INTERNATIONAL MONETARY FUND

IMF Country Report No. 25/213

EURO AREA

PUBLICATION OF FINANCIAL SECTOR ASSESSMENT PROGRAM DOCUMENTATION—TECHNICAL NOTE ON CYBER RISK AND FINANCIAL STABILITY—SELECTED ISSUES IN REGULATION AND SUPERVISION

July 2025

This paper on Cyber Risk and Financial Stability was prepared by a staff team of the International Monetary Fund. It is based on the information available at the time it was completed on July 2, 2025.

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

EURO AREA

FINANCIAL SECTOR ASSESSMENT PROGRAM

July 2, 2025

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 the euro area held during February 2025. 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
BIS	Bank for International Settlements
CCP	Central Counterparty
CERT	Computer Emergency Response Team
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CPMI	Committee on Payments and Market Infrastructures
CROE	Cyber Resilience Oversight Expectations (of the ECB)
CSD	Central Securities Depository
CSDR	Central Securities Depositories Regulation
CTPP	Critical Third-Party Provider
DORA	Digital Operational Resilience Act
EBA	European Banking Authority
ECB	European Central Bank
ESRB	European Systemic Risk Board
ESCG	European Systemic Cyber Group
ESMA	European Securities and Markets Authority
EIPOA	European Insurance and Occupational Pensions Authority
EU	European Union
EU-SCICF	EU Systemic Cyber Incident Coordination Framework
FI	Financial Institution
FMI	Financial Market Infrastructure
FSB	Financial Stability Board
ICT	Information and Communication Technology
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
ISO	International Organization for Standardization
ICT	Information and Communication Technology
JET	Joint Examination Team
JST	Joint Supervisory Team
NCA	National Competent Authority
NIS	Network and Information systems Security Directive
PFMI	Principles for Financial Market Infrastructures
TIBER	Threat intelligence-based Ethical Red Teaming
SI	Significant Banking Institution
SREP	Supervisory Review and Evaluation Process
SSM	Single Supervisory Mechanism

EXECUTIVE SUMMARY

The FSAP reviewed the supervision and oversight of cyber risk and operational resilience of Significant Banking Institutions (SIs) in the Single Supervisory Mechanism (SSM) and the Financial Market Infrastructures (FMIs) operated by the Eurosystem.[1] From an institutional perspective, the review included the ECB's relevant organizational units in the ECB Banking Supervision, Directorate General Market Infrastructure and Payments (DG-MIP), and the European Supervisory Authorities' (ESA)[2] joint Directorate in charge for Digital Operational Resilience Act (DORA) oversight; jointly referred to as 'authorities'.

The reliance of the banking sector on, and the interconnectedness of, information and communication technology (ICT) systems make cyber risk one of the most significant operational risk categories, with potentially systemic implications. The FSAP discussed the evolution of cyber threats in recent years; the preparedness of SIs and FMIs and weaknesses with potentially systemic impact; results and lessons learnt so far from simulations including the 2024 cyber resilience stress test; and implications of DORA on supervised entities and ECB's supervision and oversight activities.

ICT/cyber risk has been increasing in recent years globally; however, the observed general risk level in the EA banking sector in 2024 remained relatively stable compared to 2023. [3] The top three risk categories with worsening trends were ICT security risk, ICT outsourcing risk, and ICT change risk. Underlying causes were identified as: (i) more frequent and impactful cybersecurity incidents, (ii) rising reliance on cloud services; and (iii) a growing number of critically important ICT projects. As a result, the supervisory attention going forward is focused on targeted reviews of cyber resilience and outsourcing arrangements, the implementation of supervisory expectations on cloud computing, and the oversight framework for critical third-party providers (CTPPs) set out in DORA.[4]

DORA, applicable since January 2025, is expected to improve the stability and reliability of the financial sector in the EU by strengthening cyber resilience but has a cost impact on both supervised entities and supervisory authorities. ICT and cyber security expectations previously set out in guidance issued by ESAs have been superseded and extended, and now are binding legal requirements across the EU, underpinned by regulatory technical standards, and implementing standards. In addition, CTPPs (yet to be designated) have been brought under an oversight framework to ensure that financial entities' reliance on external service providers does not

[1] Cyber risk is defined as the probability and impact of cyber incidents, whether caused by malicious intent or not. The SSM differentiates between ICT risk (non-malicious, such as technology breakdowns) and cyber risk (malicious, such as hacker attacks) but always addresses them together. The note adopts this SSM convention.

[2] The European Supervisory Authorities (ESAs) are the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA).

[3] Sources: IMF Global Financial Stability Report (April 2024) and ECB internal analysis (October 2024).

[4] There is a partial overlap between these areas, for example a cloud service provider could be a critical third party that is in an outsourcing arrangement with a bank.

compromise their operational resilience. While payment systems are not in the scope of DORA, FMI oversight expectations are fully aligned. ESAs and the ECB are hiring additional specialists to be able to discharge their responsibilities under DORA.

The legal basis and relevant regulation convey adequate powers for effective ICT/cyber risk supervision and oversight of SIs and FMIs. There are sufficiently broad powers regarding collection of information on any relevant matter, to assess compliance, impose corrective actions, sanction, and take enforcement action as a last resort to ensure compliance.

However, the ESAs' power to impose corrective actions on CTPPs is limited under the DORA oversight framework. Periodic penalties can be levied for not providing relevant information requested in the oversight process, but there is no such possibility for non-compliance with requirements, because the ESAs can only make recommendations, which are not legally enforceable. This may become problematic in the future if the effectiveness of softer tools such as moral suasion and indirect influence through financial entities is weakened for any reason.

The reviewed ICT/cyber risk supervisory and oversight practices of the authorities with regard to SIs and FMIs in scope are materially in line with applicable regulations and guidance. Key strengths in SI supervision include: (i) effective risk-based approach and application of proportionality in supervision; (ii) detailed and well validated horizontal reviews that complement well the vertical supervisory activities; (iii) intrusive on-site examinations that provide strong assurance, on top of the off-site work. On FMI oversight, key strengths include (i) comprehensive assessments against the Cyber Resilience Oversight Expectations (CROE); and (ii) thorough follow-up of actions plans to address recommendations. Both SI supervision and FMI oversight exhibit strengths in security testing oversight and effective - albeit complicated - internal and external coordination and cooperation.

Coping with the changes brought by DORA is the most prominent operational challenge that the authorities are confronted with. Key areas where there is a need for significantly more resources as a consequence of DORA are the CTPP oversight framework and more broadly third-party risk management, including outsourcing to the cloud; threat-led penetration testing (TLPT); and incident reporting. While the need has been recognized and additional headcount approved across all authorities for DORA CTPP oversight, hiring has just started and the job market for such highly specialized cyber risk expertise is tight. This makes it difficult to fill all open positions necessary to meet challenging deadlines, such as the designation of CTPPs by late 2025 and operationalization of the oversight framework by early 2026.

The new ICT-related incident reporting regime under DORA is served by a largely decentralized infrastructure, the efficiency of which could be significantly improved. In this model, the reports are sent to the ECB Banking Supervision via the National Competent Authorities (NCAs). Each NCA operates their own reporting infrastructure and analytical tools, which is very inefficient and costly compared to a centralized model in which there is one central infrastructure,

and only one set of analytical tools is needed. [5] In addition, there is a parallel incident reporting by FMIs, and by PSPs for payment services-related incidents. Requirements largely overlap with DORA, hence a centralized EU-wide incident reporting for the entire financial sector, including FMIs and PSPs, would lead to even more efficiencies.

A number of weaknesses have a negative impact on cyber risk supervision and oversight. The most important are: (i) there is no on-site supervision of FMIs, which results in comparatively weaker risk assurance; (ii) cyber risk expertise in FMI oversight is scarce; (iii) the development of the EU systemic cyber incident coordination framework (EU-SCICF) is not finalized; EU-SCICF (iv) findings in SI supervision are piling up and create bottlenecks in follow-up work; and (v) some aspects of documentation of supervisory work are not standardized, leading to different practices across on-site examination teams.

[5] In January 2025 the ESAs issued a joint report assessing the feasibility of the establishment of a single EU Hub for ICT-related incident reporting, which also discusses the advantages.

Table 1. Euro Area: Main Recommendations			
Recommendation	**Timing[1]**	**Ref.**	**Authority**
Institutional and regulatory framework			
1. Amend the regulatory framework so that it is possible to levy fines on CTPPs for non-compliance with requirements.	MT	39 (i)	EC
2. Increase cyber risk expert capacity in FMI oversight.	ST	39 (ii)	ECB
3. Finalize the development of the EU-SCICF, commence testing, and operationalize as soon as possible	ST	39 (iii)	ESAs and EC
4. Implement an EU-wide centralized cyber incident reporting technical infrastructure.	MT	39 (iv)	EC
5. Make available anonymized granular cyber risk data to the ESRB so that more accurate systemic cyber risk estimates can be made.	ST	39 (v)	ECB and EC
Supervisory and oversight practices			
6. Carry out on-site examinations regularly as part of FMI oversight	ST	85 (i)	ECB
7. Leverage institutions' internal audit or external audit to reduce the workload of following up the increasing number of supervisory measures.	ST	85 (ii)	ECB
8. Use a systemic risk impact scenario in the next cyber stress test for banks, for example unavailability of a cloud service provider.	ST	85 (iii)	ECB
9. Strengthen internal standards on the documentation of bank supervision activities, for example using common templates across all on-site examination teams for all work products, and a unified filing and archiving approach in the supporting applications.	ST	85 (iv)	ECB

[1] Immediate (within 1 year); ST Short term (within 1-2 years); MT Medium Term (within 3–5 years)

INTRODUCTION[6]

A. Context

1. Over the last few years, with increased digitalization and rapid adoption of new technologies, cyber risks are becoming increasingly evident, particularly within the financial sector. Several relevant metrics that characterize the evolution of the cyber threat landscape point to continued elevated risk for the financial sector in the short to medium term, for example: (i) the number of cyberattacks has almost doubled since before the COVID-19 pandemic; (ii) nearly one-fifth of all incidents affect financial firms, with banks being the most frequent targets; and (iii) geopolitical tensions are a contributing factor, considering the surge of cyberattacks after Russia's invasion of Ukraine in February 2022.[7]

2. However, the observed general risk level in the EA banking sector in 2024 remained relatively stable compared to 2023. [8] The top three risk categories with worsening trends were ICT security risk, ICT outsourcing risk, and ICT change risk. Underlying causes were identified as: (i) more frequent and impactful cybersecurity incidents, (ii) rising reliance on cloud services; and (iii) a growing number of critically important ICT projects.

3. Technology failures continue to be the leading source of outages in banking and FMI services, according to incident reports received by the ECB. The primary drivers are control deficiencies in system implementation projects and changes to existing systems, but hardware failures still play a role.[9]

4. Third party providers are increasingly a potential source of a 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. Technological diversity between institutions is decreasing. Financial institutions are adopting common software solutions, acquiring similar hardware, and are migrating critical services to a small set of global cloud service providers (CSPs). This way, cyber incidents in the supply chain are more easily propagated and their impact may be felt more widely.

5. ICT/cyber risk and operational resilience have been consistently a supervisory priority for the ECB in recent years. Going forward, according to the ECB Banking Supervision's medium-term strategy for 2025-27, the topic remains in focus through Priority 3, which is about

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

[7] See for example the April 2024 IMF Global Financial Stability Report

[8] Source: ECB internal analysis (October 2024).

[9] Surprisingly, the major outage of TARGET services on 27 February 2025 was attributed to a hardware failure, despite the built-in redundancies.

strengthening digitalization strategies and tackling emerging challenges stemming from the use of new technologies.

B. Assessment Scope

6. The note reviews the cyber risk regulatory framework and supervisory practices for the SI segment in the EA and the FMIs operated by the Eurosystem.[10] This includes the role and practices of the authorities in the development and maintenance of the cyber risk regulatory framework, on-site and off-site supervisory processes, and the cyber resilience framework to detect, respond and recover from cybersecurity incidents.

7. The FMIs in scope consisted of the TARGET Services. These include the real-time gross settlement (RTGS) system T2, the securities settlement platform T2S, the instant payments system TIPS, and the collateral management system ECMS.[11]

8. The mission collected information from several sources. These include questionnaire answers provided, interviews with the authorities and supervised institutions, the study of relevant regulation, 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) DORA regulation and corresponding Regulatory Technical Standards (RTS) and Implementing Technical Standards (ITS); (ii) Principles for Financial Market Infrastructures (PFMI); (iii) Cyber resilience oversight expectations for financial market infrastructures (CROE); (iv) CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures; (v) FSB Stock take of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices; (vi) BCBS Cyber-resilience: Range of practices; and (vii) IMF Departmental Paper on Cyber risk Supervision.

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.

[10] The Eurosystem consists of the ECB and the national central banks in the euro area.

[11] A separate working stream covered broader aspects of TARGET Services Oversight.

INSTITUTIONAL AND REGULATORY FRAMEWORK

A. Legal Basis

11. DORA is fundamental for regulating and supervising cyber risk in the financial sector and also defines the institutional framework. Directive 2022/2555 on Measures for a High Common Level of Cybersecurity Across the Union (NIS2) and the Critical Entities Resilience Directive (CER) are partially overlapping, however DORA is "lex specialis" for financial entities, so its requirements take precedence. The ECB is the competent authority for the supervision of SIs. The ESAs (EBA, ESMA and EIOPA) are designated as lead overseers in CTPP oversight. The EBA develops cybersecurity standards for financial entities under its remit, including banks and payment institutions, EIOPA for insurance undertakings and institutions for occupational retirement provision, while the ESMA sets guidelines for a diversity of financial entities in its remit including central counterparties (CCPs), central securities depositories (CSDs), and trading platforms. Additionally, the Eurosystem oversees the payment systems of the EA.

B. Other Relevant Regulation and Supervisory and Oversight Expectations

12. The EBA Guidelines on ICT and security risk management (EBA/GL/2019/04) was largely superseded by DORA, thus it was updated to avoid duplications. The updated version has a narrower scope and will be applicable later in 2025. Other relevant EBA guidelines not directly related to ICT/cyber risk remain applicable, for example the EBA Guidelines on internal governance (EBA/GL/2021/05), or the EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP), and supervisory stress testing (EBA/GL/2022/03), and the EBA Guidelines on ICT Risk Assessment under the SREP (EBA/GL/2017/05).

13. The ECB issues guides on specific topics, including ICT/cyber risk, to clarify expectations based on higher level regulation. For example, a guide on outsourcing to cloud service providers has been drafted based on DORA's requirements on third party risk management.

14. The oversight of FMIs in scope is based on the ECB Regulation on oversight requirements for systemically important payment systems regulation (SIPSR) and follows the Eurosystem Cyber Resilience Strategy. The strategy, issued in 2017 and revised in 2024, is part of the Eurosystem Oversight Framework and is aligned with 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.

15. Two specific tools embody the oversight expectations of the ECB/Eurosystem 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 risk survey to support the aforementioned assessment.

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

C. Organization and Resourcing of Cyber Risk Supervision and Oversight

17. At the ECB, ICT and cyber risk supervisory expertise is organized along both vertical and horizontal criteria. Related functions are in Non-Financial Risk Inspections of the Directorate General On-Site & Internal Model Inspections, and in Non-Financial Risk Experts of Directorate General Horizontal Line Supervision. Joint Supervisory Teams (JSTs) are responsible for continuous off-site supervision of individual banks. Larger JSTs include ICT/cyber risk specialists, while smaller JSTs rely on generalist supervisors who have acquired skills in this field. Their work is supported and complemented by the horizontal function and on-site inspection teams. JSTs are comprised of both ECB and NCA staff. The Directorate Supervisory Strategy and Risk serves as the risk management function (second line of defense) of the SSM and as part of its yearly SREP benchmarking exercise, it also covers the consistency and effectiveness of SREP cyber risk supervision. In addition, there is an IT Risk Network at the SSM that includes subject matter experts from both NCAs and ECB, and an ICT Risk Hub is being formed to act as a competence center for the JSTs.

18. The headcount of ICT and cyber risk supervisory positions is comparatively strong but runs at capacity, while workload will increase in the near future. This was anticipated, based on the organizational readiness assessment, and additional permanent headcounts have been approved, and a hiring campaign is under way. However, with a tight job market for cybersecurity skills, and the EASs hiring the same skills in parallel, difficulties are to be expected in filling all open positions with suitably qualified staff. Internal upskilling and letting new hires at the ESAs to participate in the ECB curriculum for ICT/cyber risk specialists are some of the ways considered to address the issue, which nevertheless remains an ongoing challenge.

19. FMI ICT/cyber risk oversight is scarcely staffed for the ECB's lead overseer role for TARGET services, which are vital for the EA financial system. There are 3 regular staff, which is insufficient to conduct regular deep dives or on-site inspections of specific ICT/cyber risk areas, such as business continuity and disaster recovery, that would result in stronger assurance over the proper functioning of risk controls. (Also see paragraph 44. 44.

20. ICT/cyber risk supervision and oversight are fully integrated in the broader bank supervision, with formalized, mature, and well documented processes according to established internal policies. Responsibilities, organizational structures and reporting lines are clearly defined and adhered to. There is adequate planning, review, and quality assurance of supervisory activities.

21. DORA brought about much needed simplification and harmonization of incident reporting for supervised entities, however opportunities for significant efficiency gains remain. In the current model, the reports are sent to the ESAs via the NCAs, which operate their own reporting infrastructure and analytical tools. This is very inefficient and costly compared to a centralized model in which there is one central infrastructure, and only one set of analytical tools is needed. [12]

22. The European Systemic Risk Board's (ESRB) work on cyber risk is hindered by limited access to granular data. The ESRB's mandate includes the monitoring and assessing of systemic risk – including systemic cyber risk – in the EU financial system. Granular data, such as about actual cyber incidents and losses incurred are essential to estimating cyber risk more accurately. The ESRB has no access to granular data on specific institutions, e.g. from incident reporting. With appropriate privacy technologies anonymized granular data could be provided in a way that satisfies legal requirements and would allow researching, building, and testing more accurate cyber risk models.[13]

23. An EU-wide systemic cyber incident coordination framework (EU-SCICF) is gradually being implemented. The ESRB recommended the establishment of the EU-SCICF in 2021, to be set up in the context of DORA which entered into application in 2025 and required the ESAs to deliver a report on the design of such a framework by July 2024. This framework for the ESAs, the ECB, the ESRB and relevant national authorities is to support an effective EU-level coordinated response in case of systemic ICT/Cyber incidents occurring. It is envisaged to operate in two distinct modes, crisis and non-crisis. The elements regarding the non-crisis mode are largely in place but some crisis mode related elements are still work in progress. As indicated in the ESRB Recommendation, the full implementation is subject to action, either of legislative nature or other supporting initiatives that the European Commission may take.

D. Conclusions

24. The legal basis and relevant regulation convey adequate powers for effective ICT/cyber risk supervision and oversight of SIs and FMIs. There are sufficiently broad powers regarding collection of information on any relevant matter, to assess compliance, impose corrective actions, sanction, and take enforcement action as a last resort to ensure compliance.

25. However, the power to impose corrective actions on CTPPs is limited under DORA. Periodic penalties can be levied for not providing relevant information requested in the oversight process, but there is no such possibility for non-compliance with requirements because the ESAs can only make recommendations, which are not legally enforceable. The effectiveness of the oversight

[12] In January 2025 the ESAs issued a joint report assessing the feasibility of the establishment of a single EU Hub for ICT-related incident reporting, in which they deemed the centralized model feasible.

[13] Dearth of good quality risk data is a global problem and one of the key reasons why quantitative risk models are not widespread in cyber risk management. However, with the new comprehensive incident reporting regime in the EU this is bound to improve over time, perhaps uniquely compared to other regions, and it would be a beneficial to capitalize on it in systemic risk assessments.

arrangement depends crucially on CTPPs continued willingness to cooperate. Lack of cooperation by CTPPs, particularly in a crisis, would leave the ESAs with limited legal means to react and could pose significant reputational risks to the euro area and the ESAs. As a measure of last resort, institutions may be required to suspend the use of the infringing service provided by the CTPP, which could be very difficult or outright impossible to do, for example in the case of outsourcing of critical functions to the cloud.[14]

26. Availability of ICT/cyber risk related supervisory and oversight skills is an issue that affects all authorities. It is uncertain at this stage whether the approved additional headcounts will be possible to fill with adequately skilled staff. Additionally, staff numbers are insufficient in FMI cyber risk oversight, and this may become an issue at the ESAs as well when the scale of CTPP related work becomes more evident in 2026.

27. There are inefficiencies in cyber risk management at the systemic level. There would be reduced costs with an EU-wide centralized incident reporting framework and more accurate systemic cyber risk estimates would be possible if the ESRB had access to anonymized granular risk data.

E. Recommendations

28. The authorities are advised to:

(i) Amend the regulatory framework so that it is possible to levy fines on CTPPs for non-compliance with requirements;

(ii) Increase cyber risk expert capacity in FMI cyber risk oversight;

(iii) Finalize the development of the EU-SCICF, commence testing, and operationalize as soon as possible;

(iv) Implement an EU-wide centralized cyber incident reporting technical infrastructure; and

(v) Make available anonymized granular cyber risk data to the ESRB so that more accurate systemic cyber risk estimates can be made. For example, Privacy Enhancing Technologies (PETs) could be used for this purpose.

[14] Cessation of critically important technology services may bankrupt an institution in short order even if it is solvent and well capitalized. See for example https://www.gtreview.com/news/europe/solvent-but-bankrupt-how-sanctions-felled-amsterdam-trade-bank/

SUPERVISORY AND OVERSIGHT PRACTICES

A. Bank Supervision

29. The key elements of the ECB's supervisory approach are off-site (ongoing) supervision also including targeted reviews and sector-wide risk analyses, on-site inspections, and Threat-led Penetration Testing (TLPT) oversight. Off-site supervision of banks is done via the JSTs, which carry out day-to-day activities and are institution-specific; and the horizontal supervisory function, which is responsible for specialist JST support, analyses, benchmarking, targeted reviews, and supervisory policy. On-site inspections are executed by specialist teams that are not tied to any institution.

30. The ICT/cyber risk tolerance of the ECB Bank Supervision is low. This means either that banks' relevant risk controls should be without major weaknesses or if such weaknesses are found, then they must be resolved within a realistic timeframe.

31. Proportionality and a risk-based approach are applied in ICT/cyber risk supervision. The intensity of supervisory attention, and – accordingly – the resource allocation is set to be proportional with the size and complexity of the bank, its ICT operations, and risk profile. In addition, risk areas of concern are scrutinized to a much higher degree, for example with deep dives and on-site inspections.

32. JSTs are the main vehicles and focal points for bank-specific supervisory activities. JSTs assess ICT/cyber risks and operational resilience of their banks on a regular basis based on a formal methodology, which is a section of the Supervisory Evaluation and Review Process (SREP) dedicated to operational risk.[15] The most important inputs to the risk assessment are: (i) continuous collection of ICT/cyber risk relevant information from different sources, such as documentation from banks, public sources, or answers to questionnaires like the IT Risk Questionnaire (ITRQ)[16]; (ii) challenging banks on risk areas that are deemed concerning; (iii) meeting regularly with bank management responsible for ICT/cyber risk management in all three lines of defense; (iv) results of targeted reviews and benchmarks provided by the horizontal function; (v) results of on-site inspections; and (vi) results of TLPTs and CTPP oversight (planned at this stage, because these activities have not been started just yet as relevant DORA requirements are only applicable since January 2025).

33. On-site inspections are demand driven. Inspection teams carry out detailed risk and control assessments with agreed upon scope and predefined intensity, based on requests from the

[15] The SREP section has been updated recently to incorporate operational resilience, integrate DORA requirements, and raise the profile of ICT/cyber risk within operational risk. Notable in this approach is that the operational resilience rating does not impact capital requirement.

[16] The ITRQ is publicly available at https://www.bankingsupervision.europa.eu/activities/srep/2023/html/ssm.srep_ITRQ2023.en.pdf

JSTs that identify areas of concern, often in cooperation with the horizontal function. A process is in place to balance demand and availability, which sharpens the risk-based approach.

34. On-site inspections are based on a comprehensive methodology and are intrusive by design. An inspection typically spans 6 to 10 weeks and involves several specialists, who focus on gathering evidence and testing control effectiveness. The methodology used is ECB's own development, largely aligned with widely used ICT/cyber risk and control frameworks. [17] It contains detailed reference information on inspection objectives, potential risks, expected controls, and inspection techniques. At the highest intensity, on-site inspections execute detailed audits of certain areas, sometimes going beyond sample-based control testing to full population testing using analytical tools. Inspection procedures are thoroughly planned and documented using a number of support systems. Just as the JSTs, on-site examination teams are formed with staff from the ECB and NCAs as well.

35. A pooled internal ICT/cyber risk support unit (colloquially the "IT Hub") is being formed to improve the JSTs access to specialist resources. An important responsibility of the hub will be to follow up on findings. Smaller JSTs will benefit most, as they often lack ICT/cyber risk specialists. In addition, capacity will be freed in the horizontal function to focus more on core activities.

36. The horizontal function's targeted reviews and sector-wide analyses of ICT/cyber risk are based on multiple sources and is usually performed by joint teams. Targeted reviews are typically designed to cover a representative sample of banks and address a topical issue, for example outsourcing or cyber resilience. Depending on the issue at hand, any or all of the following sources could be used: ITRQ or more focused questionnaires, ICT-related incident reports, on-site inspection findings, cyber resilience stress tests, and governance data collection. A key deliverable of the horizontal function is the annual sector-wide ICT/Cyber risk analysis that informs, among others, the strategic supervisory planning process. The teams involved in horizontal work may be sourced from both ECB and NCA experts in horizontal or vertical functions, JSTs, or on-site inspectors, depending on the topic and availability.

37. All supervisory findings are graded and tracked consistently, irrespective of origin. An empirical 4-level severity grading system is used. Banks are required to develop and submit action plans to remedy findings. Such plans are followed up until resolution by the JSTs. If a critical issue is found, immediate action is required from the bank in question.

38. Repeated high-risk findings draw special attention from supervisors. These may be escalated by including them in a Supervisory Board decision, which makes them legally binding and forms the legal basis for enforcement, if necessary. The ECB may impose various measures and sanctions to mitigate the risk.

[17] The methodology is currently being updated to align it with DORA.

39. Outputs of the supervisory process, most importantly the findings are subject to internal quality assurance, several levels of approvals, and periodic reviews by the risk management function (2nd line of defense) to ensure accuracy and consistency. This is especially important as supervisory teams are diverse and members from different NCAs bring in different practices.

40. Supervisory work is thoroughly documented, however not always to the same consistent standard. For example, differences exist between onsite examination teams but generally a supervisor not familiar with a bank and previous supervisory activities can understand the process, the decisions taken in directing the work, and the rationale for the findings and recommendations by consulting existing documentation. Project management documentation (plans, meeting schedules, team composition, approvals, etc.), client communication, workpapers, evidence, and reports are stored in support systems. There is an audit trail available for important processes and key documents.

41. In recent times findings started to pile up, creating bottlenecks as more resources are needed for follow-up. As ICT/cyber risk has become a priority in recent years, more effort is spent on both horizontal and vertical supervision, resulting in more findings. In addition, targeted reviews can generate a large number of findings in a relatively short timeframe. Many findings result in several tasks for banks that can take a long time to finish. These factors contribute to the increasing number of open findings. [18]

B. FMI Oversight

42. FMI oversight is focused on compliance assessments against the CROE and assessing cyber resilience through surveys. Both the CROE oversight assessment, and the cyber resilience survey (CRS) are validated self-assessments and are regarded as complementary. Assertions made by the FMIs must be supported with documentation, which are reviewed, and any discrepancies followed up with the entities. The CROE assessment was done only once so far for TARGET services, and the CRS is done every two years.

43. No on-site activity was performed yet for TARGET services under the oversight approach.[19] The international standards are agnostic on the topic, i.e., there is no explicit requirement for on-site inspections.[20] However, the ECB has issued a Decision detailing the powers of competent authorities for SIPS, which sets out on-site inspections as an option.

[18] There is no observed tendency at banks to unnecessarily delay resolution, so this is not a significant contributing factor. JSTs are implementing a lighter (and faster) approach to assess less critical findings, allocating more resources to the most critical and urgent measures to be remediated by supervised banks. This tradeoff is expected to keep the number of open findings under control and manageable.

[19] The first deep dive on ICT/cyber risk, which involves on-site presence as well, is planned for later in 2025.

[20] 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

44. As a result, the assurance that is obtained on the adequacy of risk controls is relatively weak considering the vital nature of the FMIs overseen. Compounding the issue, the function is scarcely staffed with ICT/cyber risk experts, as discussed earlier under resourcing of supervision and oversight.

45. Security testing under the TIBER-EU framework partially compensates this weakness by providing an in-depth assessment of the tested entities' capacity to protect against, detect, respond and recover from cyber attacks. The single test so far of TARGET services was executed at a high-quality level by the service provider. It employed realistic attack scenarios based on institution-specific threat intelligence and resulted in a number of detailed findings that contributed to the further strengthening of already robust cyber defense mechanisms. However, TIBER-EU is not the right tool to uncover potential weaknesses in business continuity or disaster recovery, disciplines of utmost importance in minimizing service disruptions due non-malicious ICT risks materializing. (Also see paragraph 52.

46. While DORA is not applicable for payment systems, FMI oversight aims to maintain alignment with key DORA requirements. This is most evident in the ongoing reviews of the CROE and the TIBER-EU security testing framework.[21]

47. Similar to bank supervision, FMI oversight of cyber risk is well formalized and documented.

C. Critical Third-Party Provider (CTPP) Oversight

48. The ESAs (EBA, ESMA and EIOPA) are tasked with CTPP oversight, among other DORA related non-oversight responsibilities. The CTPP oversight process is currently being implemented, with a planned start of day-to-day activities in early 2026. The planned approach is a mix of on-site and off-site work, similar to the SSM. Organizational structures are already in place, and methodologies and supporting tools under development. It is envisaged that the methodology will use a maturity model with three levels, similar to the CROE.

49. The ESAs formed a joint Directorate for CTPP oversight, a director and key staff were assigned, and are currently hiring specialists. Oversight will be done by Joint Examination Teams (JETs) to which NCAs will contribute staff on a voluntary basis. Specialists in the directorate are also expected to contribute to non-oversight activities, such as incident reporting and supervisory convergence. It is expected that the Directorate will be fully staffed and functional by early 2026, however, it remains to be seen whether staffing levels will be sufficient, depending on the number of CTPPs (yet to be designated) and the planned intensity of activities. In this respect, much depends

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. (Continued)

[21] The TLPT requirements in DORA draw significantly from TIBER-EU.

on the ability and willingness of NCAs to complement the JETs. The ECB is expected to contribute as well.

50. The schedule for CTPP designation is very tight, and so there is a risk the deadline set in Q4 2025 for the final CTPP list might be missed. The joint Directorate has a very short time period at its disposal to process and analyze a large number of registries of third parties, to conduct consulting, and to finalize the list. The experience of registering information on outsourcing arrangements is not the same in the three financial industries and data quality may be uneven, leading to unpredictable delays. In addition, the consulting process with potential CTPPs may delay finalization as well if cooperation is not smooth.

D. Testing and Crisis Exercises

51. DORA requires Threat-led Penetration Tests (TLPTs) to be performed regularly on SIs, among others. Certain financial entities are by default in scope of the TLPT in particular based on objective quantitative indicators, however, TLPT authorities can opt-in or opt-out certain entities, based on predefined criteria related to, for example, ICT maturity, financial stability concerns, and impact of the financial entity on the financial sector. The ECB estimates that slightly over 100 tests need to be executed every three years at SIs, with the exact number to be determined in the near future. (No TLPTs have been executed just yet.) The ECB is involved in the identification of which banks are required to perform TLPT, the validation the testing scope of each TLPT, the attestation of TLPTs and the follow-up of findings and recommendations resulting from TLPTs. Capacity to deal with this additional workload is being ramped up, with the expectation that NCAs will contribute significantly.

52. Payment systems are not required to undergo TLPTs as are not in DORA's scope, however, systemically important payment systems such as TARGET services are tested under the earlier TIBER-EU framework. The overseers are involved in the validation of the testing scope of the respective tests, the follow-up of findings and recommendations, and regularly assess the improvements.

53. In terms of testing process, the TIBER-EU framework is aligned with the DORA TLPT requirements. TIBER-EU is expected to remain fully compatible with the DORA TLPT regime. DORA TLPT requirements also extend to selection of financial entities subject to TLPTs, use of internal testers and cooperation between authorities where TLPTs concern several member states.

54. The ECB, with support from the NCAs, conducted a system wide cyber resilience stress test in 2024 involving all 109 institutions under its direct supervision. [22] The scenario focused on the response to, and recovery from, a severe but plausible cybersecurity incident affecting the

[22] Unlike financial stress tests, this cyber resilience stress test did not involve impact assessments on capital and liquidity. Cyber resilience scenario testing might be a better suited term.

databases of each bank's core systems.[23] 28 banks underwent enhanced testing and were required to execute actual recovery tests and submit evidence on completion, while the rest executed tabletop testing. Results were collected using a questionnaire and were validated based on supporting documentation. In addition, the quality assurance over the stress test included on-site visits at all 28 banks that underwent enhanced testing. The results indicate that response and recovery from severe cyber incidents could be improved at many institutions.

55. In 2023 and 2024, the ECB together with the NCAs, organized Cyber Dry Run exercises as part of the SSM operational resilience testing. They aimed to test the SSM's preparedness for large-scale cyber incidents. The exercises focused on detection, escalation, robust information dissemination, and coordination capabilities during a systemic crisis, when the ECB's and the NCAs own ICT systems are affected. The exercise was an internal table-top exercise conducted exclusively within the SSM and ECB frameworks, without involvement from external authorities or supervised entities, and focusing on communication and coordination aspects rather than technical specifics.

56. In 2024 the ECB also participated in a cross-border cyber crisis coordination exercise in the financial sector conducted by the G7 Cyber Expert Group. The exercise aimed at improving communication and coordination among G7 financial authorities in case of a major cross-border cyber incident in the financial sector. The scenario was about a large-scale cyber attack against FMIs and other institutions in the G7. Besides the financial authorities, private sector institutions took part in the exercise.

57. FMI-related cyber crisis exercises are conducted regularly. Such exercises were done both in 2023 and 2024 via the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB), involving FMIs, their critical service providers, representatives of central banks, and other authorities that participate in the ECRB. An ECRB working group develops a playbook of scenarios and a multi-year testing program.

58. Even though technology breakdowns are still the leading cause of service disruptions in the financial sector, these are not considered in crisis exercises facilitated or run by the authorities. While at the institutional level there is a long-established practice of disaster recovery testing, as cases like the CrowdStrike incident affecting millions of computers world-wide and the recent major TARGET outage show, systemic impact is real a possibility from such incidents. So, system-wide tests using such scenarios may be justified.

[23] Note that this is an idiosyncratic risk scenario that tests response and recovery at the individual institutions' level, without considering system-wide effects.

E. Incident Reporting

59. DORA has consolidated and significantly changed the incident reporting regime in the financial sector. [24] Key changes entered into effect in January 2025 include the incident classification criteria and process, the way how incidents are reported, the information required, and the deadlines. Financial entities are required to report major ICT-related incidents and cyber security threats (on a voluntary basis) to NCAs within 4 hours, in accordance with clear criteria on how to classify incidents as major. ESAs then in turn route the reports according to predefined rules to the ESAs. The ESAs then disseminate them, as needed, to the other relevant authorities, in consultation with ENISA and in cooperation with the originating NCAs. Authorities only receive incident reports from institutions under their remit. Comprehensive information must be included in the reports, for example, duration of outage, severity/impact, systems affected, services affected, number of records exposed, threat vector, vulnerabilities exploited, financial loss, and root cause analysis.

60. Payment systems under Eurosystem oversight report incidents according to requirements aligned with DORA to their lead overseer. For example, TARGET services report to the ECB under the Eurosystem major incident reporting framework.

61. The authorities have documented follow up procedures in place. Typically, these entail monitoring, coordination, information sharing, risk analysis and other steps to mitigate the risk (e.g., further scrutiny and developing findings and recommendations). In addition, internal dashboards and trend analyses are prepared based on the reports received. Summaries and key observations may be published as well.

62. With major ICT operational incidents becoming reportable in all EA jurisdictions, the authorities expect a very significant increase in the number of reports.

63. At the ECB incident reports are received automatically and continuously but there is no staff on continuous duty for monitoring and follow up. However, alerts are sent to key staff outside office hours as well.

F. Coordination and Cooperation

64. Owing to the inherent complexities of the SSM, there is a significant effort spent on internal and external coordination and cooperation. At the SSM level, the IT Risk Network (ITRN) composed of subject matter experts from both NCAs and the ECB, works on IT Risk and cybersecurity topics on a regular basis. The ITRN is a collaborative forum co-chaired by the ECB and one NCA, not a decision-making body. Its objectives include the facilitation of the joint teams formed by the ECB and the NCAs (for example for the purpose of doing horizontal projects), foster information sharing, and endorse proposals to the supervisory board. FMI overseers are non-

[24] As discussed in more detail under the Regulatory and Institutional Framework chapter, the new cyber incident reporting regime is served by a largely decentralized infrastructure the efficiency of which could be significantly improved.

permanent members of the ITRN. Internal to the ECB, a Cyber Security Steering Committee (CSSC) has been established to facilitate sharing of cyber security related information among different business areas.

65. Additionally, the ECB and the ESAs participate in the European Systemic Cyber Group (ESCG) of the ESRB where systemic aspects of cyber incidents are discussed. The ECB supported the establishment of the ECRB Cyber Information and Intelligence Sharing Initiative (CIISI-EU). This brings together a community of public (including central banks in their capacity as FMI operators) and private entities with the aim of sharing intelligence and exchanging best practices. Also under the ECRB, the ECB led the work on establishing the ECRB's Crisis Coordination Network (CC-Network). The CC-Network represents a setup of designated points of contacts across the ECRB members that is activated in case of major incidents or crisis. The CC-Network is composed of a chairperson with an alternate, and appointed members with respective alternates and it reports to the ECRB. The operation of the CC-Network is set out in the CC-Protocol document of the ECRB.

66. The ECB cooperates and coordinates with other EU agencies through regular meetings, joint working groups, and collaborative frameworks. Examples include entities like the European Banking Authority (EBA) and the European Union Agency for Cybersecurity (ENISA).

67. The ECB and the ESAs represented by the EBA are members of the Cyber Experts Group (CEG) of the G-7. The CEG plans and executes activities related to cybersecurity information sharing and incident preparedness. The G7 cyber incident response protocol (CIRP) defines the communication channels to be used and the information to be shared in the G7 context in case of a significant cyber incident affecting the financial sector in G7 jurisdictions.

68. Therea are regular trilateral meetings with the Federal Reserve Board (US) and the Prudential Regulation Authority (UK). These constitute an exchange of information and views regarding cyber risk developments as well as regulatory trends.

69. In the area of FMIs and payments, cooperation on cyber risk and related standard-setting takes place under the auspices of CPMI and IOSCO. The ECB's DG-MIP is a regular participant.

G. Enforcement

70. The ECB's ability to take action to ensure compliance with cyber risk regulations is based on the corrective and sanctioning powers conveyed by the SSM Regulation. Specifically, for cyber risk related cases the following supervisory measures are deemed relevant, even if not all have been exercised yet: (i) public disclosure, (ii) operational restrictions, (iii) suspension of activities, and (iv) change of management. In addition, enforcement measures and sanctions can be used.[25] Supervisory measures, enforcement measures and sanctions are not mutually exclusive and can be

[25] In essence, these are different types of penalties.

used in parallel or sequentially, depending on the situation. In the last three years, the ECB imposed a pecuniary penalty on a supervised entity for breach of cyber risk regulation.

H. Conclusions

71. The reviewed ICT/cyber risk supervisory and oversight practices of the authorities with regard to SIs and FMIs in scope are materially in line with applicable regulations and guidance. Key strengths in SI supervision include: (i) effective risk-based approach and application of proportionality in supervision; (ii) detailed and well validated horizontal reviews that complement well the vertical supervisory activities; (iii) intrusive on-site examinations that provide strong assurance, on top of the off-site work. On FMI oversight, key strengths include the comprehensive assessments against the Cyber Resilience Oversight Expectations (CROE) and the thorough follow-up of actions plans to address recommendations. Both SI supervision and FMI oversight exhibit strengths in security testing oversight and effective albeit complicated internal and external coordination and cooperation.

72. Coping with the changes brought by DORA is the most prominent operational challenge that the authorities are confronted with. Key areas where there is a need for significantly more resources as a consequence of DORA are the CTPP oversight framework and more broadly third-party risk management oversight, including outsourcing to the cloud; threat-led penetration testing (TLPT); and incident reporting. While the need has been recognized and additional headcount approved across all authorities, hiring has just started and the job market for such highly specialized cyber risk expertise is tight. This makes it difficult to fill all open positions necessary to meet challenging deadlines, such as the designation of CTPPs by late 2025 and operationalization of the oversight framework by early 2026.

73. A number of weaknesses have a negative impact on cyber risk supervision and oversight. The most important are: (i) there is no on-site supervision of FMIs, which results in comparatively weaker risk assurance; (ii) cyber risk expertise in FMI oversight is scarce; (iii) the development of the EU systemic cyber incident coordination framework (EU-SCICF) is not finalized; (iv) findings in SI supervision are piling up and create bottlenecks in follow-up work; and (v) some aspects of documentation of supervisory work are not standardized, leading to different practices across onsite examination teams.

I. Recommendations

74. The authorities are advised to:

(i) Carry out on-site examinations regularly as part of FMI oversight;

(ii) Leverage institutions' internal audit or external audit to reduce the workload of following up the increasing number of supervisory measures;

(iii) Use a systemic risk impact scenario in the next cyber stress test for banks, for example unavailability of a cloud service provider; and

(iv) Strengthen internal standards on the documentation of bank supervision activities, for example using common templates across all on-site examination teams for all work products, and a unified filing and archiving approach in the supporting applications.