FSB FINANCIAL STABILITY BOARD

Peer Review of Spain

Review report

18 November 2025

The Financial Stability Board (FSB) coordinates at the international level the work of national financial authorities and international standard-setting bodies in order to develop and promote the implementation of effective regulatory, supervisory and other financial sector policies. Its mandate is set out in the FSB Charter, which governs the policymaking and related activities of the FSB. These activities, including any decisions reached in their context, shall not be binding or give rise to any legal rights or obligations.

Contact the Financial Stability Board

Sign up for e-mail alerts: www.fsb.org/emailalert
Follow the FSB on Twitter: @FinStbBoard
E-mail the FSB at: fsb@fsb.org

Table of Contents

Foreword

Financial Stability Board (FSB) member jurisdictions have committed, under the FSB Charter and in the *FSB Framework for Strengthening Adherence to International Standards,*[1] to undergo periodic peer reviews. To fulfil this responsibility, the FSB has established a regular programme of country and thematic peer reviews of its member jurisdictions.

Country reviews focus on the implementation and effectiveness of regulatory, supervisory or other financial sector policies in a specific FSB jurisdiction. They examine the steps taken or planned by national/regional authorities to address International Monetary Fund (IMF)-World Bank Financial Sector Assessment Program (FSAP) and Reports on the Observance of Standards and Codes recommendations on financial regulation and supervision as well as on institutional and market infrastructure that are deemed most important and relevant to the FSB's core mandate of promoting financial stability. Country reviews can also focus on regulatory, supervisory or other financial sector policy issues not covered in the FSAP that are timely and topical for the jurisdiction and for the broader FSB membership. Unlike the FSAP, a peer review does not comprehensively analyse a jurisdiction's financial system structure or policies, or its compliance with international financial standards.

FSB jurisdictions have committed to undergo an FSAP assessment every five years; peer reviews taking place typically two to three years following an FSAP will complement that cycle. As part of this commitment, Spain volunteered to undergo a peer review in 2025.

This report describes the findings and conclusions of the Spanish peer review, including the key elements of the discussion in the FSB's Standing Committee on Standards Implementation (SCSI) in September 2025. It is the second FSB peer review of Spain and is based on the objectives and guidelines for the conduct of peer reviews set forth in the *Handbook for FSB Peer Reviews.*[2]

The analysis and conclusions of this peer review are based on the responses to a questionnaire by financial authorities in Spain and reflect information on the progress of relevant reforms as of July 2025. The review has also benefited from dialogue with the Spanish authorities as well as discussion in the FSB SCSI.

The draft report for discussion was prepared by a team chaired by Jane Magill (Australian Prudential Regulatory Authority) and comprising Antoine Lhuissier (Banque de France), Tarun Singh (Reserve Bank of India), Cevdet İlker Kocatepe (Banking Regulation and Supervision Agency of Türkiye). Graham Ellis (Australian Prudential Regulatory Authority), Lara Douglas, Matt Steiger and Terence Choy (FSB Secretariat) provided support to the team and contributed to the preparation of the report.

1 FSB (2010), *FSB Framework for Strengthening Adherence to International Standards*, January.

2 FSB (2017), *Handbook for FSB Peer Reviews,* April.

Abbreviations

BCP	Business Continuity Plan
BdE	Banco de España
BME	Bolsas y Mercados Españoles group
CCN	Centro Criptológico Nacional
CERT	Computer Emergency Response Team
CNMV	Securities and Exchange Commission of Spain (Comisión Nacional del Mercado de Valores)
CROE	Cyber Resilience Oversight Expectations
CSIRT	Computer Security Incident Response Teams
CTPP	Critical Third Party Provider
DGSFP	Directorate General of Insurance and Pension Funds (Dirección General de Seguros y Fondos de Pensiones)
DORA	Digital Operational Resilience Act
DSN	Departamento de Seguridad Nacional
EIOPA	European Insurance and Occupational Pensions Authority
ENISA	European Union Agency for Cybersecurity
ESA	European Supervisory Authority
ESMA	European Securities and Markets Authority
EU	European Union
EU-SCICF	EU Systemic Cyber Incident Coordination Framework
FINMA	Swiss Financial Market Supervisory Authority
FMI	Financial Market Infrastructure
FSAP	Financial Sector Assessment Program
FSB	Financial Stability Board
IAIS	International Association of Insurance Supervisors
ICT	Information, Communication and Technology
IMF	International Monetary Fund
INCIBE	Instituto Nacional de Ciberseguridad
ISAC	Information Sharing and Analysis Centre
LSI	Less Significant Institution
NIS	Network and Information Systems security directive
SCSI	Standing Committee on Standards Implementation
TIBER	Threat Intelligence Based Ethical Redteaming
TLPT	Threat Led Penetration Testing

Executive summary

Background and objectives

The main purpose of this peer review is to assess Spain's efforts to enhance cyber resilience in its financial sector so as to address financial stability risks arising from operational incidents and cyber-attacks. The review focused on the monitoring frameworks, supervisory practices, and incident response mechanisms adopted by various Spanish financial authorities to manage the relevant risks.

Main findings

With the growing digitalisation of financial products and services, the Spanish financial sector has progressively embraced technology, including solutions provided by third-party service providers. This trend has heightened the sector's exposure to operational risks and cyber threats, necessitating ongoing monitoring and proactive risk management measures.

The Spanish authorities have placed significant focus on enhancing cyber resilience of the financial sector. Banco de España (BdE) maintains robust risk-based supervisory oversight of Less Significant Institutions (LSIs) that includes a focus on cyber resilience. Spain was an early adopter of the Threat Intelligence Based Ethical Red teaming (TIBER) framework that provides structured red-team testing for banks. Historically, there was some limited oversight of cyber resilience in the FMI and insurance sector, however, recently there has been a substantial effort across all financial sectors to prepare the industry for the increased expectations under the European Union (EU) Digital Operational Resilience Act (DORA).

Notwithstanding these good practices, the evolving cyber risk landscape warrants further enhancements from Spanish authorities to address rising challenges. These include (i) developing a sectoral cyber threat landscape, (ii) leveraging best practices in supervision approaches, (iii) considering national analysis of third-party risks, and (iv) streamlining incident notification and response.

Develop a comprehensive sectoral cyber threat landscape

Each financial authority collects and analyses their respective cyber intelligence to inform their activities, with limited sharing back to industry. There is no comprehensive sectoral or cross sectoral threat landscape created that could be disseminated to inform decision making. Such a document could provide intelligence to smaller firms that may not have their own surveillance capacity and assist both authorities and firms in prioritising areas of focus when addressing cyber risks.

Leverage best practices in supervision approaches

The maturity of supervision across the financial sectors is uneven. BdE undertakes well developed supervision with expert resources. Following DORA, the Comisión Nacional del Mercado de Valores (CNMV) and Dirección General de Seguros y Fondos de Pensiones (DGSFP) are expanding their supervision activities and should consider how to leverage the

BdE's experience when developing their supervisory plans and conducting their onsite inspections. BdE has been focusing on the mandatory Threat Led Penetration Testing (TLPTs) under DORA, there is an opportunity for BdE to consider supervisory strategies to support a wider range of entities mature their capabilities so they can take advantage of cyber resilience testing. The creation of dedicated cross-sectoral working groups and information-sharing mechanisms, under the oversight of the Spanish Macroprudential Authority (known as AMCESFI), could be a mechanism to share best practices.

Consider national analysis of third-party risks

Third-party service providers are identified as one of the major threat transmission channels. DORA introduces an EU-level framework for oversight of Critical ICT Third-Party Service Providers (CTPPs), based on a register of information of all contractual agreements on the use of ICT services provided by third-party providers. The European Supervisory Authority's (ESAs) analysis under DORA is limited to identifying CTPPs at an EU level to then be subject to direct supervision. The Spanish authorities should build on analysis already underway by leveraging the registers of information. The registers, when complete, will provide a rich source of information for national authorities to analyse at a national level for concentration risk, interdependencies and possible channels of systemic risk.

Provide a single point of contact for incident reporting and enhance crisis preparedness

There are separate incident notification arrangements for each authority which adds complexity to incident reporting. This is particularly an issue when in the midst of an incident. A single national channel for incident reporting would streamline the process and aggregate information. Automatically notifying the CERTs could facilitate faster technical support.

While there are several government agencies with important roles in a cyber security crisis, there are no dedicated intergovernmental working groups that regularly connect the various government departments with the financial authorities and institutions. There do not appear to be pre-defined playbooks that document the roles and responsibilities and expected coordination between authorities, government agencies and the financial sector in a time of crisis at a national level. Drills and rehearsals together with the industry to practice the playbook should also be considered, such that consistent and cross-sector action can be executed efficiently and effectively during high-impact cyber incidents

Recommendations

In response to these findings, the peer review makes the following recommendations to the Spanish authorities:

1. The Spanish authorities should consider developing a comprehensive threat landscape leveraging intelligence from multiple sources. Dissemination of it could assist both authorities and institutions in prioritising areas of focus.

2. The Spanish authorities should leverage best practice in Spain on supervision approach, procedures, and practices across agencies to bring greater consistency and maturity to cyber resilience across the sectors. This could be achieved through dedicated cross-

sectoral working groups and information sharing mechanisms set up under the oversight of the Spanish Macroprudential Authority. Regarding authority-specific recommendations, the CNMV should establish a plan to conduct regular on-site inspections. The DGSFP should explore recruitment strategies that provide sufficient flexibility to enhance technical expertise in supervision and cybersecurity. The BdE should consider formulating supervisory strategies to assist smaller entities in preparing for cyber resilience testing.

3. The authorities should consider formally establishing a national analysis of the registers of information to identify critical third-party providers for Spain. When the collection of DORA register of information matures, authorities could consider assessing the concentration risk and define a supervisory strategy to address domestically critical third-parties.

4. Spain could consider establishing a single national channel for incident reporting that automatically shares data with relevant authorities. Consideration should also be given to establishing dedicated intergovernmental working groups between the DSN, financial authorities and institutions to jointly prepare for crises. Documenting and communicating playbooks for and conducting drills of crisis management procedures can enhance the response to a significant incident.

1. Introduction

Spain's first peer review, published in 2011,[3] examined steps taken or planned by the Spanish authorities in response to the recommendations on regulation and supervision as well as institutional and market infrastructure in the 2006 IMF FSAP. The review found good progress had been made in addressing several FSAP recommendations whilst some further steps could be taken to address the remaining recommendations.

This peer review assesses Spain's efforts to enhance cyber resilience in the financial system, focusing on preparedness for cyber incidents, response and recovery. Cyber security and the related Information Communication and Technology (ICT) risk are important operational risks for financial institutions and cyber incidents are a potential threat to the global financial system. The threat landscape is expanding amid digital transformation, increased dependencies on third-party service providers and geopolitical tensions. Cyber incidents are rapidly growing in frequency and sophistication. The interconnectedness of the global financial system makes it possible that a cyber incident at one financial institution or one of its third-party service providers could have spill-over effects across borders and sectors.

The FSB has been focusing on response to and recovery from cyber incidents, with a range of toolkits published.

Box 1: Recommendations of the FSB

The FSB has developed a toolkit on effective practices for cyber incident response and recovery for organisations, which can be used as a basis for oversight and supervision.[4] Recognising that timely and accurate information on cyber incidents is crucial for effective incident response and recovery, the FSB then developed recommendations to address issues identified as impediments to achieving harmonised incident reporting and updated the Cyber Lexicon.[5] The FSB has also developed a format for incident reporting exchange called FIRE to collect incident information from financial institutions and that authorities could use for information sharing.[6] In addition, many ICT systems rely on third-party service providers for critical operations. If not properly managed, disruption to critical services or service providers could pose risks to financial institutions and, where there is widespread disruption such as the Crowdstrike incident, to financial stability. Cyber resilience is a component of operational resilience and as part of its work on this topic, the FSB developed a toolkit for enhancing third-party risk management and oversight with recommendations for authorities' oversight and supervision of individual institutions and identification, monitoring and management of systemic third-party dependencies and potential systemic risks.[7]

The EU has recognised the need to strengthen the digital resilience of financial entities and has harmonised regulations relating to operational resilience across 20 different types of financial entities and ICT third-party service providers.

---

3 FSB (2011), *Peer Review of Spain* , February.

4 FSB (2020), *Effective Practices for Cyber Incident Response and Recovery: Final Report*, October.

5 FSB (2023), *Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final report*, April and FSB (2023*), Cyber Lexicon: Updated in 2023*, April.

6 FSB (2025), *Format for Incident Reporting Exchange (FIRE): Final report*, April.

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

Box 2: Digital Operational Resilience Act (DORA)

DORA became applicable on 17 January 2025 and seeks to ensure that banks, insurance companies, investment firms, financial market infrastructures and other financial entities can withstand, respond to, and recover from ICT disruptions, such as cyber-attacks or system failures. The regulations have been formulated taking into consideration the tools developed at international level by the Basel Committee on Banking Supervision, the Committee on Payments and Market Infrastructures, the FSB, the Financial Stability Institute, as well as the G7 and G20.

DORA sets out principles and requirements on ICT risk management; mitigation of ICT third-party risks, including key contractual provisions; a digital operational resilience testing program; an oversight framework for ICT third-party providers that are designated as CTPP by the ESAs for the financial sector; management of ICT-related incidents, and notification of major incidents and significant cyber threats to competent authorities; and exchange of information and intelligence on cyber threats.

The testing programme includes vulnerability assessments / scans, open-source analyses, network security assessments, gap analyses, physical security reviews, source code reviews and scenario-based tests and advanced testing through TLPT.

Spain has implemented the reforms monitored by the FSB in its Annual Report, with the exception of minimum haircuts for Securities Financing Transaction. The appropriateness of these haircuts for the EU will be reviewed by the European Banking Authority by January 2027. Annex 1 provides an overview of Spain's implementation status of G20 financial reforms as of July 2025, including the steps taken to date and actions planned by the authorities in core reform areas (not covered in this peer review) where implementation has not yet been completed.

2. Framework for monitoring cyber risks

2.1. Cyber threat environment in the Spanish financial sector

The European Union Agency for Cybersecurity recently assessed the cyber threat level to the EU to be substantial, with banking and finance the third most targeted sector (after public administration and transport) at 9% of all incidents.[8] Its first overview report assessed the state of play of the cybersecurity landscape and capabilities across all sectors at the EU and national level between 16 January 2023 (entry into force of the Network and Information Systems Security (NIS2) directive) and July 2024. In this period the EU experienced a surge in cyber threats driven by the fast pace of digitisation and increased interconnectivity. The geopolitical landscape influences the goals and tactics of threat actors with malicious cyber activity becoming a prominent component of wider hybrid threats. Reflecting the increasing interconnectivity and complexity of supply chains and the increased dependence on outsourced ICT services, cyber threats rank highly in the EU because of their wide reach, difficulty in detecting and potential spill-over effects. A recent European Securities and Markets Authority (ESMA) report highlighted the potential escalation of a cyber-attack into financial stability concerns.[9]

8 ENISA (2024), *2024 report on the State of Cybersecurity in the Union*, December.

9 ESMA (2025), *Operational and cyber risks in EU financial markets: measurement and stress simulation*, July.

The high interconnectedness of the Spanish financial sector participants both financially and operationally make cyber resilience a priority for firms and authorities. Firms are impacted not only directly through their business relationships, but through operational connections of market infrastructures, common service providers, and the provision of services between firms.[10] The interconnectedness of the system is evident with Spain ranking second in terms of banking sector concentration among main European countries,[11] and a single local operator providing critical ICT services to over 60% of LSIs.

A period of rapid digital transformation after COVID inadvertently increased the sector's exposure to cyber risks, such as through the expanded use of remote financial services allowing 84% of the population to feel safe with digital banking.[12] The national Computer Security Incident Response Team (CSIRT) for private companies and individuals, Instituto Nacional de Ciberseguridad (INCIBE), managed more than 97,000 cyber security incidents in 2024. This is an increase of 16.6% from 2023. Of these, 341 were incidents related to essential and important operators (aligned with the NIS2 Directive definition as vital to the functioning of society) with nearly half of these in the financial and tax system sector, and the information and communication technologies sector.[13] The most common form of incident was malware, some with ransomware attacks attached, followed by online fraud including phishing and then intrusions and attempts to gain unauthorised access to information or systems.

Managing systemic issues such as common critical third-parties and contagion risk have become increasingly important for the sector due to the high concentration of providers supplying technology services to a wide variety of financial entities.[14] Given the increasing interlinkages between market participants as well as evolving malicious attacks, cyber risk is considered a priority by authorities.[15]

2.2. Roles and responsibilities of authorities

The Spanish financial system framework for monitoring cyber risks, ensuring operational resilience, and addressing emerging threats involves several authorities and government departments, each with distinct responsibilities and activities. Below are the responsible authorities for areas in scope of the review:

- **Banco de España** (BdE) is the national authority responsible for prudential supervision of credit institutions [16] and other supervisory tasks. As the central bank, it also seeks to promote the proper functioning and stability of the Spanish financial system. BdE has been designated the national competent authority for credit institutions under NIS, and will likely be designated under NIS2, pending the the final transposition of the Directive into the Spanish regulatory framework. BdE is the Spanish point of contact for the EU Systemic Cyber Incident Coordination Framework. BdE also maintains oversight of

10 BdE (2024), *Financial Stability Report. Spring 2024*, April.
11 BdE (2025), *The Spanish banking system and the challenges it faces*, May.
12 INCIBE (2024), *INCIBE and CECA sign a collaboration agreement to promote cybersecurity with the financial sector*, September.
13 INCIBE (2025), *INCIBE presents its 2024 cybersecurity balance sheet with more than 97,000 incidents managed*, March.
14 BdE (2021), *Cyber risk as a threat to financial stability*, May.
15 BdE (2020), *Strategic Plan 2024*, Jan.
16 Within the framework of the EU Single Supervisory Mechanism

payments systems in Spain, identifying and assessing inherent risks and verifying that the systems used have proper control mechanisms (see Box 3 below).

- **The Comisión Nacional del Mercado de Valores** (CNMV) supervises securities Markets and Financial Market Infrastructures (FMIs). Its cyber resilience responsibilities include ensuring that FMIs implement robust controls for data recovery, business continuity, and third-party management. CNMV monitors reported ICT-related incidents and coordinates with European and international authorities to address cross-border issues.

- **The Dirección General de Seguros y Fondos de Pensiones** (DGSFP) operates under the Ministry of Economy, Trade and Business and oversees insurance companies and pension funds, ensuring their compliance with regulatory standards including DORA, following the guidance of the European Insurance and Occupational Pensions Authority (EIOPA).

- **The Instituto Nacional de Ciberseguridad** (INCIBE) operates under the Ministry for Digital Transformation and the Civil Service and provides for the development of cybersecurity and digital trust for citizens, research networks, and private companies (including financial institutions). This includes cybersecurity alerts and the sharing of information on cyber threats, incidents, and vulnerabilities. While not formally designated as such, INCIBE performs many of the functions performed by an Information Sharing and Analysis Centre (ISAC). INCIBE also contains a designated Computer Emergency Response Team (CERT) function via INCIBE-CERT, which operates as Spain's reference CSIRT for the private sector.

- **The Centro Criptológico Nacional** (CCN) operates an Information Security Incident Response Centre to protect systems owned by public bodies and organisations of strategic interest (such as large financial institutions) to the Spanish security and economy from cyber-attacks.

Box 3: National extension of DORA to additional payment systems players

In the context of payments systems, DORA applies to payment institutions, account information service providers and e-money institutions. A short outage in a payment processing entity in November 2023 emphasised the role of payments systems in the functioning of the economic activity of a country and day to day needs of its citizens. Following this outage, a national Royal Decree-law was adopted in December 2023 for extraordinary and urgent reasons to extend DORA obligations to certain entities not covered by DORA (allowed under Recital 104 of DORA). The outage demonstrated that a broader set of players are critical in the functioning of the payments system, and Spain took a national decision to extend the DORA obligations on ICT management to payment system operators, payment scheme operators, electronic payment arrangements operators, payment processing entities, and other technological providers participating in the payments process. BdE is designated the competent authority for supervising and sanctioning compliance with these obligations. This extension excludes payment system operators deemed of systemic importance by the European Central Bank. A Draft Bill underway on the Modernisation and digitalisation of the financial sector will address some of the implementation challenges of this Royal decree.

3. Steps taken and actions planned

3.1. Monitoring the cyber threat landscape

Each financial authority collects and analyses their respective cyber intelligence to form their own cyber threat views. BdE gathers insights from supervisory activities, the TIBER exercises, and institution incident notifications. They also rely on networks with Chief Information Security Officers from major financial entities and the Financial Services ISAC[17] where technical issues around cyber resilience, such as Tactics, Techniques, and Procedures, are discussed. DGSFP leverages institution incident reports and intelligence from CCN and INCIBE to develop its cyber threat view. CNMV utilises an external cyber security consultancy firm to provide cyber threat information annually to inform their risk assessment.

Whilst information is collected and analysed by each of the respective authorities for internal consideration, there is no comprehensive sectoral or cross-sectoral threat landscape created to support better situational awareness. A threat landscape such as this could inform decisions on where institutions should prioritise investment, potential areas of focus for supervisory activities and the focus of TLPTs. Box 4 outlines the benefits of creating a cyber threat landscape.

Box 4: Cyber threat landscape

A cyber threat landscape refers to an overall view of the malicious cyber activities, actors, tactics, tools techniques and vulnerabilities that pose threats to ICT, data, and operations. A financial sectoral cyber threat landscape is a strategically focused consolidated view of cyber threats specific to the financial industry. They typically draw intelligence from multiple sources, including cybersecurity firms, national cyber agencies, national intelligence agencies, financial institutions, regulatory authorities and international partners.

For supervisors, it enables authorities to tailor their oversight strategies based on current and emerging risks. This proactive approach enhances the effectiveness of regulatory interventions and supports the development of risk-based supervisory frameworks. For financial institutions, access to an up-to-date threat landscape support informed decisions on cybersecurity investments and initiatives. It helps entities prioritise their cyber risk mitigation efforts based on the most relevant and pressing threats. This ensures that limited resources are directed toward initiatives that offer the greatest risk reduction and operational impact. It also fosters a shared understanding of threats across the sector, promoting coordinated responses and mutual support. It enables faster detection and attribution of incidents by providing contextual intelligence on likely threat actors and tactics. This, in turn, supports more effective containment, response, and recovery efforts. Furthermore, it facilitates timely information sharing among stakeholders, which is essential for managing cross-institutional or systemic incidents.

3.2. Supervision of the financial sector

The supervision of LSIs,[18] Insurance firms and FMIs was in scope of the review. Whilst efforts are underway in each of these sectors, the maturity of supervision is uneven across the sectors, likely reflecting the relative risk in each sector. Each of the authorities had some level of cyber

[17] See Financial Services Information Sharing and Analysis Center for more information.

[18] Significant institutions are supervised by the Single Supervisory Mechanism by the ECB and therefore were out of scope of the review.

resilience supervision activities in place before the DORA regulation was enacted, with BdE being the most comprehensive. The BdE approach to supervision of cyber resilience is mature and its practices could be leveraged by the other financial authorities as they establish closer cyber resilience supervision as part of the DORA requirements. All three authorities have put considerable effort towards supporting the industry to implement DORA and enhancing supervision of cyber security within their respective sectors accordingly.

Banking

BdE recognises cyber risks as one of the core areas of supervisory focus, given its increasing relevance to operational resilience of the sector, and ultimately financial stability. There is a robust and comprehensive risk-based supervisory model, which includes conducting annual assessments to evaluate the institution's capacity to manage both existing and emerging risks, including those stemming from technological dependencies and cyber threats. Based on these assessments, supervisory priorities are defined and translated into supervisory plans that guide the depth, scope, and frequency of inspections and engagements throughout the supervisory cycle. Several vertical and horizontal functions within the BdE interact closely. A vertical relationship team of 17 staff covers LSIs to assess the unique risk and operations of institutions. A separate team conducts onsite supervision independently, with up to two onsite inspections for LSIs each year. A third team of 19 staff provides cyber-related expertise including conducting TIBER & TLPT testing as a horizontal expert team. It is evident that a substantial effort to supervise cyber resilience in LSIs is underway and this should continue.

The TIBER-ES framework has been identified as the primary platform to meet the DORA TLPT requirements. TIBER-ES, based on the TIBER-EU framework, provides a structured approach to red-teaming exercises, simulating advanced cyber threats to test the resilience of financial institutions. To date, in the banking sector only Significant Institutions have been undertaking TIBER-ES exercises and BdE note the cost of conducting and the level of maturity required for such an exercise for an LSI could be challenging. The recent IMF FSAP recommended that Spanish authorities consider developing a lighter threat intelligence-based red-teaming framework, drawing on TIBER-ES principles. Such a framework could provide a more accessible and scalable approach for smaller entities, to assist building their maturity. To date, the Spanish authorities have focused primarily on adapting TIBER-ES to meet DORA's immediate requirements and determining the institutions required to conduct the tests. While there is recognition of the value in a lighter framework to enhance the resilience of a broader range of entities, BdE are of this view this is a longer-term objective as they prioritise compliance with DORA's TLPT expectations for the most critical financial institutions.

Significant efforts have been made to support LSIs' preparedness for DORA through conducting sector-wide surveys and bilateral discussions. Guidance and clarification on commonly identified issues was provided to the sector. BdE expects continuous refinements to occur between supervisors and institutions as DORA processes (such as the new incident reporting mechanism) are utilised.

BdE supervises two large third-party service providers to the LSIs that are considered systemically important for the Spanish financial sector. Together they provide IT infrastructure, cyber security operations and core banking services to 70% of all LSIs in Spain. These two technology

companies are each owned by a (different) large banking cooperative and therefore are closely supervised by BdE with dedicated onsite inspections.

Financial Market Infrastructures

Recently CNMV has focused oversight of FMIs' cyber resilience on their preparedness to implement DORA. Prior to the adoption of DORA, CNMV was using the Eurosystem's Cyber Resilience Oversight Expectations for Financial Market Infrastructures (CROE) for its oversight of FMIs. CNMV required FMIs to complete a questionnaire to determine a self-assessed gap analysis on compliance with DORA. The questionnaire was closely aligned with an ESMA exercise, to facilitate consistent answers from FMIs within a Group under the supervision of both authorities operating or providing their services in several European jurisdictions. Overall, CNMV observed that prior compliance to the CROE offered a strong basis for compliance with DORA. CNMV required mitigation plans for identified gaps.

Supervision of the only central clearing counterparty and central securities depository in Spain, the Bolsas y Mercados Españoles (BME) group, was in scope of the review. The Swiss Financial Market Supervisory Authority (FINMA) is the Swiss supervisory authority responsible for the consolidated supervision of SIX Group, the parent company of BME Group. As such, CNMV participated in a joint supervisory action coordinated by FINMA on IT strategy, governance and risk within the Swiss Group (see Box 5). CNMV requires an annual review of the group's Business Continuity Plan (BCP) and at least one annual BCP exercise including relevant clients and critical service providers such as SWIFT. All the supervised entities of the BME group are tested at the same time with the most recent test involving the shutdown of the main data center and corresponding building evacuation. CNMV plans to observe the next BCP exercise in October that will be based on a cyber-scenario. Notably, CNMV does not yet conduct onsite inspections but has plans to do so going forward. CNMV have recruited additional cybersecurity experts to assist in increased oversight requirements.

Box 5: Joint supervision with FINMA

In 2020 the Spanish trading platform BME was acquired by the Swiss company SIX Group. In 2022 CNMV entered into a Memorandum Of Understanding with FINMA to support information sharing and joint examination work of the Spanish subsidiary in the context of the broader holding company. Since the merger the combined entity has centralised its support functions and adopted a matrix organisation. This provides an opportunity for the two authorities to collaborate in their supervision. The two authorities scoped and performed joint on-site reviews. In addition, the authorities have regular touchpoints to discuss new developments and opportunities for further engagement. The collaboration represents not only a cross EU and Switzerland relationship in supervision of an international firm but also supervisory cooperation across differing regulatory frameworks with both authorities learning ways to improve their own supervision from the experience.

Insurance sector

- The insurance sector is significant to the Spanish economy, accounting for almost 5% of GDP and covering more than 20 million households with life and non-life products. The DGSFP provides macroprudential supervision to almost 180 insurers and re-insurers and performs conduct oversight to around 70 local branches of foreign insurance firms. The operational resilience of insurers is an area of increasing focus;

the International Association of Insurance Supervisors (IAIS) has recently published for consultation a Draft Application Paper on Operational Resilience Objectives and supporting practices and tools in the form of a toolkit. which includes cyber resilience risks.[19] The IAIS also published an Application paper specific to the supervision of Insurer Cybersecurity.[20]

- DGSFP had introduced some supervision themes of cyber resilience prior to DORA, although they were limited in scope. Since 2019, cyber resilience has been incorporated as a factor of the DGSFP's operational risk assessment framework as part of the Solvency II regime under EIOPA. The focus has been on ICT governance and how the Administrative, Management or Supervisory Body of the insurer considers the use and risks of ICT. A sector-wide assessment that simulated a ransomware scenario concluded the industry's solvency ratio was sufficient to remain above the tolerance limit. To prepare for DORA, a sector-wide survey was launched to assess firms' preparedness, and the DGSFP is updating its supervisory handbook.

- Supervision by DGSFP is limited due to resource constraints. The DGSFP has assigned responsibility for supervising the implementation of DORA to its new Division of Technological Supervision and Digital Innovation. While this team was originally set up in the traditional ICT function of the Directorate to develop supervisory technology tools for internal use, it has expanded its mandate to support policy development on the national adoption of DORA and a corresponding supervisory approach. Accordingly, the team received 2 additional staff (22 staff in total) in 2024, but the team members do not have supervisory expertise. Staffing in the team is restricted to the civil servant recruitment mechanism under the Directorate's current HR policy so recruiting of staff with relevant supervisory or technological expertise may be challenging. Following a restructure, the team is now set up as a horizontal function in DGSFP and works closely with the supervisory teams to perform its new functions by participating in the Prudential Supervision Committee responsible for inspection planning and providing advice to the regulation division. Several enhancements are necessary to strengthen the supervisory framework. Additional efforts are required to finalise and clearly communicate formal accountabilities. A comprehensive, risk-based supervisory plan with a focus on cyber resilience has yet to be developed, and on-site supervisory activities remain to be scheduled.

3.3. Third-party risk management

The Spanish authorities have been taking steps to analyse the interdependencies of the financial sector on third-party providers. The National Centre for the Protection of Critical Infrastructure has been constructing a map of interdependencies for designated Critical Operators (which will include large financial institutions) to identify the systemic impact of a failure of a supplier. BdE has for some time been collecting and analysing critical technology service providers leveraging outsourcing registers, supplementing with public information and cross checking with incident notifications. Specific analysis on LSIs has been undertaken to identify vulnerabilities with plans

19 IAIS (2025), *Draft Application Paper on Operational Resilience Objectives and Toolkit*, July.
20 IAIS (2018), *Application Paper on Supervision of Insurer Cybersecurity*, November.

to deepen analysis into nth-party relationships, dominant providers, and systemic dependencies to identify actions to strengthen resilience. BdE also maintains an ongoing dialogue with major technology firms, leveraging the requirement for indirect access of supervisors through the financial institution.

For FMIs, CNMV must authorise the proposed outsourcing of critical functions and therefore reviews contract clauses and the arrangements of the FMI to manage the outsourced function and any concentration risk. CNMV does not currently conduct any national specific analysis on third-party providers.

DGSFP requires insurance and reinsurance entities to notify critical outsourcing arrangements prior to implementation. Supervision of outsourcing has remained limited to this notification phase and monitors the inclusion of minimum contractual terms. DGSFP has future plans to build insights by analysing on an insurance segment basis the critical suppliers and then cross-referencing incident data with provider usage to identify systemic vulnerabilities.

One of the hallmarks of DORA is the direct supervision of critical ICT third-party service providers. DORA introduces annual reporting and a centralised register of information of ICT third-party service provider contracts to inform the designation of CTPPs at the EU level (expected in the second half of 2025).[21] These firms will be directly supervised to uniform standards by Joint Examination Teams hosted by the relevant ESA with the participation of staff from national competent authorities.

The registers of information, when fully completed, offer an opportunity for supervisory agencies to assess the concentration risks across the financial sectors at a national level and identify providers that may be critical at the national level but not at the EU level. They can also facilitate assessments of concentration risk, where shortcomings in the provider's cyber resilience or disruption or failure at the provider could have systemic consequences impacting multiple institutions simultaneously. Supervisory strategies could be developed to mitigate this risk. Analysis of the interdependencies in the register of information can also be a valuable source of information during an incident to determine the full set of firms potentially impacted and systemic vulnerabilities.

3.4. Incident reporting and crisis handling and coordination arrangements

Incident reporting arrangements

The DORA framework brought significant streamlining of the incident reporting in the financial sector. Under the DORA framework, financial entities are required to report major ICT-related incidents to their national competent authorities. Incidents are reported only once and by using a single template. The respective national competent authorities are responsible for receiving incident notifications at a defined threshold, with certain information required within certain timelines. Since 2020, BdE has maintained a database of banking sector incident notifications that is used for trend analysis and identification of vulnerabilities. BdE, CNMV and DGSFP have recently updated their respective incident notification channels to meet the DORA requirements

[21] To be designated a CTPP the provider must operate in at least 2 EU jurisdictions.

and have prepared industry guidance. As each authority hosts its own notification channel, financial entities that cross sectors may need to report the same information through multiple channels. Institutions may also have to report to non-financial authorities such as INCIBE, CCN and the Spanish Data Protection Agency should the incident involve public interests or personal data. These agencies are not under the scope of DORA and therefore may ask for different information at different times to the financial authorities.

Crisis handling and coordination arrangements

Each authority has its own defined incident escalation procedures including consideration for further supervisory follow up. Whilst the financial authorities monitor incidents and assess the impact on the financial sector, they do not provide technical support and are constrained by information barriers related to the confidentiality of supervisory information. Specialised technical support remains the domain of specialised bodies such as INCIBE-CERT as the CSIRT for the private sector and the Spanish Cybersecurity Coordination Office and the CCN acting as the CSIRT for the public sector. This support includes incident triage, impact assessment and mitigation measures. While efforts are made to share knowledge and provide support in a crisis, there could be additional focus on providing relevant information during an incident to assist in taking defensive action. Anonymised and aggregated incident data could also be shared periodically with the industry to further strengthen their defensive actions.

There are established processes for sharing incident notifications to the relevant ESA's platform (which interface into EU-level crisis coordination mechanisms) and INCIBE. There is high-level engagement between the national authorities, INCIBE, CCN and the Spanish Cybersecurity Coordination Office but arrangements do not seem embedded in the financial authorities and were not well understood at the operational level.

There has been substantial investment at the national level to enhance cyber security. The Ministry for Digital Transformation and the Civil Service handles the strategic vision for Spain's cyber security and released the Digital Spain 2025 plan.[22] INCIBE has been designated as the Spanish National Coordination Centre of the European Cybersecurity Competence Centre, which will coordinate national development of cyber security expertise through various channels including coordination of exercises with industry. The CyberEx[23] program run by INCIBE provides tabletop, incident simulation, and targeted attack exercises for technical and executive industry participants. They range from a three-hour exercise in the case of a tabletop exercise for executives to a more intensive multi day targeted attack simulation suitable for technical teams. In 2016 the CyberEx simulation was specifically focused on the financial sector.

The National Security Department (DSN) within the Government Presidency has responsibility for coordinating responses to significant cyber incidents reported by the CSIRTS and designated as significant. If the incident has a cross-border impact DSN engages with the EU CyCLONe[24] network. However, there are no dedicated intergovernmental working groups that regularly connect the DSN with the financial authorities and institutions. There do not appear to be pre-

---

22 MINECO (2025), *Digital Spain 2025*.

23 INCIBE, CyberEx España

24 See EU CyCLONe (ENISA)

defined playbooks that document the roles and responsibilities and expected coordination between authorities, government agencies and the financial sector in a time of crisis at a national level. Playbooks that define triage roles, escalation triggers, and communication protocols across financial and non-financial authorities should be clearly documented and communicated. Drills and rehearsals together with the industry to practice the playbook should also be considered, such that consistent and cross-sector action can be executed efficiently and effectively during high-impact cyber incidents

4. Conclusions and recommendations

The Spanish authorities and government agencies have taken significant steps to enhance cyber resilience in the financial sector and prepare the industry for the implementation of DORA. BdE has a mature cyber resilience supervisory strategy with robust and comprehensive supervision of the LSI portfolio. BdE's analysis of domestic third-party service providers and incident notifications has provided valuable supervisory insights on potential vulnerabilities. The introduction of DORA has significantly increased expectations for cyber resilience in the financial sector and the authorities have made substantial efforts to prepare the industry. BdE is well prepared for the TLPT requirements of DORA after several years of executing the TIBER-ES framework at the largest financial institutions.

At the same time, steps can be taken to further enhance cyber security resilience. This includes developing a comprehensive sectoral cyber threat landscape; leveraging best practices in supervision approaches across agencies; conducting a national analysis of third-party risks; and improvements in incident management practices.

4.1. Develop a comprehensive sectoral cyber threat landscape

Cyber threat intelligence is drawn from multiple sources and is most powerful when aggregated to a consolidated view at both a sectoral and cross sectoral level and disseminated to relevant authorities and industry. Currently each authority collects and analyses their respective cyber intelligence and there is no consolidated landscape created and disseminated, either at a sectoral or cross sectoral level. A formal regularly updated artefact that is distributed could inform decision making on prioritisation of investment by industry, highlight potential areas of focus for supervisory activities and could be a starting point for red-teaming activities, such as TLPT under DORA or to for voluntary TIBER tests. This is particularly useful for smaller firms who do not have the capacity or resources to collect threat intelligence proactively. Such a landscape would benefit from including intelligence from all financial authorities and relevant government agencies such as INCIBE and CCN to provide a consolidated and holistic view.

Recommendation 1: A comprehensive threat landscape artefact leveraging intelligence from multiple sources including financial authorities and government agencies should be created and disseminated and could assist both authorities and institutions in prioritising areas of focus.

4.2. Leverage best practices in supervision approaches

- The maturity of supervision across the banking, FMI and insurance sectors is uneven, with BdE undertaking the most comprehensive supervision with expert resources. CNMV has recently expanded its cyber resilience expertise but has not yet conducted an onsite review which is an important component of a risk-based supervisory strategy.

- The DGSFP is in the early stages of the journey to comprehensive ICT risk supervision. A new division has been set up to supervise the implementation of DORA, but it is lacking in supervisory expertise. Recruitment is restricted to the civil servant mechanism which may not be suitable to identify supervisory and cyber security expertise. Formal accountabilities need to be finalised and communicated, a structured risk-based supervisory plan with cyber resilience elements has not been developed and on-site inspections are not yet planned.

- The financial authorities should consider how to facilitate sharing of experiences and expertise to bring greater consistency and maturity to cyber resilience supervision across the sectors. This could include conducting joint training. The creation of dedicated cross-sectoral working groups and information-sharing mechanisms, under the oversight of the Spanish Macroprudential Authority (AMCESFI), would be highly beneficial. Although BdE is currently focused on providing the mandatory TLPT under DORA, it would be useful to also develop supervisory strategies to support the development of smaller entities as they build their resources and maturity to be able to undertake some form of testing. This may lessen the divide between the firms in scope of a TLPT test under DORA and those not subject to the requirement.

Recommendation 2: the Spanish authorities should leverage best practice in Spain on supervision approach, procedures, and practices across agencies to bring greater consistency and maturity to cyber resilience across the sectors. This could be achieved through dedicated cross-sectoral working groups and information sharing mechanisms set up under the oversight of the Spanish Macroprudential Authority. Regarding authority-specific recommendations, the CNMV should establish a plan to conduct regular on-site inspections. The DGSFP should explore recruitment strategies that provide sufficient flexibility to enhance technical expertise in supervision and cybersecurity. The BdE should consider formulating supervisory strategies to assist smaller entities in preparing for cyber resilience testing.

4.3. National analysis of third-party risks

Whilst DORA introduces a register of information on third-party ICT contracts, the analysis under DORA is limited to identifying CTPPs at an EU level to then be subject to direct supervision. The Spanish authorities should build on the analysis already underway by leveraging the registers of information. When they are fully completed, they will be a rich source of information for national authorities to analyse at a national level for concentration risk, interdependencies and possible channels of systemic risk. This analysis could be done using parameters such as service

provider dependency, geographical and intra-group concentration, supply chain overlaps, and substitutability.[25]

Recommendation 3: The authorities should consider formally establishing a national analysis of the registers of information to identify CTPPs for Spain. When the collection of DORA register of information matures, authorities should consider assessing the concentration risk and define a supervisory strategy to address domestically critical third-parties.

4.4. Streamlined incident notification and response and enhanced crisis preparedness

Each financial authority hosts their own incident notification channel. These separate arrangements add complexity to incident reporting, which is particularly an issue for financial entities operating in several segments of the financial sector when in the midst of an incident. A single national channel for incident reporting could streamline the process and aggregate information. Automatically notifying the CERTs could support a faster technical support.

While simulation training is in place, there does not appear to be mechanisms to connect the DSN with the financial authorities and institutions on a regular basis to prepare for crises. The authorities did not appear to have well developed and well communicated incident playbooks, either within authorities or between authorities. Playbooks that define triage roles, escalation triggers, and communication protocols promote coordinated crisis response and enable consistent, cross-sector action during high-impact cyber incidents. Drills and rehearsals together with the industry to practice the playbook should also be considered, such that consistent and cross-sector action can be executed efficiently and effectively during high-impact cyber incidents.

Recommendation 4: Spain could consider establishing a single national channel for incident reporting that automatically shares data with relevant authorities. Consideration should also be given to establishing dedicated intergovernmental working groups between the DSN, financial authorities and institutions to jointly prepare for crises. Documenting and communicating playbooks for and conducting drills of crisis management procedures can enhance the response to a significant incident.

[25] See for example s 3.8 of FSB (2023), *Final report on enhancing third-party risk management and oversight a toolkit for financial institutions and financial authorities*, December.

Annex 1: Spain's implementation of G20 reforms (as of November 2024)

This table presents the status of implementation of G20 financial regulatory reforms, drawing on information from various sources. The tables below distinguish between priority areas that undergo more intensive monitoring and detailed reporting via progress reports and peer reviews, and other areas of reform whose monitoring is based on annual survey responses by FSB member jurisdictions. See here for further information.

IMPLEMENTATION STATUS OF REFORMS IN PRIORITY AREAS

Reform Area	BASEL III					COMPENSATION	OVER-THE-COUNTER (OTC) DERIVATIVES				RESOLUTION					NON-BANK FINANCIAL INTERMEDIATION		
	Risk-based capital	Require-ments for SIBs	Large exposures framework	Leverage ratio	Net Stable Funding Ratio (NSFR)		Trade reporting	Central clearing	Platform trading	Margin	Minimum external TLAC for G-SIBs	Transfer / bail-in / temporary stay powers for banks	Recovery and resolution planning for systemic banks	Transfer / bridge / run-off powers for insurers	Resolution planning for SI>1 CCPs	Money market funds (MMFs)	Securiti-sation	Securities financing transactions (SFT)
Agreed phase-in (completed) date	*2023*	*2016 (2019)*	*2019*	*2023*	*2018*		*end-2012*	*end-2012*	*end-2012*	*2016 (2022)*	*2019/2025 (2022/2028)*							*2017/2023*
Status		C	LC		LC													

Legend: Final rule or framework implemented. Final rule published but not implemented, draft regulation published or framework being implemented. Draft regulation not published or no framework in place (dark red colour indicates that deadline has lapsed). Requirements reported as non-applicable. Basel III: **C**=Compliant, **LC**=Largely compliant, **MNC**=Materially non-compliant, **NC**=Non-compliant. Compensation: B,I=Principles and Standards deemed applicable only for banks (B) and/or insurers (I). OTC derivatives: R/F=Further action required to remove barriers to full trade reporting (R) or to access trade repository data by foreign authority (F). Non-bank financial intermediation: */**=Implementation is more advanced in one or more/all elements of at least one reform area (money market funds), or in one or more / all sectors of the market (securitisation). Further information on the legend.

Notes: CCPs=Central counterparties. G-SIBs=Global Systemically Important Banks. TLAC=Total Loss-Absorbing Capacity. SI>1=Systemically important in more than one jurisdiction.

Source: FSB, *Promoting Global Financial Stability: 2024 FSB Annual Report*, November 2024.

IMPLEMENTATION STATUS OF REFORMS IN **OTHER AREAS**

Reform area	Hedge funds			Securitisation			Supervision				Macroprudential frameworks and tools	
	Registration, appropriate disclosures and oversight of hedge funds	Establishment of international information sharing framework	Enhancing counterparty risk manage-ment	Strengthen-ing of regulatory and capital framework for monolines	Strengthening supervisory requirements or best practices for investment in structured products	Enhanced disclosure of securitised products	Consistent, consolidated supervision and regulation of SIFIs	Establishing supervisory colleges and conducting risk assessments	Supervisory exchange of information and coordination	Strengthen-ing resources and effective supervision	Establishing regulatory framework for macroprudential oversight	Enhancing system-wide monitoring and the use of macropru-dential instruments
Status	REF*	REF	REF*	REF*	REF	REF	REF	N/A*	REF	REF	REF	REF

Reform area	Credit rating agencies		Accounting standards	Risk management		Deposit insurance	Integrity and efficiency of financial markets		Financial consumer protection
	Enhancing regulation and supervision of CRAs	Reducing the reliance on ratings	Consistent application of high-quality accounting standards	Enhancing guidance to strengthen banks' risk management practices	Enhanced risk disclosures by financial institutions		Enhancing market integrity and efficiency	Regulation and supervision of commodity markets	
Status	REF*	REF	REF	REF	REF	REF	REF	REF	REF

Legend: REF=Implementation reported as completed. IOG=Implementation reported as ongoing. ABN=Applicable but no action envisaged at the moment. N/A=Not applicable. *=collected in previous year(s) for all members.

Notes: The FSB has not undertaken an evaluation of survey responses to verify the status or assess the effectiveness of implementation. In a number of cases, the complexity of the reforms and the summarised nature of the responses does not allow for straightforward comparisons across jurisdictions or reform areas. In particular, reforms whose status in a particular area is reported as complete should not be interpreted to mean that no further policy steps (or follow-up supervisory work) are anticipated in that area. CRA = Credit Rating Agency, SIFI = Systemically important financial institution.

Source: FSB, *Jurisdictions' Responses to the IMN Survey*.

Other information	Latest IMF-World Bank FSAP: Jun 2024	Latest FSB Country Peer Review: 2011	Home jurisdiction of G-SIBs: yes	Signatory of IOSCO MMoU: yes	Signatory of IAIS MMoU: no

The following table presents the steps taken to date and actions planned by the Spanish authorities in core reform areas (not covered in this peer review) where implementation has not yet been completed (as determined at last publication of the FSB Annual Report in November 2024). The actions mentioned below have not been examined as part of the peer review and are presented solely for purposes of transparency and completeness.

Reform area	Steps taken to date and actions planned (including timeframes)
Final Basel III framework	
Risk-based capital	With the entry into force on 1 January 2025 of CRR III, the European Union are now aligned with the Basel III framework for risk-based capital.
Non-Bank Financial Intermediation	
Securities financing transactions	While Regulation (EU) 205/2365 adopted the FSB recommendations on SFTs, the EU legislation does not incorporate a framework on minimum haircut floors. The recitals of CRR III highlight concerns of unintended consequences of incorporating minimum haircut floors. Article 519d of CRR III mandates the European Banking Authority to report, in close cooperation with ESMA, by 10 January 2027 on the appropriateness of implementing minimum haircut floors.