, but also what we call 'enablers'. Enablers are organisations offering advisory and consulting services, cloud security-system integration, cloud security products, application development services and cloud security operations, management and maintenance. We should also not forget that some CSPs are on 'both sides', acting as a customer of large hyperscalers, but also as a provider for the customers further down the value chain (this is the case for many organisations that rely on IaaS to provide their SaaS services). In our survey we included many types of enablers, including resellers, administrators and integrators.

While hyperscalers increasingly try to provide end-to-end services within a single-cloud vendor scenario, large system integrators reorient their strategy towards orchestration, including deployment of different cloud services in multi-cloud and hybrid-cloud settings. Most of these vendors are part of all three hyperscaler ecosystems and generate revenue from all three. Finally, in some cases, a joint venture between CSP and system integrators or consulting companies is established.

Hyperscalers have their own service branch: Microsoft has enterprise services (in 2020 Microsoft's consulting services were also launched), AWS has global services, Proserve and AWS have managed services, while Google has a cloud professional services organisation. However, a headcount of these service organisations reveals that the number of trained professionals in the partner ecosystem is still much higher than in CSP professional service branches. While cloud professional services are estimated to be around 38 % of the overall cloud

market in 2021 ([56]), we estimated that 90 % of that revenue belongs to partners in hyperscalers and other CSP ecosystems.

These considerations are indicative. It might be interesting to perform a dedicated analysis in the area of cloud computing strategies to identify the potential and prospective market footprint. Though quite specific, such an analysis could be performed either by means of an appropriately scoped market analysis or as a foresight exercise, possibly via an EU-funded research project.

([56]) https://tbri.com/tbr-insight-center/cloud-and-software-competitive-intelligence/customer-research/cloud-applications/, accessed November 2022.

9. ANNEX A: CLOUD CYBERSECURITY MARKET ANALYSIS QUESTIONNAIRE

ENISA formulated the following questions for stakeholders for its cloud computing cybersecurity market analysis. They may serve as a model or template for questions that are pertinent to other cybersecurity markets. Some questions may be more relevant than others, therefore the market analyst should feel free to adapt the questions the way they see fit. The analyst may have other questions of particular relevance to their market segment. The answers to the questions provide data for the analysis.

Demand side

- In which EU Member States are you present?
- Indicate the number of employees.
- Indicate the approximate annual revenue (for NGO or public administration, please put 0).
- Indicate the main sector of activity.
- Indicate the main subsector of activity.
- Indicate the ownership structure.
- What percentage of digital assets do you have in the cloud? (i.e. percentage of total digital assets)
- What percentage of sensitive data (finance, accounting, employee, customer intelligence, IPR, health or payment etc.) is stored in the cloud?
- What service model of cloud do you use?
- What deployment model for cloud services do you use?
- How many different cloud providers do you have (public or private)?
- What are the main cloud attributes that you use?
- Which of these categories of measures have you already implemented or plan to implement in the context of cloud cybersecurity? (Measures might be/have been implemented through purchased services.)
- Which compliance requirements are the most relevant?
- Which business or other requirements must be taken into account?
- What are the most relevant cybersecurity threats for your environment?
- What threats do you aim to reduce with cloud security solutions?
- Have you experienced an impactful incident in the last 12 months?
- Which type of impact was it?
- What was the overall impact of incidents?
- Were any of the incidents subject to mandatory reporting to a regulatory body, government, data subject, etc.?
- Were any cloud infrastructure vulnerabilities reported to you by your provider during the last year?
- Did you need to take any action on your side?
- Could you please provide some examples of such actions?
- What are the most relevant challenges for your environment?

Supply side

- Indicate the number of cloud customers.
- Indicate the approximate annual revenue of the cloud business.
- Indicate the total value-added cloud business (revenues minus the price paid for materials and services).
- Indicate the customer sectors of activity for the entire cloud business.
- Indicate any other sector.
- Indicate activities in the subsectors of banking, communications or media, education, government, healthcare, insurance, manufacturing, retail, transportation and/or utilities.
- Indicate activities in the wholesale subsectors.
- In which EU Member States are you present?
- Indicate the geographical areas of customers.
- Indicate your investment plan for cybersecurity.
- Indicate the current implementation strategy for cybersecurity offerings.
- Indicate the percentage of revenue dedicated to investment in research, development and innovation.
- Indicate the ownership structure.
- Which are the service models offered?
- Indicate available certifications and attestations (e.g. audit reports, such as SOC2) for SaaS.
- Indicate the available certifications and attestations (e.g. audit reports, such as SOC2) for PaaS.
- Indicate the available certifications and attestations (e.g. audit reports, such as SOC2) for IaaS.
- Which deployment model for cloud services do you support?
- What are the three most important cloud attributes in your offerings (by means of income)?
- Which of these categories have you already implemented or do you plan to implement in the context of cloud cybersecurity?
- Indicate detailed identity and access management (IAM) functions, antivirus and end-point protection functions, incident detection and response functions, value-added cybersecurity functions, infrastructure security and security policy enforcement, cloud hardware security.
- Which compliance requirements are the most relevant?
- Which business or other requirements must be taken into account?
- What are the most relevant cybersecurity threats for your environment?
- What threats do you aim to reduce with cloud security solutions?
- Have you experienced one or more impactful incidents in the last 12 months?
- What was the overall impact of the incident?
- Were any of the incidents discovered subject to mandatory reporting to a regulatory body, government, data subject, etc.?
- What are the most relevant cybersecurity challenges for your environment?
- How many vulnerabilities have you handled last year?
- How many of those vulnerabilities were found in the systems of your providers?
- How many of them took a week or more to fix?
- Indicate events or incidents that might impact your overall market.
- Indicate other important effects on the market (e.g. deployment, regulation, network effect, bottleneck).
- Do you think there are gaps and niche areas in the market?
- Indicate what you think are the most important cybersecurity research topics.
- What are the main technology drivers for the cybersecurity of cloud computing? Name up to three (e.g. AI, 5G/Edge).
- What are the main business drivers for the cybersecurity of cloud computing? Name up to three.

Research and development

- Indicate the total yearly budget available for research projects.
- Indicate the number of research staff in your organisation.
- Indicate the main source of research budgets/grants.
- In which countries or geographical areas in the EU do you have a physical presence?
- In which sectors does your organisation conduct research? For example, in banking, communications or media, education, government, healthcare, insurance, manufacturing, retail, transportation and/or utilities.
- Indicate what activities you carry out in wholesale subsectors.
- Indicate the average number of staff participating in a project.
- Do you collaborate on a regular basis with third-party organisations?
- Indicate the ownership structure of your organisation.
- Indicate the number of projects in cybersecurity in the past year.
- Indicate the most important research topics for you in cybersecurity.
- Indicate the developments that you think will be most impactful for cybersecurity (both negative and positive impact).
- What are the most relevant cybersecurity threats in your opinion?
- What do you consider to be the most important instruments for research funding?
- What do you regard as the most important market, financial, economic and societal drivers promoting research and/or innovation in the EU?
- What do you consider are barriers to research uptake?
- What technological barriers have you encountered?
- Does your organisation suffer from a shortage of skills?
- Indicate how easy it was to find proper funding for cybersecurity research.
- Do you know about any newcomers or companies with great innovation value?
- Do you think there are gaps and niche areas in the market?
- Name the three most important issues that research on cybersecurity must solve.

Bodies involved in regulation

- Indicate the size of the population in your area of responsibility.
- Indicate the countries or geographical areas influenced by your activities.
- Indicate the subject of cybersecurity-related regulatory activities in which your organisation is involved.
- Indicate the sectors that fall under the regulatory supervision of your organisation (e.g. in banking, communications or media, education, government, healthcare, insurance, manufacturing, retail, transportation and/or utilities).
- Indicate what activities you carry out in wholesale subsectors.
- Indicate the type of your organisation.
- Indicate the role of your organisation in regulatory work.
- Indicate which regulatory instruments are most consequential for you.
- Do you have a plan to transition to an EU-approved cybersecurity certification scheme?
- What are the most relevant cybersecurity threats, in your opinion?
- What threats or vulnerabilities do you aim to reduce with an EU-approved cybersecurity certification scheme?
- What are the most relevant challenges to be addressed through regulatory work, in your opinion?
- How many cybersecurity vulnerabilities have been reported to your organisation in the last year?
- Can you manage these vulnerability reports with your actual resources?

- Have dedicated funds been allocated to support companies in transitioning towards the use of the chosen regulatory compliance instrument?
- Indicate other market, financial, economic, societal or legal drivers for promoting regulatory compliance?
- What are the main regulatory barriers?
- What are the technological barriers encountered?
- What may be the impact of data localisation requirements and the ensuing need to invest in local infrastructure?
- Do you see opportunities from the regulatory framework (i.e. the drive to have services that are compliant with the general data protection regulation (GDPR), financial regulation, etc.)?

10. ANNEX B: SCOPING CRITERIA OF THE CLOUD CYBERSECURITY MARKET ANALYSIS

Criteria group	Criterion	Included in the scope? (Y/N)	Comment/context Criterion	Optional detailed criterion	Included in the scope? (Y/N)	Comment/context detailed criterion
Criteria demand side	**Business impact of procurement for demand side:** focuses on the value ratios between the product to be procured and the value chain	Yes		*Value rate of assets enrolled in the product*: indicates the rate between protected assets and total assets	Yes	Consequence of criterion inclusion
				Value rate of procured service: indicates the rate between the value of the cybersecurity product and the total income achieved by the entire supply chain	No	Can be omitted (simplification of survey)
	Required demand-side capability/maturity: focuses on the capability level of the demand side to deploy/manage the procured product	Yes		*Capability available*: the demand side already possesses the necessary capabilities	Yes	Consequence of criterion inclusion
				Capability to be developed: the necessary capability is not available on the demand side, but will be developed	Yes	Should be considered in order to assess implementation effort
				Capability outsourcing: the demand side plans to outsource the capabilities needed to deploy/maintain the product	Yes	An important argument for use of cloud computing
	Role in risk mitigation: focuses on the role of the product in reduction of threat exposure and consequently to risk avoidance/mitigation/reduction	Yes		*Threat landscape (e.g. emerging threats, vulnerabilities)*: the assessed/relevant threats whose exposure the demand side aims to reduce	Yes	Consequence of criterion inclusion. This optional detail provides significant insights for the role of cloud computing

Criteria group	Criterion	Included in the scope? (Y/N)	Comment/context Criterion	Optional detailed criterion	Included in the scope? (Y/N)	Comment/context detailed criterion
				Risks/impact of attacks (e.g. safety, cost, # of affected users, assets, etc.): risks to be mitigated/reduced through the product	Yes	Consequence of criterion inclusion. This optional detail provides significant insights for the role of cloud computing
	Demand-side geographies: focuses on the geography of activity of the demand side, by means of physical presence in various areas through branches	Yes		*International:* the demand side maintains an international presence	Yes	Consequence of criterion inclusion
				International with restrictions (e.g. EU): the demand side maintains a physical presence in restricted international spaces	Yes	Consequence of criterion inclusion
				National/regional: the demand side maintains a national/regional physical presence	Yes	Consequence of criterion inclusion
	Demand-side requirements: focuses on the demand-side requirements the procured product has to fulfil	Yes		*Compliance (with sectorial standards):* compliance requirements should be taken into account	Yes	Consequence of criterion inclusion
				Business requirements: indicates business requirements that may lead to the procurement of the product (including new businesses)	Yes	Can be omitted (simplification of survey)
				Other (security) requirements: the demand side provides requirements to be fulfilled by the procured product (to be developed, e.g. on the basis of ISO 27000)	Yes	Consequence of criterion inclusion
	Gap identification: focuses on gap identification of product from demand side	No		*Based on requirements (see previous criterion):* identification of a gap for a product to be procured on the basis of demand-side requirements	No	Consequence of criterion exclusion

Criteria group	Criterion	Included in the scope? (Y/N)	Comment/context Criterion	Optional detailed criterion	Included in the scope? (Y/N)	Comment/context detailed criterion
				Based on good practices: identification of a gap for a product to be procured on the basis of industry good practices	No	Consequence of criterion exclusion
				Based on Open Source Intelligence (OSINT): identification of a gap for a product to be procured on the basis of open-source information (i.e. Gartner magic quadrant, etc.)	No	Consequence of criterion exclusion
	Investment plan: focuses on the plan to finance the procurement of the product	No		*Direct financing*: the demand side performs the investment for product procurement from own funds	No	Consequence of criterion exclusion
				Incentives: investment for product procurement may be incentivised by public/private initiatives	No	Consequence of criterion exclusion
				Public/private/EU funding: investment for product procurement to be supported with funding	No	Consequence of criterion exclusion
	Demand-side company characteristics: focuses on the assessment of generic company data for the demand side	Yes	Available criteria found (DG GROW) are related to company size. These criteria can be used when evaluating potential survey responses. No need to be taken into account during the setting of scope. Just to make sure that they are foreseen as focus seems to be sufficient for this phase.	*Company size*: indicates the number of employees	Yes	Consequence of criterion inclusion (size is an important element of the survey)

Criteria group	Criterion	Included in the scope? (Y/N)	Comment/context Criterion	Optional detailed criterion	Included in the scope? (Y/N)	Comment/context detailed criterion
				Demand-side sector of activity (main value chain): indicates the main sector the demand side is active in	Yes	Consequence of criterion exclusion (sector is an important element of survey)
				Customer base: indicates the number and demographics of customers of the demand side	No	Can be omitted (simplification of survey)
				Customer geographies: indicates the geographies of customers (overlaps with demand-side geographies above)	No	Consider merging with geographies due to redundancy (eventually delete above geographies to simplify)
				Year of establishment: the year of establishment of the demand-side company	No	Can be omitted (simplification of the survey)
				Ownership structure: indicates the ownership structure of the demand side	Yes	Consequence of criterion inclusion (ownership structure is an important element of survey)
	Market barriers: focuses on barriers encountered by the demand side to procure the product	Yes		*Market/financial/economic barriers*: indicates potential financial issues in the procurement of product	Yes	Consequence of criterion inclusion (economic barriers are an important element of the survey)
				Governmental, political, regulatory barriers: indicates potential regulatory/legal issues in the procurement of the product	Yes	Consequence of criterion inclusion (political barriers are an important element of survey)
				Technological barriers: Indicates technological issues in the procurement of product	Yes	Consequence of criterion inclusion (technological barriers are an important element of survey)

Criteria group	Criterion	Included in the scope? (Y/N)	Comment/context Criterion	Optional detailed criterion	Included in the scope? (Y/N)	Comment/context detailed criterion
				Societal barriers (incl. cultural, behavioural, environmental): indicates societal barriers in the procurement of product	Yes	Can be omitted (simplification of survey)
				Ethics barriers: indicates ethics barriers in the procurement of product.		
				Compliance barriers: indicates compliance as an issue in the procurement of product	Yes	Consequence of criterion inclusion (compliance barriers are an important element of survey)
				Access to information barriers: indicates potential information unavailability as issue in the procurement of products	Yes	Consequence of criterion inclusion (information access barriers are an important element of survey under the angle of cloud computing)
				Trust barriers: indicates trust issues in the procurement of product	Yes	Consequence of criterion inclusion (trust barriers are an important element of survey)
Criteria supply side	**Business impact of product for supplier:** focuses on the role of the product in comparison to the total business volume	Yes	It characterises the role of the product for the supplier (i.e. primary vs. secondary product).	*Value rate of supplied product in supply chain*: indicates the rate between product assets and total assets	Yes	Consequence of criterion inclusion
	Covered profiles for product deployment: focuses on asserted capabilities on the demand side to deploy/manage the product	Yes		*Capability available:* the demand side already possesses the necessary capabilities	Yes	Provision of required skill sets
				Capability to be developed: necessary capability is not available on the demand side, but will be developed	Yes	Potential offering of training, provision of required skill sets

Criteria group	Criterion	Included in the scope? (Y/N)	Comment/context Criterion	Optional detailed criterion	Included in the scope? (Y/N)	Comment/context detailed criterion
				Complete capability outsourcing: the demand side can outsource the capabilities needed to deploy/maintain the product	Yes	Provision of demand-side obligations to perform the outsourcing (e.g. remote maintenance)
	Role in reduction of exposure: focuses on the asserted role of the product in the reduction of threat exposure and consequently in risk avoidance/mitigation/reduction.	Yes		*Threat landscape (e.g. emerging threats, vulnerabilities)*: the assessed/relevant threats which the supplied product aims to reduce exposure to	Yes	Consequence of criterion inclusion. This optional detail provides significant insights for the role of cloud computing
				Risks/impact of attacks (e.g. safety, cost, # of affected users, assets, etc.): risks to be mitigated/reduced through the supplied product	Yes	Consequence of criterion inclusion. This optional detail provides significant insights into the role of cloud computing
	Supply-side geography: focuses on where the supplier is physically present through branches	Yes		*International*: supplier maintains physical presence internationally	Yes	Consequence of criterion inclusion. This optional detail provides significant insights into the role of cloud computing
				International with restrictions (e.g. EU): supplier maintains physical presence in certain areas	Yes	Consequence of criterion inclusion. This optional detail provides significant insights into the role of cloud computing
				National/regional: supplier maintains physical presence regionally/nationally	Yes	Consequence of criterion inclusion. This optional detail provides significant insights into the role of cloud computing
	Assessment of product requirements: focuses on the	Yes	It seems to be equally important to	*Assessment of threat landscape*: supplier continuously assesses	Yes	Consistent with the fact that corresponding

Criteria group	Criterion	Included in the scope? (Y/N)	Comment/context Criterion	Optional detailed criterion	Included in the scope? (Y/N)	Comment/context detailed criterion
	method followed by the supplier to identify requirements to be fulfilled by the product		assess the fulfilment of cybersecurity requirements, as in the case of the demand side. This element supports the identification of market forces (supplier-driven vs. customer-driven market) and gaps.	threats related to protected assets and provided functions		criterion has been selected in the demand side and will allow for comparison of views.
				Assessment of customer requirements: supplier continuously assesses customer requirements	Yes	Consistent with the fact that corresponding criteria has been selected on the demand side
				Industry standards / good practices: supplier considers industry good practices	Yes	Interesting element for the analysis.
				Own research: supplier performs own research to assess requirements to be fulfilled by the product	Yes	Interesting element for the analysis.
				Deploying other's research: supplier uses research results of others to identify product characteristics	Yes	Interesting element for the analysis.
				Acquisitions: supplier acquires related skills through buyouts	No	Can be omitted (simplification of the survey)
	Known gaps / emerging requirements	No		*Based on requirements (see previous criterion):* identification of a gap for supplied product on the basis of requirements	No	Consequence of criterion exclusion
				Based on good practices: identification of a gap for supplied	No	Consequence of criterion exclusion

Criteria group	Criterion	Included in the scope? (Y/N)	Comment/context Criterion	Optional detailed criterion	Included in the scope? (Y/N)	Comment/context detailed criterion
				product on the basis of industry good practices		
				Based on OSINT: identification of a gap for supplied product on the basis of OSINT	No	Consequence of criterion exclusion
				Continuous improvement: gap identification and product improvement are based on permanent monitoring (e.g. by means of established incident-management processes)	No	Consequence of criterion exclusion
	Supply-side targets: focuses on the various targets set by the supplier to be achieved via the product	Yes		*Innovation targets*: identification of the innovation targets of the supplier (e.g. technological, business, societal, etc.)	Yes	Consequence of criterion inclusion.
				Conformity/quality targets: identification of conformity and/or quality targets followed by the product supplier (e.g. standards, compliance, certifications)	Yes	Consequence of criterion inclusion
				Excellence targets: identification of targets related to the excellence of the supplied product (e.g. quality of service)	No	Can be omitted (simplification of survey)
	Supplier financial/economic measures ([57]): focuses on the various financial measures of the supplier	Yes		*Accounting concept of added value*: *as a proxy for GDP creation.*	Yes	As proposed proxy for GDP.
				Gross profit margin	No	*Gross profit margin = (Revenue – Cost of sales) / Revenue * 100*
				Net profit margin	No	*Net profit margin = Net Profit / Revenue * 100*
				Working capital	No	*Working capital = Current assets – Current liabilities*

([57]) https://online.hbs.edu/blog/post/financial-performance-measures

Criteria group	Criterion	Included in the scope? (Y/N)	Comment/context Criterion	Optional detailed criterion	Included in the scope? (Y/N)	Comment/context detailed criterion
				Current ratio	No	*Current ratio = Current assets / Current liabilities*
				Quick ratio	No	*Quick ratio = (Current assets – Inventory) / Current liabilities*
				Leverage	No	*Leverage = Total assets / Total equity*
				Debt-to-equity ratio	No	*Debt-to-equity ratio = Total debt / Total equity*
				Inventory turnover	No	*Inventory turnover = Cost of sales / (Beginning inventory + Ending inventory / 2)*
				Total asset turnover	No	*Total asset turnover = Revenue / (Beginning total assets + Ending total assets / 2)*
				Return on equity	No	*ROE = Net profit / (Beginning equity + Ending equity) / 2*
				Return on assets	No	*ROA = Net profit / (Beginning total assets + Ending total Assets) / 2*
	Investment plan: focuses on the plan to finance the development of the product	Yes		*Direct financing*: supply side performs the investment for product development from own funds	No	To be covered via questions (and their potential answers)
				Incentives: investment for product procurement may be incentivised by public/private initiatives	No	To be covered via questions (and their potential answers)
				Public/private/EU funding: investment for product development to be supported with funding	No	To be covered via questions (and their potential answers)
	Supplier company characteristics: focuses on the	Yes		*Company size*: indicates the number of employees	Yes	Consequence of criterion inclusion.

Criteria group	Criterion	Included in the scope? (Y/N)	Comment/context Criterion	Optional detailed criterion	Included in the scope? (Y/N)	Comment/context detailed criterion
	assessment of generic company data of the supply side					
				Supplier sector(s) of activity (main value chain): indicates the main sector(s) the supplier is active in	Yes	Consequence of criterion inclusion.
				Supplier sector(s) of activity (secondary value chain): indicates the secondary sector(s) the supplier is active in	Yes	Consequence of criterion inclusion
				Customer base: indicates the number and demographics of customers of the supplier	Yes	Consequence of criterion inclusion
				Customer geographies: indicates the geographies of customers (overlaps with demand-side geographies above)	Yes	Consider merging with geographies due to redundancy (eventually delete geographies above to simplify)
				Year of product launch: indicates the year the product was initially launched	Yes	Consequence of criterion inclusion
				Year of establishment: the year of establishment of the supply-side company	Yes	Consequence of criterion inclusion
				Ownership structure: indicates the ownership structure of the demand side	Yes	Consequence of criterion inclusion
	Market barriers: focuses on barriers encountered by demand side to procure the product	Yes		*Market/financial/economic barriers*: indicates potential financial issues for the deployment of the product	Yes	Consequence of criterion inclusion
				Governmental, political, regulatory barriers: indicates potential regulatory/legal issues in the deployment of product	Yes	Consequence of criterion inclusion
				Technological barriers: Indicates technological issues in the deployment of product	Yes	Consequence of criterion inclusion

Criteria group	Criterion	Included in the scope? (Y/N)	Comment/context Criterion	Optional detailed criterion	Included in the scope? (Y/N)	Comment/context detailed criterion
				Societal barriers (incl. cultural, behavioural, environmental): indicates societal barriers in the deployment of product	No	Can be omitted (simplification of survey)
				Compliance barriers: indicates compliance barriers in the deployment of product	Yes	Consequence of criterion inclusion
				Access to information barriers: indicates potential information unavailability as an issue for the deployment of products	Yes	Consequence of criterion inclusion (information access barriers is an important element of survey under the angle of cloud computing)
				Trust barriers: indicates trust issues in the deployment of product	Yes	Consequence of criterion inclusion
Other overarching criteria	**Identification of 'hidden champions'/'unicorns':** focuses on companies/start-ups with products with great innovation potential/value	Yes	Start-ups/SMEs launching innovative products/ideas of potentially high market value	*Innovation types: indicates the kinds of innovation introduced in the product (e.g. technological, novel business model, novel user needs)*	Yes	Consequence of criterion inclusion
				Response to trends: identify the trends the product follows (technology, economic, societal, business, etc.)	Yes	Consequence of criterion inclusion
	Identification of research gaps/topics: focuses on research gaps, blind spots, emerging trends	Yes				
	Impact of an incident on the market: focuses on various events and incidents that may impact the market	Yes				
	Impact of deployment actions: focuses on the impact of deployment actions on the market	Yes				

Criteria group	Criterion	Included in the scope? (Y/N)	Comment/context Criterion	Optional detailed criterion	Included in the scope? (Y/N)	Comment/context detailed criterion
	Identification of market niches: focuses on market gaps in specific sectors	Yes	Assumes analysis of market gaps both on the demand and supply sides (see above). So, despite 'disabled' gaps focus, it will happen here.			

TP-04-23-077-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

enisa.europa.eu

ISBN 978-92-9204-623-1
doi: 10.2824/050402