BANCA D'ITALIA

EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

Exploratory survey of the Italian market for cybersecurity testing services

by Anna Barcheri, Luca Bastianelli, Tommaso Curcio, Luca De Angelis, Paolo De Joannon, Gianluca Ralli and Diego Ruggeri

September 2025

Number 63

BANCA D'ITALIA
EUROSISTEMA

Mercati, infrastrutture, sistemi di pagamento

(Markets, Infrastructures, Payment Systems)

Exploratory survey of the Italian market for cybersecurity testing services

by Anna Barcheri, Luca Bastianelli, Tommaso Curcio, Luca De Angelis, Paolo De Joannon, Gianluca Ralli and Diego Ruggeri

Number 63 – September 2025

The papers published in the 'Markets, Infrastructures, Payment Systems' series provide information and analysis on aspects regarding the institutional duties of the Bank of Italy in relation to the monitoring of financial markets and payment systems and the development and management of the corresponding infrastructures in order to foster a better understanding of these issues and stimulate discussion among institutions, economic actors and citizens.

The views expressed in the papers are those of the authors and do not necessarily reflect those of the Bank of Italy.

The series is available online at www.bancaditalia.it.

Printed copies can be requested from the Paolo Baffi Library: richieste.pubblicazioni@bancaditalia.it.

ISSN 2724-6418 (online)
ISSN 2724-640X (print)

Banca d'Italia
Via Nazionale, 91 - 00184 Rome - Italy
+39 06 47921

Designed and printing by the Printing and Publishing Division of the Bank of Italy

EXPLORATORY SURVEY OF THE ITALIAN MARKET FOR CYBERSECURITY TESTING SERVICES

by Anna Barcheri,* Luca Bastianelli,* Tommaso Curcio,* Luca De Angelis,* Paolo De Joannon, Gianluca Ralli,*** Diego Ruggeri*****

Abstract

Authorities and market participants have long been committed to strengthening the cybersecurity of the entire financial sector. The recent EU regulation on digital operational resilience (DORA) has introduced harmonized rules, including the requirement for certain financial institutions to conduct advanced cybersecurity tests – known as Threat-Led Penetration Testing (TLPT).
This paper analyses the supply of TLPT services in Italy, assessing the sector's size and examining the structure of the market. Based on a voluntary-response questionnaire, we evaluate the key characteristics of the supply side, including service volumes, enabling factors, and barriers to the sector's development. The findings point to a dynamic and growing market, with a predominance of domestic providers. TLPT service provision is concentrated in the hands of a small number of players, and there is significant variability in the resources allocated to individual services, indicating a market offering that is not yet fully standardized. Regulatory frameworks coexist with proprietary methodologies. Among the main obstacles to market development are a shortage of skilled professionals and persistently high costs.

JEL Classification: G28, K24, L11, L86

Keywords: Cybersecurity, Cybersecurity services, Cyber resilience, Cyber risk, DORA, Financial sector, Market Analysis, Red Teaming, Testing, Third party provider, Threat Intelligence, TIBER-EU, TIBER-IT, TLPT.

Sintesi

Autorità e operatori sono da tempo impegnati nel rafforzare la cybersicurezza dell'intero settore finanziario. Il recente regolamento europeo sulla resilienza operativa digitale (DORA) introduce regole armonizzate tra cui l'obbligatorietà, per alcune istituzioni finanziarie, di svolgere i test avanzati di cybersicurezza – cc.dd. *Threat-Led Penetration Testing* (TLPT). L'indagine si propone di analizzare l'offerta di tali servizi in Italia, individuando la dimensione del settore e approfondendo la struttura del mercato. Attraverso un questionario su base volontaria, sono state valutate le caratteristiche dell'offerta tra cui i volumi, i fattori abilitanti e gli ostacoli allo sviluppo del settore. L'indagine ha evidenziato un mercato dinamico e in espansione, con una prevalenza di operatori italiani. L'erogazione dei servizi TLPT è concentrata. Emerge una forte variabilità nell'impiego delle risorse, evidenziando un'offerta non ancora standardizzata: l'adozione di framework di riferimento coesiste ancora con l'impiego di metodologie proprietarie. Tra gli ostacoli principali allo sviluppo del mercato emergono la carenza di personale qualificato e i costi che si mantengono a livelli elevati.

* Banca d'Italia, Directorate General for Payments and Market Infrastructures.

** Banca d'Italia, Directorate General for Payments and Market Infrastructures, until March 2025; currently at the ECB, Digital Euro Directorate.

*** Banca d'Italia, Directorate General for Financial Supervision and Regulation.

INDEX

1. INTRODUCTION[1]

The digitalization of the financial system, the development of business models based on online services offered to users, and the increasing complexity of the supply chain exacerbate exposure to IT risks, including those of a malicious nature. The financial sector is a prime target for cyber threats, due to several factors: the interconnections, the predominant technological content, the profitability of attacks, and the increasing speed of market operations and payment transactions (IMF, 2024).

Financial entities can leverage several tools to strengthen their cyber resilience, including advanced cybersecurity testing, in the form of Threat-Led Penetration Testing (TLPT). In 2018, the G7 defined TLPT as a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors (G7, 2018). It is based on two main phases: the collection of targeted and useful information on the entity being tested, known as "targeted threat intelligence", and the "attempt to compromise" known as "red teaming".[2]

TLPT is increasingly important for authorities to safeguard the stability, efficiency and business continuity of the financial system, both at the level of individual supervised institutions and at the sector as a whole. The European Central Bank (2018) defined a standardized methodology for TLPT, the Framework for Threat Intelligence-Based Ethical Red Teaming (TIBER-EU), recently updated.[3] It was adopted in Italy jointly by Banca d'Italia, Consob and Ivass in 2022 with the TIBER-IT methodology, which allowed tests to be conducted on a voluntary basis. From January 17, 2025, EU Regulation 2022/2554 on digital operational resilience (DORA) applies, which mandates this type of test for certain critical financial entities identified according to qualitative and quantitative criteria.

TIBER-EU mandates the use of external providers for Threat Intelligence (TI) services, while their use for Red Teaming (RT)[4] services is strongly recommended. These services, especially red teaming, need particular attention, considering that they involve access to confidential data and information of the financial entity and they play a fundamental role in the execution of the test. Although TIBER-EU establishes guidelines for providers, there are currently no accreditation schemes. Additionally, there is no in-depth knowledge of the maturity level of TLPT service offerings due to the scarcity of data and analyses related to this market.

The paper aims to analyze the structure of the Italian market for cybersecurity services, with a particular focus on threat intelligence and red teaming. A voluntary survey was addressed to companies based in Italy that are identified as providers of the services under examination.

After summarizing the main findings of the survey (§2), testing activities, regulatory context, and research on cybersecurity markets are described (§3). Then, survey results are reported in progressively detailed levels: characteristics of the selected companies and respondents (§4); characteristics of the cybersecurity service offerings, specifically testing (§5); detailed analysis of TLPT service offerings (§6). The last chapter contains final considerations (§7).

[1] We would like to express our sincere gratitude to Claudio Impenna, Giuseppe Grande, Caterina Beccarini and Antonino Fazio for their support and accurate, timely reviews, as well as to the colleagues from the Outsourcer and Third-Party Supervision Unit for their valuable comments. We also thank Barbara Massalin and Wojciech Zamiar for their significant contributions to the development of the questionnaire in the early stages of this work. A special thanks goes to Marco Bottone for his valuable advice on statistical and methodological aspects.

[2] Red teaming is a concept that has long been known in the military sector and other areas with a strong focus on security. It has only recently been introduced into the world of cybersecurity, where the most established practices were penetration testing and vulnerability assessment. In the field of cybersecurity for the financial sector threat-led red teaming gained prominence with the introduction of the CBEST framework by the Bank of England in 2013. This was followed by conceptually comparable frameworks in other jurisdictions, such as iCAST in Hong Kong (2016) and finally TIBER, born in the Netherlands and developed within the Eurosystem with TIBER-EU (2018).

[3] The update, from February 2025, incorporated lessons learned during several tests and was necessary for full alignment with the DORA regulatory technical standards. See ECB press release: https://www.ecb.europa.eu/press/intro/news/html/ecb.mipnews250211.en.html.

[4] In exceptional cases, it is possible to use internal testers.

Finally, three appendices present a methodological note, a description of the structure and the questionnaire, and a glossary of some technical terms.

2. MAIN FINDINGS

The survey was sent to 180 companies with a registered office in Italy that offer cybersecurity testing or related services. Due to missing specific ATECO[5] code for cybersecurity services, these companies were identified by combining various information sources (the methodology is described in Appendix A). Our reference population is distributed almost evenly among the various size classes (micro enterprises are 42, small ones are 43, medium ones are 52, large ones are 43). 71 of the 180 companies responded, with a response rate of 39.4 percent. No significant differences were found between the distribution of population and of respondents in terms of size class, geographical macro-area and company age.

Companies' characteristics. – Most of them belong to the software production and IT consulting sector (ATECO division 62), although there is a non-negligible share of respondents classified in other sectors. Companies focus their activities in Italy: over three-quarters declare that revenue is generated for over 90 percent at national level. Companies belonging to a foreign entity represent about 20 percent of respondents. The market structure is dynamic, with several young entities and companies that have changed corporate structure in recent years.

Supply of cybersecurity and testing services. – Almost all respondents claim to offer cybersecurity services. Based on the number of employees in specific business lines, it can be inferred that these services are provided by both specialized companies and general IT companies. For about a third of them, cybersecurity is the main activity (over three-quarters of revenue). Within cybersecurity services, the weight of testing services in terms of revenue decreases as the company size increases. Forty-four percent of those offering testing services declare that over 80 percent of their personnel are certified in this field. Four out of five respondents use artificial intelligence in the provision of cybersecurity services, especially in threat intelligence. Almost half of the companies offer services to five or more types of financial entities, with banks being the most frequent.

Supply of TLPT services. – About 70 percent of respondents offer or intend to offer TLPT services, with a higher percentage for larger companies. Looking at the number of services provided (threat intelligence and/or red teaming), the sector is concentrated (Gini index of 0.7). Based on the data collected, the supply of these services grew significantly in 2023, and two out of three respondents consider the market to be expanding. Some of the factors that would most favor market development are regulation, the adoption of public and/or public-private frameworks, the use of accreditation and/or certification schemes. For about 80 percent of companies, the limited availability of skilled personnel and the cost of the service represent the main obstacles. In the provision of TLPT services, there is a strong variability in the resources employed for a single service in terms of man-days. This highlights that there is not yet a fully standardized offering: TIBER-EU is the main used framework, but the use of proprietary methodologies, reported by almost a third of companies active in this area, is not negligible.

[5] ATECO is the classification of economic activities adopted by the Italian National Statistics Institute (Istat) for statistical purposes and represents the Italian version of the European NACE nomenclature. For this survey, reference was made to the ATECO 2007 classification, updated in 2022.

3. CONTEXT

The international context. – Cyber resilience[6] is a priority for many international organizations and financial authorities. The World Economic Forum highlighted in the annual risk report that cybersecurity issues are among the main perceived risks, both in short and long term (World Economic Forum, 2024). The financial system is particularly exposed to technological malfunctions (e.g. the recent Crowdstrike case) and represents a prime target for cyberattacks. The Single Supervisory Mechanism has also included cyber resilience among its supervisory priorities.[7]

Regarding financial market infrastructures (FMIs), in 2016 the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (jointly CPMI-IOSCO) defined the Guidance on cyber resilience for financial market infrastructures (CPMI-IOSCO, 2016) to integrate the Principles for Financial Market Infrastructures (PFMI) (CPMI-IOSCO, 2012) on cyber resilience. The Guidance has informed further work at national and international levels. It also includes specific indications for red team testing within the general testing principles, which represent one of the foundational components of the document (i.e. *overarching component*). In the same year, the G7 published the Fundamental Elements of Cybersecurity for the Financial Sector,[8] emphasizing the importance of testing as one of the main elements of security: monitoring.

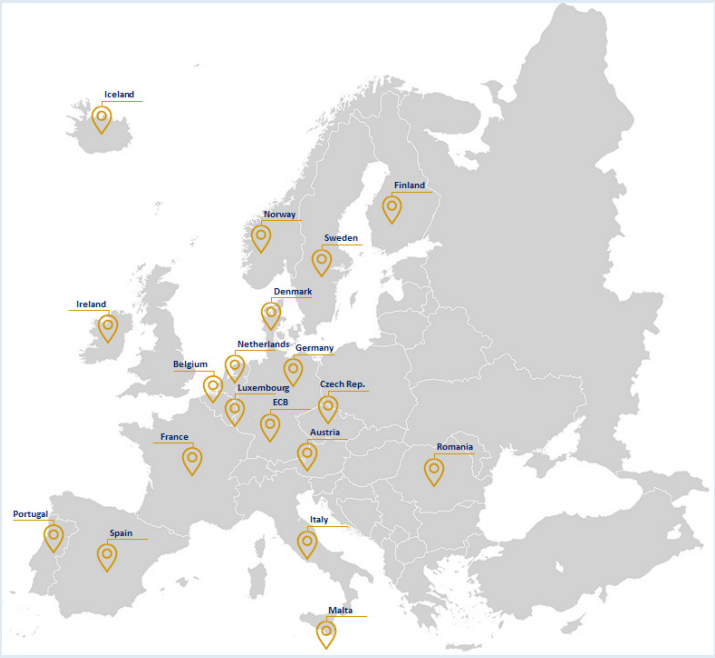
In 2018, the G7 published the Fundamental Elements for Threat-Led Penetration Testing,[9] providing financial entities with a guide for assessing their own resilience against malicious cyber incidents through simulated attacks, and authorities with a tool to promote and harmonize the use of TLPT in various jurisdictions, considering national specificities. In the same year, the G7 also published the Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector, which were revised in 2022[10] to address the development of the sector and the evolution of cyber threats with the indication to explicitly include requirements on the frequency and types of cyber resilience tests (e.g. penetration tests, TLPT) in contractual clauses between financial entities and third parties.

The European context. – In 2017, the ECB published the Eurosystem Cyber Resilience Strategy for FMIs[11] with the aim of improving the cyber resilience of the financial sector in the euro area and promoting collaboration among FMIs, their critical service providers, and authorities. The strategy, which has been recently updated,[12] includes several tools to verify the preparedness of financial entities, including the TIBER-EU, a reference model for conducting advanced cybersecurity tests harmonized at European level and adopted in 2018 (Figure 3.1).

[6] The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents. (FSB, *Cyber Lexicon*, 2023). In this paper, cyber resilience, cybersecurity and digital operational resilience represent the same concept.
[7] SSM Supervisory priorities and risk assessment for 2023-2025, Priority 2: *Addressing digitalisation challenges and strengthening management bodies' steering capabilities*.
[8] See G7 (2016).
[9] See G7 (2018).
[10] See G7 (2022).
[11] See ECB (2017).
[12] See ECB (2024).

Figure 3.1

Countries that have adopted the TIBER-EU framework



Source: analysis on data from the ECB and the TIBER Knowledge Center.

On the regulatory level, the European Union has recently adopted specific measures with the Digital Operational Resilience Act (DORA),[13] which establishes harmonized requirements for cyber risk management for many financial entities and introduces an oversight framework for critical IT service providers (so-called critical ICT third parties, cTPPs). Regarding testing, DORA requires financial entities, identified by national competent authorities, to conduct advanced tests based on TLPT at least every three years. The process and methodology that operators must use in these tests have been developed by European supervisory authorities in accordance with the TIBER-EU framework. Since the entry into force of DORA, TLPT has become a supervisory tool thus changing the current landscape represented by TIBER-XX,[14] usually based on a voluntary approach in most jurisdictions that have adopted the framework.

European cybersecurity legislation not strictly directed at the financial sector has also been recently updated with the NIS2 directive.[15] The Directive emphasizes the importance of security service providers to support their customers' activities in areas such as incident response, penetration testing and security audits. Moreover, providers could be targeted by cyber-attacks, and for this reason they should be selected accurately.

The Italian context. – In Italy, the regulatory framework has been consolidated starting from the transposition of the first version of the NIS directive.[16] The National Cybersecurity Perimeter was defined and the National Cybersecurity Agency (Agenzia per la Cybersicurezza Nazionale, ACN)[17] was established. For example, the minimum-security measures for operators included in the National Cybersecurity Perimeter require that penetration tests are regularly conducted, at least for critical functions. These acts are cross-sectoral and include a part of the financial sector within their scope.

[13] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

[14] TIBER-XX refers to one of the national implementations of TIBER-EU. For example, TIBER-IT, TIBER-DE, TIBER-NL.

[15] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

[16] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[17] Reference is made respectively to Decree-Law No 105/2019, converted by Law No 133/2019, and Legislative Decree No 82/2021.

In August 2022, Banca d'Italia, jointly with Consob and Ivass, adopted the TIBER-IT,[18] as a contextualization of TIBER-EU from a financial stability perspective (within the mandate of the three Authorities in terms of stability, efficiency, and competitiveness of the financial system, as well as those concerning the supervision of the regular functioning, reliability, and efficiency of the payment system). TIBER-IT is primarily aimed at critical financial entities for the Italian financial system among the following:

- financial market infrastructures;
- payment systems and supporting technological or network infrastructures;
- trading venues;
- banks;
- payment and electronic money institutions;
- financial intermediaries pursuant to Art. 106 of the Consolidated Banking Act (TUB);
- insurance companies;
- insurance intermediaries.

As of February 2025, Banca d'Italia supervised the execution of voluntary tests on 12 different legal entities, including banks, insurance companies and other operators active in the payments system (Scotti, 2025).

Market research in the field of cybersecurity

In recent years, many market analyses and research on cybersecurity have been published, mainly conducted by private entities and aimed at analyzing the demand for products and services (the target being companies as clients and not as providers), the investments made by companies, or the level of security perceived by the companies themselves.

The investigative survey presented in this work analyses the supply side, instead. Similar analyses have been conducted from a sectoral perspective, focusing on the products and services offered to a particular industry or sector (e.g. ENISA, 2022). Additionally, as highlighted by the EU Agency for Cybersecurity (ENISA), although cybersecurity has been considered in market analyses in the past, the customization and scope of cybersecurity analyses are still at a relatively low level of maturity (ENISA, 2023).

The context is also affected by the lack of specific identification of cybersecurity services in economic activity classifications, both at the national level by ISTAT and in the NACE[19] classification by Eurostat.

Regarding analyses of investments made by companies, according to the ENISA NIS Investments 2024 report,[20] in 2023 companies allocated 9 percent of IT investments to cybersecurity (an increase of 1.9 percentage points compared to the previous year) and 11.1 percent of full-time IT resources (FTE) (a decrease of 0.8 percentage points compared to 2022). The average IT spending of companies was 98.5 million euros (median 15 million); the banking sector was in a leading position, with an average spending of 222 million. The average cybersecurity investment of companies was 6.75 million, still led by the banking sector, with an average of 13.9 million. The FMI sector, although very small in terms of total spending, is the first in the ratio of FTEs dedicated to cybersecurity to total IT FTE (22.8 percent on average). From a general perspective, there is a strong variability in spending both at the intersectoral and intrasectoral level. Finally, in view of the application of DORA, the report shows that 84 percent of companies in the banking sector and the FMI sector will need to

[18] See Banca d'Italia, Consob and Ivass (2022).
[19] *Nomenclature statistique des activités économiques dans la Communauté européenne*.
[20] The report aims to provide regulators with evidence to assess the effectiveness of the current EU cybersecurity regulatory framework, particularly through data on the impact of NIS on cybersecurity investments and the overall maturity level of the entities to which NIS is addressed.

hire new specialized cybersecurity personnel. The skills gap is higher in the area of cybersecurity that includes testing ("cybersecurity operations").

At national level, the Interbank Convention for Automation (Convenzione Interbancaria Per l'Automazione, CIPA), in collaboration with the Italian Banking Association (Associazione Bancaria Italiana, ABI), periodically runs a survey of IT investments in the banking sector. Results of the 2023 survey (CIPA, 2024) show that the total average IT spending of responding banking groups is 290.6 million euros, of which 16.4 million on average allocated to cybersecurity, increasing of about 9 percent compared to 2022.

According to the Cybersecurity and Data Protection Observatory of the Politecnico di Milano (2024), the cybersecurity market in Italy has grown steadily in recent years (16 percent in 2023 compared to the previous year, reaching an estimated value of 2,146 million). Among the main growth factors there are actions to comply with new regulations, including DORA.

This trend is also confirmed by data collected by the Italian industry association for ICT companies (Anitec-Assinform, 2024). Cybersecurity investments by Italian companies are estimated at around 1,790 million, with an increase of 12.2 percent compared to 2022. The largest increase was recorded in the healthcare and public administration sectors, while in absolute value the banks invest more than other sectors, in line with ENISA's findings. Analyzing spending for each offered service, consulting activities, which include services such as testing, are the segment with the lowest spending (96.6 million, up 11.8 percent compared to 2022). The report has predicted significant growth for the entire cybersecurity sector in 2024, driven by regulations requiring the adoption of specific measures in an increasingly wide range of sectors.

Italian small and medium-sized enterprises (SMEs) are lagging behind in cybersecurity investments, with wide room for development. The Cyber Index PMI 2023 report[21] shows a correlation between company size and their level of maturity. 83 percent of respondent SMEs use digital tools to support their business processes, but in almost half of the cases there is not a clear strategy that involves shareholders and/or senior management, and no dedicated funds are allocated to protect IT systems.

In 2021, following the adoption of the Cybersecurity Act,[22] ENISA launched a series of activities in the field of cybersecurity market research with the aim of analyzing the supply side. In April 2022, the Cybersecurity Market Analysis Framework (ECSMAF) was published and recently updated (ENISA, 2023). It represents a European standard that can be used to define, customize and conduct market analyses.

The survey presented in this work leveraged the ENISA's methodology and considered its indications in various steps.

[21] Developed as part of activities under an agreement between the General Confederation of Italian Industry (Confindustria), ACN and the insurance company Assicurazioni Generali.

[22] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

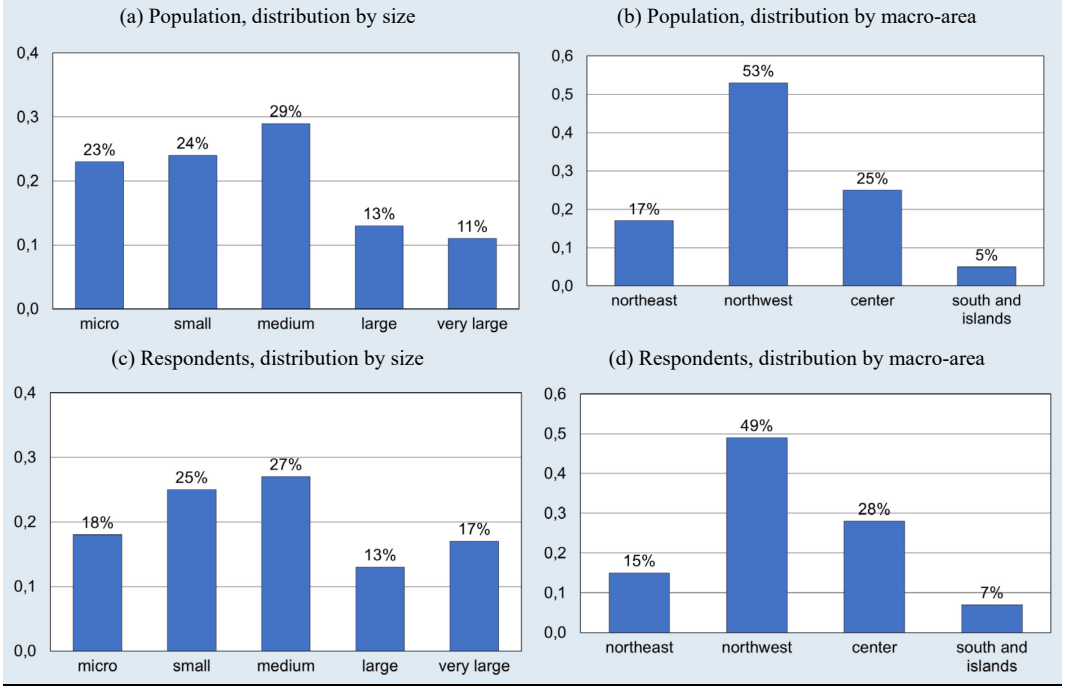
4. CHARACTERISTICS OF RESPONDING COMPANIES

Selected companies. – A reference universe of 180 companies was identified, built selecting IT companies that provide cybersecurity testing or related services and have a legal headquarter in Italy. The selection process was necessary due to the absence of a clear and official taxonomy of activities in the sector of interest.[23] This process provided an indication of the sector size, although the list of identified companies should not be considered exhaustive due to the dynamic nature of this market segment.[24] The Appendix A includes methodological details and criteria adopted for constructing the reference universe.

Regarding the size, companies were classified according to the 2003/361/EC recommendation,[25] with the addition of the "very large" category for companies with a revenue greater than 100 million euros.[26] The distribution of the 180 companies by size differs from that of companies belonging to the closest ATECO section:[27] they are evenly distributed among the various size categories (Figure 4.1a). Considering the distribution by geographical macro-area, it emerges that companies are predominantly (70 percent) concentrated in northern Italy, with a high concentration in the northwest (over half of the population, Figure 4.1b).

Figure 4.1

Comparison between population and respondent distributions
Population = 180 companies; Respondents = 71 companies;
(percentage values)



Source: ORBIS data elaborations.

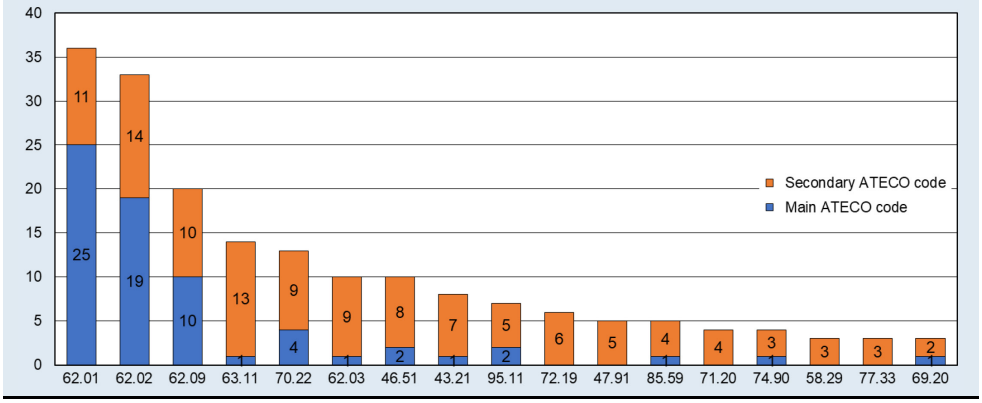
[23] For example, there is no ATECO code that specifically identifies cybersecurity testing services.
[24] During the implementation phase of the survey, which lasted about six months, five companies changed corporate structure.
[25] The European recommendation distinguishes between “micro”, “small” and “medium-sized” enterprises by number of employees, assets and revenue. The remaining enterprises form the “large” category. Master data and economic information was collected from various sources (Italian Business Register, the National Institute for Social Security – INPS, Orbis), with reference to data as of the end of 2023.
[26] These companies have specificities and form a separated cluster from the “large” category. Their average revenue far exceeds that of other large companies, at a ratio of 10 to 1.
[27] Section “J - Information and communication services” and class “62.01 - Computer programming activities”.

Responding companies. – 71 companies responded to the questionnaire, with a response rate of 39.4 percent.[28] In terms of size and geographical macro-area, there are no significant differences between the frequencies of the distribution of responding companies and distribution of reference population (Figure 4.1c and Figure 4.1d). Other analyzed variables (e.g. company age) do not show significantly different distributions.

ATECO codes of responding companies. – The absence of a specific ATECO code for cybersecurity services affected the process of defining the reference universe. Among the respondents, there is a high representation of companies belonging to division 62 ("Software production, IT consulting, and related activities") of section J ("Information and communication services"), distributed in all the four classes provided (Figure 4.2 and Table 4.1).[29] Twenty-two percent of respondents do not belong to division 62,[30] with 70.22[31] as the prevailing code.

Figure 4.2

Distribution of ATECO codes of responding companies
(units)



Source: elaborations on InfoCamere and Orbis data.
Notes: Each company has a single primary ATECO code and may have one or more secondary codes. The chart reports primary and secondary ATECO codes with a total occurrence of three or more.

[28] The analyses presented in the paper do not always refer to the 71 respondents, considering that not all questions were mandatory, and outliers were removed in some cases. Specifically: i) two respondents for question 9 of the TLPT section, "Indicate the number of Generic Threat Intelligence reports (GTIs) drafted in 2022 and 2023"; ii) one respondent for questions 7 and 8 of the same section, respectively, "Indicate the number of TLPT tests for which services were provided in 2022 and 2023" and "Indicate the percentage of TLPT tests for which services were offered to the financial sector in 2022 and 2023."

[29] Classes 62.01 – "Computer programming activities", 62.02 – "Computer consultancy activities", 62.03 – "Computer facilities management activities" and 62.09 – "Other information technology and computer service activities".

[30] Companies carrying out activities other than their predominant or primary activities may have one or more secondary ATECO codes.

[31] Code 70.22 relates to the activities "Business and other management consultancy activities", found in section M "Professional, scientific and technical activities".

Table 4.1

ATECO Code	Description	Primary and secondary ATECO occurrences
62.01	Computer programming activities	36
62.02	Computer consultancy activities	33
62.09	Other information technology and computer service activities	20
63.11	Data processing, hosting and related activities	14
70.22	Business and other management consultancy activities	13
62.03	Computer facilities management activities	10
46.51	Wholesale of computers, computer peripheral equipment and software	10
43.21	Electrical installation	8
95.11	Repair of computers and peripheral equipment	7
72.19	Other research and experimental development on natural sciences and engineering	6
47.91	Retail sale via mail order houses or via Internet	5
85.59	Other education n.e.c.	5
71.20	Technical testing and analysis	4
74.90	Other professional, scientific and technical activities n.e.c.	4
58.29	Other software publishing	3
77.33	Rental and leasing of office machinery and equipment (including computers)	3
69.20	Accounting, bookkeeping and auditing activities; tax consultancy	3

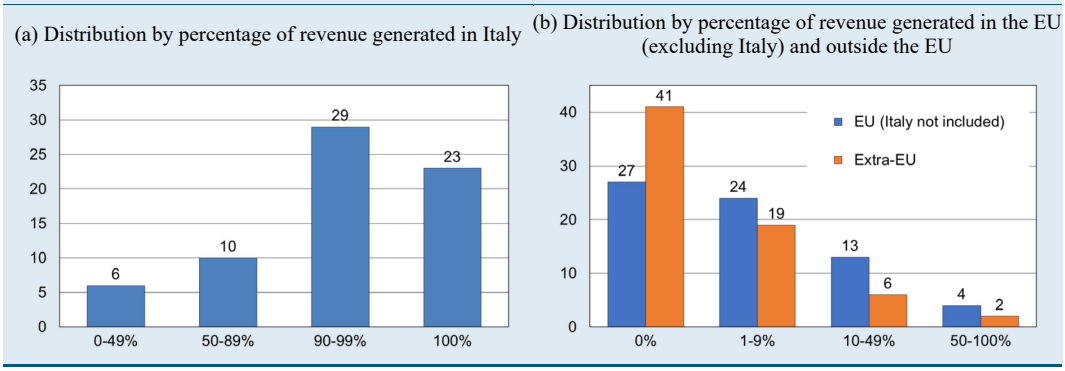
Corporate Structure. – Considering the central role that cybersecurity services play and the sensitivity of the handled data, they represent a fundamental component of Italian technological autonomy, which is one of the challenges to be addressed in the digital sector, both nationally and at the European level, according to the National Cybersecurity Strategy 2022-2026 (ACN, 2022b).

56 percent of the companies responding to the questionnaire are part of a corporate group, and more than half of these groups are based in Italy. About 20 percent of respondents are part of a foreign entity. In the Italian cybersecurity market, there is a predominance of domestic operators.

Revenue. – In the revenue analysis, three geographical areas are considered: i) Italy; ii) Europe, excluding Italy; iii) non-European countries (Figure 4.3). 33.8 percent of the companies generate all their revenue within Italy, another 42.6 percent generate between 90 and 100 percent. Therefore, companies operating in the Italian cybersecurity and testing services market derive most of their revenue from the national market. Only six companies have a share of Italian revenue below 50 percent. 60 percent of the responding companies do not operate in countries outside the Union; another 28 percent generate less than 10 percent of their revenue outside the EU. Companies that generate more than half of their revenue within the EU (excluding Italy) or outside the continent are a marginal component (about 9 percent of respondents).

Figure 4.3

Distribution of enterprises by revenue geographic area (1)
(units)

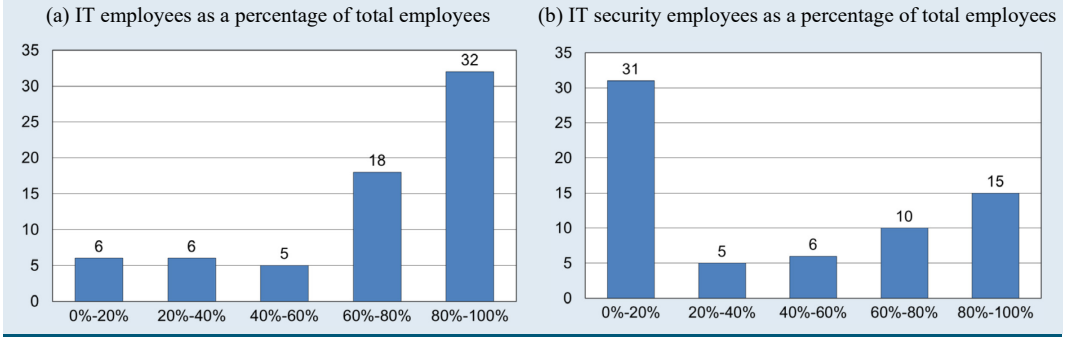


Source: elaborations based on data from 68 respondents.
(1) For companies belonging to groups, the distribution by geographic area refers to company revenue, not the corporate group.

IT Employees. – 74 percent of respondents report that most of their employees (more than 60 percent) works in the IT sector. About half of the companies (48 percent) declare that they employ almost all their staff in IT services (between 80 and 100 percent); only 9 percent of respondents declare that they have less than 20 percent of employees working in IT (Figure 4.4a). Conversely, focusing on cybersecurity services, slightly less than half of respondents (46 percent) declare that they have less than 20 percent of employees dedicated to such services, while this utilization reaches the majority for 37 percent of companies (Figure 4.4b). Considering the number of employees as a proxy for a company specialization in a specific sector or line of business, it can be inferred that in the reference universe, cybersecurity services are provided by both specialized companies and general IT companies.

Figure 4.4

Distribution of enterprises by the ratio of specialized employees to total employees
(units)



Source: elaborations based on data from 67 respondents.

5. SUPPLY OF CYBERSECURITY AND TESTING SERVICES

Cybersecurity Services

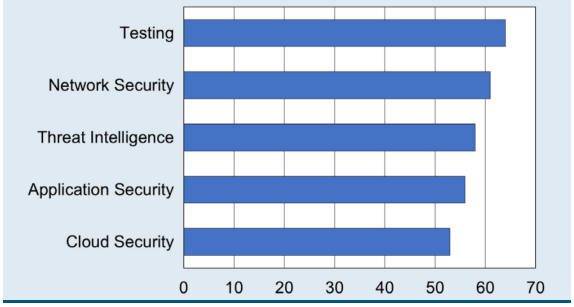
Almost all respondents (96 percent) offer cybersecurity services.[32] The main service offered is testing (see below for details), followed by others closely related (Figure 5.1). This confirms the adequacy of the process used to construct the survey universe.

In particular, large and very large companies declare that they offer all the aforementioned services, demonstrating a diversified business in the field of cybersecurity.

Use of Artificial Intelligence. – Four out of five companies use artificial intelligence-based technologies.[33] This data ranges from 60 percent in the south and islands macro-area to 85 percent in the northwest. Threat intelligence is the service that applies most frequently AI-based solutions.

Figure 5.1

The five most offered cybersecurity services
(units)

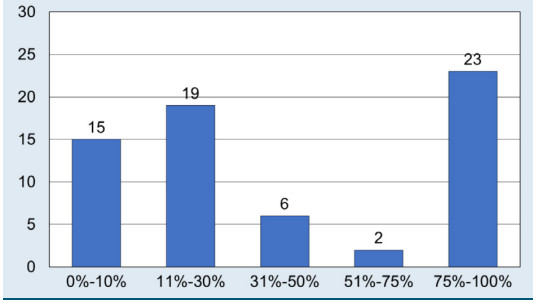


Source: elaborations based on data from 68 respondents.

Revenue from Cybersecurity Services. – For 35 percent of the responding companies, cybersecurity services account for over 75 percent of total revenue (Figure 5.2). The 23 companies in this range, which are therefore the most specialized, offer the entire range of cybersecurity services considered in the survey. Almost two out of three are micro and small enterprises, the remaining are medium and large enterprises (very large enterprises are not represented). Therefore, even if large companies offer more types of cybersecurity services, they generate a lower share of revenue in this market.

Figure 5.2

Distribution of companies by revenue ranges related to cybersecurity services
(units)



Source: elaborations based on data from 65 respondents.

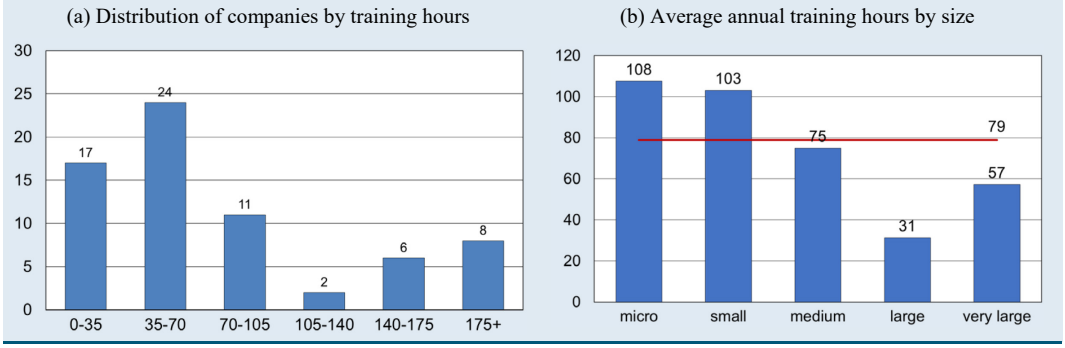
Training in Cybersecurity. – On average, the respondents allocate 79 hours of annual training in cybersecurity per employee (Figure 5.3a); the data is influenced by some companies that are particularly active in training, indeed 60 percent of respondents allocate less than 70 hours. The companies that invest the most in training are the smaller ones (Figure 5.3b); among large and very large companies, only one dedicates more than 175 hours of annual training. The average training hours increase with the percentage of IT employees involved in cybersecurity services; for example, the most specialized companies (with over 80 percent of IT employees dedicated to cybersecurity) invest an average of 126 annual training hours per employee, while the less specialized ones (with less than 20 percent) invest an average of 57 hours.

[32] The following services were considered: Application Security; Cloud Security; Consumer Security; Data Security; ICS and Critical Infrastructure Security; Identity and Access Management; Integrated Risk Management; IoT and Embedded Security; Mobile Security; Network Security; Testing; Threat Intelligence; other.

[33] This data aligns with the adoption trends of these technologies in the banking sector, where the use of generative AI in the areas of Documents-Content and Governance, Security, Audit and Compliance is expected to exceed 90 percent (CIPA, 2023).

Figure 5.3

Training in cybersecurity in 2023
(number of companies and average annual training hours per employee)

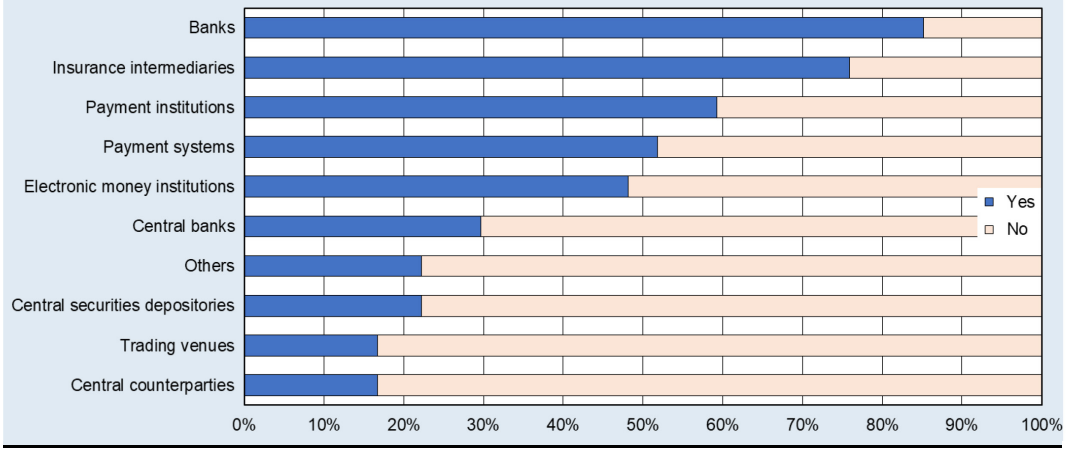


Source: elaborations based on data from 65 respondents. In the figure (b) the red line represents the average of training hours.

Provision of Cybersecurity Services. – 76 percent of respondents provide cybersecurity services to the financial sector. The percentage rises to 94 percent for companies in the northwest. Additionally, all very large companies offer services to the sector. The most frequent clients are, in descending order: banks, insurance intermediaries, and payment institutions (Figure 5.4). Almost half of the respondents (48 percent) that offer cybersecurity services to the financial sector provide services to five or more types of operators.

Figure 5.4

Main clients of cybersecurity services within the financial sector
(percentage values)



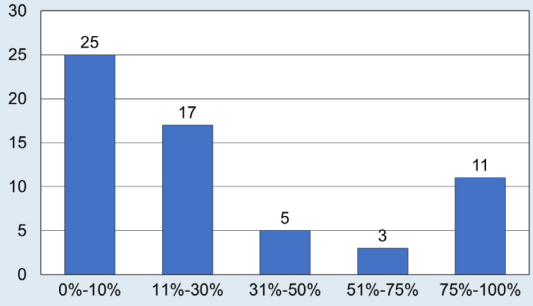
Source: elaborations based on data from 54 respondents.

Testing Services

93 percent of respondents offer cybersecurity testing services. Generally, as the company size increases, the percentage of revenue related to testing decreases in relation to the total revenue from cybersecurity services. This share is over 30 percent for only one of the "large" companies. Seven of the eleven companies that derive over 75 percent of their revenue from testing services (Figure 5.5) are micro-enterprises. As the age of the companies increases, the percentage of revenue from testing decreases, but among the 11 most specialized companies, there are both newly established ones (less than 5 years) and others that have been operating in the sector for over 20 years.

Figure 5.5

Distribution of companies by percentage of revenue from testing services relative to total revenue from cybersecurity services
(units)



Source: elaborations based on data from 61 respondents.

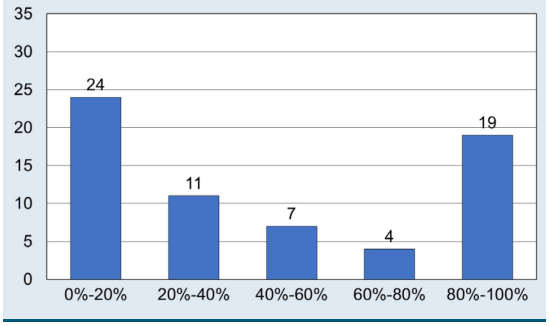
Furthermore, excluding companies with a testing revenue share of less than 10 percent (Figure 5.5, first column), nearly 90 percent of companies offer or plan to offer TLPT services to the financial sector.

A similar distribution is found in the weight of testing services in terms of the percentage of employees engaged in cybersecurity services (Figure 5.6); a significant portion of companies (29 percent) specialize in testing activities, with at least four out of five cybersecurity employees assigned to this area.

The responses do not reveal a dependence on a single client: for companies offering testing services, the most relevant client accounts for an average of 16 percent of testing revenue and in 15 percent of cases the main client contributes more than 30 percent of the revenue.

Figure 5.6

Distribution of companies by employees providing testing services as a percentage of total cybersecurity service employees
(units)

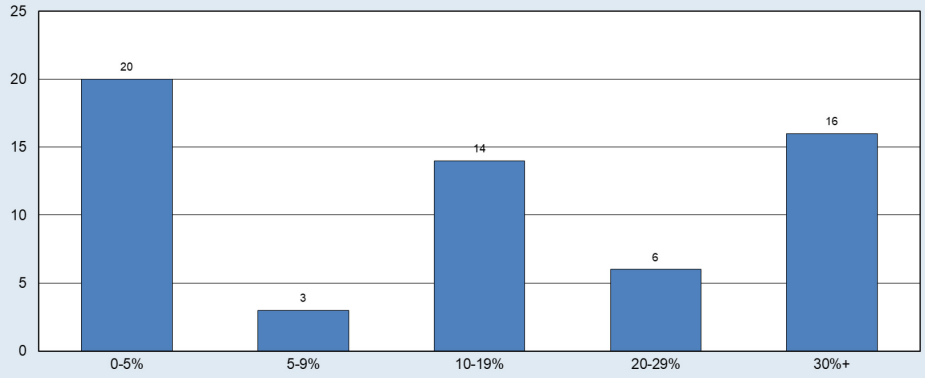


Source: elaborations based on data from 65 respondents.

Revenue Comparison: 2023 vs 2022. – For about a third of respondents, the revenue from testing services in 2023 has grown by no more than 5 percent, for 40 percent between 5 and 29 percent, and for the remaining part by over 30 percent (Figure 5.7). Overall, the responses indicate that the sector is experiencing a growth phase in terms of revenue, positively influenced by the provision of TLPT services. Among the companies with the highest growth (over 20 percent), 76 percent declare that they offer these services.

Figure 5.7

Distribution of companies by percentage of testing revenue growth 2023 vs 2022
(units)

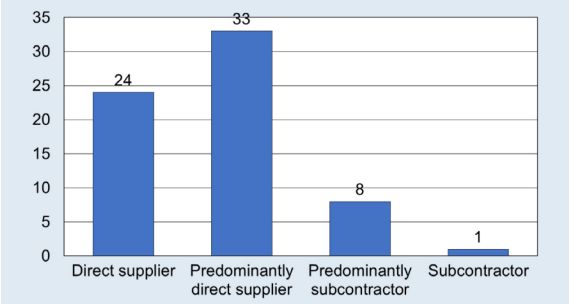


Source: elaborations based on data from 59 respondents.

Role of Supplier in Testing Services. – Testing services are predominantly offered directly (Figure 5.8). Less than ten respondents operate mainly or entirely as subcontractors; these are mainly smaller companies, of which only two offer TLPT services.

Figure 5.8

Distribution of companies by approaches to delivering testing services
(units)

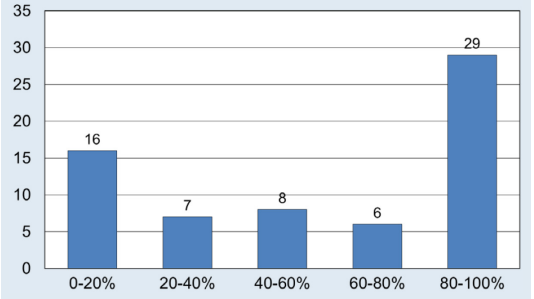


Source: elaborations based on data from 66 respondents.

Certified Personnel. – 44 percent of companies offering testing services have over 80 percent of their personnel certified in cybersecurity. In 24 percent of companies, certified personnel are less than 20 percent (Figure 5.9). Companies with the highest percentages of certified personnel generally have been operating for a longer time (16-20 years or over 20 years).

Figure 5.9

Distribution of companies by percentage of certified employees
(units)



Source: elaborations based on data from 66 respondents.

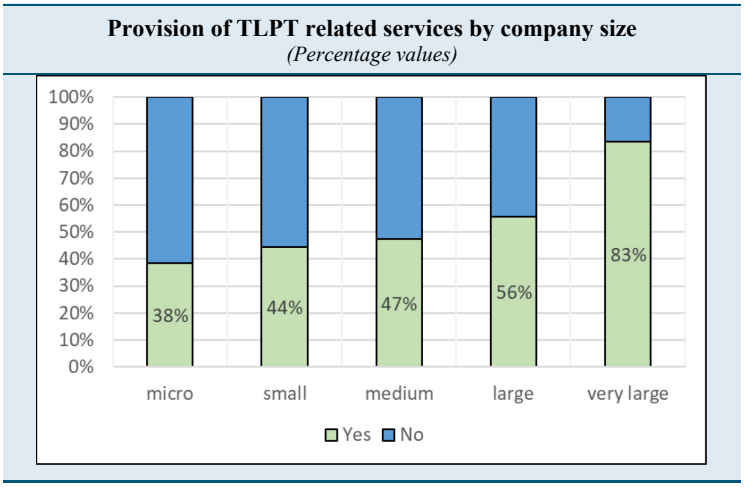
The most frequently reported certifications[34] by respondents are in the field of testing and attack simulations, in particular: Certified Ethical Hacker (60 percent), Offensive Security Certified Professional (48 percent), and eLearnSecurity Certified Professional Penetration Tester (39 percent). Generic cybersecurity certifications, such as Certified Information Systems Security Professional (28 percent), are also present. Among those not listed, companies indicated Certified Information Security Manager, CompTIA Security+, Certified Red Team Professional and eLearnSecurity Web App Pen Tester eXtreme.

[34] The questionnaire provided the list of certifications included (now removed) in the TIBER-EU Services Procurement Guidelines, with the option to indicate others. This list is used as a non-exhaustive reference in the procurement process for a TIBER-EU test.

6. PROVISION OF TLPT SERVICES

Who provides TLPT services? – 52 percent of the respondents provide TLPT services, which include one or both threat intelligence (targeted and/or generic) and red teaming services.[35] This percentage increases with the size of the company (Figure 6.1). However, the presence of micro and small companies is not negligible. An additional 20 percent of respondents plan to expand their services to include those related to TLPT. The provision of these services is not conditioned by the sector of the client companies (financial and non-financial), making these services transversal. The availability of a large pool of potential clients from different economic sectors could foster further market expansion, especially considering new cross-sector regulations. Additionally, it should be considered that the TIBER-EU framework and its national implementations, although born within the financial sector, are agnostic to the sector of application and have already been contextualized in some jurisdictions for other sectors (e.g. utilities).

Figure 6.1



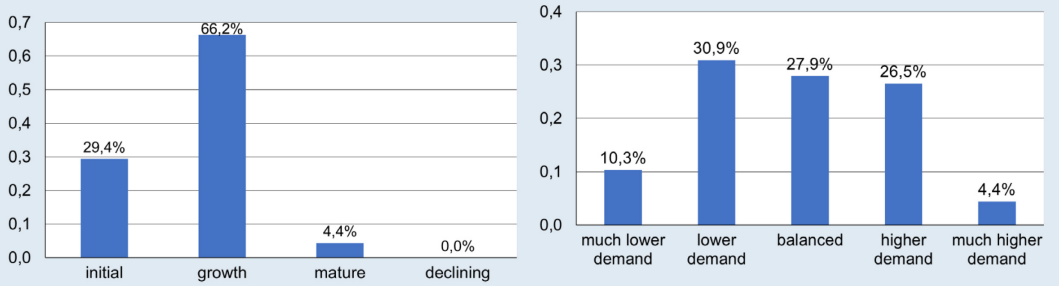
Source: elaborations based on data from 71 respondents.

Opinions on the TLPT sector. – Almost all respondents believe that the market is in an initial or growth phase (Figure 6.2a). For 27.9 percent, supply and demand are balanced (Figure 6.2b); for the rest, perceptions of excess supply prevail over demand (41.2 vs. 30.9 percent, respectively). Even if the analysis is limited to companies that claim to provide these services, results are the same.

[35] See Appendix C - Glossary for definitions.

Figure 6.2

TLPT sector growth phase
(Percentage values)



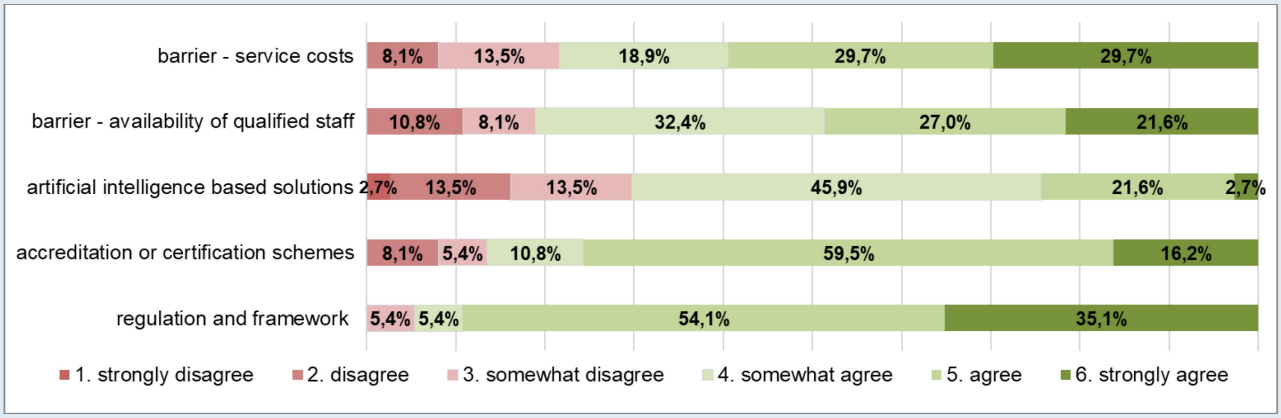
Source: elaborations based on data from 68 respondents.

To capture respondents' opinions on the main trends in the TLPT market, they were asked for the level of agreement or disagreement with some predefined statements, according to a six-level *Likert* scale.[36] Results (Figure 6.3) show that, according to companies, the main factors that would promote market development are regulation, adoption of public and/or public-private frameworks (about 95 percent of companies agree with this statement) and use of accreditation and/or certification schemes for companies offering these services (86.5 percent of companies responded positively). These results are in line with the evidence collected by ENISA in a demand-side analysis of cybersecurity services (ENISA, 2024).[37]

Among the main obstacles to market development, 80 percent of responding companies include the cost of service relative to customers' budgets and the limited availability of qualified personnel; the latter is a well-known issue and one of the enabling factors of the national cybersecurity strategy, for which various measures are planned in the relevant implementation plan (ACN, 2022a).

Figure 6.3

Main barriers and drivers for TLPT market growth
(Percentage value)



Source: elaborations based on data from 68 respondents.

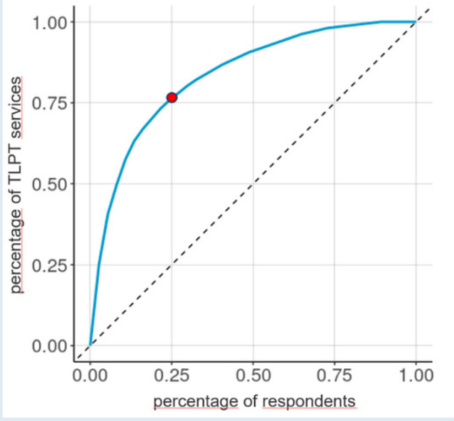
[36] 1. Strongly disagree; 2. Mostly disagree; 3. Slightly disagree; 4. Slightly agree; 5. Agree; 6. Strongly agree.

[37] Indeed, in the ENISA analysis 86 percent of respondents stated that a European cybersecurity certification would be beneficial for their sector. Moreover, this opinion is particularly strong in the banking sector, where 99 percent of the organizations surveyed by ENISA acknowledged its importance.

Figures about provision of TLPT services. – The 37 companies that provide TLPT services report having delivered 318 TI or RT services in 2023, a significant increase compared to 2022, when they delivered 198. According to 2023 data, the sector would be highly concentrated: a quarter of companies providing about three-quarters of all TLPT services provided by respondents. This is shown by the Lorenz curve (Figure 6.4) and the Gini index, which for services offered in 2022 and 2023 is 0.7.[38]

Figure 6.4

TLPT market concentration in 2023 (1)
(Percentage values)



Source: elaborations based on data from 37 respondents.
(1) The light blue line is the Lorenz curve, which represents the share of TLPT services offered relative to the share of respondents; the red dot indicates the concentration level described in the text.

The financial sector is an important client for TLPT services. Almost a quarter of tests in 2022 and over 30 percent in 2023 were provided to financial entities. A key factor in the market growth may have been the regulatory push. Additionally, the main reference framework for companies in providing TLPT services is the TIBER-EU: about 80 percent of companies declare that they offer TLPT services for TIBER-XX. However, the use of proprietary methodologies, reported by 32 percent of respondents active in this area, is not negligible. Among the companies offering TLPT services, only five declare that they are certified according to accreditation schemes provided for such services, such as CBEST. It should be noted that the TIBER-EU currently does not provide for an accreditation and certification scheme. 51 percent of companies adhere to formal codes of conduct and/or ethics specific to TLPT activities.

In general, all TLPT-related services experienced a strong growth in 2023, particularly the red teaming services (Figure 6.5a). In terms of resources employed for a single service, there is a significant discrepancy between threat intelligence and red teaming: an average of 37 man-days for the former, compared to 69 for the latter (Figure 6.5b). Considering the size class of the company, responses also highlight an uneven resources allocation, probably due to the non-standardized delivery of TLPTs among companies (with different approaches and interpretations of TLPT activities and objectives). It should be noted that companies that declare providing TLPT services according to the TIBER-XX framework show higher average resource utilization levels: 43 man-days for TI and 82 for RT.

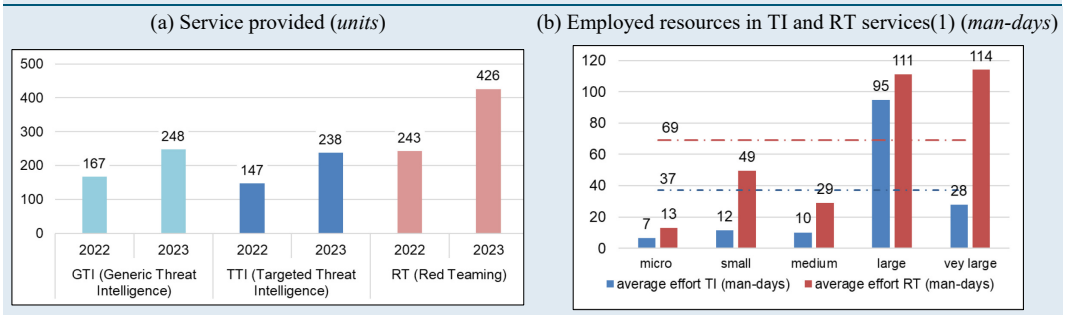
In terms of experience of the personnel leading the execution of the two main TLPT-related services, a high percentage of companies would meet the requirement for the RT and TI Manager included in both the TIBER-EU Guidance for Service Provider Procurement and the DORA RTS

[38] The Lorenz curve is typically used to represent the distribution of inequalities within a population. The Gini index provides the degree of inequality in the distribution of a variable and is also used to measure the degree of concentration of a phenomenon. The index varies between 0 (perfect equality) and 1 (maximum inequality); a concentration is considered medium-high when its value is greater than 0.5.

(*Regulatory Technical Standards*) on TLPT (i.e. five years). The years of experience of RT and TI Managers exceed this threshold in 82 and 57 percent of cases, respectively.

Figure 6.5

TLPT – Numbers and employed resources in services provision



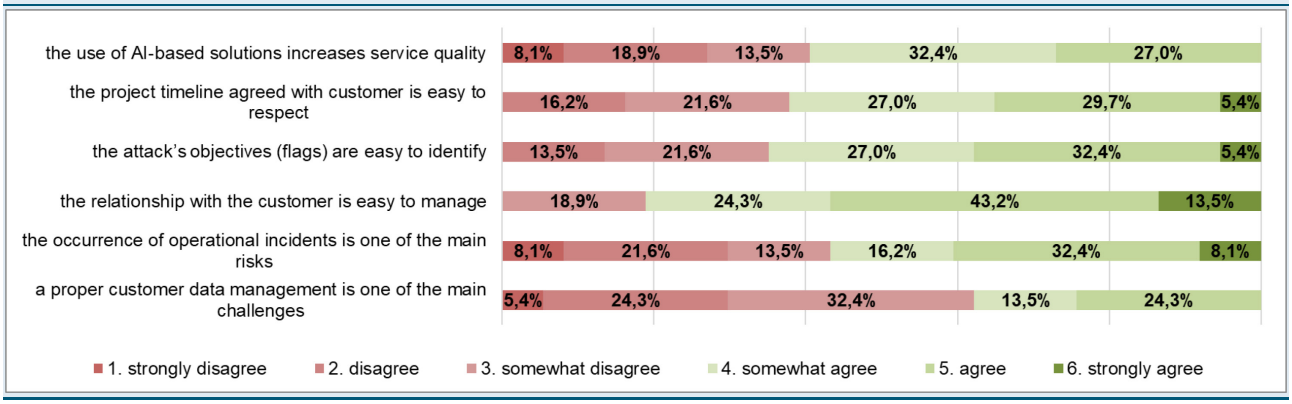
Source: elaborations based on data from 37 respondents.
(1) Blue and red horizontal lines indicate respectively average number of man-days for threat intelligence and red teaming services.

Using the *Likert* scale, companies' opinions on some detailed elements of TLPT activities were evaluated (Figure 6.6). The relationship with the client is the easiest topic to manage (86.5 percent). The processing of client data, often a sensible issue especially in red teaming, does not appear to be a significant difficulty in service delivery, too. An analysis of the corporate structure of responding companies that perform *red teaming* activities shows that their ownership is mostly attributable to an Italian entity. The parent company is a foreign entity in about a third of cases.[39] There are no polarized opinions on the perception of the risk of operational incidents occurring during activities: only a slight majority of the respondents (56.7 percent) consider it to be one of the main risks. This could be due to the requirement of a pre-test risk analysis and during the activity itself, which is required by various methodological frameworks. Furthermore, to date, no serious incidents have been reported from performing TLPT according to the TIBER-EU framework, or one of its national implementations.

Notwithstanding the growing attention and recent developments in artificial intelligence, respondents' opinions do not show polarized views regarding benefits that AI-based solutions can provide to the services in scope.

Figure 6.6

TLPT – Service delivery details
(Percentage values)



Source: elaborations based on data from 37 respondents.

[39] The analysis of group structures is based on Orbis data.

7. CONCLUSIONS

The increasing weight of cyber risks in the financial sector has led authorities to strengthen actions aimed at enhancing the digital operational resilience of individual operators and the whole system. The recent adoption of the DORA Regulation is a milestone; indeed, among other obligations, it requires certain types of financial entities to conduct TLPT. Technological and regulatory developments increase the role of ICT companies, particularly cybersecurity service providers.

The survey presented in this work analyses the supply of these services in Italy, standing out from other available analyses that focus on the demand side. Based on the current sectoral classifications of economic activities, a first result is that companies offering cybersecurity services cannot be directly linked to specific economic sectors. Therefore, to identify the market from the supply side, this survey combined various information sources, such as sector association lists of members, commercial databases, data available to Banca d'Italia (such as the Invind questionnaire), and other publicly available information on individual companies. This resulted in a reference universe of 180 companies. The questionnaire was sent to all, and 71 responded, with a response rate of about 40 percent.

Results show the rapid change in this market in Italy. Indeed, 15 percent of respondent companies were established or changed their corporate structure in the last five years, and five companies were subject to mergers or acquisitions during the six months of the survey. Additionally, half of the those that declared not to provide the services in scope plan to do so in the near future.

The market is predominantly composed of domestic operators, both in terms of corporate structure and with reference to country of revenue generation. One in five companies is part of a foreign entity.

The business strategies are varied. Some companies offer a wide range of ICT services, while others offer only specific types. Regarding testing activities, for almost two out of three companies, they generate less than 30 percent of revenue, but there is a significant portion of respondents (17 percent) that are highly specialized, with a revenue share of over 75 percent.

As for TLPT, they currently represent a smaller portion of testing activities, and the sector is concentrated: in 2023, a quarter of active companies provided three-quarters of all TLPT services provided by respondents.

The data also show a high variability in resource utilization and, as a consequence, in the way red teaming and threat intelligence services are provided. These differences could be linked to several factors: i) the absence of a standardized and shared model, at least until the recent publication of TIBER-IT for the financial sector; ii) the lack of a national or European accreditation or certification scheme; iii) the need to customize the service for the client; iv) the heterogeneity of demand.

The significant differentiation of client needs and availability of economic resources, as well as the technical skills required for these activities, are reflected in the resources' allocation for the execution of TLPTs (in terms of man-days). In some cases, this may indicate that the activities are carried out similarly to a traditional penetration test, which generally requires fewer resources, being much more limited in both the scope to be tested and the duration; moreover, a traditional penetration test does not involve the use of threat intelligence.

With regulatory developments, at European and national levels, authorities - financial and non-financial - are promoting reference models for the TLPT market, which could lead to greater homogeneity in the provision of services. For example, about 80 percent of companies that provide TLPT services declare that they follow the TIBER-EU framework. Most companies agree that the introduction of accreditation and certification schemes would facilitate market growth and hope for their introduction. The possibility of developing such schemes is also present in DORA and is under the attention of the ECB TIBER Knowledge Center. More generally, the European regulator, under the Cyber Security Act, is evaluating the certification of managed security services, which include

penetration tests, too. This would promote greater homogeneity in both supply and demand, with effects on market competitiveness.

REFERENCES

ACN, Agenzia per la Cybersicurezza Nazionale (2022a), *Piano di implementazione - Strategia Nazionale di Cybersicurezza 2022-2026,* May 2022.

ACN, Agenzia per la Cybersicurezza Nazionale (2022b), *Strategia Nazionale di Cybersicurezza 2022-2026,* May 2022.

Anitec-Assinform (2024), *Il digitale in Italia 2024 - Mercati, dinamiche e policy*.

Banca d'Italia, Consob and Ivass (2022), *TIBER-IT National Guidance: Threat Intelligence Based Ethical Red-Teaming – Italy*, August 2022.

ECB, European Central Bank (2017), *Cyber resilience and financial market infrastructures*, March 2017.

ECB, European Central Bank (2018), *TIBER-EU FRAMEWORK*, May 2018.

ECB, European Central Bank (2024), *Eurosystem Cyber Resilience Strategy*, October 2024.

CIPA, Convenzione Interbancaria Per l'Automazione (2024), *Rilevazione sull'IT nel settore bancario italiano - Profili economici e organizzativi - year 2023*.

CPMI-IOSCO, Committee on Payments and Market Infrastructures - International Organization of Securities Commissions (2016), *Guidance on cyber resilience for financial market infrastructure*, June 2016.

CPSS-IOSCO, Committee on Payment and Settlement Systems - International Organization of Securities Commissions (2012), *Principles for financial market infrastructures*, April 2012.

ENISA, European Union Agency for Cybersecurity (2022), *EU Cybersecurity Market Analysis - IoT in Distribution Grids*, April 2022.

ENISA, European Union Agency for Cybersecurity (2023), *Cybersecurity market analysis framework V2.0*, March 2023.

ENISA, European Union Agency for Cybersecurity (2024), *NIS investments 2024*, November 2024.

IMF, International Monetary Fund (2024), *Global financial stability report*, April 2024.
G7 (2016), *G7 Fundamental elements of cybersecurity for the financial sector*, October 2016.

G7 (2018), *G7 Fundamental elements for threat-led penetration testing*, October 2018.

G7 (2022), *G7 Fundamental elements for third party cyber risk management in the financial sector*, October 2022.

Politecnico di Milano (2024), *Lo scenario della cybersicurezza in Italia nel 2023*.

Scotti C. (2025), *I test di tipo TLPT: dalle esperienze del TIBER-IT alle regole di DORA,* speech at the Banca d'Italia conference: *"THREAT-LED PENETRATION TESTING: from TIBER-IT experiences to DORA's TLPT rules",* February 2025.

World Economic Forum (2024), *Global risks report*, January 2024.

APPENDIX A – METHODOLOGICAL NOTE

This note presents the main methodological characteristics of this exploratory survey. It describes the criteria for identifying the reference universe and its characteristics, as well as the main information requested through a questionnaire (see Appendix B).

Composition of the reference universe

The reference universe of the survey comprises active companies, based in Italy and operating in the ICT sector, that offer cybersecurity testing or related services, with the exception of: i) partnerships (which are assumed to be less likely to offer complex services such as TLPT); ii) companies referable to financial entities.

A tailored approach was used for the process of building the reference universe, due to the absence of specific selection criteria in the standard classifications of economic activities. Indeed, considering the ATECO classification, the market under analysis is presumably included in section J - "Information and communication services", which counts about 40,000 companies, but is not directly associated with a specific division, group, class, category, or subcategory (ATECO code). ATECO codes attributable to the ICT sector or ICT consulting[40] were used as a filter to query the Italian Business Register. This resulted in a list of remarkable size (over 18,000 companies), containing many companies generically active in the ICT sector but not directly involved in cybersecurity services.

Therefore, to limit the universe of the survey, i.e. the list of companies to contact, an analysis was conducted by combining various sources:

- sector associations: companies included in the public lists of members of sector associations;[41]
- commercial databases: companies identified by applying keywords related to cybersecurity and testing services as filters in the activity description fields;[42]
- INVIND questionnaire conducted in 2023:[43] companies that responded positively to a specific question related to the provision of cybersecurity services;
- information already collected by Banca d'Italia on ICT providers of financial entities.[44] It should be noted that, from a regulatory perspective, the services of interest for the survey are not usually framed as outsourcing.

This process led to the identification of a subset of 633 companies. On this subset, a detailed and manual analysis was conducted on each individual company, based on any available information, including their official websites, to narrow down the set of companies that claim to provide cybersecurity testing or related services.

[40] In particular it is the section J – "Information and communication services", 62.01, 62.02 classes and subcategory 62.09.09, respectively "Computer programming activities", "Computer consultancy activities" and "Other information technology and computer service activities".

[41] E.g.: i) CLUSIT: Associazione Italiana per la Sicurezza Informatica (Italian association for information security); ii) ASSINTEL: Associazione nazionale delle imprese ICT (association of Italian ICT companies); iii) AIPSA: Associazione Italiana Professionisti Security Aziendale (Italian association of business security professionals).

[42] The research was conducted on Bloomberg and Orbis databases, filtering by ATECO codes of class 62 and/or by keywords, e.g.: Cyber, Cybersecurity, Penetration test, Threat intelligence, Red team, CBEST, TLPT and Tiber.

[43] This is an annual survey of industrial and service companies conducted by Banca d'Italia. The INVIND survey included the following question, addressed only to companies operating in certain ATECO codes: 'Does your company offer cybersecurity services (e.g. threat intelligence, penetration testing, red teaming, TLPT)?'

[44] This list is built on the basis of information from outsourcing contracts between financial entities and providers.

This further screening resulted in a reference universe for this survey of 185 companies. During the survey, the population was reduced to 180 companies due to some changes in corporate structures.

Comparison between population and respondents

To verify that companies' population and the respondents' distribution are similar regarding the main study variables, size class, and geographical macro-area, the *chi-squared test*[45] was used. Tables below show the observed and expected frequencies for the two variables considered, with P=180 representing the number of companies in the population and R=71 the number of respondents.

Expected frequencies are calculated as: $e_i = (p_i/P) \times R$ where p_i is the population related to the reference category.

Table A.1

Size class	p_i (population)	o_i (respondents)	e_i (expected frequencies)
micro	42	13	16.57
small	43	18	16.96
medium	52	19	20.51
large	23	9	9.07
very large	20	12	7.89

Table A.2

Geographical macro-area	p_i (population)	o_i (respondents)	e_i (expected frequencies)
northwest	95	35	37.47
northeast	31	11	12.23
centre	45	20	17.75
south and islands	9	5	3.55

The test variable X^2 is obtained as the sum of the quadratic deviations between the observed frequencies (o_i) and the expected frequencies (e_i), weighted by the expected frequencies. The null hypothesis of independence, i.e. the hypothesis that the two distributions by size and geographical macro-area do not depend on the responses received and that therefore the frequencies of the observed values fit the expected frequencies, is demonstrated if the test variable is less than the value of the chi-square distribution with k-1 degrees of freedom and a tolerated error fixed at α=0.05. In the case of the size class variable, k=5 and the degrees of freedom are 4. For the geographical macro-area variable, k=4 and the degrees of freedom are 3.

$$\chi^2 = \sum_{i=1}^{k} \frac{(o_i - e_i)^2}{e_i}$$

The reference value of the chi-square distribution for 4 degrees of freedom is 9.49; for 3 degrees of freedom, it is 7.82. The values of X^2, 3.09 for the size class variable and 1.16 for the geographical macro-area variable, are below the thresholds in both cases; for this reason, the null hypothesis is not rejected, and therefore there are no significant differences between the distributions of population and respondents.

[45] To summarise, the objective of the test is to verify that the frequencies of the values observed in the respondents are not statistically different from those expected.

APPENDIX B – QUESTIONNAIRE STRUCTURE

Section 1. General Information	
Question Number	*Question Text*
1	Enter the name of the organization.
2	Enter the VAT number of the organization.
3	If the organization is part of a group, enter the name of the parent company, too.
	If the organization is part of a group, enter the nationality of the parent company, too.
4	Enter the name and surname of the person responsible for filling the questionnaire.
	Enter the email address of the person responsible for filling the questionnaire.
	Enter the phone number of the person responsible for filling the questionnaire.
	Enter the business role of the person responsible for filling the questionnaire.
5	For the purposes of the questionnaire, unless otherwise specified, reference is made to the last available fiscal year. Indicate the closing date of the last available fiscal year.
6	Indicate an estimate of the geographical distribution of the revenue from IT services provided by the organization to its customers in the last available fiscal year: • In Italy • In the European Union (including Italy) • In the rest of the world
7	What is the total number of employees providing IT services (including cybersecurity services) as of 31-12-23?
Section 2. Cybersecurity Services	
Question Number	*Question Text*
1	Does the organization provide cybersecurity services?

2	Select the types of cybersecurity services provided: • Application Security • Cloud security • Consumer security • Data Security • ICS and critical infrastructure security • Identity & Access Management • Integrated Risk Management • IoT and embedded security • Mobile security • Network security • Testing (including VA, PT, Red Teaming, etc.) • Threat intelligence • Other
3	Indicate the percentage of revenue related to cybersecurity services on total revenue in the last available fiscal year.
4	Enter the number of employees providing cybersecurity services as of 31-12-23.
5	Indicate the average number of training hours related to cybersecurity services provided in 2023 per employee providing cybersecurity services.
6	Indicate whether cybersecurity services are provided to the financial sector. If so, select the type of financial entities that are clients: • No services are provided to the financial sector • Banks • Electronic money institutions • Payment institutions • Payment systems • Market infrastructures • Trading venues • Insurance intermediaries • Central banks • Other
7	Indicate whether the organization uses AI-based solutions in the provision of cybersecurity services.
8	Select the types of services for which AI-based solutions are used: • Application Security • Cloud security • Consumer security • Data Security • ICS and critical infrastructure security • Identity & Access Management • Integrated Risk Management • IoT and embedded security • Mobile security • Network security • Testing (including VA, PT, Red Teaming, etc.) • Threat intelligence • Other

Section 3. Testing Services	
Question Number	*Question Text*
1	Does the organization provide cybersecurity testing services?
2	Enter the percentage of revenue from cybersecurity testing services compared to the revenue related to cybersecurity services in the last available fiscal year.
3	Indicate an estimate of the variation in revenue from cybersecurity testing services comparing the last available fiscal year with the previous one.
4	Indicate an estimate of the percentage of revenue from the most relevant client for cybersecurity testing services in the last available fiscal year.
5	Enter the number of employees providing cybersecurity testing services as of 31-12-23.
6	Considering the total number of employees providing cybersecurity testing services, enter the percentage of personnel certified in cybersecurity testing as of 31-12-23.
7	Select the certifications held by the employees mentioned in the previous question: • Certified Ethical Hacker • Certified Information Systems Security Professional • CREST Certified Infrastructure Tester • CREST Certified Simulated Attack Manager • CREST Certified Simulated Attack Specialist • CREST Certified Threat Intelligence Manager • CREST Registered Threat Intelligence Analyst • Cybersecurity Nexus • EC-Council Certified Security Analyst • eLearnSecurity Certified Professional Penetration Tester • GIAC Accessing and Auditing Wireless Networks • GIAC Advanced Penetration Tester • GIAC Cyber Threat Intelligence • GIAC Gold Cyber Threat Intelligence • GIAC Mobile Device Security Analyst • GIAC Penetration Tester • GIAC Web Application Penetration Testing • Licensed Penetration Tester • Offensive Security Certified Expert • Offensive Security Certified Professional • Offensive Security Exploitation Expert • Offensive Security Web Expert • Offensive Security Wireless Professional • Systems Security Certified Practitioner • Other
8	Select the prevailing mode by which the organization provides cybersecurity testing services.
Section 4. TLPT Services	
Question Number	*Question Text*

1	Does the organization provide Threat-Led Penetration Testing (TLPT) cybersecurity services?
2	Does the organization plan to provide TLPT services to the financial sector?
3	Select the type of TLPT framework for which services are offered: • CBEST (UK) • TIBER-EU / TIBER-XX • ICAST (HK) • AASE (ABS-SG) • REDFIN (IT) • CORIE (AUS) • FEERET (SA) • PTFSI (GFMA) • Proprietary • Other
4	Is the organization certified according to accreditation schemes provided for TLPT services by some public and/or private frameworks (e.g., CBEST)? Indicate the accreditation schemes for which the organization is certified.
5	Indicate an estimate of the percentage of revenue related to TLPT services in the last available fiscal year compared to the total revenue from cybersecurity services.
6	Indicate an estimate of the variation in revenue from TLPT services comparing the last available fiscal year with the previous one.
7	Enter the number of TLPT tests for which services were provided in 2022. Enter the number of TLPT tests for which services were provided in 2023.
8	Enter the percentage of TLPT tests for which services were offered to the financial sector in 2022. Enter the percentage of TLPT tests for which services were offered to the financial sector in 2023.
Threat Intelligence	
9	Enter the number of Generic Threat Intelligence reports (GTI) drafted in 2022. Enter the number of Generic Threat Intelligence reports (GTI) drafted in 2023.
10	Enter the number of TLPT tests for which the role of threat intelligence provider was performed in 2022 (e.g. producing the Targeted Threat Intelligence report - TTI). Enter the number of TLPT tests for which the role of threat intelligence provider was performed in 2023 (e.g. producing the Targeted Threat Intelligence report - TTI).
11	Indicate the overall average effort of human resources for targeted threat intelligence services used for a single TLPT.
12	Indicate the average years of experience of the TI team manager in threat intelligence activities.
Red teaming	
13	Enter the number of TLPT tests for which the role of red team provider was performed in 2022 (e.g. producing the Red Team Test Report - RTTR). Enter the number of TLPT tests for which the role of red team provider was performed in 2023 (e.g. producing the Red Team Test Report - RTTR).

14	Indicate the overall average effort of human resources for red teaming services for a single TLPT.
15	Indicate the average years of experience of the RT team manager in red teaming activities.
16	Indicate whether the organization has subscribed to specific insurance for the provision of TLPT services.
17	If the organization conducts research activities in the field of cybersecurity, indicate the number of vulnerabilities discovered and published since 2022.
18	Does the organization adhere to formal codes of conduct and/or ethics specific to TLPT activities? Indicate the formal codes of conduct and/or ethics to which the organization adheres.
Opinions on the TLPT-related services market	
19	Regarding the TLPT-related services market, express your degree of agreement with the following statements: a) Regulation and adoption of public and/or public-private frameworks or sector standards promote growth of the TLPT-related services market. b) Companies' awareness of cyber risks promotes growth of the TLPT-related services market. c) Technology development promotes growth of the TLPT-related services market. d) The use of AI-based solutions promotes growth of the TLPT-related services market. e) The limited availability of personnel with adequate experience and skills is one of the main problems for the development of the TLPT-related services market. f) Compared to the economic budget allocated by clients to cybersecurity activities, the cost of TLPT-related services limits the development of the TLPT-related services market.
20	Regarding the provision of TLPT-related services, express your degree of agreement with the following statements: a) Adequate treatment of clients' confidential data is one of the main difficulties. b) Occurrence of operational incidents is one of the main risks. c) Relationship with the client is easily manageable. d) Objectives (flags) of the attack are easy to identify. e) Managing the project schedule agreed with the client is easy to respect. f) Use of AI-based solutions increases the quality or effectiveness of the service.
21	How does your organization assess the maturity level of the TLPT-related services market?
22	How does your organization evaluate the relationship between supply and demand for TLPT-related services?

APPENDIX C – GLOSSARY

Application security testing
Security test in which the unit under test is a single application.

Generic Threat Intelligence (GTI)
Intelligence activity for the analysis of the generic threat scenario (e.g., for an entire sector) even outside the perimeter of the individual TLPT.

Penetration Testing (PT)
A test methodology in which assessors typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.
Source: FSB Cyber Lexicon

Red team report
The Red team report is the document drafted in the closing phase of red teaming activities.

Red Teaming (RT)
A security test in which human operators attempt to achieve predetermined objectives by acting as a threat actor, without, or with limited, constraints and without any prior notification or warning to the defense teams (blue team) of the organization under test. Sometimes also referred to as TLPT.

Regulatory Technical Standards (RTS)
Delegated acts of the EU Commission supplementing or amending certain non-essential elements of a basic regulatory act and requiring the expertise of subject-matter experts, usually drafted by the European Supervisory Authorities.

Security testing
A structured process that reveals whether a system under test has weaknesses that can be exploited to cause undesirable effects (e.g. data manipulation, denial of service).

System security testing
Security test in which the unit under test is a defined set of interconnected components.

Targeted Threat Intelligence (TTI)
TTI provides detailed insights into the entity's attack surface and its defence posture.
Source: National TIBER-IT Guide

Targeted Threat Intelligence (TTI) Report
The TTI Report is a tailored threat intelligence report for the entity under test. The same TTI report can be updated multiple times during a TLPT.

Threat Intelligence (TI)
Threat information that has been aggregated, transformed, analysed, interpreted or enriched to provide the necessary context for decision-making processes.
Source: FSB Cyber Lexicon

Threat-Led Penetration Testing (TLPT)[46]

A controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations.

Source: FSB Cyber Lexicon

Vulnerability Assessment (VA)

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.

Source: FSB Cyber Lexicon

[46] As defined in Article 3, paragraph 17 of the DORA Regulation: "means a framework that mimics the tactics, techniques and procedures of real- life threat actors perceived as posing a genuine cyber threat, that delivers a controlled, bespoke, intelligence-led (red team) test of the financial entity's critical live production systems".

Recently published papers in the 'Markets, Infrastructures, Payment Systems' series

n. 26 Integrating DLTs with market infrastructures: analysis and proof-of-concept for secure DvP between TIPS and DLT platforms, *by Rosario La Rocca, Riccardo Mancini, Marco Benedetti, Matteo Caruso, Stefano Cossu, Giuseppe Galano, Simone Mancini, Gabriele Marcelli, Piero Martella, Matteo Nardelli and Ciro Oliviero* (Research Papers)

n. 27 Statistical and forecasting use of electronic payment transactions: collaboration between Bank of Italy and Istat, *by Guerino Ardizzi and Alessandra Righi* (Institutional Issues) (in Italian)

n. 28 TIPS: a zero-downtime platform powered by automation, *by Gianluca Caricato, Marco Capotosto, Silvio Orsini and Pietro Tiberi* (Research Papers)

n. 29 TARGET2 analytical tools for regulatory compliance, *by Marc Glowka, Alexander Müller, Livia Polo Friz, Sara Testi, Massimo Valentini and Stefano Vespucci* (Institutional Issues)

n. 30 The security of retail payment instruments: evidence from supervisory data, *by Massimiliano Cologgi* (Research Papers)

n. 31 Open Banking in the payment system: infrastructural evolution, innovation and security, supervisory and oversight practices, *by Roberto Pellitteri, Ravenio Parrini, Carlo Cafarotti and Benedetto Andrea De Vendictis* (Institutional Issues) (in Italian)

n. 32 Banks' liquidity transformation rate: determinants and impact on lending, *by Raffaele Lenzi, Stefano Nobili, Filippo Perazzoli and Rosario Romeo* (Research Papers)

n. 33 Investor behavior under market stress: evidence from the Italian sovereign bond market, *by Onofrio Panzarino* (Research Papers)

n. 34 Siamese neural networks for detecting banknote printing defects, *by Katia Boria, Andrea Luciani, Sabina Marchetti and Marco Viticoli* (Research Papers) (in Italian)

n. 35 Quantum safe payment systems, *by Elena Bucciol and Pietro Tiberi*

n. 36 Investigating the determinants of corporate bond credit spreads in the euro area, *by Simone Letta and Pasquale Mirante*

n. 37 Smart Derivative Contracts in DatalogMTL, *by Andrea Colombo, Luigi Bellomarini, Stefano Ceri and Eleonora Laurenza*

n. 38 Making it through the (crypto) winter: facts, figures and policy issues, *by Guerino Ardizzi, Marco Bevilacqua, Emanuela Cerrato and Alberto Di Iorio*

n. 39 The Emissions Trading System of the European Union (EU ETS), *by Mauro Bufano, Fabio Capasso, Johnny Di Giampaolo and Nicola Pellegrini* (in Italian)

n. 40 Banknote migration and the estimation of circulation in euro area countries: the italian case, *by Claudio Doria, Gianluca Maddaloni, Giuseppina Marocchi, Ferdinando Sasso, Luca Serrai and Simonetta Zappa* (in Italian)

n. 41 Assessing credit risk sensitivity to climate and energy shocks, *by Stefano Di Virgilio, Ivan Faiella, Alessandro Mistretta and Simone Narizzano*

n. 42 Report on the payment attitudes of consumers in Italy: results from the ECB SPACE 2022 survey, *by Gabriele Coletti, Alberto Di Iorio, Emanuele Pimpini and Giorgia Rocco*

n. 43 A service architecture for an enhanced Cyber Threat Intelligence capability and its value for the cyber resilience of Financial Market Infrastructures, *by Giuseppe Amato, Simone Ciccarone, Pasquale Digregorio and Giuseppe Natalucci*

n. 44 Fine-tuning large language models for financial markets via ontological reasoning,

by Teodoro Baldazzi, Luigi Bellomarini, Stefano Ceri, Andrea Colombo, Andrea Gentili and Emanuel Sallinger

n. 45 Sustainability at shareholder meetings in France, Germany and Italy, *by Tiziana De Stefano, Giuseppe Buscemi and Marco Fanari* (in Italian)

n. 46 Money market rate stabilization systems over the last 20 years: the role of the minimum reserve requirement, *by Patrizia Ceccacci, Barbara Mazzetta, Stefano Nobili, Filippo Perazzoli and Mattia Persico*

n. 47 Technology providers in the payment sector: market and regulatory developments, *by Emanuela Cerrato, Enrica Detto, Daniele Natalizi, Federico Semorile and Fabio Zuffranieri*

n. 48 The fundamental role of the repo market and central clearing, *by Cristina Di Luigi, Antonio Perrella and Alessio Ruggieri*

n. 49 From Public to Internal Capital Markets: The Effects of Affiliated IPOs on Group Firms, *by Luana Zaccaria, Simone Narizzano, Francesco Savino and Antonio Scalia*

n. 50 Byzantine Fault Tolerant consensus with confidential quorum certificate for a Central Bank DLT, *by Marco Benedetti, Francesco De Sclavis, Marco Favorito, Giuseppe Galano, Sara Giammusso, Antonio Muci and Matteo Nardelli*

n. 51 Environmental data and scores: lost in translation, *by Enrico Bernardini, Marco Fanari, Enrico Foscolo and Francesco Ruggiero*

n. 52 How important are ESG factors for banks' cost of debt? An empirical investigation, *by Stefano Nobili, Mattia Persico and Rosario Romeo*

n. 53 The Bank of Italy's statistical model for the credit assessment of non-financial firms, *by Simone Narizzano, Marco Orlandi and Antonio Scalia*

n. 54 The revision of PSD2 and the interplay with MiCAR in the rules governing payment services: evolution or revolution?, *by Mattia Suardi*

n. 55 Rating the Raters. A Central Bank Perspective, *by Francesco Columba, Federica Orsini and Stefano Tranquillo*

n. 56 A general framework to assess the smooth implementation of monetary policy: an application to the introduction of the digital euro, *by Annalisa De Nicola and Michelina Lo Russo*

n. 57 The German and Italian Government Bond Markets: The Role of Banks versus Non-Banks. A joint study by Banca d'Italia and Bundesbank, *by Puriya Abbassi, Michele Leonardo Bianchi, Daniela Della Gatta, Raffaele Gallo, Hanna Gohlke, Daniel Krause, Arianna Miglietta, Luca Moller, Jens Orben, Onofrio Panzarino, Dario Ruzzi, Willy Scherrieble and Michael Schmidt*

n. 58 Chat Bankman-Fried? An Exploration of LLM Alignment in Finance, *by Claudia Biancotti, Carolina Camassa, Andrea Coletta, Oliver Giudice and Aldo Glielmo*

n. 59 Modelling transition risk-adjusted probability of default, *by Manuel Cugliari, Alessandra Iannamorelli and Federica Vassalli*

n. 60 The use of Banca d'Italia's credit assessment system for Italian non-financial firms within the Eurosystem's collateral framework, *by Stefano Di Virgilio, Alessandra Iannamorelli, Francesco Monterisi and Simone Narizzano*

n. 61 Fintech Classification Methodology, *by Alessandro Lentini, Daniela Elena Munteanu and Fabrizio Zennaro*

n. 62 The Rise of Climate Risks: Evidence from Expected Default Frequencies for Firms, *by Matilde Faralli and Francesco Ruggiero*