INTERNATIONAL MONETARY FUND

IMF Country Report No. 26/240

ITALY

FINANCAL SECTOR ASSESSMENT PROGRAM

September 2026

TECHNICAL NOTE ON CYBER RISK SUPERVISION AND OVERSIGHT

This Technical Note on Cyber Risk Supervision and Oversight for the Italy FSAP was prepared by a staff team of the International Monetary Fund as background documentation for the periodic consultation with the member country. It is based on the information available at the time it was completed on July 2026.

Copies of this report are available to the public from

International Monetary Fund • Publication Services
PO Box 92780 • Washington, D.C. 20090
Telephone: (202) 623-7430 • Fax: (202) 623-7201
E-mail: publications@imf.org Web: http://www.imf.org

International Monetary Fund
Washington, D.C.

INTERNATIONAL MONETARY FUND

ITALY

FINANCIAL SECTOR ASSESSMENT PROGRAM

August 3, 2026

TECHNICAL NOTE

CYBER RISK SUPERVISION AND OVERSIGHT

Prepared By

Monetary and Capital Markets Department

This Technical Note was prepared by IMF staff in the context of the Financial Sector Assessment Program in Italy during November 2025 led by Naomi Nakaguchi Griffin, IMF, and overseen by the Monetary and Capital Markets Department, International Monetary Fund. The note contains the technical analysis and detailed information underpinning the FSAP assessment's findings and recommendations. Further information on the FSAP can be found at http://www.imf.org/external/np/fsap/fssa.aspx

CONTENTS

Glossary

ABF	Banking and Financial Ombudsman
ACN	National Cybersecurity Agency
AI	Artificial Intelligence
API	Application Programming Interface
BCBS	Basel Committee on Banking Supervision
BCM	Business Continuity Management
BdI	Banca d'Italia
BI-COMP	BdI Retail Payment System
CCP	Central Counterparty
CEG	Cyber Expert Group (of the G7)
CER	Critical Entities Resilience Directive
CERT	Computer Emergency Response Team
CERTBI	Computer Emergency Response Team of Banca d'Italia
CERTFin	National Computer Emergency Response Team for the Financial Sector
CODISE	Unit for business continuity of the Italian financial marketplace
CIISI-EU	Cyber Information and Intelligence Sharing Initiative—European Union
CIO	Chief Information Officer
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CMP	Committee for Macroprudential Policies
COBIT	Control Objectives for Information and Related Technologies
CONSOB	National Commission for Companies and the Stock Exchange
COVIP	Pension Fund Supervisory Commission
CPMI	Committee on Payments and Market Infrastructures
CROE	Cyber Risk Oversight Expectations
CSD	Central Securities Depository
CSIRT	Computer Security Incident Response Team
CSP	Critical Service Provider
CTI	Cyber Threat Intelligence
CTPP	Critical Third-Party Provider
DDoS	Distributed Denial of Service
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
EIOPA	European Insurance and Occupational Pensions Authority
ENISA	European Union Agency for Cybersecurity
ESA	European Supervisory Authorities
ESCG	European Systemic Cyber Group
ESMA	European Securities and Markets Authority
ESRB	European Systemic Risk Board
EU	European Union
EU-SCICF	European Union Systemic Cyber Incident Coordination Framework

FIRE	Format for Incident Reporting Exchange
FIRST	Forum of Incident Response and Security Teams
FMI	Financial Market Infrastructure
FSB	Financial Stability Board
FS-ISAC	Financial Services Information Sharing and Analysis Center
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IMF	International Monetary Fund
IOC	Indicators of Compromise
IOSCO	International Organization of Securities Commissions
ISAE	International Standard on Assurance Engagements
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IVASS	Institute for the Supervision of Insurance
JET	Joint Examination Team
JSON	Java Script Object Notation
LSI	Less Significant Institution
MEF	Ministry of Economy and Finance
MoU	Memorandum of Understanding
NBFI	Nonbank Financial Intermediaries
NCS	National Cybersecurity Cell
NIS2	Network and Information Security Directive 2
NIST	National Institute of Standards and Technology
ORC	Operational Risk Committee (of the Banca d'Italia)
PFMI	Principles for Financial Market Infrastructures
PISA	Payment Instruments, Schemes and Arrangements
POR	Principles for Operational Resilience
PSNC	National Cybersecurity Perimeter Regulation
PSP	Payment Service Provider
ROI	Register of Information
RTO	Recovery Time Objective
SI	Significant Institution
SIPS	Systemically Important Payment System
SREP	Supervisory Review and Evaluation Process
SSM	Single Supervisory Mechanism
TI	Trusted Introducer
TIBER-EU	Threat Intelligence Based Ethical Red-teaming for the European Union
TIBER-IT	Threat Intelligence Based Ethical Red-teaming for Italy
TLPT	Threat-led Penetration Testing
TTP	Tactics, Techniques and Procedures
TV	Trading Venue
UIF	Italian Financial Intelligence Unit

EXECUTIVE SUMMARY

The Italian financial sector is undergoing rapid digital transformation, marked by significant investments in innovative technologies, especially in payments, insurance, and banking. Digital payments surpassed cash transactions since 2022. This transformation has led to increased reliance on third-party service providers, particularly cloud services, with 64 percent of Less Significant Institutions (LSIs) and Nonbank Financial Intermediaries (NBFIs) using cloud solutions. The insurance sector reports 96 percent cloud adoption, and digital channels are now the primary interface for most policyholders. As a result, cyber and operational risks have become a major concern, with rising incidents of fraud, ransomware, phishing, distributed denial-of-service (DDoS) attacks, supply chain vulnerabilities, and data breaches. In 2024, 35 major cyberattacks occurred and three of them resulted in estimated losses exceeding EUR 2 million each. Payment fraud losses reached EUR 246 million. Fraud accounts for only a marginal share of total payment transactions (around 0.003 percent in value) and was broadly in line with averages in the European Union. The sharp increase of operational incidents in 2024 highlighted the risk from using and depending on third-party service providers to deliver financial services.

Cyber risk supervision in the Italian financial sector is managed by several authorities. They include Banca d'Italia (BdI), National Commission for Companies and the Stock Exchange (CONSOB), Pension Fund Supervisory Commission (COVIP), Institute for the Supervision of Insurance (IVASS), and the Ministry of Economy and Finance (MEF). The majoirity of these institutions already have a collaboration in place with the National Cybersecurity Agency (ACN) and participate in the Computer Emergency Response Team for the Financial Sector (CERTFin). In matters of national security, financial sector entities classified as critical also fall under the supervisory authority of ACN, pursuant to the National Cybersecurity Perimeter Law adopted in 2019. In case of operational crisis (including those derived from ICT and cyber incidents), system-wide response and recovery actions are coordinated through CODISE, the unit for business continuity, which liases with the CERTFin for technical analysis and support. CODISE was successfully activated in recent years to deal with major operational incidents. The National Cybersecurity Cell (NCS) is the main interministerial coordination body to deal with cyber crisis including those impacting different sectors. Italy's National Cybersecurity Strategy aligns with EU frameworks and emphasizes, among others, sectoral Computer Security Incident Response Teams (CSIRTs) and Information Sharing and Analysis Centers (ISACs). Financial authorities have developed dedicated strategies and action plans, focusing on principles, good practices, and system-wide resilience exercises. A cybersecurity strategy for the financial sector was launched in 2020. The Digital Operational Resilience Act (DORA) was implemented in 2025.

The threat landscape is assessed using intelligence from global, national, and supervisory sources. CERTFin acts as a central hub for sector-specific intelligence, while the Computer Emergency Response Team of BdI (CERTBI) and ACN, through the CSIRT Italia, share actionable threat indicators. Incident reporting frameworks have revealed a sharp increase in cyberattacks and operational incidents. The rise in complaints and disputes related to scams, credential theft, and social engineering highlights the evolving nature of cyber threats. Authorities monitor payment

fraud and operational disruptions, emphasizing the need for robust incident response and recovery plans.

Italy's regulatory framework for cyber risk in the financial sector is primarily shaped by the DORA, while earlier achievements were made to strengthen cyber resilience. Italy's financial sector had already spearheaded incident reporting, advanced testing, industry-wide exercises, and contingency planning, among others, before the implementation of DORA. The current regulatory framework is complemented by the Network and Information Security Directive 2 (NIS2; Italy is among the few European countries which transposed the Directive into national jurisdiction), Critical Entities Resilience Directive (CER), and national regulations. The DORA harmonizes digital resilience requirements across the financial sector, covering information and communication technology (ICT) risk management, incident reporting, resilience testing, third-party risk management, and information sharing. Sector-specific regulations apply to payment systems, insurance, and securities market infrastructures. Supervisory practices include offsite and on-site inspections, thematic reviews, and the use of control frameworks such as from the International Organization for Standardization (ISO) and the International Electrotechnical Commission (ISO/IEC), National Institute of Standards and Technology (NIST), and Control Objectives for Information and Related Technologies (COBIT). Moreover, the National Cybersecurity Perimeter Law, which applies to the financial sector entities critical for national security, provides strengthened obligations in terms of cybersecurity measures, incident reporting, and technological scrutiny in ICT products and services procurement. Furthermore, ICT service providers (except if qualified as small or micro companies) fall within the scope of the NIS2.

Around 196 on-site cybersecurity examinations on LSIs were performed in the past three years as part of the inspection of operational risk in full scope inspections. The supervisory strategy has focused on ICT third-party service providers given their high-level of interdependency with LSIs and NBFIs. Most financial market infrastructures (FMIs), including Trading Venues (TVs), and critical service providers (CSPs), but not all, have undergone cyber resilience assessments. Authorities apply proportionality in oversight, tailoring the depth of inspections to risk exposure and systemic relevance.

Financial authorities actively participate in national, European, and international cybersecurity crisis management exercises. These exercises include those organized by CODISE, the G7 Cyber Expert Group (G7-CEG), European Union Systemic Cyber Incident Coordination Framework (EU-SCICF), and CERTFin. Advanced security testing is mandated for entities meeting DORA criteria. Information sharing is facilitated through structured arrangements at national and international levels, with CERTFin and CERTBI serving as focal points. Incident reporting templates and protocols are standardized under DORA, ensuring timely and comprehensive data collection and dissemination. CSIRT Italia maintains a national cross-sectoral database of cyber incident notifications, supporting coordinated response and tracking.

Financial authorities have strengthened cyber risk supervision capabilities by creating specialized units, internal committees, and advanced training programs. BdI created a new unit for the oversight of third-party service providers and outsourcers, and reinforced its work on business continuity and cyber resilience through another specialized unit. BdI, CONSOB and IVASS

have implemented recruitment plans for IT and cybersecurity experts, and staff participate in Joint Examination Teams (JETs) as part of the DORA oversight framework. Training options include internal specialist courses, external programs at European supervisory authorities, and professional certifications.

Italy's financial sector faces significant cyber and operational risks amid rapid digital transformation, artificial intelligence (AI)-enabled cyber threats, and increased reliance on third-party service providers. The regulatory and supervisory framework, anchored by DORA and complemented by various national legislative acts, which also contribute to the implementation of EU directives, provides a robust foundation for resilience. Continued investment in governance, capacity development, information sharing, industry-wide exercises, and advanced testing will be essential to safeguard financial stability and consumer protection in an evolving threat landscape. This should aim to mitigate service disruptions from operational and cyber incidents and cyber-enabled fraud, which could grow in scale and sophistication. Financial authorities should step in and exercise sanctioning powers, as needed, for non-compliance with cyber risk related regulations. This technical note includes recommendations for further consideration by financial authorities (Table 1), for which many were consistent with authorities' views and ongoing efforts.

Table 1. Italy: Recommendations on Cybersecurity Risk Supervision and Oversight

Recommendations	Timing	Responsible Authorities
1. Revise the cyber strategy for the financial sector and enhance cyber governance practices across organizations. (¶17 to ¶20)	NT	BdI, CONSOB, COVIP, IVASS
2. Operationalize cyber mapping. (¶33)	NT	BdI
3. Assess the financial stability implications of cyber risk caused by a disruption to a third-party service provider. (¶34)	NT	BdI
4. Complete cyber resilience assessments for the remaining FMIs and CSPs based on the proportionality principle with ongoing monitoring on a periodical basis to induce action. (¶61)	I	BdI, CONSOB
5. Complement offsite inspections and ongoing monitoring of cyber risks with audit and testing reports by independent parties for LSIs and NBFIs. (¶61)	I	BdI
6. Increase the focus on cyber risks during on-site inspections in supervised entities (LSIs, NBFIs, FMIs, CSPs) and give close attention to new entrants. (¶61)	NT	BdI, CONSOB
7. Conduct thematic cybersecurity reviews for the insurance and pension sectors. (¶61)	I	COVIP, IVASS
8. Promote operational resilience to effectively manage operational risks that may arise from disruptions from cyberattacks and technology failures, and exercise enforcement powers, as needed, for non-compliance with cyber risk related regulations. (¶61)	NT	BdI, CONSOB, COVIP, IVASS
9. Continue cyber stress testing exercises with supervised entities (LSIs, NBFIs, FMIs) to test exit strategies from third-party service providers. (¶71)	NT	BdI, CONSOB, COVIP, IVASS
10. Use results from advanced security testing methods for the continuous improvement of cyber response and recovery plans. (¶71)	MT	BdI, CONSOB, IVASS
11. Improve information sharing with respect to cyber risk supervision and evaluate onboarding the Pension Fund Supervisory Commission to CODISE and CERTFin. (¶71, ¶87)	NT	BdI, COVIP, IVASS
12. Support ongoing staff training on cyber risk supervision and oversight and reallocating resources for on-site cyber risk supervision. (¶93)	I	BdI, CONSOB, COVIP, IVASS

Note: I Immediate (within 1 year); NT Near Term (within 1-2 years); MT Medium Term (within 3–5 years).

INTRODUCTION[1]

1. The Italian financial sector is undergoing digital transformation, with significant investments in innovative technologies, while AI has added new layers of complexity to cybersecurity oversight. Lending, savings, deposits, and payments have attracted the most financial resources, with web and mobile platforms being the most widely adopted solutions. AI and application programming interfaces (APIs) are increasingly used, following the adoption of digital platforms. Digital transformation is especially evident in payments and insurance, with over 3.5 billion electronic transactions recorded in the first quarter of 2025. Cash usage has declined, digital payments now surpass cash at physical points of sale, and cyber insurance offerings have risen over 22 percent year-on-year, reflecting growing demand for digital risk coverage.

2. Financial institutions in Italy increasingly depend on third-party service providers, especially for cloud services, and this trend is expected to grow. Two hundred and fifty LSIs and NBFIs (64 percent of the total) use cloud services, mainly for software-as-a-service, with some use for infrastructure and platform services. Ninety six percent of the Italian insurance market reported using cloud computing, with many outsourcing essential activities to cloud providers. Migration to cloud services remains limited for systemically important FMIs, but multi-cloud and hybrid-cloud adoption is expected to increase. Some trading venues (TVs) have outsourced critical functions to cloud providers, and an Italian central securities depository (CSD) is developing a cloud-based data lake, which is a large, centralized repository for data storage, for the ECB-led T2S Recovery Project.

3. Cyber and operational risks are a major and growing concern due to digital transformation in the Italian financial sector. Key cyber threats in 2024 included fraud (AI/deepfake scams), ransomware, social engineering/phishing, DDoS attacks, supply chain attacks, and data theft. These trends were confirmed by BdI's incident reporting framework, which showed a rise in cyberattacks from 2022 to 2024. In 2024, 35 major cyberattacks occurred, and three of them resulted in estimated losses exceeding EUR 2 million each. At the same time, the threat landscape is shifting rapidly, with increasingly advanced AI models dramatically lowering the barriers to discovering and exploiting cyber vulnerabilities. Payment fraud losses reached EUR 246 million. Fraud accounts for only a marginal share of total payment transactions (around 0.003 percent in value) and was broadly in line with averages in the European Union. There was a sharp increase in operational incidents in 2024, highlighting the risk of widespread payment disruptions from reliance on third-party service providers.[2]

4. The objective of this note is to assess the cybersecurity risk supervision and oversight arrangements in the financial sector. This includes a review of topics relating to governance and strategy, cyber threat landscape, cyber mapping, cyber regulatory framework and supervisory practices, response and recovery, information sharing, incident reporting, cyber deterrence, and capacity development. The scope covers banking, insurance, securities, and pension fund sectors

[1] This Technical Note was prepared by Tanai Khiaonarong.

[2] BdI (2025). Financial Stability Report, April.

under the responsibilities of the main financial authorities in Italy. This includes the cybersecurity risk supervision and oversight arrangements for LSIs, NBFIs, and FMIs, including TVs, where Italian financial authorities serve as the competent authority or lead authority. The assessments of the cyber resilience of supervised entities are not covered in the scope of this technical note.

5. The review is guided by the conceptual framework developed by the IMF. The framework analyzes supervision activities aimed at building resilience, including identification of the threat landscape; mapping of the cyber and financial network; creation of coherent regulation; conduct of supervisory assessment; set-up of formal information sharing and reporting mechanisms; adequacy of response and recovery; and preparedness of supervisory agencies.[3] The conceptual framework is further complemented with material developed by international standard-setting bodies and regulatory good practices. This includes the following: BCBS Principles for Operational Resilience (March 2021); BCBS Revision of the Principles for the Sound Management of Operational Risk (March 2021); BCBS Cyber Resilience: Range of Practices (December 2018); CPMI-IOSCO Guidance on Cyber Resilience for FMIs (June 2016); CPMI-IOSCO Principles for FMIs (April 2012); FSB Enhancing Third-Party Risk Management and Oversight (December 2023); and G7 Fundamental Elements for Third Party Cyber Risk Management in the Financial Sector (October 2022).

6. The review is based on both public and non-public sources of information. This includes written documentation from responses to the pre-mission questionnaire on cybersecurity risk supervision and oversight, inspection reports, relevant laws and regulations, and regulatory guidance. Additionally, information was also obtained from discussions with authorities and relevant stakeholders.

[3] IMF (2019) Cybersecurity Risk Supervision, Monetary and Capital Markets Department, Departmental Paper No. 19/15, September 24, Washington, D.C.

CYBER RISK SUPERVISION AND OVERSIGHT

A. Governance and Strategy

7. Several financial authorities are responsible for addressing cyber risk. They include: (i) BdI, including the Italian Financial Intelligence Unit (UIF); (ii) National Commission for Companies and the Stock Exchange (CONSOB); (iii) Pension Fund Supervisory Commission (COVIP); (iv) Institute for the Supervision of Insurance (IVASS); and (v) Ministry of Economy and Finance (MEF). They focus on systemic risk prevention, market integrity and orderly functioning, the sound and prudent management of financial institutions, the reliability of payment system, and consumer protection. Efforts span across banks, nonbank financial intermediaries (NBFI), insurance companies, FMIs, TVs, and pension funds (Table 2). Under the DORA, the BdI, CONSOB, COVIP, and IVASS are the national competent authorities. Moreover, public and private entities responsible for exercising essential functions of the State or for providing services that are essential for maintaining civil, social or economic activities fundamental to the interests of the State, including the most critical financial sector entities, are supervised by ACN under the National Cybersecurity Perimeter Law.

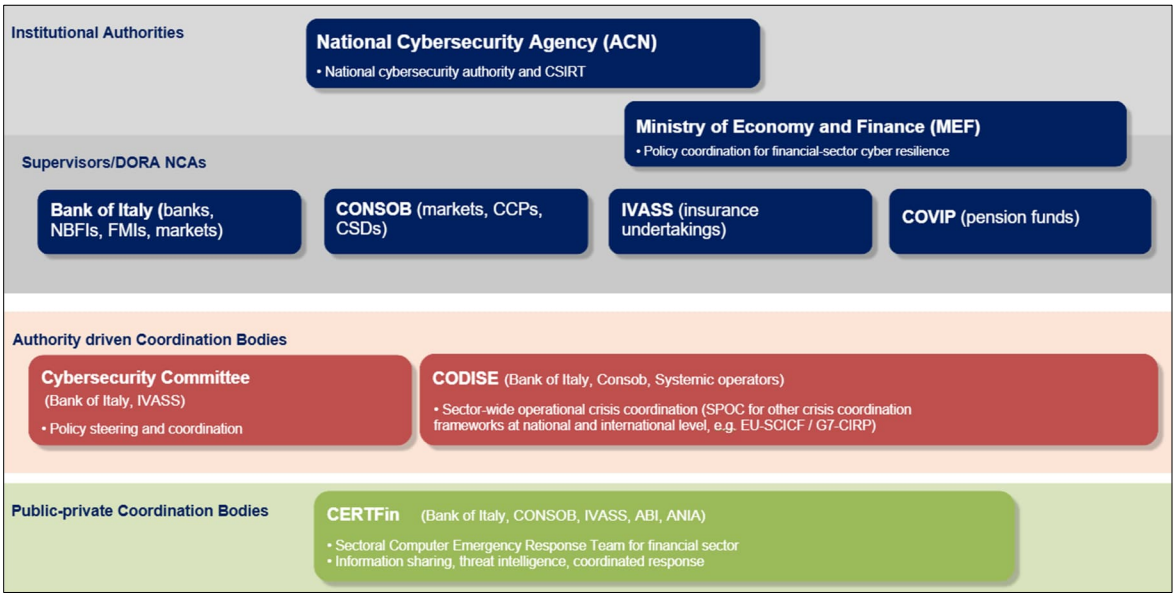
Table 2. Italy: Main Financial Authorities Responsible for Cybersecurity

Authority	Responsibilities
BdI	• supervises cyber risk as part of the operational risk for banks (LSIs), NBFIs (e.g. investment firms, managers of alternative investment funds, management companies, e-money institutions, payment institutions, account information service providers, crypto-asset service providers, issuers of asset-referenced tokens, crowdfunding service providers), FMIs, payment systems and scheme operators and supporting technological and infrastructure providers, wholesale trading venues for government bonds and multilateral trading facilities for euro denominated deposits. • shares supervisory responsibilities with CONSOB for some of the abovementioned entities according to their respective supervisory powers (e.g. issuers of asset-referenced tokens, investment firms, crypto-asset service providers, management companies and managers of alternative investment funds, crowdfunding service providers, TVs for wholesale markets in government securities, CSDs, and central counterparties (CCPs)).
CONSOB	• supervises cybersecurity of TVs, CCPs, and CSDs either exclusively (for trading venues other than wholesale markets in government securities) or with the BdI (see above).
COVIP	• supervises pension funds, including occupational pension funds, insurance-based personal plans and open pension funds.
IVASS	• supervises ICT and cyber risks for insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries, and ancillary insurance intermediaries.
MEF	• defines national financial policies and regulatory strategies, including digital and cyber resilience; contributes to interministerial coordination and oversees legislative alignment; serves as sectoral authority for the Directive on Security Network and Information Security (NIS) and for Critical Entities Resilience Directive (CER) for the financial sector, supported by Banca d'Italia and CONSOB.
UIF	• integrates cyber threat indicators into anti-money laundering and counter-terrorism financing activities, and shares insights with law enforcement and supervisory bodies.

Source: BdI.

8. The coordination mechanism among financial authorities is based on the national cybersecurity architecture, including several institutional coordination arrangements (Figure 1). In case of operational crisis (including those derived from ICT and cyber incidents), system-wide responses and recovery actions are coordinated through the CODISE which is the unit for business continuity of the Italian financial marketplace, chaired by the BdI and participated by CONSOB and major financial operators, while other relevant stakeholders, including the MEF and IVASS, can be invited on a case by case basis. The unit is responsible for coordinating system-wide responses and recovery actions, promoting sector-wide business continuity and crisis management exercises, and enhancing the overall operational and cyber resilience of the financial system. The coordinating mechanism involves the ACN and the National Computer Emergency Response Team for the Financial Sector (CERTFin) and, when needed, other relevant public and private institutions.

Figure 1. Italy: Key Stakeholders for Cybersecurity Coordination in the Financial Sector



Source: BdI.

9. Cyber governance arrangements for the financial sector are part of the national cybersecurity architecture. Specific mechanisms have been introduced to foster collaboration and exchange of information between ACN and other authorities that are relevant to the financial sector. The National Cybersecurity Cell (NCS) is the main interministerial coordination body (including the MEF) at the technical and operational level, supporting the President of the Council of Ministers, tasked with promoting prevention and preparedness for potential cyber crises as well as activating alert procedures when necessary. NCS ensures a structured and continuous dialogue between the relevant institutions (including BdI) and fosters a coordinated and effective response to cyber incidents, with reference to those that may generate significant effects on critical infrastructures, essential services or have an impact on national security. The NCS also serves as a platform to discuss and coordinate cyber security-relevant initiatives among national administration and further stakeholders. The MEF has been formally designated as the NIS sectoral authority and the CER

sectoral authority for the financial sector, supported by BdI and CONSOB. ACN collaborates with the Italian Data Protection Authority, which is an independent authority set up to protect the fundamental rights and freedom in connection with the processing of personal data. Furthermore, without prejudice with current formal and informal collaboration agreements, the NIS2 national transposition provides for the adoption of multiple Prime Minister Decrees aimed at structuring the collaboration of ACN, as national NIS competent authority, with the Italian DPA, national CER authorities, national DORA authorities and NIS sectoral authorities.

10. Cyber risk is also addressed at macroprudential level by the Italian Committee for Macroprudential Policies (CMP). The CMP serves as the independent authority responsible for implementing macroprudential policy in Italy. The CMP was established by Legislative Decree No. 207 of 2023, following a recommendation from the European Systemic Risk Board (ESRB), with the aim of contributing to the safeguard of the Italian financial system by preventing or mitigating risks that could threaten its stability. It is chaired by the Governor of the BdI and participated by the Presidents of CONSOB, COVIP, IVASS and the Director General of the Treasury.

11. Italy has formulated a National Cybersecurity Strategy that includes actions relevant for the financial sector. Aligned with EU frameworks such as the 2020 EU Cybersecurity Strategy and the NIS1 Directive[4] as well as EU's Strategic Compass, the National Cybersecurity Strategy (2022-2026) identifies critical infrastructure, including the financial sector, as a prime target for cyber adversaries. The Strategy is complemented by a detailed Implementation Plan, which includes the establishment of sectoral CSIRTs and of an ISAC network, that reinforce the cyber posture of essential industries, including financial ones. The Strategy ensures that banks, FMIs and other financial institutions are active participants in a coordinated national-level cyber security and resilience ecosystem and are compliant with regulatory requirements under the National Cybersecurity Perimeter Regulation (PSNC) (see paragraph 40) and NIS2. This framework helped establish two Memoranda of Understanding (MoU), one between the ACN and CERTBI, and the other for the ACN and CERTFin, to strengthen collaboration and foster coordinated threat intelligence sharing and joint response capabilities across the sectors.

12. Financial authorities have developed dedicated strategies and action plans to enhance cybersecurity within their respective sectors. These initiatives have been complemented by the establishment of cooperation frameworks aimed at strengthening the overall resilience of the financial system. Such strategies and action plans cover: (i) defining principles, good practices, rules, new methodologies and updating of controls and technological standards for cybersecurity to strengthen the prevention, protection, and response capabilities; (ii) organizing and participating in system-wide business continuity and cyber resilience exercises, promoting and conducting testing activities — including cyber stress tests and advanced security tests; and (iii) carrying out horizontal

[4] The Strategy was adopted in 2022 before the entry into force of NIS2 Directive's implementing legislation (Legislative Decree n. 138/2024), so it complies with the NIS1's implementing legislation, in particular Article 6 of Legislative Decree n. 65/2018 on national cybersecurity strategies. By the end of 2026, the Strategy will be updated and will ensure compliance with NIS2 Directive's provision on national cybersecurity strategies (Article 9 of Legislative Decree n. 138/2024).

analyses and in-depth assessments on cyber risk affecting both individual financial entities and the financial system as a whole.

13. BdI has carried out strategies and actions aimed at strengthening its governance and cyber risk management framework. This is due to the central bank being a provider of advanced technology infrastructures and financial services to Italy and Europe's financial marketplace. Cyber resilience has been a key component of the BdI Strategic Plan 2023-2025, which includes two major action plans.

14. BdI and CONSOB launched a joint cybersecurity strategy in 2020. This was to ensure the effective implementation of the Eurosystem Cyber Resilience Strategy. This strategy (adopted in 2017; revised in 2024) focuses on enhancing the cyber resilience of critical TVs and FMIs — including payment systems, CCPs, CSDs under their respective supervision. The joint action plan covers several areas of intervention: regulation and supervision, public private cooperation, training and development of awareness on cyber risks. It emphasizes the need for coordination and methodological alignment, particularly through the adoption of common oversight tools such as the CROE and the national implementation of TIBER-IT, Italy's implementation of TIBER-EU framework for Threat-Led Penetration Testing (TLPT). Developed in synergy with IVASS and CONSOB, this framework fosters a consistent approach to voluntary testing across regulated financial entities, reinforcing Italy's operational alignment with European standards. Under this joint strategy, regular cyber resilience assessments based on the oversight tools have been carried out on supervised entities, such as Italian TVs and post-trading infrastructures. In addition, since 2017, FMIs supervised by BdI and national retail payment systems have been included in the ECB-led biennial cycles of cyber resilience survey. In 2025, the survey was also extended to the payment instruments, schemes and arrangements (PISA) entities.

Observations and Recommendations

15. Financial authorities have demonstrated strong leadership in advancing the cyber resilience of the financial sector. This has included their engagements and contributions through the G7-CEG, European Union, and Financial Stability Board (FSB), among others. Domestically, CODISE has served as a dedicated unit to coordinate operational crises affecting the Italian financial system, facilitate sector-wide crisis management exercises, and strengthen overall cyber resilience. The financial sector's cyber resilience strategy focuses on FMIs, including TVs, and is aligned with the Eurosystem's regional framework.

16. DORA has further set out uniform requirements for cyber governance, risk management, and operational resilience across the financial sector. These requirements cover governance structure and accountability, Board involvement and oversight, ICT risk management framework, third-party risk management, incident reporting and information sharing, operational resilience testing, and continuous improvement.

17. The cyber strategy for the financial sector should be revised. The implementation of DORA in 2025 provides an opportunity to revise the current cyber strategy for the financial sector to

include the remit of all the four DORA authorities. In addition to the important roles of the BdI and CONSOB, COVIP supervises pension funds that include around 10 million members (end-2024) and manages total net assets of EUR 243.4 billion. IVASS oversees the insurance market where around 60 percent of Italian policyholders use digital channels and outsources its ICT services (and handling of sensitive data) to the BdI. IVASS has also observed that 96 percent of the Italian insurance market uses cloud computing. The revision could also be aligned with the forthcoming revision of the national cybersecurity strategy.

18. In addition, further considerations could include the reinforcement of existing cooperative initiatives to explore and address payments and digital fraud. Given the multi-faceted nature of digital fraud, such considerations should involve cooperation with the relevant competent authorities, including law enforcement agencies and the telecommunications authority. Financial authorities use the reporting obligations of supervised firms to monitor the occurrence and trends of payment fraud. At the national level, public-private initiatives are in place to exchange information on fraudulent accounts and fraud patterns (at CERTFin, based on a MoU with the Postal and Communication Police) and to discuss policy and regulatory issues (at the Italian Payment Committee). In this context, an improved understanding of the evolving fraud landscape could be reached by complementing current data with other cyber-enabled fraud (e.g. scams associated with cryptoassets, that have been monitored in other jurisdictions such as by law enforcement agencies in Canada and the United States). This aligns with the identification by authorities of fraud being one of the major cyber threats.

19. Enhancing cyber governance practices across organizations is recommended. Many organizations have designated a senior executive, typically a Chief Information Security Officer (CISO), although this is not a requirement under DORA. The EU framework (DORA and EBA GL on internal governance currently under review) is harmonized and requires a three-lines of defense model. Within this model, an independent control function responsible for managing and overseeing ICT risk, including cyber risk, must be established (e.g. one with a direct reporting line to the Board and segregated from security operations). Governance practices, however, differ and partly reflect the risk profile of the organization. Practices differ on the scope of responsibilities, reporting lines to the Board, and cyber skills and experiences of Board members. For example, one common governance arrangement is the reporting line of the CISO to the Chief Information Officer (CIO), where there could be competing priorities. Given the importance of cyber governance under DORA and the CROE, it is recommended the regular evaluation of cyber governance arrangements with a view for continuous improvement. This should include: (i) reporting lines to ensure the functional independence of the cyber risk supervision and oversight areas to the Board to avoid competing priorities, (ii) designation of an independent function, including a senior executive (e.g. CISO), responsible for cybersecurity relative to the risk profile of the organization, and (iii) greater involvement of senior management and Board members, according with their respective roles and responsibilities, in the effective oversight and implementation of third-party cyber risk management (including using metrics which are applicable to cyber resilience).[5] Board members should also be

[5] BCBS (2018). Cyber-Resilience: Range of Practices, December.

encouraged to participate in industry-wide cyber exercises where scenarios requiring their decision-making (in addition to their involvement in inductions or afterwards for the purpose of hearing debriefs of lessons learned from an exercise). Enhancements could be guided by inspection results and benchmarking against international practices, for example, among CPMI-IOSCO jurisdictions (for FMIs).

20. BdI should continue enhancing its cyber governance. This is relative to its risk profile and operational responsibilities in providing FMI and ICT services, including as: (i) one of the four central bank operators of TARGET Services of the Eurosystem, which encompasses services of systemic importance that ensure the free flow of cash, securities and collateral across Europe; (ii) operator of the BI-COMP retail payment system; and (iii) ICT service provider to IVASS. Such opportunities to improve cyber governance have already been identified by staff in the payment systems oversight function during their CROE compliance assessment of BI-COMP. While CISO activities were reflected in staff responsibilities, there was no designation of a dedicated senior executive that oversees such responsibilities. Under current arrangements, CISO duties are carried out by an Operational Risk Committee (ORC), participated by Heads of all Directorates General, which also acts as a Chief Risk Officer (CRO). The ORC is chaired by a board member, who is also responsible for the overall IT function in the BdI. A 'contact group' of six people supports the functions of a CISO and the ORC on cyber risk and resilience. BdI staff noted that the 'contact group' and the ORC do not have any role in IT operations or development. In addition to operational responsibilities, the BdI also has FMI supervision and oversight responsibilities, including an important CSP for TARGET Services. Therefore, the continuous enhancement of BdI's own cyber governance would also be important to set a higher standard for overseen entities.

B. Identification of Cyber Threat and Fraud Landscape

21. Multiple sources of information are used to assess cyber threats. The approach integrates strategic, tactical, and operational-level information from global, national, and supervisory sources. For the BdI, the main information sources are institutional counterparts and fora, sharing communities, commercial Cyber Threat Intelligence (CTI) providers, international publications, and the reporting of major IT and cybersecurity incidents. The BdI has established bilateral agreements with ACN to share actionable threat intelligence, indicators of compromise (IOCs) and joint alerting during large-scale events. Agreements have been made with law enforcement and financial intelligence units for supporting the analysis of criminal trends and the early detection of phishing, ransomware and coordinated fraud attacks. The BdI is also a member of other sharing communities such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), Trusted Introducer (TI), Forum of Incident Response and Security Teams (FIRST), and Cyber Information and Intelligence Sharing Initiative—European Union (CIISI-EU).

22. CERTFin acts as a central hub for the exchange of cyber threat information. This includes financial entities (banks, insurers, FMIs, TVs) and supervisory bodies (BdI, CONSOB, IVASS). CERTFin produces sector-specific intelligence, which integrates data from its optimized platform and trusted financial-operator contribution (constituency) such as the semiannual Threat Landscape Report, monthly security bulletins and the Annual Report on Cybersecurity and Fraud. In addition,

CERTBI collects CTI, monitors cyberspace, and looks for information related to threats that could potentially affect the BdI or the financial sector. All external sources are analyzed, complemented and validated through internal information gathered by the Italian banking and financial authorities via supervisory and oversight activities, including direct interactions with financial intermediaries and market infrastructures and sector-wide intelligence cooperation and coordination platforms (e.g. CODISE, CIISI-EU, G7-CEG, European Union Systemic Cyber Incident Coordination Framework (EU-SCICF)).

23. Incident reports give useful information on cyberattacks. Prior to the implementation of the new incident reporting framework under DORA in 2025, Italian financial authorities have already observed a rising trend of cyberattacks in the financial sector. Under the BdI's incident reporting framework, the number of major cyberattacks on banks (SIs and LSIs) and payment and e-money institutions increased from 10 to 35 incidents between 2020 and 2024. Malware and unauthorized access were the main types of cyberattacks, while e-banking and mobile banking were the main types of targets. As for FMIs and payment systems, BdI supervised entities reported 78 operational incidents during the period 2020–2024, including 53 related to payment systems and 25 to FMIs (including TVs). Of these, 7 were classified as cyber incidents and were all related to malicious DDoS attacks. IVASS received 12 reports of major cyberattacks from supervised entities during 2018 to 2025, which involved ransomware, data exfiltration, and incidents involving servers third-party service providers. CONSOB did not receive reports of any major cyber-attacks from its supervised entities (mainly trading venues, CCPs, and CSDs). ACN official data has also identified the financial sector among the top ten sectors targeted by cyberattacks where the total number of incidents doubled between 2023 and 2024 (from 81 to 178 cyber incidents).

24. Supervisory reports by payment service providers (PSPs) help identify payment fraud. The number of payment frauds and estimated losses is collected through a reporting scheme based on statistical and supervisory data, which is provided by all Italian PSPs and refers to transactions with the main payment instruments used (payment cards, electronic money, credit transfers). In 2024, the number of fraudulent transactions using card payment accounted for the bulk of payment frauds (63 percent of the total) and recorded a modest increase with respect to the previous year. In terms of fraud estimated losses from fraudulent transactions, credit transfers accounted for the highest value of total losses (63 percent of the total in 2024) and recorded a sharp increase on an annual basis (100 percent).

25. CERTFin fraud alerts and analytical reports are another source of information. Around 7,700 fraudulent International Bank Account Numbers were reported during 2024, a 230 percent increase from 2023, and more than 400 alerts were shared on lists of merchants involved, directly or indirectly, in fraudulent activities. CERTFin has also observed that more than 90 percent of fraud cases involved transactions finalized by the user with strong customer authentication, which suggest fraud techniques have become increasingly sophisticated with payer manipulation.

26. BdI monitors the complaints received by banking customers, including those related to fraud, while the Banking and Financial Ombudsman (ABF) handles disputes on a wide range of issues, including payment fraud. In 2024, over 730 complaints related to suspected scam

were received by the BdI (6 percent of the total amount), with a 32 percent increase over 2023. Fifty percent of cases involved the theft of account login credentials, payment transaction authentication codes, or victim identification data to obtain loans or open bank accounts without their knowledge. Just over half of the credential thefts were carried out through attacks based on social engineering techniques including smishing, vishing, and phishing, sometimes combined with spoofing.[6] The ABF managed 4,123 disputes regarding scams in 2024, which represented 20 percent of the total volume of Ombudsman's litigation. Most of these disputes were related to phishing, spoofing, smishing, and vishing.

C. Cyber Mapping and Financial Stability Analysis

27. Financial authorities have undertaken initiatives to map cyber and ICT risk interdependencies in the financial system. Key activities have included mapping essential financial services; monitoring risks from institutional and service provider interconnections, with emphasis on outsourcing and concentration risks; conducting periodic surveys on Fintech and technological innovation; identifying vulnerabilities through supervisory activities; leveraging data acquired from trusted forums and threat intelligence platforms; and analyzing technological surveys.

28. In 2020, BdI launched a pilot survey to collect detailed information on ICT and non-ICT outsourcing agreements of LSIs and NBFIs. This resulted in a census of over 10,500 contracts, 2,500 direct providers, and more than 1,000 sub-providers. The findings informed a comprehensive report on concentration patterns and critical nodes. Subsequently, BdI implemented a structured, periodic reporting framework on outsourcing arrangements for directly supervised entities, and now also collects the DORA-mandated register of information (ROI) to continuously monitor outsourcing and third-party risk. This supports risk assessment, operational resilience, and identification of systemic vulnerabilities.

29. IVASS has not developed a cyber map but requires companies to report on technologies and third-party relationships during supervisory activities. IVASS and BdI have contributed to the ESRB's European Systemic Cyber Group (ESCG) in developing conceptual models for cyber maps and analyzing financial stability implications of cyber risk.

30. BdI, CONSOB and IVASS have established a methodology to identify systemic operators. This is based on criteria such as substitutability and operational thresholds. The methodology identifies systemically important processes and services from whose malfunctioning and/or interruption can result in significant impacts on the Italian financial marketplace. They include real-time gross settlement systems, CSDs, CCPs, and securities settlement systems; market access services relevant to system liquidity, including multilateral deposit exchanges, ECB operations, Treasury auctions, and wholesale repurchase markets; widely used retail payment services; and services supporting basic liquidity needs, such as automated teller machine cash dispensing and

[6] Consumers' associations point out that the phenomenon of scams is still a concern, partly due to the increasing level of sophistication, especially scams via payment apps. The increase in crypto-asset scams was also reported, probably owing to the growing investment in these instruments, especially among young people.

interbank data transmission. The methodology is being updated to better align the national framework for identifying critical and/or systemic operators with recent regulatory developments, including new requirements under DORA. In parallel, efforts are underway to enhance the understanding of interdependencies and resilience in payments and cash infrastructure, particularly regarding telecommunications and workforce continuity.

31. BdI is developing a model to analyze cyber risk transmission channels affecting financial stability. This focuses on operational, financial, and confidence contagion. Further work will develop indicators and a modeling framework to assess the impact of cyber events on the banking system, supporting comprehensive risk assessment. BdI has not yet fully mapped cybersecurity risk contagion scenarios. In the insurance sector, systemic risk assessments carried out by IVASS, through its risk dashboard, have incorporated cyber risk for several years.

Observations and Recommendations

32. Financial authorities have made efforts to map cyber and ICT risk interdependencies, focusing on critical services, outsourcing risks, and technological innovation.[7] Structured reporting and monitoring of outsourcing and third-party arrangements have been implemented, also leveraging on DORA requirements to assess third-party dependencies and systemic vulnerabilities. Financial institutions must maintain cyber maps of critical assets and dependencies under DORA, supporting risk management and operational resilience, while specific FMIs (such as payment systems and schemes, and related technological infrastructure providers) are currently exempt from this requirement.

33. Operationalizing cyber mapping is recommended. Financial authorities are encouraged to leverage information on third-party service providers from the Register of Information (ROI), which is required under DORA, to create cyber maps at firm and sectoral levels. The authorities have already made work-in-progress, especially in identifying and regularly inspecting the cyber risks of two major ICT third-party service providers that are relevant for LSIs in Italy, according to their supervisory strategy that focused on the dependence of ICT third-party service providers. While this is non-binding for specific FMIs (such as payment systems and schemes, and related technological infrastructure providers), such cyber mapping would be equally useful given their systemic importance. In fact, at the higher-level and in a different context, the payment oversight function already collects information on outsourcing contracts and interdependencies between overseen entities.

34. The financial stability implications of cyber risk caused by disruptions to a third-party service provider should be carefully assessed.[8] Financial authorities should conduct a quantitative

[7] At the regional level, the European Supervisory Authorities (EBA, EIOPA, and ESMA – the ESAs) published a list of 19 designated critical ICT third-party providers (CTPPs) under the DORA on 18 November 2025.

[8] Khiaonarong, T., K. Korpinen, and E. Islam (2025). "Using Simulations for Cyber Stress Testing Exercises," IMF Working Paper, WP/25/85. See also, Chang, Jin-Wook, Jacob Dice, Shengwu Du, Adam Flury, Sam Jerow, Seung Jung

(continued)

assessment of liquidity and settlement risks, including a scenario involving the failure of a common critical third-party service provider to banks. The simulation results could be used to identify and complement offsite and on-site inspections of LSIs and FMIs, to ensure effective cyber incident response and recovery plans.

D. Cyber Regulatory Framework and Supervisory Practices

Regulatory Framework

35. The regulatory framework for cyber risk in the financial sector is primarily based on DORA and the DORA decree. The Legislative Decree No. 23/2025 designates the BdI, CONSOB, IVASS, and COVIP as the competent authorities responsible for ensuring compliance with DORA requirements. DORA was published in the Official Journal of the European Union on 27 December 2022 and started to be applicable from 17 January 2025. DORA aims to harmonize digital resilience requirements across the European financial sector covering five major areas, including: (i) ICT risk management; (ii) ICT-related incident reporting; (iii) digital operational resilience testing; (iv) third-party risk management; and (v) information sharing. Following the introduction of the DORA Regulation, national secondary legislation is undergoing an update which is currently being finalized. This revision also considers the national decree that extends certain provisions of DORA to domestic financial intermediaries that were otherwise excluded by the European legislator.

36. In addition to DORA, the European cybersecurity landscape is complemented by two cross-sectoral directives which were transposed in the Italian jurisdiction. The NIS2 Directive (Directive (EU) 2022/2555), transposed into Italian law through Legislative Decree No. 138/2024, establishes a harmonized framework to ensure a high common level of cybersecurity across the Union. It applies to a wide range of public and private entities operating in critical and highly critical sectors, including banking and FMIs (TVs and CCPs). The CER Directive (Directive (EU) 2022/2557), transposed in Italy through Legislative Decree No. 134/2024, focuses on the physical and operational resilience of critical entities that provide essential services across eleven sectors, including banking and FMIs (TVs and CCPs).

37. DORA acts as a *lex specialis* for the financial sector in relation to NIS2 and CER. That is, their provision concerning security measures, incident reporting, supervision and enforcement do not apply to financial entities already subject to DORA. DORA entities falling under NIS2 scope are still required to register as NIS2 entities through ACN portals and to submit mandatory and voluntary incident notification, under DORA, to the national CSIRT.

38. DORA does not cover payment systems and schemes, and related technological infrastructure providers, for which the applicable regulatory framework is defined by sector-specific regulation. They include the BdI regulation on oversight (9 November 2021) and annexes; ECB Systemically Important Payment System (SIPS) recast regulation (Regulation (EU) 2025/1355 of

Lee, Stacey Schreft, and Craig Vandre (2025). "https://www.federalreserve.gov/econres/feds/files/2025103pap.pdf," Finance and Economics Discussion Series 2025-103. Washington: Board of Governors of the Federal Reserve System.

the ECB on oversight requirements for systemically important payment systems (ECB/2025/22) (recast); and Eurosystem oversight policy framework and the Eurosystem Cyber Resilience Strategy.

39. DORA is complemented by specific Italian regulations for insurance and securities market infrastructures. For the insurance sector, IVASS Regulation No. 38 of 3 July 2018 lays down requirements on governance, including the governance of IT processes, cybersecurity and outsourcing. Also, EU-level guidelines issued by the ESAs (in particular, EIOPA) are relevant. For trading and post-trading market infrastructures, CONSOB Regulation No. 20249 of 28 December 2017, Legislative Decree No. 58 of 24 February 1998 (Consolidated Law on Finance), and the BdI Instructions of 22 December 2017, are relevant.

40. The financial sector is considered critical under the PSNC. This was introduced by Decree Law No. 105/2019. PSNC institutes a reinforced cybersecurity framework for public or private entities responsible for exercising essential functions of the State or for providing services that are essential for maintaining civil, social or economic activities fundamental to the interests of the State, considering that the malfunctioning, interruption, even partial, or improper use of certain of their networks, information systems and IT services may result in a prejudice to national security. The framework establishes mandatory and strengthened cybersecurity measures, incident reporting framework with tight deadlines (1 or 6 hours for incidents affecting ICT critical assets depending on the severity of the incident), as well as prior notification of ICT procurement to the National Evaluation and Certification Centre of ACN for technological screening of ICT products and services to be employed in the ICT critical assets included in the PSNC. It fully applies only to banks and FMIs, including TVs, considered critical and governmentally identified on the proposal of the MEF.

41. The organization of functions and responsibilities related to cyber risk supervision vary across financial authorities given their mandates.

- BdI. Cyber risk-related functions related to financial institutions supervision and internal resilience are distributed across three Directorate Generals (Table 3).

Table 3. Italy: Organization of Cybersecurity Functions at the BdI	
Function	Responsibilities
Financial institutions supervision	
• Directorate General for Financial Supervision and Regulation	• Banking Supervision 2 Directorate and the local branches are responsible for LSI offsite supervision. • Financial Supervision Directorate and the local branches are responsible for the offsite supervision of payment and electronic money Institutions and other NBFIs. • Supervisory Institutional Relations Directorate, which includes a dedicated ICT and cyber risk analysis unit (Statistical and IT Support Division), is responsible for conducting horizontal analyses on cyber risk and providing technical support to all vertical units in cyber risk analyses. • Directorate Inspectorate is responsible for conducting full-scope on-site inspections that include cybersecurity as a key component of IT risk assessment. This Directorate carries out also inspections on TVs, CCPs and CSDs, in coordination with the Directorate General for Payments and market infrastructures that is responsible for their off-site supervision.
• Directorate General for Payments and Market Infrastructures	• Vertical units are responsible for cyber risk offsite supervision of individual financial entities (e.g. CCPs, CSDs, TVs, payment systems and schemes, and supporting technological or network infrastructures). • One horizontal unit (Financial System Operational Division) is responsible for: (i) enhancing systemic operational resilience including sector-wide preparedness and crisis coordination through CODISE; (ii) facilitating information sharing and cyber threat intelligence through CERTFin and promoting sector-wide awareness initiatives; and (iii) supporting the implementation of cybersecurity testing frameworks (TIBER-IT/EU and DORA TLPT).
Internal resilience	
• Directorate General for IT	• CERTBI Division performs the functions of the CERT of the BdI.
• Directorate General for Planning, Organization and Accounting	• Operational Resilience Division coordinates the BdI's general emergency system.
Source: BdI.	

- CONSOB. Cyber risk supervision falls under the remit of the relevant supervisory units (Table 4).

Table 4. Italy: Organization of Cybersecurity Functions at CONSOB

Function	Responsibilities
• Markets Supervision Division	• leads cyber supervision for regulated TVs, CCPs, and CSDs.
• Market Infrastructures Office	• authorizes and supervises operators of trading systems, and the correct functioning of trading infrastructures, APAs, and ARMs, managing the related registers. Oversees transparency, operational resilience, governance, and critical outsourcing of TVs, assessing their organizational structures and rulebooks.
• Post-Trading Office	• authorizes post-trading infrastructures and supervises their functioning; supervises intermediaries for centralised management profiles, those participating in the CSD and CCP and their clients; monitors counterparties to securities financing operations and counterparties to derivatives operations; manages post-trading infrastructure crises.
• ICT and Artificial Intelligence Division	• provides specialized technical expertise to the Supervisory Divisions as necessary. It is also in charge of internal ICT systems.

Source: CONSOB

- IVASS. Cyber risk responsibilities are allocated according to the mandates of each of its departments, including for Prudential Supervision for Insurance Companies, Conduct Supervision for Insurance Intermediaries, Macro-prudential Supervision for the impact on Financial Stability and IT resources for technical competence and coordination on security issues and measures with other national entities.
- COVIP. Staff in the Pension Funds Supervisory Department have cross-functional expertise for the different types of pension funds.

42. Italian financial entities use a wide range of cybersecurity and IT control frameworks. The most common include ISO/IEC 27000 series, NIST Cybersecurity Framework (NIST-CSF), Control Objectives for Information and Related Technologies (COBIT); Information Technology Infrastructure Library (ITIL); International Standard in Assurance Engagement (ISAE 3402) Type II, and ISO/IEC 22301:2019. In addition, other internationally recognized standards have drawn inspiration, including the Center for Internet Security (CIS) Controls, European Union Agency for Cybersecurity (ENISA) Guidelines on Cybersecurity, and TIBER-IT framework.

43. Financial authorities use national regulations, methodologies, and EU regulations related to cybersecurity and IT control frameworks or standards in the supervisory process. At the BdI, the offsite supervision methodology has been aligned with the EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP) (EBA-GL-2017-05) and,

more recently, with the provisions of DORA. For full-scope inspections, on-site assessment of IT risk is carried out according to a dedicated methodology. To perform cybersecurity assessments, inspectors use a wide set of control frameworks or standards providing updated lists of cyber threats, security safeguards and vulnerabilities. For TVs, FMIs, payment systems and PISA entities, supervision and oversight practices are based on relevant EU regulatory frameworks (e.g. MiFID, DORA, EMIR, CSDR) and on assessment methodologies and tools (e.g. the Eurosystem CROE and Cyber Survey). At IVASS, supervisory standards are established at the international and national levels in specific guidelines (e.g. EIOPA Supervisory Handbook, IVASS Guida per la Vigilanza).

Supervisory Practices

44. Offsite cyber risk supervision involves both horizontal and vertical analyses. BdI prioritizes areas set by DORA, including ICT risk management, incident reporting, and third-party risk management. It also covers risks in payment services, emerging technologies, DORA readiness, and IT Risk Questionnaire (ITRQ) analysis. BdI classifies IT risk for LSIs as part of operational risk within the SREP framework, using ITRQ data; examines third-party risk across different supervisory phases, ICT change risk, and the impact of digital transformation on LSIs; assesses ICT risk under SREP for NBFIs and applies proportionality with both simplified and comprehensive approaches; and supervises all cyber risk domains for payment systems and FMIs, including wholesale trading venues for government bonds and multilateral trading facilities for euro-denominated deposits. IVASS conducts annual off-site benchmarking exercises to assess the adequacy of ICT risk and cybersecurity management in the insurance market. The supervision process focuses on the key ICT risk domains, ensuring compliance with DORA and supporting overall cyber resilience.

45. On-site cybersecurity examinations include comprehensive and targeted approaches. BdI assesses cybersecurity risks of supervised entities in full scope prudential inspections as part of its operational risks. All LSIs and NBFIs are regularly subject to full on-site inspections. This also applies for all FMIs, wholesale trading venues for government bonds and multilateral trading facilities for euro-denominated deposits infrastructure providers. Payment systems and scheme operators and supporting technological and infrastructure providers were subject to on-site inspection if they were supervised as a payment institution for prudential reasons. Accordingly, no payment systems and scheme operators or providers of critical services that are not supervised financial entities have been subject to on-site inspections. This is largely due to considerations of proportionality in relation to risk—given that certain retail payment systems have limited operational activity—as well as the fact that some entities have only recently entered the market or have been designated as critical providers in the recent past. IVASS targeted on-site examinations focus on the governance, management, and control of ICT risks and cybersecurity in insurance companies. Specific ICT risks may also be reviewed as part of broader on-site investigations related to other supervisory issues. CONSOB on-site examinations are expected to focus on vulnerabilities identified during off-site supervisory activities with the recent application of DORA.

46. On-site inspections of CSPs for payment systems have not been conducted to date with the exception of entities already subject to prudential supervision. Payment overseers participate in prudential on-site inspections. It is important to highlight that CSPs—broadly defined

as entities that manage and deliver technological or network infrastructure services supporting a payment system or the provision of payment services in the Italian financial ecosystem—are identified by the BdI based on several criteria outlined in Article 20 of BdI's Oversight Regulation.

47. Intrusiveness of on-site cybersecurity examinations is tailored. BdI tailors the depth of on-site inspections to each institution's cyber risk exposure, following a risk-based and proportional approach. Factors considered include past cyber incidents, institution size, operational complexity, and reliance on third-party IT providers. Inspections intensify for higher-risk institutions, involving IT experts, thorough document reviews, staff interviews, and direct system checks. IVASS uses a structured process, extracting and analyzing up to three years of security and operational data, focusing on significant risk scenarios. IVASS's methodology is based on international standards and EU guidelines and is being updated to fully align with DORA requirements.

48. Financial authorities have developed databases or knowledge bases on IT and cybersecurity of supervised firms. BdI maintains a structured database with information from the DORA ROI, supplemented by documents and contacts gathered during off-site and on-site activities. Not all data is stored in a structured way. LSIs must submit annual ITRQ data, except for certain mutual banks. For payment systems and related infrastructures, a knowledge base is maintained as required by oversight regulations. CONSOB collects information from DORA ROI together with ICT facilities data, audit reports, and similar information for trading venues, government bond markets, multilateral trading facilities, CCPs, CSDs, and centralized management. IVASS keeps documentation and assessments from both offsite and on-site examinations.

49. On-site cybersecurity examinations of LSIs are performed as part of the wide-scope analysis of their operational risks, and inspections also cover third-party service providers. For the past three years (2022-2024), and the first half of 2025, there were 196 on-site inspections, covering cybersecurity as part of the operational risk on-site assessment. Furthermore, given that Italian LSIs and other financial institutions (e.g. payment systems provider) strongly rely on IT services provided by third-parties, full-scope inspections were carried out in the period on 4 ICT service providers. Another full-scope inspection is on-going on a further IT service provider and will be finalized by the end of 2025. Some on-site inspections highlighted material deficiencies on the cybersecurity topic that were identified in specific findings.

50. Thematic cybersecurity reviews have been completed across multiple topics. As part of supervisory practices, BdI carried out thematic reviews as follows: assessing the compliance of LSIs with the EBA GL on ICT and security risk management (2024), IT Risk Questionnaire analysis (annually), Risk Data Aggregation and Risk Reporting (2023), review of ICT-related incidents (periodically), ICT change management (2024), deep dive into cyber incidents (2023, 2024), comprehensive analysis on ICT risks and operational resilience (2025), self-assessments regarding the implementation of the DORA framework (2025), ICT risks for NBFI (ongoing), Eurosystem Cyber Resilience Survey (since 2017; every 2 years), Cyber Resilience Oversight Expectations (CROE) (since 2020). The insurance and pension sectors have not performed thematic cybersecurity reviews in the past three years.

51. CROE assessments have so far been completed for seven entities where the lead overseer is BdI. Three FMI entities, which have recently become clearing mechanisms, have not been assessed against the CROE (as of November 2025) and will be assessed after the update of the CROE methodology (which is now ongoing under the Cyber resilience strategy task force). In addition, one recently designated CSP has not yet been assessed against Annex F of the PFMIs or the CROE.

52. The proportionality principle is applied across various dimensions of oversight. BdI applies proportionality mainly in selecting which LSIs undergo full IT risk assessments, with frequency and depth based on risk factors such as incidents, IT changes, and business model complexity. For NBFIs, DORA allows simplified ICT risk management for the smallest entities. Payment systems are classified as systemically important (SIPS) or not, with oversight tailored accordingly. Only SIPS are subject to the full set of international standards. CONSOB does not apply simplified treatment to CCPs and CSDs due to their systemic importance, despite DORA's proportionality principle. IVASS calibrates supervisory expectations for insurance companies based on their size and systemic relevance, requiring more advanced measures for systemic firms, while allowing simplified frameworks for non-systemic ones, provided DORA's minimum standards are met.

53. A formal rating system is used to quantify the cyber risk profile and effectiveness of cyber risk management in supervised institutions. BdI banking and financial supervision uses a four-level scale for overall ICT risk assessment: 1 (Satisfactory), 2 (Broadly satisfactory), 3 (Broadly unsatisfactory), and 4 (Unsatisfactory). The score is based on combining Risk Level and Risk Control scores, with analysts able to adjust based on available information. For on-site inspections of IT third-party service providers, no overall score is assigned since they are not directly supervised entities. For NBFIs, analysts use a tool to harmonize evaluations across risk areas, assigning scores between 0 and 4 for both risk level and controls. An automated macro calculates the overall ICT risk score. IVASS assesses cyber risk within its operational risk rating system for the insurance sector, also using a four-level scale (1–4).

54. The practice of financial institutions making provisions against future cyber losses vary. For banks, there are no specific supervisory expectations regarding provision against future cyber loss. However, in this context general accounting rules are applicable. Therefore, a provision is expected in the case of probable outflow of resources. For NBFIs, provisions are not specifically required, but some of them take out cyber insurance. FMIs and entities operating regulated markets are required to maintain adequate liquid resources to cover potential losses, as identified by these financial entities in risk-based scenarios, which could include those arising from cyber events. For the insurance sector, potential cyber losses are included in provisions against operational risk.

55. As a general principle, for both IT/cyber risk and other risk categories, the BdI and IVASS supervisory process does not exclusively rely on external or independent attestations. During both on-site and off-site assessments, supervised entities falling in the competence of the Italian authorities are requested to provide the result of a specific examination carried out by the internal audit or any available independent or third-party attestations, such as reports issued by the

third line of defense, ISO/IEC 27000 series audit certifications, or equivalent documentation. Regarding the IT risk, reliable information is collected also through the on-site inspections on IT providers.

56. Financial entities generally receive feedback on risk assessments, but the exact risk rating is not always disclosed. For LSIs and NBFIs supervised by BdI that are recipients of recommendations, annual assessment results and priorities are summarized in a letter. Third-party service providers are encouraged to inform clients about inspection findings and remediation plans. Authorities may also communicate findings directly to supervised intermediaries. For FMIs, TVs, and payment systems, feedback reports include analysis results and prioritized recommendations, sometimes with numeric or qualitative priority levels. IVASS formally communicates exit reports and follow-up actions after on-site examinations, while CONSOB assigns priority levels (high, medium, low) to recommendations and informs institutions accordingly.

57. The practice of follow up of findings and dealing with high-risk repeat findings vary. BdI incorporates the follow-up process for IT risk in its overall general supervisory follow-up. After inspections, banks and NBFIs must submit action plans, which are monitored by off-site supervision. For third-party service providers, BdI requests timely remediation actions and monitors implementation and the supervised institutions are required to consider the findings and to monitor the remediation plan. For payment systems, BdI monitors follow-up plans after issuing recommendations. CONSOB and BdI, in line with the powers conferred on them by the Consolidated Law on Finance, follows up on findings in the securities sector (CCPs, CSDs, TVs). High-risk repeat findings can be escalated to the entity's board or result in fines. IVASS follows up on all findings from on-site and off-site analyses, verifies remedial actions, and may conduct further inspections if high-risk vulnerabilities persist.

58. Use of third-parties or the supervised institutions' third line of defense to provide assurance on the appropriate implementation of authorities' recommendations varies. BdI and CONSOB primarily monitor and directly assess the implementation of their recommendations. Supervised entities are required to provide, annually, a report of all (internal and external) audit assessments carried out with a summary of the main findings and the relevant remediation actions. Moreover, the results of the most critical IT audits are required in the annual ITRQ. In addition, when circumstances warrant, BdI may request a specific audit investigation. These measures are not systematically applied. For payment systems, authorities can obtain independent third-party reports requested by the entity and reports from the entity's third line of defense. IVASS does not use the first and second lines of defense for this purpose.

59. The sanctions regime is diverse and, until the entry into force of DORA, deficiencies in the management of cyber risk were considered within the broader framework of organizational shortcomings and internal controls weaknesses related to operational risk. Therefore, no specific sanctions for non-compliance with cyber risk regulations have been imposed in the past three years. Italian financial authorities (BdI, CONSOB, IVASS, COVIP) have the power to impose penalties or remedial measures for breaches under DORA and other sectoral acts. For insurance, the sanctioning framework is detailed in Regulation no. 38/2018. For payment systems,

schemes, and related infrastructures, BdI can take measures such as prohibiting transactions, restricting activities, or suspending operations to address infractions. Non-compliance with the PSNC or NIS2 Directive can trigger significant sanctions, including fines up to EUR 10 million or 2 percent of global turnover, binding instructions, management bans, and other remedial actions; no court challenges have occurred to date.[9]

Observations and Recommendations

60. The regulatory and institutional framework for cyber risk in Italy is largely shaped by the broader regulatory framework for cybersecurity in Europe. This is primarily led by DORA and complemented by NIS2, CER, and by assessment methodologies and tools such as CROE. The legal basis for cybersecurity also comprises national laws and regulations. Supervisory practices for cyber risk are also informed by the results of on-site inspections of third-party service providers given the wide usage of outsourcing by financial entities. Audit reports are largely used on a case-by-case basis. Thematic cybersecurity reviews have been completed across multiple topics (ITRQ, CRS, CROE, DORA-readiness, among others) but have not been conducted for the insurance and pension sectors. While self-assessments or disclosure frameworks are not aimed at monitoring the implementation of remedial action for FMIs and payment systems, all recommendations are addressed by the relevant overseen entity through a Remediation Plan, which is jointly agreed upon with the competent authority. Remedial actions are typically monitored on a quarterly basis and are only closed after the submission and verification of adequate supporting evidence. This process could be lengthy and take several years where financial entities need to be induced to remediate deficiencies in a timely manner, if needed, given the evolving cyber threat landscape. Until the entry into force of DORA, deficiencies in the management of cyber risk were considered within the broader framework of organizational shortcomings and internal controls weaknesses related to operational risk. Where such deficiencies were identified, they have also been subject, if material, to sanctioning measures. With the entry into force of the national legislation implementing the DORA framework (March 2025), shortcomings in cyber risk management have acquired a more autonomous significance and could, going forward, be subject to dedicated enforcement actions, including the imposition of sanctions.

61. The following is recommended:

- Complete cyber resilience assessments for the remaining FMIs and CSPs based on the proportionality principle with ongoing monitoring on a periodical basis to induce action. In line with the current practices, this would imply the following: (i) folding CROE high-level assessment results into the overall assessment of FMIs and CSPs and considering results relative to the rating for each relevant principle (such as for operational risk); (ii) continuing the ongoing monitoring of remedial actions through greater disclosure, where applicable, to induce action (such as communication through annual reports, financial stability reports, or other special dedicated reports such as part of an FMI or payment systems oversight report); and (iii)

[9] BdI publishes in electronic form the administrative sanctions adopted for violations in prudential matters, transparency and protection of customers, prevention and combating of money laundering and terrorist financing.

continuing to ensure the consistent application of the CROE across central bank and privately-operated FMIs, taking into account existing regulatory frameworks applicable to the relevant entities.

- Complement offsite inspections and ongoing monitoring of cyber risks with audit and testing reports by independent parties for LSIs and NBFIs. Offsite inspections and ongoing monitoring of third-party service providers of supervised entities should continue with the regular submission of audit or testing reports by independent parties. For example, this could include pooled audits and results from TLPT, as applicable and relative to the risk profile of the supervised entity. For benchmarking purposes, the practice of regularly collecting ICT audit reports, among other information, has been performed on supervised entities under BdI and CONSOB. Such practices are also common at the international level.[10]

- Increase the focus on cyber risks during on-site inspections in supervised entities and give close attention to new entrants (LSIs, NBFIs, FMIs, CSPs). Consider the risk profile of supervised entities and determine the investigation depth to be devoted during on-site inspections to cyber risks (comprehensive versus focused examinations), taking into account the proportionality principle. For LSIs and NBFIs, this could consider a few selected domains of cybersecurity risks (such as governance and third-party risk management) for focused examinations to complement offsite inspections, regular full scope on-site inspections where cyber risk is covered as part of operational risk assessments, and on-site inspections of third-party service providers. If the supervised entity has a higher risk profile relative to others, a full scope on-site inspection of cyber risk should be considered. As risks could be higher for new entrants, this should warrant close attention from supervisors.

- Conduct thematic cybersecurity reviews for the insurance and pension sectors. Given that ITRQs focus on LSIs and the CRS and CROE are applicable to FMIs, a thematic cybersecurity review focused on financial entities providing insurance and pension services would help provide a more comprehensive view of the cyber maturity levels of firms in these sectors.

- Promote operational resilience to effectively manage operational risks that may arise from disruptions from cyberattacks and technology failures, and exercise enforcement powers, as needed, for non-compliance with cyber risk related regulations. While the digital operational resilience of LSIs and NBFIs would be guided by DORA, financial authorities could complement the inspection of supervised entities with the BCBS Principles for Operational Resilience (POR).[11] The inspections could focus on whether supervised entities have assumed that disruptions will occur to define their overall risk appetite and tolerance for disruption accordingly. For FMIs, CROE assessments could be complemented with the PFMI, particularly to assess the ability of FMIs to meet defined recovery time objectives (RTOs) under extreme but plausible cyberattack scenarios, and if necessary, remedial actions that should be induced and

[10] FSB (2023). Final Report on Enhancing Third-party Risk Management and Oversight – A Toolkit for Financial Institutions and Financial Authorities, December.

[11] BCBS (2021). Principles for Operational Resilience, March.

taken for their continuous improvement.[12] For systemically important FMIs, the oversight expectation is two-hours RTO, including for extreme but plausible scenarios. Given the occurrence and rising trend of cyber and operational incidents, considering the recent entry into force of the national legislation implementing the DORA framework (March 2025), financial authorities should consider exercising their enforcement powers (such as fines, suspension of activities, change of management), if necessary, for regulatory compliance.[13]

E. Response and Recovery

62. Financial authorities have been involved in industry-wide cybersecurity crisis management exercises. This occurs at the national, European and international levels.

- At the national level, the BdI designs, organizes, and conducts exercises within the CODISE, in collaboration with Consob and other relevant stakeholders. The last cybersecurity exercises were connected to the G7-CEG exercises.

- At the European level, the BdI participates in yearly table-top exercises organized by the ECRB. BdI participated in the 2024 SSM Cyber Resilience Stress Test for SIs, assessing banks' response and recovery capabilities following a severe cyber incident. The test involved 109 banks (including all Italian SIs), with 28 undergoing extensive testing and on-site supervisory visits. Results indicated established response and recovery frameworks, though areas for improvement remain. BdI is also involved in discussions on extending cyber stress tests to LSIs.

- At the international level, the BdI and CONSOB, together with the MEF, participate in the cybersecurity exercises organized by the G7-CEG. In this case the BdI usually contributes with the G7 jurisdictions and on a rotation bases, to the organization, scenario design, management of the exercises, and follow-up. The last exercises helped improve the level of readiness, while areas of improvement were on coordination and communication.

- In addition to authority-driven exercises, all members of CERTFin, including financial authorities, are invited to participate in the industry-wide cybersecurity exercises promoted annually by the organization. These initiatives aim to strengthen the collective readiness and resilience of the Italian financial ecosystem.

63. A wide range of financial institutions participate in industry-wide cybersecurity exercises coordinated by BdI through CODISE. This includes the main banks, CCPs, CSDs, trading venues, payment system operators, and service providers. National-level exercises typically involve 10–20 entities. CERTFin, MEF, CONSOB, IVASS, and other relevant institutions (such as ACN) are also

[12] CPMI-IOSCO (2012). Principles for Financial Market Infrastructures, April. See also, Khiaonarong, T., H. Leinonen, and R. Rizaldy (2021). "Operational Resilience in Digital Payments: Experiences and Issues," IMF Working Paper, WP/21/288.

[13] For context, European authorities were recommended to amend the regulatory framework so that it is possible to levy fines on CTPPs for non-compliance with requirements. See IMF (2025). Euro Area: Technical Note on Cyber Risk and Financial Stability, July.

involved. CERTFin organizes exercises using REDFin methodologies, ranging from red teaming to table-top simulations, open to its constituency and sometimes initiated by participants. From 2023 to 2024, an average of two table-top exercises were held annually. In 2025, the first exercise involved about 10 financial entities, with another planned for November 2025. As to the insurance sector, IVASS, major companies and, on a voluntary basis, smaller companies, have been involved in sectoral crisis management exercises. IVASS has evaluated cyber stress scenarios for the insurance sector in coordination with EIOPA, assessing impacts on insurers' resilience and portfolios. In March 2024, IVASS participated in a two-phase EIOPA walkthrough exercise, simulating both idiosyncratic and system-wide cyber crises.

64. Cybersecurity testing constitutes an integral component of the cybersecurity strategy and framework mandated for supervised institutions. Under DORA, financial entities in scope of the regulation are required to establish a structured testing program. This program must adopt a risk-based approach and encompass a variety of testing methodologies, including but not limited to vulnerability assessments and penetration testing. Furthermore, a subset of these institutions—identified by competent authorities based on criteria such as risk profile, threat landscape, and systemic relevance set out in the Commission Delegated Regulation (EU) 2025/1190—must conduct advanced testing at least once every three years. This is to be carried out through TLPT. CSDs and CCPs are obligated to perform vulnerability assessments prior to the deployment or redeployment of new or existing applications, infrastructure components, and ICT services that support critical or important functions. For all institutions within the scope of DORA, security requirements must be tested before deployment into the production environment. For payment systems and the supporting technological or network infrastructures subject to the BdI's Regulation on Oversight (9 November 2021), the "Controls Operational Guidance" requires the implementation of a comprehensive program of audits and related outcomes. This program may include various testing methodologies and cyber risk scenarios. The guidance draws extensively from the CROE and mandates that entities adopt a risk-based approach in defining their testing programs. These should include multiple testing methodologies such as vulnerability assessments, penetration testing, and TLPT.

65. Under DORA, insurance companies that satisfy the criteria reported in Commission Delegated Regulation (EU) 2025/1190 must perform at least one TLPT within three years. Other companies could conduct a TLPT voluntarily, in compliance with the TIBER-IT methodology. Indeed, IVASS has adopted, together with BdI and CONSOB, the TIBER-IT Guide, i.e. the national implementation of the TIBER-EU framework, which defines the methodology for red teaming test activities.

66. Cyber resilience stress testing for FMIs and PISA entities have not yet been conducted. This tool, part of the revised Eurosystem Cyber Resilience Strategy, will assess entities' ability to recover from successful cyberattacks. Financial institutions are required to prepare cyber maps, unlike those that are not in scope of DORA. Prior to DORA, entities mapped critical assets, interconnections, third-party dependencies, and potential contagion channels as part of ICT and operational risk management. DORA now requires identification and mapping of all critical

information and ICT assets, including dependencies on third-party providers supporting critical functions.

67. CODISE acts as Italy's national unit for business continuity, coordinating crisis communication among BdI, CONSOB, systemic operators, and other authorities. CODISE manages operational crises, including those derived from ICT and cyber incidents, and is activated for systemic events, serving as the main contact point for cross-border cyber crises. It enables structured, secure information exchange, early alerts, and joint impact assessment during systemic operational crises (among Authorities of the financial sector, other Authorities, and systemic operators), supporting coordinated response and recovery in the financial sector. CODISE conducts business continuity exercises at the national and international levels (G7, EU-SCICF, Eurosystem) and provides a forum for analysis and discussion among participants. In the context of the CODISE, a dedicated crisis communication protocol (e.g. joint press releases) has been developed between BdI, CONSOB and the MEF and successfully tested in both exercises and real-life situations, incorporating lessons learned.

68. CERTFin has developed and regularly updates playbooks for various cyber risk scenarios, such as ransomware and DDoS attacks, detailing steps for preparedness, detection, response, and recovery. Workshops and briefings are organized by CERTFin, involving industry experts and authorities, to share experiences and raise awareness of different attack scenarios. Italian financial authorities benefit from G7-CEG scenario libraries, including cross-border crisis exercises. BdI has internal incident management processes and playbooks that define clear roles and procedures for all stages of cyber incident response, including emergency communication templates. IVASS follows BdI's rules and playbooks for managing crisis scenarios affecting its IT systems, under a collaboration protocol renewed every five years.

69. BdI coordinates the advanced security testing methods. The TIBER-IT framework (jointly adopted in 2022 by BdI, as lead authority, CONSOB, and IVASS and introduced on a voluntary basis) provides a common methodology for TLPT in the financial sector. It constitutes the Italian implementation of the European framework for advanced security testing (European Threat Intelligence Based Ethical Red Teaming – TIBER-EU). Such tests simulate sophisticated, intelligence-based cyberattacks to assess the real detection and response capabilities of financial organizations. TIBER-IT has been aligned with DORA requirements and with Delegated Regulation (EU) 2025/1190. This helps ensure consistency between national testing practices and the EU-wide TLPT regime. TIBER-IT helps enhance entity-level and systemic preparedness by promoting realistic scenario testing and follow-ups on identified weaknesses. TIBER-IT is also an important instrument for evaluating operational resilience in live environments and for coordinating with other national authorities on cyber testing and oversight convergence. Since 2022, eleven voluntary TLPT have been conducted on Italian entities. This has included five banks, one ICT provider, two e-money institutions, and three insurance undertakings.

Observations and Recommendations

70. Financial authorities are actively involved in cybersecurity crisis management exercises and advanced security testing methods. National exercises are organized by BdI through CODISE, involving major banks, market infrastructures, and service providers. These exercises often connect with G7-CEG initiatives. European and international participation includes yearly table-top exercises (ECRB) and G7-CEG events, with BdI contributing to organization and scenario design, in collaboration with CONSOB where appropriate. CERTFin promotes annual industry-wide exercises, using methodologies like red teaming and table-top simulations, targeting a broad constituency. CODISE serves as the national unit for business continuity and crisis communication, ensuring structured, secure information exchange and coordinated response across authorities and the financial sector in case of operational crises affecting the Italian financial system. DORA advanced testing and the TIBER-IT guide establish an integrated framework for TLPT, covering both mandatory and voluntary testing, to assess and enhance cyber preparedness.

71. The following is recommended:

- Continue cyber stress testing exercises with supervised entities (LSIs, NBFIs, FMIs) to test exit strategies. Plan cyber stress testing exercises with supervised entities, including scenarios such as supply chain attacks that test exit strategies for third-party service relationships involving critical services, and cross-sectoral exercises with other critical infrastructures such as for energy and telecoms.

- Use results from advanced security testing methods for the continuous improvement of cyber response and recovery plans.[14] Such testing methods could include TLPT such as the TIBER-IT. This would be relevant for supervised entities that fall under the criteria established under DORA. For those FMIs, which are guided by the CROE and out-of-scope of DORA, such tests could help assess the ability of the FMI to realistically meet defined RTOs. For systemically important FMIs, the oversight expectation would be two-hour RTO. As many systemically important FMIs may find it challenging to meet this oversight expectation in practice, the use of results from advanced methods could nevertheless help identify opportunities for improvement and remedial actions to ensure the practicability of workarounds for business continuity (such as using manual procedures), where applicable.

- Evaluate onboarding COVIP to CODISE. COVIP is one of the four DORA authorities and has a common interest in the supervision of cyber risk due to the interconnection within the financial system (e.g. banks and insurance firms offering pension services).

[14] FSB (2020). Effective Practices for Cyber Incident Response and Recovery, Final Report, October.

F. Information Sharing and Incident Reporting

Information Sharing

72. In general, financial authorities regularly share information on cyber incidents and threats affecting supervised entities on which there is a common interest. CERTBI is the focal point for the collection, analysis and sharing of information related to cyber threats, and for the coordination of activities aiming at preventing and supporting the response to cyber emergencies that could harm IT-assets of the BdI and IVASS.

73. CERTFin was established as the cyber information and intelligence sharing arrangement for the whole financial sector, including public and private entities. CERTFin represents the cooperation forum for cyber threat intelligence, incident coordination, and fraud prevention across the national financial ecosystem. Its mission is to enhance cyber resilience, promote situational awareness, and facilitate operational coordination among key financial sector stakeholders. CERTFin also collaborates with peer financial CERTs and sectoral response teams globally through bilateral cooperation agreements (e.g. Nordic Financial CERT, FS-ISAC Japan, FinCERT Jordan, FinCERT Kuwait).

74. Financial authorities in Italy participate in multiple information-sharing groups at both national and international levels. Nationally, BdI, CONSOB, and IVASS leverage CERTFin for structured cyber threat intelligence, incident coordination, and public-private cooperation. CERTFin maintains bilateral agreements with peer organizations, enhancing sector-wide cyber resilience. CERTBI is active in global intelligence communities like TI, FIRST, and FS-ISAC. At the European level, BdI's dual role in CIISI-EU provides broad access to intelligence for both regulatory and operational needs.

75. Financial authorities in Italy have established information-sharing arrangements with foreign counterparts, as encouraged by DORA. CERTFin participants benefit from agreements with peer entities, including those operated by authorities in foreign countries (e.g. Jordan and Kuwait. The 4CB group (BdI, Deutsche Bundesbank, Banco de España, Banque de France) exchanges cyber threat information to protect TARGET Services. BdI is active in the ESCB's Operational Security Contacts and participates in the Operational Security Situational Awareness Teleconference with 40 national central banks. At the G7 and SSM levels, protocols and exercises (like Cyber Incident Response Protocol, SSM Cyber Incident Group, and SSM Cyber-Dry Run) coordinate responses and test information sharing for major cyber incidents affecting the financial sector.

76. Under DORA, financial authorities in Italy have begun formalizing information-sharing arrangements with other domestic authorities. BdI and CONSOB are working on an information-sharing arrangement for operational and informational coordination of tasks for entities they both supervise. Similar MoUs are envisaged with IVASS and COVIP. DORA Authorities and the Italian Financial Police are finalizing a MoU to exchange information on ICT incidents and cyber threats, aiming to prevent and address criminal offenses affecting digital operational resilience. DORA Authorities and ACN will stipulate an agreement to regulate consultancy, technical assistance, and

rapid responses for cyber incidents, also with regards to activities involving critical ICT third-party service providers.

77. CERTBI and ACN signed an MoU to exchange information and cooperate in defending against cyber threats. The MoU enables reciprocal sharing of information to prevent and counter cyber threats, including reports on techniques, tactics, and attack procedures. BdI has a bilateral agreement with the Carabinieri military police for cyber threat information exchange and cooperation. Another convention exists between BdI and the Dipartimento della Pubblica Sicurezza of Ministero dell'Interno for cybercrime prevention. This convention supports cooperation between the Postal Police and CERTBI to prevent and combat cybercrimes, including sharing cyber threat information.

Incident Reporting

78. Starting January 17, 2025, DORA introduced a unified European framework for reporting ICT-related incidents, which replaces the incident frameworks previously adopted. All financial entities in scope of DORA must mandatorily report major ICT-related incidents and may voluntarily report significant cyber threats to their competent authority. DORA designates a single competent authority for each type of supervised entity to receive these reports. For entities under shared supervision, the receiving authority must promptly forward reports to other relevant authorities according to information-sharing arrangements.

79. In the first six months of the new incident reporting framework, BdI received 27 cyber-attack notifications. The attacks included 13 data exfiltration/manipulation, 10 supply-chain attacks, 9 ransomware/data encryption, 6 social engineering/phishing, 5 identity theft, 4 DDoS, and 3 other types. Most attacks targeted SIs (10), followed by LSIs (5), payment institutions (2), and e-money institutions (1). Nine incidents were reported by entities not previously subject to DORA, including 8 asset management companies and 1 investment firm. As of October 2025, no cyber incidents have been reported by entities operating payment systems or FMIs within DORA's scope. One incident on a TV was reported at the end of October.

80. The incident reporting framework for payment systems and schemes, and the supporting technological or network infrastructures are guided by the ECB. Recently, it has been updated with the oversight instructions of the BdI (November 2021) and aligned to the ECB incident reporting framework for systemically important payment systems and has been informed by the EBA Guidelines on major incident reporting under the Payment Services Directive 2.

81. Data on cybersecurity incidents is routinely collected by financial authorities under the provision of DORA. Major ICT-related incidents that could impact operational resilience must be reported. This includes system outages, cyber-attacks, data breaches, failures in major service components, including third-party services, and any event that may significantly disrupt business operations or affect financial stability. Financial entities classify ICT-incident as "major" or not, based on criteria and thresholds outlined in the Commission Delegated Regulation (EU) 2024/1772. Data are collected in accordance with Commission Delegated Regulation (EU) 2025/301 and Commission

Implementing Regulation (EU) 2025/302, which supplement DORA. A similar criterion is established for payment system and the supporting technological or network infrastructures with the annex to the oversight instructions of the BdI.

82. DORA guides the taxonomy, severity, and materiality of cyber incidents for financial entities. An ICT-related incident is defined as any unplanned event that compromises network or information system security and adversely affects data or services. Severity is assessed using criteria such as client and transaction impact, duration, geographical spread, data loss, service criticality, and economic impact. Materiality is determined according to Commission Delegated Regulation (EU) 2024/1772. For payment systems and related infrastructures, specific taxonomy and materiality methodologies are detailed in the BdI's oversight instructions.

83. Cyber incident reporting templates are issued to supervised institutions in line with DORA requirements. The ESAs have developed two official formats for reporting incidents and significant cyber threats: Excel (XLSX) and Java Script Object Notation (JSON). Currently, Italian financial entities must submit reports using the XLSX format. Each national competent authority provides specific reporting instructions and channels for entities under its supervision. For payment systems and schemes, and related technological or network infrastructures, reporting templates are shared bilaterally with entities.

84. CSIRT Italia is mandated to maintain a national cross-sectoral database of cyber incident notifications at the national level. The database collects information from financial entities required to report incidents directly to CSIRT. Specific financial entities have direct reporting obligations for cyber incidents to CSIRT. Finally, for DORA purposes, the competent authorities will enter into agreements with the ACN to regulate information exchange, which may include data on ICT-related incidents notified by other DORA financial entities. CSIRT Italia, within ACN, also supports national cyber situational awareness by helping correlate incidents across sectors where cyber events affecting financial entities may be part of a broader threat picture.

Observations and Recommendations

85. Financial authorities routinely share information on cyber incidents and threats affecting supervised entities, focusing on common interests. CERTBI is the central hub for collecting, analyzing, and sharing cyber threat information, coordinating prevention and response activities for BdI and IVASS. CERTFin serves the entire financial sector acting as a public-private forum for cyber threat intelligence, incident coordination, and fraud prevention within its constituency. It enhances resilience, situational awareness, and operational coordination, and collaborates globally with peer CERTs. There are industry-wide groups, international arrangements, and MoUs.

86. Financial entities must report major ICT incidents mandatorily and significant cyber threats voluntarily to their competent authority under DORA. Each supervised entity has a designated authority for incident reports. For entities under shared supervision, reports are forwarded to all relevant authorities. Incident reporting for payment systems is guided by the ECB

and aligned with European oversight and EBA guidelines. CSIRT Italia maintains a database of cyber incident notifications, receiving reports directly from some financial entities and via DORA authorities for major incidents.

87. The following is recommended:

- Improve information sharing on cyber risk supervision and evaluate onboarding COVIP to CERTFin. Financial authorities should establish MoU to share information in the areas of building capacity on cybersecurity and sharing supervisory information related to cyber risk management in the financial sector. This goal could be reached also through the adhesion to the already established CERTFin. COVIP is one of the four DORA authorities in Italy and has a common interest in the supervision of cyber risk due to the interconnection within the financial system (e.g. banks and insurance firms that offer pension services).

G. Cyber Deterrence

88. Cybercrime regulation is included in the Italian Criminal Code, detailing types of cybercrimes and corresponding punishments, and is updated in line with EU directives and international conventions like the Budapest Convention. Law enforcement assists with cyber incidents. The Italian CSIRT (within ACN) coordinates with law enforcement, focusing on both cyber resilience and investigations, and shares incident reports for prosecution. ACN has signed three MoUs with law enforcement agencies to facilitate information sharing on cyber incidents. BdI and IVASS cooperate with law enforcement and financial institutions to detect, investigate, and prosecute cyber criminals. Major banks, the Italian Banking Association, and other financial entities have collaborative arrangements with law enforcement. CERTFin works with the Italian National Police, and Poste Italiane and the Ministry of the Interior have agreements to strengthen cybersecurity for public services, focusing on prevention, information sharing, and joint response.

H. Capacity Development

89. Financial authorities have demonstrated commitment to strengthen cyber risk supervision capabilities. BdI created or reinforced three specialized units: one for oversight of third-parties and outsourcers, one for ICT risk horizontal analysis, and another for business continuity and cyber resilience. Internal committees (Cybersecurity Committee and DORA Steering Committee), staff exchanges, and recruitment of IT/cybersecurity experts support these efforts. Advanced training programs enable flexible use of generalist staff, including in cyber risk supervision. Staff participate in JETs as part of the DORA oversight framework. BdI, CONSOB and IVASS have implemented a dedicated recruitment plan for IT/cybersecurity specialists and offers staff training programs, including those by the EU Supervisory Digital Finance Academy.

90. Multiple methods are used to raise cybersecurity awareness. Workshops and conferences are organized by BdI also with financial authorities, market operators, and stakeholders. The central bank's website features a dedicated cybersecurity section, and awareness is integrated into broader financial education and consumer protection strategies targeting diverse audiences.

CONSOB collaborates with national authorities, participates in workshops and public-private partnerships, and maintains a cybersecurity section on its website, complementing consumer protection resources. IVASS engages in workshops, partnerships, and academic collaborations to raise cybersecurity awareness among insurance firms, intermediaries, and customers, with a website section focused on threats and scams. CERTFin runs multi-year public cybersecurity awareness campaigns and recent efforts focus on financial and payments frauds via social media platforms. ACN is also strongly involved in activities to raise cybersecurity awareness, both from a regulatory and from a substantial risk perspective, taking part in hundreds of seminars, workshops, and events that include financial operators as well as ICT service providers, promoting initiatives aimed at small and medium sized enterprises and NIS2 entities and their third-parties, videos on social media as well as television spots and, more recently, a weekly segment on national radio. Moreover, initiatives involving multiple institutional actors have been deployed, such as the Navigati campaign on television.

91. Financial authorities offer various cybersecurity training programs for supervisors. This has included internal specialist training and external courses at ESAs, ECB, and Eurosystem level. Staff can participate in courses at Italian universities, academies, research centers, and in workshops or seminars by international organizations and trade associations. BdI's Corporate Academy covers cybersecurity in its thematic schools, such as Banking and Financial Supervision and New Technologies and Data Science. Staff can pursue certification programs (e.g., ICT Auditors, Certified Information Systems Auditor, Certified Information Systems Security Professional) and Master's degrees, with costs partly covered by BdI. IVASS collaborates with BdI for internal training, offering a yearly catalogue of technical courses, and occasionally hosts expert-led sessions on new technologies and cybersecurity risks.

92. Financial authorities have progressively increased cybersecurity staffing due to the rising relevance of cyber and ICT risk and new policies like DORA. BdI employs 40 staff with ICT/cyber expertise in Banking and Financial Supervision, 30 in Payments and FMIs, and 20 in Information Technology. CONSOB has 15 staff dedicated to cyber and ICT risk supervision and internal cybersecurity. COVIP employs 26 staff with cross-functional expertise in pension fund supervision but lacks a centralized cyber risk supervision function. IVASS has 4 staff for supervision and one IT department expert and relies on external consultants and BdI staff for cybersecurity tasks.

Observation and Recommendations

93. The following is recommended:

- Support ongoing staff training on cyber risk supervision and oversight and reallocating resources for on-site cyber risk supervision. Support staff training and professional certifications in cybersecurity risk management. Reallocate resources to support the on-site inspection of cyber risk in all the supervised entities relative to their risk profile.