INTERNATIONAL MONETARY FUND

IMF Country Report No. 24/263

SPAIN

FINANCIAL SECTOR ASSESSMENT PROGRAM

August 2024

TECHNICAL NOTE ON CYBER RISK AND FINANCIAL STABILITY

This paper on Spain was prepared by a staff team of the International Monetary Fund as background documentation for the periodic consultation with Spain. It is based on the information available at the time it was completed on July 12, 2024.

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

SPAIN

FINANCIAL SECTOR ASSESSMENT PROGRAM

July 12, 2024

TECHNICAL NOTE

CYBER RISK AND FINANCIAL STABILITY

Selected Issues in Regulation and Supervision

Prepared By
Monetary and Capital Markets Department

This Technical Note was prepared in the context of an IMF Financial Sector Assessment Program (FSAP) mission in Spain. It contains technical analysis and detailed information underpinning the FSAP's findings and recommendations. Further information on the FSAP program can be found at http://www.imf.org/external/np/fsap/fssa.aspx

CONTENTS

Glossary

BCBS	Basel Committee on Banking Supervision
BCM	Business Continuity Management
BdE	Banco de España
BIS	Bank for International Settlements
BME	Bolsas y Mercados Españoles
CCP	Central Counterparty
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNPIC	National Centre for the Protection of Critical Infrastructure
CNMV	Comisión Nacional del Mercado de Valores
CPMI	Committee on Payments and Market Infrastructures
CROE	Cyber Risk Oversight Expectations
CSD	Central Securities Depository
CSDR	Central Securities Depositories Regulation
CSP	Cloud Service Provider
CTP	Critical Third Party
DG.OMS	Directorate General of Operations, Markets and Payment Systems of the BdE
DG.SUP	Directorate General of Banking Supervision of the BdE
DGSFP	Directorate General Insurance and Pension Funds of the Ministry of Economy
DORA	Digital Operational Resilience Act
EA	Euro Area
EBA	European Banking Authority
ECB	European Central Bank
ECBR	European Cyber Resilience Board
EMIR	European Market Infrastructure Regulation
ESRB	European Systemic Risk Board
EU	European Union
EU-CCP	European Union- Central Counterparty
FMI	Financial Market Infrastructure
FSB	Financial Stability Board
FS-ISAC	Financial Services Information Sharing and Analysis Center
ICT	Information and Communication Technology
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
ISO	International Organization for Standardization
IT	Information Technology
JST	Joint Supervisory Team
LSI	Less Significant Banking Institution

NIS	Network and Information systems Security Directive
PFMI	CPMI-IOSCO Principles for Financial Market Infrastructures
RTS	Regulatory Technical Standards
SI	Significant Banking Institution
SREP	Supervisory Review and Evaluation Process
SSM	Single Supervisory Mechanism
TIBER-ES	Threat intelligence-based Ethical Red Teaming
TTP	Tactics, Techniques and Procedures
SI	Significant Banking Institution
SREP	Supervisory Review and Evaluation Process
SSM	Single Supervisory Mechanism

EXECUTIVE SUMMARY

The scope of the assessment covered the regulation and supervision of cyber risk at the Spanish Less Significant Banking Institutions (LSIs) and Financial Market Infrastructures (FMIs).[1] Thus, the financial supervisory authorities in scope were the Banco de España (BdE) and the Comisión Nacional del Mercado de Valores (CNMV), collectively referred hereinafter as authorities. Supervision of Significant Banking Institutions (SIs) in Spain is within the remit of the European Central Bank's Single Supervisory Mechanism (ECB/SSM) and was not assessed.

Technology risk and cyber resilience of the financial sector has become a focus area of the authorities, within the broader context of operational risk and resilience. For example, this is clearly spelled out as a supervisory priority of the BdE for 2023. The CNMV has also intensified cyber risk oversight activities in recent years.

This intensified focus by authorities is timely and important from the perspective of the continuity of financial service provision and the stability of the Spanish financial system. A cyber incident impacting a large number of LSIs, or a critical third-party service provider to these firms could cause abrupt and significant adverse spillovers that result in a systemic disruption, such as interruption of financial services on a wide scale. Single-firm incidents like a disruption or an integrity compromise of a Financial Market Infrastructure (FMI) could also have an adverse impact on the financial system, because of the FMI's non-substitutability and interconnectedness. In addition, because of the size and international importance of the Spanish financial system, there is scope for domestic cyber incidents to be transmitted well beyond national borders through interconnectedness and financial contagion.

The authorities discharge their duties based on a regulatory framework that is fully aligned with the European Union (EU) regulation. Pertinent EU legislation is either transposed or directly applicable in Spain. In addition, the BdE is part of the SSM since its establishment in 2014 and both the CNMV and the BdE take part in the European Union-Central Counterparty (EU-CCP) Colleges of Supervisors, according to EU legislation.[2]

The legal basis and relevant regulation convey adequate powers to effectuate cyber risk supervision. There are sufficiently broad powers regarding collection of information in any form on any relevant matter, to assess compliance, impose corrective actions to have supervised institutions and FMIs rectify matters within a reasonable timeframe, and impose sanctions and take enforcement action as a last resort to ensure compliance.

The FSAP found cyber risk supervisory practices of the authorities with regard to LSIs and FMIs in scope to be materially in line with applicable regulations and guidance and prevailing

[1] "Supervision" is used to collectively denote both bank supervision and FMI oversight and supervision. When addressing FMIs only, the term oversight is used.

[2] The European Market Infrastructure Regulation (EMIR).

international good practice. Key strengths include: (i) clear supervisory expectations that are well communicated; (ii) an effective risk-based approach and application of proportionality in supervision; (iii) useful and well validated horizontal reviews at the BdE; (iv) strong emphasis on evidence-based onsite examinations at the BdE, and thorough and detailed offsite oversight process at the CNMV and the BdE, especially considering their resource constraints; (v) emphasis placed on security testing; (vi) the proactive approach to changes in the regulatory framework, for example to ensure future Digital Operational Resilience Act (DORA) compliance; and (vii) effective internal coordination and cooperation at both the BdE and the CNMV.

Resource constraints are the most prominent challenge that the authorities are confronted with. Rigid hiring and employment policies and rules have a negative impact on authorities' practical ability to discharge their duties and keep pace with the rapidly changing cybersecurity threat landscape and resulting risks. International standards require budgetary processes that secure adequacy of resources so as to preserve operational autonomy. In this context, the annual process that the CNMV has to follow to secure government approval for its budget introduces uncertainties regarding its ability to ensure adequate number of staff and expansion in staffing, including expert and specialized human resources in the highly competitive area of cyber security. This is a significant issue in light of the challenges identified by the FSAP in current supervisory practices, and will only grow in the near-term, reflecting rapidly expanding cyber threats and implementation of new EU regulations, such as DORA. The authorities' cyber risk supervision delivery capacity is already fully utilized and in addition CNMV's capacity is well below current needs. It will be important to ensure that the BdE and the CNMV are adequately prepared and resourced to undertake their expanded responsibilities.

A number of further weaknesses have a negative impact notwithstanding the overall strength of cyber risk supervision. The most important are: (i) there is no onsite supervisory process either at the CNMV's or BdE's FMI oversight business areas, which results in comparatively weaker assurance over compliance; (ii) with the current approach at the BdE, there are few onsite examinations, and it is difficult to increase the coverage; (iii) neither the BdE nor the CNMV are involved in national critical infrastructure related matters, even though they are probably in the best position to address the complexities of continuity of critical services in the financial system; (iv) the current threat intelligence-based ethical red teaming framework (TIBER-ES) is not well suited to the majority of LSIs, but there is a need for a testing framework along its principles for this segment as well; and (v) the cost/benefit ratio of the institution specific threat intelligence reports in TIBER-ES is unfavorable.

Table 1. Spain: Key Recommendations			
Recommendation	**Timing**	**Reference**	**Agency**
Institutional and Regulatory Framework			
1. Prioritize filling existing open positions and assess the need for increasing the cyber risk specialist headcount by considering current and projected workloads over a three to five years period.	I	31. (i)	BdE
2. Estimate current and projected future workload, ensure alignment of resources to these, and have full autonomy over the recruitment and retention process so that they become more effective at hiring additional staff at the right experience and competence levels.	ST	31. (ii)	CNMV Government
3. Establish and staff a small cyber risk competence center with a horizontal (cross-cutting) mandate to provide specialist support of all activities that have a cyber risk supervisory component.	ST	31. (iii)	CNMV
Supervisory practices			
4. Start planning and executing onsite examinations as part of FMI supervision. BdE's existing cyber risk expertise in banking supervision could be leveraged in the beginning as such expertise is highly transferable. At CNMV, external support clearly limited to executing technical tasks should be considered as an interim measure.	ST	99. (i)	BdE CNMV
5. Conduct more, and more focused, thematic reviews while maintaining the validation based on the short onsite visits to a sample of the reviewed population.	ST	99. (ii)	BdE
6. Both the BdE and CNMV should be involved in critical infrastructure related matters, such as designation and compliance assessments	ST	99. (iii)	Government
7. Consider using sector-specific threat intelligence to be tailored to specific institutions in each test in TIBER-ES to reduce costs, while maintaining compatibility with TIBER.	I	99. (iv)	BdE
8. Develop a lighter threat intelligence-based red teaming framework based on TIBER-ES principles, considering the generally lower complexity, maturity and cost-bearing ability of a typical LSI.	MT	99. (v)	BdE CNMV DGSFP
1/ Immediate (within year); ST Short term (within 1-2 years); MT Medium Term (within 3–5 years)			

INTRODUCTION[3]

A. Context

1. Malicious cyber actors continue to evolve and improve their tactics, techniques, and procedures. Cyber risk in recent years has been characterized by a marked increase in the number of data breaches detected.[4] Exploitation of critical vulnerabilities in the supply chain (e.g., highly impactful breaches of MOVEit, GoAnywhere, and Microsoft Azure), phishing campaigns, and distributed denial-of-service attacks have continued unabated. Notably, in 2023, financial services firms ranked third globally as phishing targets, with key services in their supply chains, such as telecommunications, cloud and email providers also featuring in the top five.[5] Additionally, non-malicious incidents like accidental data disclosures and configuration, as well as implementation or processing errors, continue to be an important source of cyber risk.

2. The shift towards more digitalized workflows and widespread use of remote access technologies have further increased the exposure to cyberattack.

3. Critical third parties are increasingly identified as a potential source of systemic cyber risk. Compromising widely adopted technology solutions or commonly used providers can be an effective way of breaching a series of financial institutions at the same time, as shown for example in the case of the hacking of the MOVEit file exchange platform earlier this year. Due to economies of scale and network effects, technological diversity between institutions is decreasing. Financial institutions are adopting common software solutions, acquiring highly similar hardware components, and migrating to a small set of global cloud service providers (CSPs). This way, cybersecurity incidents in the supply chain could be more easily propagated to wide swathes of the financial system.

4. Therefore, financial services firms need to continuously enhance their operational and cyber resilience as cybersecurity incidents are bound to happen. Strong capabilities to detect such incidents in timely fashion and to respond and recover are critical in the current cyber threat landscape.

5. Responding to these developments, the Spanish authorities have identified cyber risk as a major concern within the broader context of operational risk, with potential systemic implications. For example, this is one of the BdE's priorities for LSI supervision in 2023, and the CNMV has also focused greater attention to it requiring and following up on self-assessments, also

[3] This technical note has been prepared by Tamas Gaidosch (IMF).

[4] See for example the 2023 Verizon Data Breach Investigation Report.

[5] Phishing is one of the most prevalent attack vectors that lead to data breaches. Often, phishing of suppliers of financial sector firms is done to facilitate more targeted cyberattacks against them.

in cooperation with the BdE.[6] The authorities' work in 2022-2023 reflects the priority level assigned to cyber risk, and in case of the BdE, builds on its longer history of doing detailed and intrusive cyber risk supervision.

B. Assessment Scope

6. The note reviews the cyber risk regulatory framework and supervisory practices for the LSI and FMI segments of the financial sector in Spain. This includes the role and practices of the authorities in the development and maintenance of the cybersecurity regulatory framework, onsite and offsite supervisory processes, and the cyber resilience framework to detect, respond and recover from cybersecurity incidents. Microprudential supervision of SIs in Spain is within the remit of the ECB/SSM and was not assessed.

7. The FMI segment in scope consists of (i) the payment systems operated by Iberpay; (ii) Bolsas y Mercados Españoles Clearing (BMEC), the central counterparty (CCP); and (iii) Iberclear (IC), the central securities depository (CSD). The BdE supervises and oversees Iberpay, which runs SNCE, the Spanish national electronic payment system, jointly owned by Spanish financial institutions. The CNMV supervises IC and BMEC, both subsidiaries of the Swiss SIX Group, which in turn is supervised by FINMA, the Swiss Financial Market Supervisory Authority. According to the Spanish Securities Market Law, the BdE is also in charge of the securities FMIs' oversight and therefore, is also the overseer of IC and BMEC, but there is no articulation in place for the coordination of the oversight of cyber risk between the CNMV and the BdE.[7]

8. The mission collected information from several sources. These include questionnaire answers provided by the BdE, the CNMV and the Ministry of the Interior, interviews with these authorities and supervised institutions, the study of relevant laws and decrees, as well as documentation of the authorities' work, such as supervisory plans, workpapers, reports, and other evidence as needed.

9. The analysis, conclusions and recommendations of the review are guided by international regulatory and supervisory good practices. The following documents were used as the basis of the assessment: (i) the European Banking Authority (EBA) Guidelines on Information and Communication Technology (ICT) Risk Assessment under the Supervisory Review and Evaluation Process (SREP); (ii) EBA Guidelines on ICT and security risk management; (iii) EBA Guidelines on outsourcing arrangements; (iv) Cyber resilience oversight expectations for FMIs (CROE); (v) CPMI-IOSCO Guidance on cyber resilience for FMIs; (vi) the Financial Stability Board (FSB) Stock take of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices; (vii) the Basel Committee on Banking Supervision's (BCBS) Cyber-resilience: Range of Practices; and (viii) the IMF's Departmental Paper on Cyber Risk Supervision.

[6] Such as the survey based on the ECB's Cyber Resilience Oversight Expectations for FMIs, administered by the BdE and also followed up by the CNMV.

[7] The only activity of the BdE in this regard is the cyber survey as described in later in Paragraph 21.

10. The note considers cyber risk and ICT risk as materially overlapping and both categories of operational risk. This is in line with the authorities' own risk taxonomies and the FSB Cyber Lexicon's definitions.

INSTITUTIONAL AND REGULATORY FRAMEWORK

A. Legal Basis

11. Both the BdE and the CNMV operate according to a national legal framework in which all relevant EU legislation is either fully transposed to domestic law or directly applicable. Thus, the cyber risk supervision and regulation framework for Spanish LSIs and FMIs is very similar to other EU member jurisdictions' frameworks, especially to those that are in the Euro Area (EA).

12. The BdE's responsibilities for the supervision of credit institutions are primarily based on the Law on the Autonomy of the BdE and the SSM Regulation of the European Union (EU). Since 2014, Spanish SIs are supervised within the SSM in which the ECB has the leadership role and the BdE and other national financial supervisory authorities in the Banking Union participate.[8] In case of LSIs, the ECB has an indirect role and national authorities are the direct microprudential supervisors.

13. The BdE's approach to cyber risk supervision of LSIs is aligned with the principles of SI supervision of the SSM. This alignment facilitates interoperability between the Joint Supervisory Teams (JST) of the SSM and local LSI supervisory teams. This is significant because the BdE delegates members to JSTs who could at a later time be involved in LSI supervision, and vice versa.

14. The BdE is the single overseer of Spanish payment systems including Iberpay as per domestic law and acts in accordance with the Eurosystem oversight policy framework. This framework sets out the procedures to determine which European authority is in charge for the oversight of a specific payment system and establishes common oversight rules for all Eurosystem central banks. The BdE also participates in joint oversight teams of the pan-European payment systems, such as TARGET2 or TIPS.

15. The BdE has recently been designated as supervisor of the compliance of certain payment related entities with the cyber risk management rules of the DORA Regulation. Recital 104 of DORA states that Member States may draw inspiration from the DORA requirements when applying rules to operators of payment systems and processing entities, which are outside of the scope of DORA. With the objective of increasing the digital operational resilience of the Spanish payment systems, Article 4 of Royal Decree-Law 8/2023 mandates that operators of payment systems, schemes and arrangements, payment processors and other technical service providers comply with Chapter II of DORA, that includes rules on ICT risk management (governance, protocols,

[8] The term used within the EU is "national competent authorities".

prevention, recovery, backup, communication). To this end, the BdE has been given supervisory and sanctioning powers.

16. The CNMV discharges its supervisory duties according to relevant EU legislation. However, in the case of the FMIs supervised by the CNMV**,** there is no similar construct to the SSM. Two key EU regulations that govern the CNMV's work at a high level are the European Market Infrastructures Regulation (EMIR) and the Central Securities Depositories Regulation (CSDR), along with their corresponding Regulatory Technical Standards (RTS).

B. Other Relevant Regulation and Supervisory Expectations

17. The EBA's guidelines are applicable to European credit institutions and financial supervisory authorities, thus also to the Spanish LSI's cyber risk management and the BdE's supervision thereof. The most relevant guidelines in this respect are: (i) EBA Guidelines on ICT and security risk management (EBA/GL/2019/04); (ii) EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02); and (iii) EBA Guidelines on ICT Risk Assessment under the SREP (EBA/GL/2017/05). In addition, many requirements of other EBA guidelines apply to cybersecurity related matters, for example in cybersecurity governance, the EBA Guidelines on internal governance (EBA/GL/2021/05), or in the broader supervisory approach, the EBA Guidelines on common procedures and methodologies for the SREP and supervisory stress testing (EBA/GL/2022/03).

18. International standards for ICT risk management and cybersecurity are taken into account in the BdE's cyber risk supervision of LSIs as supplementary sources, because of their non-binding nature.

19. The BdE's cyber risk oversight of payment systems follows the Eurosystem Cyber Resilience Strategy. The strategy, issued in 2017, is part of the Eurosystem Oversight Framework and is based on international standards and guidance issued by the Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (CPMI-IOSCO): (i) Principles for financial market infrastructures (commonly referred to as PFMIs), and (ii) Guidance on cyber resilience for FMIs. Within the PFMIs, key principles concerning how cyber risk is managed are Principle 2 on governance, Principle 3 on the comprehensive risk management framework, and Principle 17 on operational risk. The Guidance on cyber resilience for FMIs in essence expands on these principles by adding a set of more specific and detailed requirements to ensure the continuity of critical services through disruptions caused by cyber incidents. To this end, it covers cyber governance, identification, protection, detection, response, and recovery (including a two-hour recovery time objective), testing, situational awareness, and learning and evolving. The guidance stays principles-based, which allows for a degree of flexibility in its implementation.

20. Two more specific tools embody the oversight expectations of the BdE regarding payment systems cybersecurity. These are: (i) the ECB's Cyber Resilience Oversight Expectations for FMIs (CROE), which provides details and assessment criteria for the implementation of the CPMI-IOSCO Guidance on cyber resilience for FMIs, including a maturity model; and (ii) a cybersecurity survey to support the aforementioned assessment.

21. For the CNMV and its supervised FMIs, the most important international standards that are applicable for cybersecurity matters are the CPMI-IOSCO's PFMIs and Guidance on cyber resilience for FMIs.[9] In addition, the above-mentioned CROE and the cybersecurity survey are also used, since the BdE, with the cooperation of the CNMV, extended the survey to the Spanish CCP and CSD as well.

22. The EU's DORA harmonizes and strengthens the resilience requirements in the financial sector and is directly applicable to Spanish LSIs and FMIs as well as stipulating requirements for supervisors, both the BdE and the CNMV. Specifically, DORA sets out new or strengthened requirements in the areas of (i) ICT risk management; (ii) incident reporting; (iii) resilience testing; (iv) third party risk management; and (v) critical third parties' oversight. While DORA entered into force in January 2023, its requirements will be applicable only from January 2025. On that date, according to Article 4 of Royal Decree-Law 8/2023, operators of payment systems, schemes and arrangements, payment processors and other technical service providers that provide services in Spain will also need to comply with those provisions of DORA related to ICT risk management (Chapter II). The implementation of DORA will require a varying degree of effort depending on current practices and maturity levels, with the LSI sector and smaller FMIs expected to spend relatively more to achieve compliance. Supervisors resource needs are expected to increase as well.

23. Key EU regulations that are not financial sector specific but have a direct bearing on the financial sector entities and authorities in scope are related to cybersecurity in general, and data protection. These are the Directive on measures for a high common level of cybersecurity across the Union (NIS2, replacing a narrower predecessor commonly known as the Network and Information systems Security or NIS Directive), and the General Data Protection Regulation (GDPR). Besides setting out requirements generally aligned with previously mentioned sector specific EU regulation, both require entities and supervisors to co-ordinate with non-financial sector authorities, for example the Data Protection Authority, in specific situations such as data breaches involving personal data.

C. Internal Organization and Resourcing of Cyber Risk Supervision

24. At the BdE, ICT and cyber risk supervisory expertise is organized along both vertical and horizontal criteria. In general, LSI microprudential supervision belongs to the Directorate General Banking Supervision, while FMI oversight is with the Payment Systems Department (DD.SPA) of the Directorate General Operations, Markets and Payment Systems. On the vertical, there are fully dedicated experts in SI and LSI offsite supervisory teams and in DD.SPA, albeit these are not fully dedicated to ICT or cyber risk. Experts in SI supervision are part of the Joint Supervisory Teams (JST) within the SSM. Only the Directorate General Banking Supervision has a horizontal structure. Here,

[9] The CPMI-IOSCO PFMIs are not legally binding, but members committed themselves to implement them in their jurisdictions and agreed to monitor compliance, which makes them de-facto regulation. See also, on this point, this FSAP's Technical Note on Spain: Regulation, Supervision, Oversight, and Crisis Management of FMIs.

there are experts in (i) the ICT Risk Inspections Division, who perform on-site examinations[10] both at SIs (Spanish and other) and LSIs (Spanish only), among other duties; and (ii) the IT Risk Division, who do regular horizontal analyses across both SIs and LSIs, are responsible for the TIBER-ES security testing framework, provide specialist support to other supervisory functions, and collaborate with other jurisdictions on a series of ICT risk topics.

25. The headcount of ICT and cyber risk supervisory positions at the BdE is comparatively strong but runs at capacity even as the workload looks set to increase in the near future. Nominally, this headcount is around 10 percent of the total supervisory headcount, but several positions remain unfilled due to a very tight job market for cybersecurity skills, exacting expectations, and a slow hiring process. The lingering vacancies and the projected increase in workloads do not bode well for the continued ability to deliver at current levels of high professional performance.

26. Given the large number of ICT and cybersecurity experts distributed in several organizational units, the BdE strives to break silos and foster coordination and cooperation. To this end, there was a recent reorganization within the BdE's Directorate General Banking Supervision to arrive at the structure described above, which is better suited to cross-divisional cooperation. In addition, there are three fora that facilitate cooperation, coordination, sharing of experience and professional development: (i) a strategy committee for ICT risk; (ii) an ICT outsourcing committee; and (iii) an IT Risk forum.

27. Scarcely resourced, cyber risk supervision of FMIs at the CNMV is done out of the Markets Directorate General. There is only one dedicated cybersecurity position in a support role at the Policy, Innovation and Sustainable Finance Department within the Policy and International Affairs Directorate General. Out of necessity, the CNMV fulfills its cybersecurity supervisory duties mainly with experts whose primary specialization is not in cybersecurity. Given the considerable experience with FMI oversight—including for operational risk—and the significant effort expended by those involved, this has worked well so far, importantly also reflecting favorable external conditions.[11] However, the inadequate headcount of dedicated specialists puts the CNMV at risk as workloads are expected to increase, and the risk of (major) cybersecurity incidents due to exogenous reasons. There is a pending request for two additional headcounts, but it can take extremely long to approve and fill them, due to the high rigidity of HR processes, which are not under the CNMV's control.

28. Cyber risk supervision at both the BdE and the CNMV is fully integrated into the broader supervision, with formalized, mature, and well documented processes according to established internal policies. Responsibilities, organizational structures and reporting lines are

[10] Called inspections in the ECB/SSM parlance.

[11] The integration of both IC and BMEC in SIX Group has greatly benefited the cybersecurity stance of these FMIs, as evidenced by before/after cyber maturity assessments. In addition, a common IT infrastructure simplifies their cyber risk management and consequently supervision as well.

clearly defined and adhered to. There is adequate planning, review, and quality assurance of supervisory activities.

D. Conclusions

29. The legal basis and relevant regulation convey adequate powers to effectuate cyber risk supervision. There are sufficiently broad powers regarding collection of information in any form on any relevant matter, to assess compliance, impose corrective actions to have supervised institutions and FMIs rectify matters within a reasonable timeframe, and impose sanctions and take enforcement action as a last resort to ensure compliance.

30. However, rigid hiring and employment policies and rules have a negative impact on authorities' practical ability to discharge their duties and keep pace with the rapidly changing cybersecurity threat landscape and resultant risks. This has led to the BdE's resources continuously running at full capacity and the CNMV being inadequately staffed, while workloads are expected to steadily increase starting in the short term with the implementation of DORA, and the phasing in of TIBER-ES testing. In addition, it is very unlikely that authorities are able to improve their coverage or depth of supervision in general, while risk levels are on a rising trend across the board and are expected to continue that way in the foreseeable future.

E. Recommendations

31. The authorities are advised to prioritize addressing the human resource bottlenecks in cyber risk supervision. More specifically:

(i) The BdE should assess the need for increasing the cyber risk specialist headcount and prioritize filling existing open positions. A calculation considering current and projected workloads over a three-to-five years period would be most useful to support such an assessment and develop a formal case for additional headcount. Given the uncertainties regarding the amount of additional supervisory work due to the implementation of DORA, a more precise estimate can be made after the technical standards are finalized.

(ii) International standards require budgetary processes that do not undermine autonomy and adequacy of resources. In this context, the annual process that the CNMV has to follow to secure government approval for its budget introduces uncertainties regarding ability to ensure adequate number of, and expansion in staff, including expert and specialized human resources in the highly competitive area of cyber security. This is a significant issue in light of identified challenges in current supervisory practices, such as in onsite supervision of cyber risk (discussed below), and will only grow in the near-term, reflecting rapidly expanding cyber threats and implementation of new regulations, such as DORA. Consequently, it is recommended that the CNMV estimate current and projected future workload, ensure alignment of resources to these, and have full autonomy over the recruitment and retention process so that they become more effective at hiring additional staff at the right experience and competence levels.

(iii) In the meantime, the CNMV should establish and staff a small cyber risk competence center with a horizontal (cross-cutting) mandate to provide specialist support of all activities that have a cyber risk supervisory component.

SUPERVISORY PRACTICES

32. The authorities consider cyber risk supervision a priority. Priorities at the BdE for LSI supervision are aligned with those set for SIs by the ECB, which include cybersecurity and ICT risk since 2022. Similarly, payment system oversight at the BdE and FMI supervision at the CNMV focuses—among others—on cyber resilience as set out in the CROE and the CPMI-IOSCO Guidance.

33. There is an effective risk-based approach to cyber risk supervision at the authorities, which is implemented by (i) prioritizing resources for institutions where manifestation of cyber risk can have higher impact on the financial sector; (ii) considering the wider risk context; and (iii) using risk and maturity ratings consistently. For example, in case of LSIs 6 such institutions were identified and grouped together for more intense monitoring. Three ICT and cyber risk experts have been assigned to the supervision of this group. Further, both the BdE and the CNMV look at cyber risk within the wider context of operational risk and resilience, the ultimate goal being to ensure that LSIs and FMIs can continue to deliver critical services through disruption.[12] Finally, the BdE rates every deficiency identified at LSIs using the same criteria as for SIs in the SSM and has an internal mechanism to ensure consistency of ratings. Moreover, FMI oversight (both by the BdE and the CNMV) is driven by assessed maturity levels as defined in the CROE. These ratings in turn help making objective decisions in the prioritization of resources mentioned before.

34. The authorities apply the proportionality principle in cyber risk supervision primarily by setting expectations on control maturity. Institutions are expected to have a baseline IT and cyber risk control environment, irrespective of size and complexity. However, the expected maturity[13] depends on the size and complexity of the institution, i.e., levels of sophistication, documentation, optimization, automation, scalability, and redundancy, that the control exhibits are expected to rise with size and complexity. It is also expected that larger and more complex institutions will have more controls, but as there is a rather strong baseline, this is less of a differentiator. Questionnaires used by both the BdE and the CNMV take account of proportionality. In case of the FMIs there is the maturity model and "comply or explain" principle of the CROE that also facilitate a proportional approach.[14]

35. Overall, the key elements of the authorities' supervisory approach are offsite (ongoing) supervision, onsite examinations (inspections), thematic reviews, and security testing oversight. All elements are mature and are performed in a planned, controlled, and

[12] In turn, at the BdE operational risk ratings feed into entity level risk ratings, but this is not in scope for this technical note.

[13] Approximately, how the control should be implemented (control procedure), as opposed to what is expected to do (control objective).

[14] The maturity model embedded in the CROE requires more sophisticated controls at systemic FMIs.

documented fashion as described under the *Internal Organization and Resourcing of Cyber Risk Supervision* section of this report (see next sections for further details). However, there are differences regarding how these elements feature in the BdE's and the CNMV's approach, and in the BdE, between LSI supervision and FMI oversight.

36. The BdE materially adheres to the SREP methodology for LSI supervision, including for cyber risk.[15] As such, it complies with the applicable EBA guidelines. With regard to cyber risk, the process is deliberately kept very similar to SI supervision (but outputs differ). This is so that there is a high degree of fungibility of LSI and SI cybersecurity supervision expertise, and indeed the same team members can work both on LSI and SI onsite examinations.

37. The majority of Spanish LSIs rely on two important ICT outsourcing service providers, which increases concentration risk. Both providers are owned by LSIs and thus fall under the BdE's direct supervision. Well aware of the risk concentration, the BdE focuses its LSI supervisory attention on these two providers. The providers are placed in the special monitoring group mentioned in paragraph 33 and are under more scrutiny, a more intense onsite examination schedule, and generally kept in close contact.

38. Onsite examinations feature prominently in BdE's supervisory approach. While the EBA guidelines remain neutral on the appropriate mix of onsite and offsite supervisory activities, traditionally the BdE emphasizes onsite examinations because this way it can obtain stronger assurance on the effectiveness of risk management, more specifically on key controls' effectiveness.

39. However, there is no onsite activity either in the CNMVs or the BdE's FMI oversight approach. This is common in FMI oversight internationally and indeed the applicable regulation and international standards are agnostic on the topic, i.e., there is no explicit requirement for onsite inspections.[16]

A. Offsite Supervision

40. Generalist supervisors with the support of a small team of ICT and cyber risk experts are responsible for BdE's offsite (ongoing) LSI cyber risk supervision. The LSI and other institutions outside the SSM department has three dedicated ICT and cyber risk experts who provide the specialist support. Activities are embedded in the overall offsite supervisory process and are focused on the entities in the special monitoring group, among which the two ICT outsourcing providers are prioritized further.

41. Offsite supervisory activities focus on information gathering using a variety of sources, validation, and ongoing risk assessment in accordance with the LSI SREP methodology and

[15] The methodology was developed in cooperation by the ECB and a number of European central banks.

[16] In fact, there are only high-level expectations directed to FMI overseers, as opposed to FMIs. For example, the CPMI-IOSCO sets out 5 responsibilities for central banks, market regulators, and other relevant authorities for financial market infrastructures, one of these being the responsibility to subject FMIs to appropriate and effective regulation, supervision, and oversight; and the CROE are directly aimed at FMIs and not overseers.

EBA SREP guidelines. Accordingly, the cyber risk assessment, as a category of operational risk, feeds into to the broad assessments of the LSI entities' (i) business model, (ii) governance and risk assessment frameworks, and (iii) risks to capital.

42. The BdE uses the unmodified IT risk taxonomy of the EBA SREP guidelines. This defines five risk categories: IT security risk, IT availability and continuity risk, IT change risk, IT outsourcing risk, and IT data integrity risk.

43. Certain LSIs business models rely heavily on digital services, consequently the BdE prioritizes the assessment of digital transformation programs. A highly digitized bank can achieve competitive advantages in the marketplace, which is a key driver of such programs (others being internal operational efficiency and cost optimization). However, comprehensive digital transformation programs are complex and come with specific ICT and cyber risks stemming from the changes in the IT architecture and associated processes. Disruption risk, for example, typically increases until the transition is complete and IT operations stabilize.

44. Cybersecurity governance is another focus area of the offsite LSI supervision. Risk buildup, higher incidence of cybersecurity incidents and associated disruptions, and increased losses often have their root causes in governance deficiencies, so the supervisory attention is well justified. Some of the important considerations in this regard are formally set and approved risk tolerance levels, board involvement, appropriate responsibilities, competencies, and reporting lines in all three lines of defense.

45. An important tool in the offsite LSI supervision is the IT risk self-assessment questionnaire. The same questionnaire is used for both LSIs and SIs. For LSIs, this has been administered for three years. The tool is revised from time to time to reflect changes, for example a revision is expected this year because of the changes brought by DORA. The questionnaire collects data on the IT environment, risk levels, and control strength. Risk categories are defined according to the EBA taxonomy and individual risks are assessed on a 4-grade empirical scale to avoid the observed tendency to categorize most risks as medium in a 3-grade scale. Risk levels must be assessed taking into account the inherent risk. Control levels also must be assessed based on a 4-grade empirical scale, considering indicators of effectiveness, maturity, and implementation status. All in all, this leads to a rather mainstream qualitative IT risk assessment where the supervisor calls the shots on residual risk level determination, based on the data collected and other information available, and decides on the course of actions depending on the outcome. The results of the self-assessments are stored in a specific database, which facilitates later analyses and benchmarking.

46. The BdE took action to nudge LSIs to a more conservative approach after observing that the early self-assessments were too optimistic. Based on first-hand information such as past examination results, BdE saw that there was a tendency to underestimate risk and overestimate control strength, which skewed the residual risk determination. Feedback to the LSIs resulted in more realistic self-assessments.

47. Other notable sources of information are the regular meetings with supervised entities and audit reports, and certifications. BdE seeks to keep in contact with key LSI's IT and cyber risk senior management to emphasize supervisory attention. Audit reports and certifications are considered as corroborative information but are not relied on as evidence.

48. There is latitude in what weight the BdE assigns to ICT and cyber risk within the operational risk assessment. Factors considered by the BdE in assigning the weight include the complexity of the IT architecture, major projects, dependency on fully digitalized services, and track record of incidents. It is expected that in the near future the ICT and cyber risk weight will be raised to around 50 percent in SI supervision at the SSM level, which would be more in line with current developments in the financial sector. BdE aims at maintaining the alignment between SI and LSI supervisory methodology and thus will apply the same weight in LSI supervision.

49. FMI offsite supervision is based on regular discussions with management and validated self-assessments and analysis. Both the BdE's Payment Systems Department and the CNMV meet with relevant FMI management regularly to discuss developments on cyber risk topics, follow up recommendations, review progress on improvement initiatives, validate assertions, and to communicate expectations going forward.

50. The BdE's Payment Systems Department and the CNMV conduct regular reviews based on CPMI-IOSCO guidance and the CROE as applicable. The BdE's DD.SPA administers the cyber survey to all FMIs within its remit. While in theory this is a voluntary exercise, all entities participate. In the context of the Eurosystem, DD.SPA adjusted the survey over the years to better align it with the CROE and to elicit more differentiated answers. Validation methods include outlier analysis, challenging less plausible assertions, and corroborating answers with information collected through other means. Also, within the Eurosystem, DD.SPA prepares a report on each FMI, maintains a dashboard for the sector and does trend analyses. Similarly, the CNMV prepares reports regularly on the results of their own compliance assessments.

B. BdE's Onsite Examinations of LSIs

51. Onsite cybersecurity examinations are harmonized with the offsite supervisory process at the BdE in the risk-based approach. Results of the offsite supervision feed into the planning and execution of examinations, which then in turn inform the former in a feedback loop. Thus, onsite examinations are predominantly conducted at LSIs exposed to higher cyber risk typically because of size, complexity, potential for impact on others, or significant weaknesses.

52. By design, BdE's onsite cyber risk examinations of LSIs are broad and intrusive, and as a result, resource intensive and relatively infrequent. It is typical to cover a very substantial subset of cyber risk areas and there is much attention paid to obtaining first-hand evidence. The actual onsite work can exceed two months in duration and an examination can last three to four months end-to-end, with as much as six experts participating with a varying degree of intensity across this period. In addition, the process is highly regulated and must be thoroughly documented. Given the available resources, this means that delivery is limited to two examinations per year in

average and takes up around 20 percent of the BdE's total delivery capacity, the 80 percent being expended on SIs.

53. The main goal of the examination is to obtain strong assurance on the functioning of the cyber risk control environment. Such assurance is based on observing the controls being executed, reviewing artifacts on past control execution, and even control effectiveness tests, however the latter technique is used sparingly and reserved to high-risk cases due to it being the most resource intensive.

54. Examinations are done according to detailed internal policies that prescribe a highly structured approach, set deadlines for deliverables, and requirements for internal documentation and approvals. Key elements of the process are: (i) planning and approval of plans, including the scope, procedures to be executed and the timeline; (ii) documentation review based on formal documentation requests; (iii) interviews according to communicated and agreed upon meeting schedules; (iv) direct extraction of information from systems to support the risk and control assessment; (v) analysis and validation of the information collected by various means; (vi) risk and control assessment; (vii) drafting of findings and recommendations, including severity rankings; (viii) follow-ups and clarification requests as needed on open issues; (ix) internal review; (x) preliminary conclusions; (xi) reporting and related internal approvals; and (xii) issuance of a requirements letter.

55. A less commonly seen feature of the examination is the direct extraction of information on the functioning of the control environment.[17] Significantly, this is done with read-only access, and only on selected support systems and not business systems. For example, various IT service management systems, policy repositories and internal information portals fall into this category. The governing principle is to enable efficient first-hand evidence gathering without incurring unnecessary risk by having too broad access. If information needs to be extracted beyond the scope of this access, then a specific request is issued for the LSI to provide it.

56. The examination is a sufficiently documented to the level that experts not involved in the examination are able to understand the process, the decisions taken in directing the work, and the rationale for the findings and recommendations. Project management documentation (plans, meeting schedules, team composition, approvals, internal approvals, etc.), client communication, workpapers, evidence, and reports are stored in a standardized and easy to understand folder structure, in a document management system.

C. Thematic Reviews of LSIs

57. Only the BdE performs thematic reviews as in the case of the CNMV, thematic reviews are not nearly as useful or necessary for the FMIs in scope, because there are only two of them.

[17] Commonly, supervisors avoid directly accessing systems of the bank and rely on information requests, sometimes observing the extraction, e.g., they could require a system administrator to list all cyber incidents recorded in an incident management system on the spot but would not run the query themselves.

58. Thematic reviews at the BdE are done to enhance cyber risk supervision by obtaining a better understanding of a risk issue or the state of play in a specific area, typically, across a segment of the financial sector. Such reviews provide useful input to strategic and tactical planning of supervisory activities, resource needs, possible risk concentrations, problem areas, outliers, and so on. It also allows benchmarking of individual institution against peers and the industry in general.

59. Thematic reviews are questionnaire-based and there is a strong validation built into the approach. Supervisors do short two-to-three-day visits to a selected sample of institutions, to either fill in the questionnaire in an interview setting or to validate already filled in questionnaires. For some, but not all questions, there is some form of supporting evidence requested. Knowing of the possibility of being selected in the validation sample, all LSIs are nudged to provide better substantiated answers.

60. With the strongly validated thematic reviews the BdE also aims to balance the overall supervisory approach, which traditionally leans on deep examinations at the expense of horizontal breadth. This a less common hybrid approach between purely self-assessment-based reviews and thematic examinations, both widely used tools internationally.

61. In the last three years, the BdE did three thematic reviews, out of which one had in scope the LSI segment. This review dealt with the overall IT and IT risk landscape, with a special focus on cybersecurity.

D. Cybersecurity Testing and Crisis Exercises

62. Cybersecurity testing has gained prominence in recent years as an effective way to assess the cybersecurity stance with real-life attacks. There is a wide variety of such testing done at financial institutions, with varying methods, scope quality, and taxonomies. However, for supervisory purposes and thus for the 2023 FSAP, the real deal is the Threat Intelligence-Based Ethical Red Teaming (TIBER). This is a framework developed jointly by the ECB and other European central banks, including the BdE, hot on the heels of the pioneering work of the Bank of England, their framework known as CBEST.[18]

63. The BdE approved TIBER-ES in 2020, an adaptation of TIBER that keeps all its mandatory requirements. Therefore, tests done according to TIBER-ES can be certified as TIBER tests and are acceptable to all jurisdictions that recognize the framework. It is expected that most European jurisdictions will recognize TIBER, greatly contributing to the harmonization and standardization of threat intelligence-based ethical red teaming, also—hopefully—reducing the burden of internationally active financial firms in this space. The BdE took responsibility for maintaining and developing the TIBER-ES framework with assistance from the CNMV and the

[18] For more on the world of TIBER, see a good introduction at https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html

Directorate General of Insurance and Pension Funds (DGSFP) of the Ministry of Economy, Trade and Enterprise. Practically, TIBER-ES is recognized in the entire Spanish financial system.

64. Because of the significant risks involved, TIBER-ES and TIBER tests in general are lengthy, complex, elaborately controlled and thus expensive undertakings. On the technical level the targets are usually critical production systems at large institutions, so errors in testing could result in high-impact disruptions that may propagate outside of the tested entity. It is necessary therefore to pay special attention to vendor vetting, planning, coordination between multiple stakeholders, contingency arrangements, quality assurance and validation, which drive up costs.

65. TIBER-ES and TIBER in general emphasize the importance of targeted threat intelligence in driving the testing process in an effort to be as realistic as possible, but early results indicate that the benefit is less than expected. It has been observed, for example, that most threat intelligence reports are in fact not that target-specific, probably because threat intelligence providers often cannot identify threat actors that are specifically after the tested institution. This is not very surprising, given the clear financial motivation of most threat actors that target the financial sector, which incentivizes them to act opportunistically.[19]

66. By design, authorities' involvement in TIBER-ES testing is restricted to facilitator, overseer, and validator roles. Their role is centered on the TIBER Cyber Team and the TIBER Test Manager Team activities. A key role is the validation and formal certification of the test, which is needed to be accepted by other supervisory authorities.[20]

67. TIBER-ES, as all compatible adaptations, is intended for large institutions but it is expected that a number of LSIs and FMIs will be tested as well. Some of the Spanish LSIs are sufficiently large, complex, and interconnected for such testing to be desirable as a method to assess their true cyber resilience. Also, they are at the expected cybersecurity maturity level to be able to handle the requirements and manage the risks. The rationale behind testing FMIs is that their high level of cyber resilience is crucial to the functioning of the financial system.

68. However, TIBER-ES is not mandatory just yet, and it is not a supervisory tool in itself. There is genuine interest from financial firms, and a clearly expressed expectation from the authorities for qualifying firms to take it up, as it is envisaged to become mandatory in the near term (see DORA) for a subset of institutions.

69. The BdE and a number of supervised LSIs and FMIs participate in voluntary cyber crisis exercises. While the BdE does not organize exercises, they participate in national exercises as

[19] In other words, it makes economic sense for rational financially motivated threat actors to cast a wide net, which makes the threat landscape rather similar to most institutions.

[20] For details, see https://www.bde.es/f/webbde/INF/MenuHorizontal/Servicios/TIBER-ES/Guia_de_Implementacion_TIBER-ES_Ing.pdf

observers, and in cross-border ones as national authority.[21] At the national level, the Spanish National Cybersecurity Institute (INCIBE) runs exercises (CyberEx) every year since 2012, which are well-regarded by participants. The financial sector is well represented, for example in the last iteration one third of participants were from the financial sector.

70. CyberEx is a graded individual level exercise that does not test co-ordination between participants. Participants are involved in three different activities: (i) solving a crisis situation in a role play setting for management; (ii) a technical simulation for the incident management teams; and (iii) a targeted cyberattack executed by INCIBE. After concluding the activities, participants are graded on a five-level scale based on their effectiveness in solving the crisis scenario. Over the years the average score has improved and now it stands at 3.94 (5 being the best) which indicates a surprisingly good level of readiness. However, it is difficult to extrapolate this result to conclusions about sectoral readiness, because of still low participation ratios and selection bias.[22] The exercise is complemented with a cyber-resilience measurement each year, with more than 45 cybersecurity indicators in the areas of anticipating, detecting, preventing, protecting, responding, mitigating and recovering from cybersecurity incidents.

71. The Spanish Inter-Bank Cooperation Centre (CCI) ran a crisis exercise in 2023 that added the much-needed collective aspect. With the participation of a critical service provider, the exercise tested participant institutions' individual response and recovery capacity as well as their co-ordination and collective response.

72. On the international stage, BdE participates in exercise run by the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the Eurosystem. Due to the logistical complexities and risks involved, these are tabletop exercises only. Examples include the 2022 European Cross Border Tabletop Exercise, the 2023 Locked Shields Strategic Exercise (by FS-ISAC) and the UNITAS crisis communication exercise (by Eurosystem).

73. While CNMV has not participated so far in crisis exercises due to very limited specialist capacity, they encourage FMIs to participate, and discuss results. With the advent of TIBER-ES and DORA it will be necessary for CNMV to be more actively involved.

[21] This technical note does not address cyber crisis exercises at the authorities themselves, i.e., exercising the response and recovery form major incidents affecting them directly.

[22] Better prepared institutions tend to participate in larger numbers in voluntary exercises, especially if graded, so the test population is not random.

E. Topical Issues in Cyber Risk Supervision

Third-party Risk

74. Third-party risk has risen significantly due to the ever-increasing reliance on outsourcing and other services of technology providers, including in the Spanish financial sector. For example, there are over 3,000 third-party arrangements on technology services in the Spanish LSIs, based on reporting to the BdE.

75. Cloud outsourcing is on the rise as well, but for the time being core banking systems are kept on-premises. According to the BdE's information, there are no cloud migration plans for the short- and medium-term involving core banking sectors in the LSI segment. LSIs typically migrate office, collaboration, analytics, customer relationship management, and other business support systems to the cloud.

76. LSIs also use cybersecurity managed services, a form of outsourcing. Security Operations Centers (SOC) are among the most commonly outsourced functions, with established specialist providers in the Spanish managed services market.

77. As noted earlier, there is a concentration risk in the LSI segment as approximately 60 percent of these banks rely on two ICT service providers for critical services. These providers are owned by LSIs and thus are under direct BdE microprudential supervision (including onsite examinations). The situation has both upsides and downsides. The main upsides are that many LSIs are in a better cybersecurity stance given that on their own they could not operate on ICT systems and services that are as well protected as what the service providers offer them. In addition, the BdE's microprudential supervision has an impact multiplier. By focusing on these two entities, it can cover most key ICT and cyber risks for the majority of the sector. The main downside is the risk concentration at the providers that can result in higher impact cybersecurity incidents, the worst case being breaches or disruptions across the served LSIs all at once. Arguably, the likelihood of such an extreme occurrence is low, given the capabilities of the providers and the close attention of the supervisor, but cannot be ruled out.

78. The BdE requires notification from LSIs on planned third-party arrangements. Besides key information on the nature of the planned arrangement, (including whether it is cloud outsourcing), LSIs must also send for review the draft contract, their outsourcing policy, and a risk and materiality assessment. The IT Risk Division processes the notifications. Given the high number of submissions and the resulting workload, the division uses workflow and project management tools to increase efficiency. In addition, the arrangements are put in a database that makes it possible to obtain a consolidated view of all third-party arrangements and identify common dependencies.

79. In a similar vein to the LSIs' use of common providers, the FMIs under CNMV supervision have much of their ICT infrastructure and cybersecurity framework shared, as they belong to the same group that has started integrating them within group-wide

structures.[23] The implications are similar too, both for FMIs and the CNMV. There are benefits from a more mature and robust operational environment, better cybersecurity stance, and simplified oversight, but there is risk concentration.

80. FMIs must obtain authorization from the CNMV for outsourcing which involve core services. Both IC and BMEC have in place processes to classify outsourcing providers for criticality and assess them on several relevant indicators (e.g., on BitSight cyber score and financial soundness). The CNMV reviews the results regularly and keeps track of all arrangements.

Incident Reporting

81. Authorities require supervised institutions to report cyber incidents according to formally defined criteria and deadlines. Both the BdE and the CNMV treat cyber incident reporting with priority and follow up on the incidents reported that cross a threshold. However, there are differences in reporting criteria and number of cyber incidents reported to each authority.

82. Starting 2022, the two CNMV-supervised FMIs in scope must report all operational incidents. Major incidents must be reported immediately, while minor ones are reported on a monthly basis. The monthly report contains the major incidents as well, making for easier aggregation and analysis. Repeated incidents trigger further scrutiny, and a specific report must be submitted that explains why the incident reoccurred and what measures have been taken to avoid further recurrence. The CNMV reviews and analyses all reports to proactively find worsening trends, if any. Since the number of incidents is relatively small, this approach works quite well.

83. LSIs must report cyber incidents that meet certain criteria to the BdE. The reporting threshold is calibrated to capture all relevant incidents that may need supervisory attention and ignore the rest and is implemented so that if one or more of seven predefined criteria are triggered, then the incident must be reported. The criteria are qualitative and partially overlap to better capture incidents that otherwise might have gone under the radar. For example, the requirement to report an incident that triggered the activation of disaster recovery or business continuity plans overlaps, i.e., is not distinct from, the requirement to report if emergency escalation procedures were activated, and so on. For all reportable incidents, at least three reports must be submitted: initial, interim, and final.[24] The final report must contain, among other information, a root cause analysis, details on mitigating measures for the future, and financial impact, both direct and indirect. This reinforces the continuous improvement loop in the cybersecurity management framework at the reporting institution.

84. Payment systems in scope under BdE oversight must report cyber incidents according to the Eurosystem procedure for major incidents in the oversight policy framework. The approach is similar to the banking supervision side, including the types of reports required, but

[23] The integration and improvement program is still in progress.

[24] There could be more than one interim report, depending on the progress of response.

reporting criteria are different, because of the differences in operational risk. Both sets of criteria work well to identify incidents of supervisory interest.

Supervisory Technology (SupTech) in Cyber Risk Supervision

85. The BdE has a SupTech strategy with the core objective to further improve prudential supervision and help the BdE become an international reference institution in this regard. Four pillars support this approach: (i) collaboration with the SSM, in which the BdE is the SupTech center for graph analysis; (ii) in-house development of SupTech tools; (iii) creating an innovation culture; and (iv) specialised training, e.g., in data science, artificial intelligence and machine learning.

86. SupTech tools developed at the BdE so far proved to be effective in areas where there has been granular structured data available over longer time periods. For example, SupTech assisted reconciliations between credit registry information and collateral reports were very successful in identifying discrepancies and resulted in improved data quality.

87. While the success is promising for cyber risk supervision, the dearth of useful data is an impediment. Data availability on cyber risk at financial institutions globally is nowhere near to financial data in terms of quality, coverage, granularity, and metadata consistency for a variety of reasons beyond the scope of this note. Advanced data analytics tools are less effective in this situation. However, tools under consideration that work on unstructured data may be more successful, such as natural language processing tools that could be applied for board meeting minutes analysis or sentiment analysis.

Preparation for DORA

88. The authorities are acutely aware of the implications of DORA for both supervised entities and themselves. The most impactful changes in terms of workload are expected in supervision of critical third parties, applicability of TIBER testing, and incident reporting. Regulatory Technical Standards (RTS) and Implementations Standards (ITS) are currently developed so for the time being it is difficult to forecast the additional resource needs, both at institutions and the authorities. There is broad agreement however, that the increase will be significant.

89. At the same time, key DORA requirements are well understood conceptually and thus the authorities have started preparatory work. The BdE conducted an information campaign for the sector and the CNMV discussed the implications with its supervised FMIs. It appears that the application of the proportionality principle that is explicitly stated in the regulation is one of the most debated aspects but without the final RTSs and ITSs any prediction in this regard is premature.

F. Coordination and Cooperation

90. Domestically, the authorities mostly cooperate, and coordinate based on informal mechanisms and personal relationships. This has worked satisfactorily so far, for example there has been frequent and fluid interaction between the BdE and the CNMV, information sharing and training with INCIBE, and ad-hoc contacts with law enforcement and national security agencies. A

formal agreement is being negotiated between the BdE, the CNMV and the DGSFP on the development and deployment of TIBER-ES.

91. However, there is no cooperation or coordination between these financial supervisory authorities and the National Centre for the Protection of Critical Infrastructure (CNPIC). The financial supervisory authorities are not involved and do not officially know which institutions under their supervision are classified as critical operators or what infrastructures are designated as critical.

92. Internationally, the BdE plays an active role in the European co-operation mechanisms and bodies on banking supervision and systemic risk oversight. Work under these mechanisms is based on EU regulations and agreements. Examples include: (i) the ECB Joint Supervisory Teams; (ii) various cyber risk working groups and expert networks at the ECB and the EBA; (iii) the European Systemic Cyber Group (ESCG) of the European Systemic Risk Board; (iv) the European Cyber Resilience Board for pan-European Financial Infrastructures and its Cyber Information and Intelligence Sharing Initiative (ECRB CIISI-EU); and (v) the ECRB Crisis Coordination Network.

93. In addition, the BdE takes part in a significant number of international initiatives beyond the EU. Within the Basel Committee on Banking Supervision (BCBS), the BdE participates in the Operational Resilience Working Group (ORG), the Financial Technology Group and the Work stream on Non-Financial Risks (WNFR) of the Supervisory Cooperation Group (SCG). The BdE has been also an active member of the Cyber Incident Reporting (CIR) Group of the Standing Committee on Supervisory and Regulatory Cooperation of the Financial Stability Board (FSB) and its involvement will continue in the group continuing the work of the CIR, the FIRE (Format for Incident Reporting Exchange) group. Also at the FSB, the BdE is involved in the Workstream on Third-Party Risk and Outsourcing under the Standing Committee on Supervisory and Regulatory Cooperation (SRC). Work carried out by the group includes the development of a third-party risk taxonomy and a toolkit for institutions and supervisors. Less formally, the BdE is an active member of cyber risk-related international groups such as the Cyber Security and Operational Resilience Group (CSOR) of the Senior Supervisors Group (SSG) and the IT Supervisors Group. The BdE also cooperates closely with the Association of Supervisors of Banks of the Americas (ASBA) sharing best practices in the supervision of cyber risk (among other risks). Finally, the BdE is a member of the CPMI where it cooperates in the setting up of standards and conducting Level 3 assessments.

94. The CNMV also takes part in in EU and broader international cooperation mechanisms. For example, in accordance with EMIR, the CNMV shares information with the College of Supervisor of EU CCPs; is a member of the European Securities and Markets Authority's (ESMA) CCP Standing Committee; and contributed to FSB and CPMI-IOSCO output. In addition, the CNMV regularly meets with FINMA, to discuss concerns and developments at SIX Group that have a bearing on IC and BMEC.

G. Enforcement

95. The authorities' powers to take enforcement action for non-compliance with cyber risk regulations is based on the general sanctions regime set out for the sector. The legal

framework stipulates the classification criteria of infractions, and the sanctions applicable to each type of infraction including fines, suspension of activity, sanctions to upper management, and publication of sanctions. However, it was not necessary to levy sanctions recent years for such non-compliance because institutions implemented satisfactorily the directions received from the authorities.

H. Conclusions

96. The reviewed cyber risk supervisory practices of the authorities regarding LSIs and FMIs in scope are materially in line with applicable regulations and guidance and prevailing international good practice, but there are challenges to be addressed.

97. Key strengths include:

(i) Clear supervisory expectations that are well communicated;

(ii) Effective risk-based approach and application of proportionality in supervision;

(iii) Useful and well validated horizontal reviews at the BdE;

(iv) Strong emphasis on evidence-based onsite examinations at the BdE that are detailed and intrusive, and thorough and detailed offsite oversight process at the CNMV, especially considering the resources situation;

(v) Emphasis on security testing;

(vi) Proactive approach to changes in the regulatory framework, for example to ensure future DORA compliance; and

(vii) Effective internal coordination and cooperation at both the BdE and the CNMV.

98. Key challenges are identified as follows:

(viii) There is no onsite supervisory process either at the CNMV's or the BdE's department responsible for FMI oversight, which results in comparatively weaker assurance over compliance at FMIs;

(ix) With the current approach at the BdE there are few onsite examinations, and it is difficult to increase the coverage;

(x) Neither the BdE nor the CNMV are involved in national critical infrastructure related matters, even though both are in a very good position to address the complexities of

continuity of critical services in the financial sector, especially from the business process and systemic interdependencies points of view.[25]

(xi) TIBER-ES is not well suited to the majority of LSIs, but there is a need for a testing framework along its principles for this segment as well; and

(xii) The cost/benefit ratio of the institution specific threat intelligence reports in TIBER-ES is unfavorable.

I. Recommendations

99. Recommendations to address the challenges set out above are:

(i) Both the BdE and the CNMV should start planning and executing onsite examinations as part of FMI supervision. The BdE's existing cyber risk expertise in bank supervision could be leveraged in the beginning as such expertise is highly transferable.[26] At the CNMV, external support clearly limited to executing technical tasks should be considered as an interim measure. It may be necessary to revise the regulatory framework to explicitly grant onsite examination powers in this respect.

(ii) The BdE should do more, and more focused, thematic reviews while maintaining the validation based on the short onsite visits to a sample of the reviewed population. This will result in a better balance with the few but deep onsite examinations. More focus, both horizontally (i.e., not all LSIs need to be included) and vertically (i.e., limit a review to a topical issue) can help managing the workload.[27]

(iii) Both the BdE and the CNMV should be involved in critical infrastructure related matters, such as designation and compliance assessments. The involvement can range from information sharing and consultative roles that can be done within the existing legal framework to fulfilling formally delegated roles that may require changes in the legal framework.

(iv) Consider using sector-specific threat intelligence to be tailored to specific institutions in each test in TIBER-ES to reduce costs, while maintaining compatibility with TIBER.

[25] Key reasons why this is the case are that both authorities have a thorough understanding of the industries they supervise, including interconnectedness, cascading effects and the potential systemic impact of disruptions.

[26] It is acknowledged that at current utilization and staffing levels this is going to be difficult.

[27] This should be taken into consideration when assessing the need for additional resources on a forward-looking basis, as recommended in Paragraph 31.

(v) The BdE, in cooperation with the CNMV and the DGSFP, should develop a lighter threat intelligence-based red teaming framework based on TIBER-ES principles, considering the generally lower complexity, maturity and cost-bearing ability of a typical LSI.