INTERNATIONAL MONETARY FUND

IMF Country Report No. 25/237

FRANCE

FINANCIAL SECTOR ASSESSMENT PROGRAM

August 2025

TECHNICAL NOTE ON CYBER RISK AND FINANCIAL STABILITY

This paper on France 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 31, 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
Price: $18.00 per printed copy

International Monetary Fund
Washington, D.C.

INTERNATIONAL MONETARY FUND

FRANCE

FINANCIAL SECTOR ASSESSMENT PROGRAM

July 31, 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 by Gabriella Biró (IMF external expert) in the context of the Financial Sector Assessment Program (FSAP) in France, led by Charles Cohen. 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

ACPR	Autorité de Contrôle Prudentiel et de Résolution (Prudential Supervision and Resolution Authority)
AIF	Alternative Investment Funds
AMF	Autorité des Marchés Financiers (Financial Markets Authority)
ANSSI	Agence nationale de la sécurité des systèmes d'information (the national cybersecurity agency)
BdF	Banque de France
CASP	Crypto-asset service providers
CCP	Central counterparty
CDC	Caisse des Dépôts et Consignations
CER	Critical Entities Resilience Directive, Directive (EU) 2022/2557
CERT	Computer Emergency Response Team
CPMI	Committee on Payment and Market Infrastructures
CROE	Cyber resilience oversight expectations for financial market infrastructures
CSD	Central Securities Depositories
CSDR	Central Securities Depositories Regulation
DASP	Digital Asset Service Provider
DORA	Digital Operational Resilience Act, Regulation (EU) 2022/2554
EBA	European Banking Authority
ECB	European Central Bank
EIOPA	European Insurance and Occupational Pensions Authority
EMIR	European Market Infrastructure Regulation
ENISA	European Union Agency for Cybersecurity
ESMA	European Securities and Markets Authority
EU	European Union
FIRE	Format for Incident Reporting Exchange
FMI	Financial Markets Infrastructure
FTE	Full time equivalent
FSB	Financial Stability Board
GDPR	General Data Protection Directive
ICT	Information and Communication Technology
IMF	International Monetary Fund
IOSCO	International Organization of Securities Commissions
FSAP	Financial Stability Assessment Program
LPM	French Military Programming Act of December 18, 2013
LSI	Less Significant Banking Institution
MICA	Markets in Crypto-Assets Regulation, Regulation (EU) 2023/1114
MoEF	French Ministry of the Economy, Finance and Industrial and Digital Sovereignty
NCA	National Competent Authority
NIS	Network Information Security Directive

NIS2	Network Information Security Directive 2, Directive (EU) 2022/2555
OVI	Operator of Vital Importance
PRG	Paris Resilience Group
SAIV	Public Policy for Securing Vital Importance Activities
SHFDS	Service du Haut Fonctionnaire de Défense et de Sécurité
SGDSN	Secrétariat général de la défense et de la sécurité nationale (General Secretariat for Defense and National Security)
SI	Significant Banking Institution
SIPSR	Regulation ECB/2014/28 on oversight requirements for systemically important payment systems
SPOT	Supervision of Operational and Thematic Practices
SREP	Supervisory Review and Evaluation Process
SSM	Single Supervisory Mechanism
TCT	TLPT/TIBER cyber team
TIBER	Threat Intelligence Based Ethical Red Teaming
TLPT	Threat-Led Penetration Test
UCITS	Undertakings for Collective Investment in Transferable Securities

EXECUTIVE SUMMARY

The scope of the assessment covered the cyber risk supervision and regulation of the financial sector in France. Thus, the financial supervisory authorities in scope were the Autorité de Contrôle Prudentiel et de Résolution (ACPR), and Autorité des Marchés Financiers (AMF) and the Banque de France (BdF). Supervision of Significant Banking Institutions (SIs) in France is within the remit of the European Central Bank's Single Supervisory Mechanism (ECB/SSM) and was therefore outside the scope of the France FSAP.

The overall complexity of the cyber risk supervision within the French financial sector is high, with four dedicated teams within the three financial authorities (ACPR, AMF, BdF), a financial regulator (Trésor) and the cybersecurity agency (ANSSI) in the picture. The institutional and regulatory framework is strong, but the supervisory practices are not fully standardized and there is a potential for improvement in some practical aspects of the cooperation and common tasks of the authorities.

The French authorities consider cyber risk one of the key topics that may escalate to a financial stability issue. BdF dedicated parts of its 2023 and 2024 financial stability reports to drawing attention to the relevance of cyber risk in evaluating the potential threats to financial stability. The number and sophistication of cyberattacks in the European Union have been constantly rising due to technological developments and the increase in geopolitical tension. According to the EU Agency for Cybersecurity (ENISA), the financial sector remains one of the most targeted sectors in all geographical regions, with 9 percent of all attacks in the European Union (EU) targeting banking and finance. France experienced one of its largest ever data breaches in 2024, when two of its healthcare payment providers were compromised, impacting the personal data of more than 33 million people.

Three of the most significant cyber risk related regulations in the EU entail far-reaching changes for the cybersecurity landscape. The Digital Operation Resilience Act (DORA) is in force since January 16, 2022, and applicable from January 17, 2025. Transposition of the Network Information Security Directive 2 (NIS2) and the Critical Entities Resilience Directive (CER) should have taken place by October 17, 2024 (transposition to be expected first half of 2025). These new legislative acts require coordinated efforts from the national competent authorities. The Markets in Crypto-Assets Regulation (MiCA) is in force since July 2023 and its delegated acts are also gradually entering applicability in the next 18 months, bringing a hitherto unseen level of regulation to crypto-asset service providers, who are largely dependent on information technology. The authorities' preparation for the application of DORA from January 17, 2025, is an ongoing effort. Organizational changes for a dedicated ACPR team and new national legislation were in the pipeline at the time of the FSAP assessment.

The supervision of cyber risk in France is found to be effective, building on the relevant EU regulatory framework and strong national laws. The French supervisory authorities operate according to a national legal framework in which all relevant EU legislation is either transposed into domestic law or directly applicable. Thus, the cyber risk supervision and regulation framework for

French LSIs and FMIs is very similar to other EU member jurisdictions' frameworks, especially those in the Euro Area.

The legal basis and relevant regulations convey adequate powers for effective cyber risk supervision. The French supervisory authorities have sufficiently broad powers to collect relevant information, assess firms' compliance with the cyber risk framework, impose corrective actions or sanctions, and take enforcement action as a last resort to ensure compliance.

The cyber risk supervisory practices of the supervisory authorities are materially in line with applicable regulations and guidance as well as prevailing international good practice. Key strengths include: (i) strong educational and awareness raising approach to help the supervised entities prepare for the applicability of DORA, (ii) cross-functional working groups for DORA preparation, (iii) the AMF knowledge base for cyber risk supervision, (iv) the Paris Resilience Group's (PRG) mature approach to crisis management, (v) the ACPR insurance supervisory team's comprehensive approach to enhancing the understanding of the cyber risk landscape through available cyber insurance data, and (vi) the AMF cyberattack first aid page. However, common tools for DORA related new activities should be developed and shared between the financial supervisors.

Resource constraints and staffing challenges are the most prominent challenges that supervisory authorities are likely to face. More dedicated, specialized resources will be needed for cyber risk supervision and digital operational resilience supervision (including DORA) within AMF and ACPR. The necessary headcount should be estimated based on work plans for the next 2-3 years, including onsite and offsite supervisory activities, as well as additional tasks such as cyber risk expertise needed in joint examination and oversight, international work, regulatory activities, and licensing.

Stronger information sharing, cooperation and coordination among the authorities are necessary in the fragmented cyber supervisory landscape. Cooperation should be formalized and regular at the operational and management levels, in addition to the existing informal and flexible approach. More cooperation is needed on critical infrastructure protection, including the currently confidential list of critical entities and incident information to cover technical aspects (in the domain of the French Cybersecurity Agency, ANSSI) as well as financial stability aspects to identify potential threats and high-risk areas for the French financial sector.

Other identified weaknesses have a negative impact on the otherwise strong cyber risk supervision and leave room for improvements. The most important are: (i) the need for common tools and information sharing among the authorities, (ii) cyber crisis management protocols need to be strengthened and formalized, (iii) the cyber risk supervisory methodologies of the financial supervisory authorities should become more convergent with the applicability of DORA, (iv) authorities should explore the possibility of using automated tools, and (v) the current coverage of onsite cyber risk supervisory controls needs to be increased in the coming years.

Table 1. France: Key Recommendations			
Recommendation	**Reference**	**Authority**	**Timing[1]**
Institutional and regulatory framework			
1. Formalize and enhance the collaboration among authorities in the protection of designate critical entities to facilitate optimal cooperation and information sharing.	43	ACPR AMF BdF	I
2. Develop and share common tools for DORA related new activities.	45	ACPR AMF BdF	ST
3. Allocate more dedicated, specialized resources for cyber risk supervision and digital operational resilience supervision (including DORA).	47	ACPR AMF	MT
Supervisory practices			
4. Ensure that cyber risk supervisory practices become more consistent, and methodologies converge with the applicability of DORA.	67	ACPR AMF BdF	ST
Common Supervisory Tasks			
5. Define crisis management roles and procedures for cyber crisis.	94	ACPR AMF BdF	ST
6. Formalize information sharing about specific incidents and general cybersecurity trends both within the authorities and among BdF, ACPR, AMF and build a strong partnership with ANSSI.	95	ACPR AMF BdF	ST
7. Increase the use of automated tools to evaluate documents, reports, and questionnaires and trigger actions on red flags.	96	ACPR AMF BdF	MT
8. Plan for an increased onsite supervisory presence for the coming years.	97	ACPR AMF BdF	MT

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

INTRODUCTION[1]

A. Context

1. French authorities consider cyber risk to be one of the key concerns that may escalate to a financial stability issue. BdF, with ACPR's contribution, dedicated parts of its 2022[2], 2023[3] and 2024[4] semi-annual financial stability reports to draw attention to the relevance of cyber risk (alongside with climate and environmental risk) in evaluating the potential threats to financial stability.

2. The number and sophistication of cyberattacks have been constantly rising due to technological developments and the increase in geopolitical tension. According to the European Union Agency for Cybersecurity (ENISA)[5], the finance sector remains one of the most targeted sectors in all geographical regions, with 9 percent of all attacks in the European Union (EU) targeting banking and finance. Though the most prevalent types of threats to the French financial sector are still traditional data exfiltration and ransomware attacks, one of the largest entities also encountered a deepfake attempt to impersonate one of its executives. In France, ransomware attacks increased by 30% between 2022 and 2023[6], with the trend continuing in 2024[7]. The threat landscapes prepared by ANSSI use a different methodology than ENISA, so the French data is not comparable to the EU threat landscape, but qualitative data and the ENISA threat landscape on the financial sector published in March 2025[8] suggests that the French landscape is similar to the rest of Europe.

3. France experienced one of its largest ever data breaches in 2024. Two of its healthcare payment providers were compromised, impacting the personal data of more than 33 million people.[9] Though the healthcare payment providers are not directly supervised by the French financial authorities, they are part of the supply chain for financial institutions, especially insurance undertakings.

---

[1] This Technical Note has been prepared by Ms. Gabriella Biró, Cyber Security Expert (STX). The on-site work supporting the findings and conclusions was conducted in Paris during December 2024. The information in this note is current as of December 20, 2024.

[2] Évaluation des risques du système financier français - Juin 2022 | Publications

[3] Assessment of risks to the French financial system, June 2023, Banque de France, Assessment of risks to the French financial system – December 2023

[4] Assessment of risks to the French financial system, June 2024, Banque de France, Financial stability report - December 2024

[5] ENISA Report on the State of the Cybersecurity in the Union 2024

[6] https://www.cert.ssi.gouv.fr/uploads/CERTFR-2024-CTI-001.pdf

[7] The latest threat landscape was published on March 11, 2025 : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-004.pdf

[8] https://www.enisa.europa.eu/publications/enisa-threat-landscape-finance-sector

[9] https://www.bleepingcomputer.com/news/security/data-breaches-at-viamedis-and-almerys-impact-33-million-in-france/

4. The need to continually improve cyber resilience prompted authorities to prioritize cyber risk and increase their efforts to ensure the resilience of the finance sector. Over the past five years, the European Central Bank (ECB), the European Supervisory Authorities (ESAs) and French authorities have consistently identified operational resilience and, in particular, IT outsourcing and IT security/cyber risks as a supervisory priority.

5. DORA was adopted by the EU in 2022 to introduce a unified approach and baseline expectations on cyber resilience for all finance sector participants. DORA and its delegated acts are directly applicable in France and other EU member states from January 17, 2025. The regulations create new tasks and mandates for supervisors and new requirements for the supervised institutions. DORA introduces stringent requirements for financial entities, mandating comprehensive ICT risk management, incident reporting, and third-party risk oversight to enhance digital resilience across the sector. In France, financial supervisory authorities must now enforce these harmonized standards, ensuring that institutions proactively assess cyber risks and implement robust resilience frameworks in compliance with EU regulations.

6. There is an overlap in scope between DORA and other EU regulations, particularly the NIS2 and the CER. While DORA as an act/regulation is directly applicable, NIS2 and CER are directives that need to be transposed into national law. France had not fully transposed the Directives at the time of the FSAP assessment, and the European Commission decided to start a formal infringement notification procedure in November 2024.

B. Assessment Scope

7. The scope of the assessment covered the cyber risk supervision and regulation of the financial sector in France. Thus, the financial supervisory authorities in scope were the BdF, ACPR, and AMF, collectively referred hereinafter as authorities. Supervision of SIs in France is within the remit of the ECB/SSM and was therefore outside the scope of this FSAP.

9. The note considers cyber risk as well as information and communication technology risk as materially overlapping, in addition to both being subcategories of operational risk. This aligns with the authorities' own risk taxonomies (except AMF, where a distinction is maintained) and the FSB Cyber Lexicon's definitions.

8. Cybersecurity is an increasingly complex issue where cooperation is essential. Thus, the French Treasury Directorate within the Ministry of the Economy, Finance and Industrial and Digital Sovereignty (MoEF-Trésor) and the French cybersecurity agency (ANSSI) were interviewed during the assessment to better understand the French cyber ecosystem. As the representative of France at the European Council, Trésor is the lead institutional contributor to financial regulatory matters, including notably the DORA regulation during the French EU presidency between January and June 2022. ANSSI is the national competent authority (NCA) for NIS2, so the agency has overall responsibility for the cyber security of France, with some mandates related to the financial sector and its suppliers.

9. The assessment covered the authorities' risk-based supervision practices, cyber incident response and recovery, the incident reporting regime, cyber security testing, and crisis exercises. DORA related topics included the Threat-Led Penetration Testing (TLPT) regime and the supervisory expectations for entities not covered by DORA. One area of focus was the cyber supervisory and oversight framework for Financial Market Infrastructures (FMI). Another focus area was the financial sector's (specifically banks and FMIs) and authorities' preparedness to deal with a potential cyber crisis, including cooperation between authorities, the crisis management framework, and its testing through simulations.

10. The assessment collected information from several sources. These include questionnaire answers provided prior to the on-site mission by the BdF, ACPR, AMF, and Trésor, interviews with these authorities, ANSSI, and supervised institutions, the study of relevant laws and decrees, and documentation of the authorities' work, such as internal documents, supervisory plans, reports, and other evidence as needed.

11. 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) 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) European Insurance and Occupational Pensions Authority (EIOPA) Guidelines on information and communication technology security and governance (EIOPA-BoS-20/600); (v) EIOPA Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002); (vi) European Securities and Markets Authority (ESMA) Guidelines on outsourcing to cloud service providers; (vii) Cyber resilience oversight expectations for financial market infrastructures (CROE); (viii) Committee on Payments and Market Infrastructures and the International Organization of Securities Commissions (CPMI-IOSCO) Guidance on cyber resilience for financial market infrastructures; and (ix) the Financial Stability Board (FSB) Cyber Lexicon and Format for Incident Reporting Exchange (FIRE).

INSTITUTIONAL AND REGULATORY FRAMEWORK

A. Legal Basis

12. The legal basis for cyber risk supervision is strong, ACPR, BdF and AMF operate according to a national legal framework in which all relevant EU legislation is either transposed to domestic law or directly applicable. Thus, the cyber risk supervision and regulation framework for French LSIs and FMIs is very similar to other EU member jurisdictions' frameworks, especially those in the Euro Area. The authorities have the relevant internal procedure and decision mechanisms in place to impose sanctions or penalties on supervised entities that do not comply with the legal requirements.

13. ACPR, AMF and BdF supervise the cyber risks faced by French financial institutions in cooperation (Table 2). When several authorities are involved, the oversight framework allocates roles and responsibilities to the authorities for each oversight/supervisory issue (e.g. incident, cyber, outsourcing, etc.) by designating a lead NCA and one or two supporting NCAs. For co-supervised financial institutions, the authorities developed a brief tripartite agreement in 2019. The agreement on shared responsibilities that was presented during the onsite mission is a simple table format list of activities without date, signature, versioning, or specific contact information to share responsibility in cyber supervision. This agreement, and more specifically the division of competences, is likely to evolve with the implementation of DORA in order to account for entities and responsibilities that were not previously included.

Table 2. France: Cyber Risk Supervisory Competence

ACPR's competence on the insurance sector	ACPR's competence on the banking sector	Banque de France's competence	AMF's competence	Cybersecurity agency (ANSSI)
Insurance and reinsurance organizations	Central counterparty	Central counterparty		Operators of vital importance in the French financial sector
Insurance and reinsurance intermediaries and incidental insurance intermediaries	Credit institutions	Central securities depository		Operators of essential services in the French financial sector
Occupational pension institutions	Investment firms and investment services providers	Payment systems	Management companies	
	Electronic money institutions		Digital asset service providers, as defined by the future MICA regulation, and issuers of tokens indexed on assets	
	Payment institutions		Trading venues	
	Account information service providers		Participative financing service providers / Crowdfunding	
	Custodians of securitization vehicles		Alternative investment fund managers	
	UCITS and AIF depositories			

14. The authorities have decided to extend DORA to French financial entities not under the scope of the regulation. Though the DORA regulation is directly applicable to most French financial entities, two types of entities are not covered by DORA: (i) Sociétés de Financement, which are specific to France and not regulated in the EU framework; and (ii) Caisse des Dépôts et des Consignations (CDC), which are recognized in the EU law as special financial institutions and their inclusion in the DORA regime may be decided by national authorities. The authorities plan to design a national framework inspired by DORA to address the structural specificities of the CDC. The DORA requirements will also be extended to the financial entities in overseas French territories which are not part of the EU and branches of third-country credit institutions and investment firms.

15. Payment systems are not within the scope of DORA. Their oversight and supervision are carried out in accordance with the Eurosystem Cyber Resilience Strategy. The preamble of DORA mentions the possibility that national regulators may "draw inspiration from the digital operational resilience requirements" for payment systems, but the French regulator does not intend to expand the scope of DORA requirements to this extent.

16. The BdF discharges its supervisory duties according to relevant EU legislation: (i) The Central Securities Depositories Regulation (CSDR) is applicable for Central Securities Depositories (CSD); (ii) the European Market Infrastructure Regulation (EMIR) is applicable for central counterparties (CCP); and (iii) the Regulation of the European Central Bank (EU) No 795/2014 of July 3, 2014 on oversight requirements for systemically important payment systems (ECB/2014/28) (SIPSR) is applicable for the Payment Systems.

17. AMF and ACPR have distinct competences under the Market in Crypto-Assets Regulation (MiCA). AMF is mainly in charge of provisions related to crypto-asset service providers (CASPs), crypto-assets' white papers as well as market abuse, whereas the ACPR is competent for provisions related to stablecoins (i.e. e-money tokens and asset-referenced tokens under MiCA). MiCA aims to create a comprehensive and harmonized regulatory framework for crypto assets across the European Union, and it is gradually applicable with the last of titles entering into applicability in December 2024. The MiCA regime is replacing the stricter French requirements for market and digital assets (PACTE law), in which an external security audit was mandatory part of the licensing procedure for Digital Asset Service Providers (DASPs). During 2024, six digital assets service providers (PSAN in French) have been authorized under the stricter requirements of the PACTE law. DASPs that had already obtained "simple" registration before 1 January 2024 benefit from a grandfathering clause and will continue to be subject to the prior registration requirements.

18. In addition to EU regulations, national laws contain applicable provisions for cybersecurity. The French Monetary and Financial Code, the French Insurance Code, the AMF General Regulation and the ACPR Decree of November 3, 2014, on internal control are the main relevant national regulations for the financial sector. There is also a dedicated French Mutuality Code for the mutual societies and another French Social Security Code for the provident institutions. These cover various aspects of risk management and the ICT and cyber risk governance framework and provide the basis for supervisory actions.

B. Other Relevant Regulations

19. The overall regulatory landscape for the French financial sector is more complex than in other European jurisdictions, because of the interplay with national critical infrastructure protection laws. The financial entities are used to managing this complexity, but they look forward to some of the simplification opportunities offered by DORA.

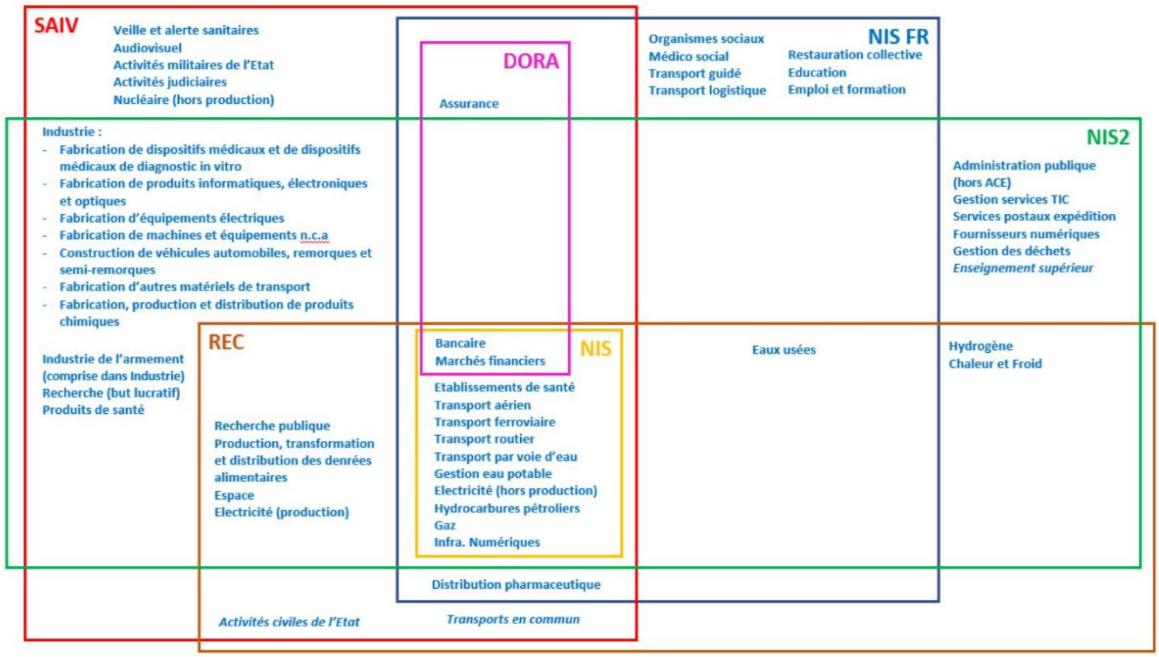
20. ANSSI supervises some financial entities that fall under the mandate of critical infrastructure protection. These are (i) operators of essential services from the banking, market infrastructure and insurance sectors, designated on the basis of the NIS Directive; and (ii) operators of vital importance in the French financial sector from the banking, market infrastructure, insurance and payment systems sectors, designated on the basis of the Public Policy for Securing Vital Importance Activities (SAIV). SAIV is designed and implemented by the General Secretariat for Defense and National Security (SGDSN), an interministerial body placed under the authority of the French Prime Minister. Once designated by the MoEF, operators of vital importance must secure their critical information system on the basis of the article 22 of the French Military Programming Act of December 18, 2013 (LPM in French).

21. The NIS2 Directive will be applicable to some financial entities that are already designated as critical infrastructure, and the supervision mandate will remain with ANSSI. DORA is the lex specialist of NIS2, therefore the financial entities that fall under NIS2 will have to comply with DORA instead. DORA intends to simplify the supervision of such financial entities and move some of the current responsibilities of the national NIS2 authorities to the financial national competent authorities for the entities under the DORA regime. The French implementation gives some responsibilities granted under DORA to ANSSI as the NIS2 authority in addition to the supervisory responsibilities of BdF, ACPR and AMF. The bill No. 33[10] that implements the NIS2 and CER Directives in France, and also contains the changes related to DORA, is still pending (as of December 2024). The EU General Data Protection Regulation (GDPR) is not covered in this report, but no change is anticipated in the GDPR related activities of the financial institutions due to the other new regulations.

22. Insurance undertakings are not under the scope of NIS2, but some of them will be included in the French NIS2 implementation due to their past status as operators of essential services under NIS and their criticality specific to the French financial sector in managing funds. The NIS2 implementing bill No. 33. will modify the Insurance Code to extend the applicability of NIS2 to insurance undertakings, thereby giving ANSSI a mandate over insurance undertakings (Figure 1).

[10] https://www.senat.fr/leg/pjl24-033.html

Figure 1. Regulatory Landscape for French Critical Infrastructure



SAIV = "Secteur d'Activité d'Importance Vitale," regulation for sectors of vital importance
REC = CER (French)

Source: Impact study on the bill relating to the resilience of critical infrastructures and the strengthening of cybersecurity

23. The exact list of entities designated as critical and thus falling under the remit of ANSSI is strictly confidential, but the number of such entities in the finance sector is published by ANSSI.[11] The financial authorities are officially not informed if an entity under their supervision or oversight is designated as critical infrastructure, or if any particular ICT systems fall under the additional requirements and supervisory mandate of ANSSI based on their criticality. Though the list of critical financial entities and their critical systems are treated as confidential or classified in most EU countries, the classifier (data owner) usually specifically allows the sharing of such information with the financial supervisors of the entities. The new EU legal framework (NIS2, CER, and DORA) also foresees a much stronger cooperation and information sharing among the authorities. A cooperation framework is currently being designed to foster information sharing to comply with NIS2 and DORA, but the scope of critical systems falling under the LPM requirements will remain the restricted competence of ANSSI.

[11] https://www.sgdsn.gouv.fr/files/files/Publications/plaquette-saiv-anglais.pdf

C. Supervisory Expectations

24. The landscape of regulatory expectations is very fragmented. This is the case in all European countries that directly rely on all the guidelines of the three ESAs without additional national legislation to standardize those requirements. This is the exact reason that prompted the European Commission to draft DORA in order to unify the regulatory landscape for the financial sector.

25. The French regulatory expectations rely on a national regulatory framework in line with European regulations and the guidelines of the ESAs. The French authorities are deeply involved in the drafting of the ESA guidelines. These guidelines will be reviewed by the relevant ESA working groups after the preparation for DORA is completed, therefore some simplification and convergence may be expected.

26. The European Banking Authority's (EBA) guidelines are applicable to European credit institutions and their financial supervisory authorities, thus also to French LSI's cyber risk management and ACPR's supervision thereof. The most relevant guidelines in this respect are: (i) the EBA Guidelines on ICT and security risk management (EBA/GL/2019/04); (ii) the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02); and (iii) the EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation (SREP) process (EBA/GL/2017/05).[12]

27. The Solvency II and European Insurance and Occupational Pensions Authority's (EIOPA) guidelines are applicable to European insurance undertakings and occupational pension funds and their financial supervisory authorities, thus also to French insurance sector's cyber risk management and ACPR's supervision thereof. The most relevant guidelines in this respect are: (i) the EIOPA Guidelines on information and communication technology security and governance (EIOPA-BoS-20/600); (ii) the EIOPA Guidelines on outsourcing to cloud service providers (EIOPA-BoS-20-002); and (iii) the EIOPA Guidelines on system of governance (EIOPA-BoS-14/253).[13]

28. The European Securities and Markets Authority's (ESMA) guidelines are applicable to European securities and markets institutions and their financial supervisory authorities, thus also to the French sector's cyber risk management and AMF's supervision thereof. The most relevant guidelines in this respect are the ESMA Guidelines on outsourcing to cloud service providers (ESMA50-157-2403).[14]

29. The BdF's cyber risk oversight of the 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):

[12] The EBA guidelines will be reviewed to reflect the necessary changes introduced by DORA.

[13] The EIOPA guidelines will be reviewed to reflect the necessary changes introduced by DORA.

[14] The ESMA Cloud Guidelines are likely to be withdrawn in 2025.

(i) Principles for Financial Market Infrastructures (commonly referred to as PFMIs), and (ii) Guidance on cyber resilience for FMIs (Cyber Guidance). The PFMIs set out a series of 24 principles covering key areas such as governance, credit and liquidity risk management, settlement, default management, transparency, and business and operational risk management, in order to ensure that FMIs are resilient and capable to withstand financial shocks. The Cyber Guidance expands on these principles by adding a set of more specific and detailed requirements to ensure the continuity of critical services under disruptions caused by cyber incidents. Both are applied by BdF in its oversight of FMIs in addition to the Cyber Resilience Oversight Expectations (CROE) applicable to payment systems, T2S, payment schemes, and payment arrangements that were published in 2018 as part of the Eurosystem oversight cyber resilience strategy. The CROE (i) provides FMIs with detailed steps on how to operationalize the Guidance, (ii) provides overseers with clear expectations to assess the FMIs for which they are responsible and (iii) provides the basis for a meaningful discussion between the FMIs and their respective overseers.

30. ACPR issues notices to clarify supervisory guidelines or expectations. Currently there is an ACPR notice for the banking sector[15] and one for the insurance sector[16] on IT risk management. The supervisor is planning to publish notices on some specific DORA requirements.

31. International standards for ICT risk management and cybersecurity are used in cyber risk supervision as supplementary sources. The National Institute of Standards and Technology's (NIST) cybersecurity framework, the ISO27001 standard and Control Objectives for Information Technologies (COBIT) are the most frequently used resources.

32. ANSSI provides methodologies and guidelines that may be used by financial entities. Some examples are the cloud security guidelines, secure coding, virtualization, or the EBIOS risk management methodology. ANSSI also issues qualifications for auditors (PASSI), advisors and various service provides, and qualifications for services such as the SecNumCloud label for cloud services.

D. Organization and Resourcing of Cyber Risk Supervision

33. The overall structural complexity of the cyber risk supervision within the French financial sector is high with four distinct teams working across three authorities, which is an inherent risk in itself if not mitigated. The complexity does not necessarily come from the DORA regulatory environment, as other EU countries such as Germany or Spain have a more streamlined approach to cyber risk supervision. BdF, ACPR and AMF share the tasks and responsibilities of cyber risk supervision as well as the overall financial supervision of the French financial sector. The cooperation of BdF and ACPR is easier because they are within the same organization, with some shared IT systems and organizational resources. AMF is a separate entity, with separate infrastructure and resources.

[15] https://acpr.banque-france.fr/system/files/import/acpr/media/2021/07/08/20210707_notice_risque_it.pdf

[16] https://acpr.banque-france.fr/system/files/import/acpr/media/2021/07/02/20210702_notices_orientations_aeapp.pdf

34. BdF has a dedicated Cyber Unit for the oversight of cyber and operational risk issues. The Cyber Unit provides its expertise to the three other oversight units (Payments, CSD and CCP). The Cyber Unit consists of three experts with professional certifications and experience in IT and cyber security audit. They perform oversight duties, but do not routinely engage in onsite supervisory activities for the three French FMIs (ACPR performs these activities at the request of BdF, see below), though they have the necessary mandate to do so. They participate in the cooperative oversight of SWIFT and contribute to international work such as the G7 Cyber Expert Group.

35. ACPR has an onsite banking supervisory team of 12 FTE dedicated to ICT and cyber risk supervision. The ICT Risk Assessment Unit (Cellule d'Évaluation des Risques des Systèmes d'Information – CERSI) is responsible for the onsite inspection of credit institutions and investment firms. They supervise LSIs locally, contribute to SSM missions and perform onsite visits on behalf of BdF. The team members are experienced professionals with internationally acknowledged certifications. The team has subject matter experts on data center physical security and cloud security who provide expertise for the whole SSM. They also contribute to national and international methodological work in different working groups and represent ACPR in many international fora working on regulatory or supervisory topics related to IT and cyber risk.

36. ACPR has an onsite insurance supervisory team with 5.5 FTEs dedicated to the supervision of information systems. Onsite supervision of insurance undertakings is carried-out by the Permanent Group for Insurance Companies' Inspections (GPEOA) within the Cross-functional and Specialized Supervision Directorate (DCST). In the GPEOA, the Information Systems – Data Quality (SI-QDD) Unit is composed of 12 onsite inspectors under the responsibility of the Heads of mission, of which 5.5 FTEs are dedicated to the supervision of information systems. The team members have backgrounds in IT and most of them are engineers.

37. Within ACPR, IT and cyber security expertise is mainly gathered in the onsite teams, with additional DORA related competence in the offsite and international teams. Offsite supervisory teams in general do not have dedicated resources to cyber risk supervision. Offsite supervisors follow up on ICT related topics and findings with the supervised entities and consult with the specialized onsite teams as needed. There are specializations within the offsite team and operational risk (including IT risk) being one of such specialized topics.

38. A new dedicated team is expected to be set up within ACPR in order to provide DORA related expertise as a cross-sectoral function, independent of the banking and insurance supervisory teams. During the assessment interviews it was confirmed that no new FTEs will be allocated for the team, instead existing resources will be utilized.[17]

39. AMF currently has one fully dedicated FTE for cyber risk supervision and DORA. The internal cybersecurity team of AMF lends one expert to the supervisory teams when necessary and it also relies on external audit service providers that hold ANSSI qualifications (PASSI). Currently with

[17] Details were not shared during the assessment because of a pending management decision, but the new unit has been operational since February 2025.

the ongoing DORA and MiCA implementations and the licensing related to MiCA, the expert from the internal cyber security team works almost exclusively on supervisory tasks. AMF is also making great efforts to educate supervisors on the DORA and cyber resilience requirements and "spread cyber all over the organization", so these are able to evaluate cyber risk during regular onsite and offsite supervision. 2 FTEs are specifically working on MiCA cyber related activities. Since the existing digital asset services providers (DASPs) have 18 months to fully comply (July 2026), it is anticipated that additional resources will be needed on the supervisory team after that to be able to supervise the new entities and requirements. Currently the 106 DASPs only have to register for Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) purposes, but about half of them are expected to apply for licenses under MiCA and become fully supervised entities.

E. Conclusions and Recommendations

40. The institutional and regulatory framework of the cyber risk supervision is generally strong. The legal basis and relevant regulations convey adequate powers for effective cyber risk supervision. Thanks to the EU framework and French laws, the French supervisory authorities have sufficiently broad powers regarding collection of information in any form on any relevant matter, to assess compliance, impose corrective actions or sanctions and take enforcement action as a last resort to ensure compliance.

41. The DORA regulation does not fundamentally change the key principles of the cyber risk supervisory framework in France, but it takes the responsibilities and tasks to a new level. The requirements already existing in ESA guidelines will be elevated to the level of EU law, requiring a more stringent supervisory approach. New reporting requirements are introduced, and existing reports are enhanced, therefore the supervisors will have to be able to process more information and perform necessary supervisory actions accordingly. New frameworks, tools and cooperation agreements are currently being developed by the authorities to meet the requirements set out by DORA.

42. The supervisory landscape with different actors involved is very complex, which calls for strong coordination, cooperation and information sharing within the framework. The cooperation of BdF, ACPR and AMF on cyber risk supervision is governed by a simple 3-page tripartite agreement signed in 2019. The information sharing between AMF and ANSSI is allowed by the law, which will be modified in the context of DORA preparation to allow the information sharing between ACPR, BdF and ANSSI. The cooperation of ACPR and AMF on one side and of AMF and ANSSI on the other side is governed by a 2018 letter of intention which has never evolved to a more concrete Memoranda of Understanding (MoU) due to SSM and French law limitations. A new cooperation framework is currently being designed with two agreements: one between ANSSI and BdF+ACPR and one between ANSSI and AMF. Once the implementing bill No. 33 for NIS2, CER and DORA is adopted, ANSSI, ACPR, BdF and AMF will be able to officially share more information. At the time of the mission, the French law does not allow all authorities to share information. Some information available to ANSSI is classified, so it may only be shared under the strictest confidentiality and access to that information requires a security clearance for the individuals accessing the data.

43. The collaboration should be formalized and enhanced among BdF, ACPR, AMF and ANSSI to facilitate optimal cooperation and information sharing. Regular interaction at operational as well as management level of the agencies is recommended in addition to the current informal and flexible approach. The legal basis for sharing all information necessary for each authority to perform their respective duties should be clearly established at the sufficient level of legal documents (for example MoU or law) depending on the sensitivity of the information to be shared. The necessary procedures and channels should be set up for the collaboration, with specific contact details for each topic and regular review/update procedures. More cooperation is needed on critical infrastructure protection to cover the technical aspects (ANSSI) as well as the financial stability aspects to be able to identify potential threats and high-risk areas. Legal limitations and requirements set by the classifier of the information must be respected.

44. While each supervisor collects DORA related reports, the efforts of developing tools for managing this data are sometimes duplicated. Incident reporting and the Register of Information for third party service providers of financial entities are collected by each authority, and these reports are all in the same format in accordance with the DORA delegated acts. The data collected by the authorities is not correlated at a national level, though each authority forwards the data to the ESAs. Therefore, a holistic view of all available French data will only be accessible to the European authorities, not to any of the French authorities. For example, concentration risk may span across different types of financial entities and reach a critical national level but not exceed the EU level of criticality. If there is no complete view or overview available to any of the French authorities, they will not be able to anticipate certain types of risks before those materialize and reach a critical level.

45. Common tools for DORA related new activities should be developed and shared among the financial supervisors to create a holistic risk landscape of the financial sector. Incident reporting tools and databases as well as the Register of Information on third party service providers should be standardized for all supervisory authorities. While the templates are standardized by DORA and its delegated acts, the tools to process the information from the templates are still under development. At least one authority should be in a position to have a complete overview of the incident and outsourcing information for the whole French financial sector with enough details (not full granularity) to be able to recognize and manage cyber risk in a holistic way and in a timely manner.

46. At the time of the FSAP mission, there were only 22.5 FTEs across ACPR, BdF, and AMF dedicated to ICT and cyber risk supervision (17.5 at ACPR across 2 teams, 3 in BdF, 2 in AMF), with some additional FTEs performing related activities. According to the estimation of ACPR in March 2025 there are about 24.5 FTEs currently dedicated to cyber risk, with more than 40 persons in the ACPR working on cyber risk supervision/cyber risk topics. The skills and approaches of the teams are very different. The teams also participate in international, European and SSM work and will be increasingly involved in the new joint oversight activities established by DORA, so the FTEs are not fully dedicated to tasks within France or fully related to the French financial system. There is 1 FTE within BdF working on the Threat-Led Penetration Testing (TLPT) exercises and ACPR is also

planning to have 1 FTE dedicated to TLPT, but these are distinct activities, and most EU countries do not include their TLPT experts in their headcounts for cyber risk supervision.

47. More dedicated, specialized resources will be needed for cyber risk supervision and digital operational resilience supervision (including DORA). The necessary headcount for ACPR and AMF should be estimated based on workplans for the next 2-3 years including onsite and offsite supervisory activities as well as additional tasks such as cyber risk expertise needed in international work, regulatory activities, and in the support functions dedicated to regulatory development and monitoring. It is good practice to employ supervisors with international certifications such as Certified Information Systems Auditor (CISA) or Certified Information Systems Security Professional (CISSP). It is also worth noting that the knowledge of the DORA regulatory environment is not equivalent to cyber risk governance or technical cyber security knowledge. The ENISA Cyber Skill Framework[18] is a good reference for determining necessary skills.

SUPERVISORY PRACTICES

A. ACPR: Banking Supervision

48. Onsite inspections on cyber risk in the banking sector are carried-out by the ICT risk assessment Unit (CERSI) of ACPR. ICT risk is not part of the general inspections, but there is an indication from the SSM that it should be integrated. The CERSI unit carries out 3-4 dedicated ICT missions for ACPR each year, in addition to the 2-3 SSM missions and onsite missions for FMIs and retail payment entities overseen by BdF. They use the SSM methodology for all their missions.

49. At the time of the onsite mission there were no banking onsite cyber missions planned for 2025 in France in line with the request of the ECB.[19] In future, the CERSI unit is to take part in BdF onsite inspections and possibly SSM missions or DORA joint examination teams abroad.

50. The results and findings of onsite inspections are communicated to supervised entities by their offsite supervisors, who also follow up on any necessary actions. The deadlines for the action plans are agreed with the institutions. So far, no onsite cyber related findings have resulted in sanctions or penalties.

51. The offsite cyber risk supervision of banking sector entities is carried out by the two Bank Supervision Directorates of ACPR. Cyber risk is considered as part of operational risk, and the supervisors assess it in the framework of the annual SREP. Every supervisor has a portfolio of LSIs and covers all the different types of risk.

52. Offsite supervisors send out an annual IT risk questionnaire to LSIs to evaluate their level of ICT risk. The aggregated results are communicated to LSIs and used by supervisors to identify key issues such as insufficient risk management related to outsourcing.

[18] https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf

[19] The intention of ECB and ACPR is to allow their supervised entities to better prepare for DORA.

B. ACPR: Insurance Supervision

53. Onsite inspections on cyber risk in the insurance sector are carried-out by the Permanent Group for insurance companies' inspections (GPEOA) of ACPR. The group carries out 3-4 dedicated ICT missions each year according to their own methodology, covering Information Systems Security (ISS) Governance, operational security, the IT continuity plan, and outsourcing.

54. There were two insurance onsite cyber missions planned for 2025 at the time of the FSAP mission, both focusing on the DORA compliance of the entities. The focus is currently shifting to offsite supervision in order to allow the supervised entities to better prepare for DORA.

55. The results and findings of onsite inspections are communicated to supervised entities by their onsite supervisors, then received officially from offsite supervisors, who also follow up on any necessary actions. The deadlines for the action plans are agreed with the institutions. So far, no onsite cyber related findings have resulted in sanctions or penalties. One of the most typical findings mentioned during the mission was the insufficient independence of the ICT security function.

56. The offsite cyber risk supervision of insurance sector entities is carried out by the two Insurance Supervision Directorates of ACPR. Cyber risk is considered as part of operational risk, and the supervisors assess it in the framework of Solvency II as part of the annual reporting and through regular meetings with the entities.

57. The insurance offsite supervisors have a very good understanding of the cyber threat to insurers through their continued attention to the cyber risk insurance landscape. They use this as an additional information source on top of the insight gained from supervision. One of their especially insightful sources of information is the annual AMRAE report (Association pour le Management des Risques et des Assurances de l'Entreprise) on cyber insurance.[20]

C. BdF: FMI Oversight and Supervision

58. Cyber risk related topics are overseen by BdF's dedicated Cyber Unit, which works closely with the three general oversight units and takes part in the regular oversight discussions with the overseen entities. The three other BdF units are dedicated to the general oversight of all three French FMIs: (i) payment systems, (ii) CCPs and (iii) CSDs. The BdF Oversight division cooperates with the supervisory departments within AMF and ACPR for the continuous oversight of institutions.

59. The quarterly oversight meetings with the FMIs usually include ICT and cyber risk related topics, but there are also additional dedicated meetings for IT topics. A recent example is the data center migration of an entity. For 2024, the focus areas of cyber risk oversight were the

[20] AMRAE LUCY Light upon Cyber Insurance, https://www.amrae.fr/bibliotheque-de-amrae/lucy-light-upon-cyber-insurance-2024-edition

governance of cyber and operational risk and the "three lines of defense". DORA was an additional topic for discussion with all overseen FMIs.

60. All FMIs are sufficiently covered by cyber risk supervision. There is a three-year cycle for the onsite supervision of FMIs and all FMIs are covered within the cycle.

D. AMF: IT and Cyber Risk Supervision

61. IT and cyber risk are a key issue for AMF due to the increased reliance of their supervised entities, especially crypto asset managers, on technology. The AMF strategic plan includes cybersecurity as a focus area. Inspection target entities and thematic inspection topics are identified via supervisory activity and based upon ESMA's heatmap and AMF's annual priorities of supervision.

62. Onsite supervisory activities are performed by the Investigations and Inspections directorate, while offsite/operational supervision is conducted by the Markets directorate and Asset Management directorate. IT and cyber risk supervision is within the responsibility of the Investigations and Inspections directorate, which also engages external ANSSI qualified auditors to perform more technical reviews such as penetration tests or system configuration reviews.

63. AMF has conducted three Supervision of Operational and Thematic Practices (SPOT) inspections dedicated to cyber risk between 2019-2023 and overall, 26 cyber security inspections since 2019. The summarized findings and of the SPOT results are published[21] and presented to supervised entities and their associations in order to raise their awareness of cyber issues and share good practices.

64. AMF uses an internal tool to collect the results of each supervision and the documents or workpapers used in order to build a supervisory knowledge base. The aim is to enable all the supervisors to participate in a cyber inspection by making the related knowledge accessible to them. This approach enables AMF to perform consistent inspections even without a dedicated team of cyber risk supervisors.

65. AMF uses a questionnaire for the licensing of crypto companies that covers all major IT and cyber topics in about 100 questions with supporting documents to be attached. There is a separate questionnaire for regular inspections as well, which also contains an asset mapping ("Carthographie") of the IT equipment, system configurations and other IT resources used by the institution. No automated tools are used to evaluate the questionnaire.

[21] https://www.amf-france.org/en/news-publications/publications/spot-inspection-campaigns/summary-spot-inspections-asset-management-companies-cybersecurity-measures-no-3-2023

https://www.amf-france.org/en/news-publications/publications/spot-inspection-campaigns/summary-spot-inspections-cybersecurity-systems-asset-management-companies-no-2

https://www.amf-france.org/en/news-publications/publications/spot-inspection-campaigns/summary-spot-inspections-cybersecurity-systems-asset-management-companies

E. Conclusions and Recommendations

66. All onsite supervisory teams have relevant IT experience and some of them also have experts with national (ANSSI) qualifications[22] or internationally recognized certifications of IT audit. BdF and ACPR mentioned during the interviews that their primary source of recruitment is the IT department of BdF. All three supervisory authorities have some excellent practices within their teams.

67. Authorities should ensure that cyber risk supervisory practices become more consistent, and methodologies converge with the applicability of DORA. A regular platform should be set up with all three financial supervisors for sharing and discussing cyber risk related technical case studies, good practices, and methodologies. The main objective would be to be able to formulate standard types of recommendations based on DORA requirements that are the same for banks, insurance undertakings and financial infrastructures. This platform could also be utilized for relevant technology, cyber security, or audit training.

68. All French authorities use cyber risk supervision to educate supervised entities about the ICT and cyber risk. No penalties or sanctions related to IT issues have been imposed by BdF or ACPR. AMF imposed some sanctions related to cyber issues. With the applicability of DORA from January 2025, the educational focus will have to change due to the more rigid regulatory framework.

69. At the time of the FSAP mission, ACPR planned to reduce onsite supervisory activity for cyber risk supervision in 2025, while AMF intended to increase it. The ACPR focus would shift to offsite supervisory practice to allow the supervised entities more space to proceed with their DORA compliance tasks.[23] AMF, on the other hand, plans to implement more formal onsite controls, on the grounds that they have been providing cyber related educational activities for years now and in their understanding the requirement framework and communications of supervisory expectations are mature enough by now.

70. The DORA requirements have already been evaluated by all authorities during their onsite missions performed in 2024 and feedback was included in the reports. As DORA is only applicable from January 2025, the supervisors intended to help the institutions in the preparation by providing an early evaluation of their expected level of compliance.

[22] https://cyber.gouv.fr/referentiels-dexigences-pour-la-qualification

[23] After the FSAP mission, ACPR confirmed that it intends to maintain its inspections on LSIs and insurance undertakings.

COMMON SUPERVISORY TASKS

A. Testing and Exercising

72. Cyber security testing and exercising are performed regularly and adhere to high professional standards. External or independent penetration testers are used by the onsite supervisory teams to perform penetration tests.

73. ACPR and BdF onsite cyber risk supervisory teams utilize the Red Team[24] of BdF for penetration testing during onsite inspections. The supervised entities may choose which of their IT systems would be tested and the test is limited to a timeframe of one week. The results are communicated in a special report, independent from the supervisory report. Remediation actions are followed up by the respective offsite supervisory teams.

74. AMF engages external companies to perform penetration tests on behalf of AMF during onsite supervision. About a third of the cyber security onsite controls include penetration testing. The external penetration testers are selected through public tender. The scope of the tests is determined based on the risk level and criticality of systems. Systems that have undergone a penetration test in the last three years are excluded.

75. Based on the Threat Intelligence Based Ethical Red Teaming (TIBER) EU framework, the French TIBER FR[25] was implemented at the beginning of 2024 with BdF and ACPR, then joined by AMF, forming a common TIBER cyber team (TCT) to manage the tests. The Threat Led Penetration Tests (TLPT) required by DORA will be conducted according to the TIBER FR framework. The authorities stated that they have the necessary expertise and resources to allocate the test manager and alternate for each TLPT. Though the TCT test managers need special skills to be able to follow the ethical hacking exercise, each authority has qualified individuals to provide the necessary resources if they cooperate strongly. It is expected that around 30 entities will be covered within the three-year TLPT cycle, but the exact plan is dependent on ECB decisions for the "Significant Institutions" in the banking sector where the ECB is the TLPT competent authority. The results of the TLPTs will be followed up by the offsite supervisors in a similar way to the already established practice of following up on penetration test results and action plans. For entities that do not fall under the DORA requirement of performing a TLTP, simple penetration tests will be carried out (as has been the case before the DORA regime) or a voluntary TIBER test could be considered depending on the criticality of the entity.

76. Supervised entities that are subject to TLPT due to their criticality, but are also designated as critical infrastructure, may only be tested by threat intelligence and red team providers who have an adequate level of qualification from ANSSI. As supervisors are not informed if one of their supervised entities is designated as critical infrastructure, it is up to the

[24] An offensive security team tasked with performing cyber attacks in order to test the defences.

[25] https://www.banque-france.fr/fr/stabilite-financiere/cadre-institutionnel/systemes-paiement-infrastructures-marche/surveillance-risque-cyber.

entity to comply with this requirement. The role of the national cybersecurity agency in the TLPT is up to the discretion of each country. In France it has been agreed by all parties that ANSSI will not be involved in the scoping or result sharing of TLPTs but may provide a general threat landscape as input, which is in line with good practice.

B. Crisis Management

77. France has a mature practice of public-private cooperation and exercises in crisis management, but a formalized crisis management cooperation procedures and agreements of the public authorities is missing. In practice, the informal and voluntary cooperations work well, but defining the procedures can further improve the crisis preparedness and resilience of the French financial sector authorities.

78. BdF chairs the Paris Resilience Group (PRG), which is a collaborative group of key private sector participants from the Paris financial sector and the authorities, aiming to bolster the financial system's capacity to withstand external shocks. It was established in 2005, and the participation of its members is voluntary, based on mutual trust. Members include major French banks and FMIs as well as the ACPR, AMF, ANSSI, the MoEF and the Interministerial Defense and Security Official Service. BdF provides the secretariat of the PRG under its Innovation and Market Infrastructure Directorate. The Secretariat pays special attention to separating the voluntary information sharing within the PRG from the BdF/ACPR information flow as a supervisor and authority. PRG is structured into two working groups, responsible for the crisis management system and for organizing sector-wide simulation exercises to develop operational response capabilities. There is a dedicated unit for coordinating authorities on crisis communication (Inter-authority Crisis Communication Subgroup – PCCA). The simulation capabilities cover the communication part, but technical simulations or cyber ranges are not possible within the PRG framework.

79. In recent years, the PRG has been increasingly involved in cyber security related information sharing and in organizing exercises where the trigger was a cybersecurity event. The PRG organizes annual functional exercises aimed at testing the contingency measures in place within the member entities and training for information sharing and coordination both internally and externally. The scenarios are multidimensional and cover a wide range of activities (cyber/IT, communication, financial markets, card payment systems, cash management) to engage a large number of teams within the participating entities. The communication channels and protocols set up by the PRG are very efficient and mature. In 2024 it organized a successful exercise for the G7. The ACPR has also modelled its own internal cyber crisis protocol for its supervised entities based on the PRG crisis management protocol. The crisis management mechanism can be triggered by phone call, with the BdF analysts working at the PRG Secretariate being available any time (24/7).

80. The PRG is more focused on payments and financial stability and does not cover all the critical entities within the French financial sector. Specifically, insurance undertakings are not included. Overall, the composition of the group has not changed since its beginning. The PRG is a

public-private initiative, it does not have any official role or public mandate in the protection of the critical financial infrastructure in case of crisis. ANSSI is in charge of the critical infrastructure protection and has its own crisis protocol that it would apply independently from all the financial supervisory authorities or the PRG.

C. Incident Reporting

81. The French financial sector experiences a large number of attacks, but very few cyber security events escalate to significant incidents. Large financial sector entities confirmed during the FSAP mission that they experience a constant flood of attacks, some of them very sophisticated, with the use of the latest technology tools. The DORA regime will further improve the current incident reporting practices by extending the reporting obligations to all supervised entities in case of major incidents and provides detailed templates for the content of the reports.

82. No major cyber security incidents regarding their supervised entities were reported to ACPR and BdF since the last FSAP. ACPR received an average of 2-3 voluntary incident reports since the introduction of voluntary incident reporting in 2023. The supervisory authorities are confident that they get timely information on incidents. As of December 13, 2024, for the 2024-year, 1.9 percent of total cyber events reported to ANSSI concern the financial sector, which supports the assessment of ACPR and BdF.

83. AMF was informed about several ransomware and data exfiltration incidents during the past few years. They are notified of about 20 major incidents each year, some of which are discovered through AMF being among the addressees of phishing emails sent from the compromised entities. Some of the attacks on crypto asset companies are technically sophisticated, but most of the attacks are still the results of standard phishing. AMF expects to receive a few dozen additional incidents under the new DORA reporting regime, and they expect that the reporting quality will improve.

84. AMF created an internal "first aid list" of recommendations and links to additional resources that may be used by supervisors to support entities that suffer a cyberattack. The list contains advice such as how to contact authorities and service providers to seek help for the resolution of the incident, and references to standards or guidelines for device hardening and technical settings.

85. To meet the incident information requirements of ANSSI on critical infrastructures, the French authorities intend to implement double incident reporting. DORA aims to simplify multiple reporting obligations by regulating the information exchange of the financial supervisory authorities and the NIS2 national competent authorities, so that the financial supervisor gets the report and shares the information with the NIS2 authority. However, as ANSSI does not share the critical infrastructure details with the supervisory authorities, they do not have the necessary information to know what incidents need to be shared. On the other hand, ANSSI argues that they have a 24/7 capability of incident management, while the supervisors do not have the same type of availability. ANSSI is looking for indicators of compromise and technical information to help in the incident response process while DORA authorities will look for other types of information. The

details of the incident reporting regime are still under discussion, but for the time being, some institutions may have to do double reporting if they wish to be compliant with all legal requirements.

86. The information flow on cyber risk and cybersecurity incidents is not efficient among the authorities. Cyber security risk has been repeatedly featured in the semiannual financial stability report prepared by BdF, but the data sources of the report are largely outside the French financial ecosystem. Data collected by supervisors does not feed into the financial stability report. ANSSI regularly prepares a threat landscape specifically for the financial sector, but the incidents reported to AMF do not feature in the report. BdF has gathered a lot of cyber security information from its own Computer Emergency Response Team (CERT), but that is not shared outside BdF and ACPR. The BdF CERT, the French CERT (CERT-FR) and the CERTs of large financial entities participate in the InterCERT France community. The information sources for the French financial stability reports are expected to significantly improve with the DORA reporting requirements. Aggregated data on incidents and service outages from the supervisors could be channeled into the reports without compromising the confidentiality requirements and adding more substance to the sections on cyber risk.

D. Coordination and Cooperation

87. The internal information exchange and cooperation within each authority is sufficient in general. The DORA implementation and international work in particular generate a strong need for cooperation and information sharing between different competence lines.

88. Since 2015, there is an internal cooperation group within ACPR for developing a cross-functional approach to ICT security. This ICT security network is an internal group gathering 16-20 cyber and ICT risk experts and supervisors representing each of the ACPR units involved in cyber risk supervision, dedicated to information-sharing, benchmarking, and exchange of best practices. The group meets on an ad hoc basis and its main focus has been the DORA preparedness since 2022. With the planned setup of a dedicated DORA unit, the future of the group is to be decided.

89. The banking and insurance onsite cyber risk supervisory groups have distinct methodologies and approaches. DORA unifies the hitherto fragmented supervisory expectations, introducing the same requirements for banks and insurance undertakings and overriding the distinct EBA and EIOPA guidelines on ICT risk management. Even though the requirements under DORA are exactly the same for both sectors, and many of the key players in the French financial sector are bancassurance conglomerates, so far, the two onsite cyber supervisory teams have shown no sign of convergence of practices.

90. Cooperation between the three supervisory authorities is operating well in a flexible, informal manner. Meetings are organized as needed for operational topics. Because a lot of international work and supervisory tasks require cooperation, this is often a daily activity. In the case of newly emerging topics, the international coordinators of the three authorities can help identify additional contact persons.

91. The cooperation of the supervisory authorities and ANSSI is based on formal or informal bilateral agreements, with little information sharing, but working operational interactions. Though all four authorities are members of the PRG, the group's composition involving private actors and its remit, does not allow for specific information sharing related to common topics, such as critical financial infrastructure.

92. The protection of critical financial infrastructure is currently the sole mandate of ANSSI, with ad hoc consultation or input from the other authorities. The designation of an entity as an Operator of Vital Importance (OVI) in the financial sector is made by order of the Minister of Economy and Finances on proposal of the French Treasury and the Service du Haut Fonctionnaire de Défense et de Sécurité (SHFDS). Prior the decision of designation of an OVI, ANSSI may be consulted when cybersecurity issues are at stake. ACPR, AMF and BdF may be involved in this designation process if needed and with the necessary degree of confidentiality. As mentioned before, ACPR, AMF and BdF supervisors do not know if their supervised entities are designated as critical infrastructure, because the information is classified and the law prevents them from having this information. The pertinent EU directive requires that the horizontal and sectoral criteria (including economic impact) for the identification should be documented, but these constitute classified information. Therefore, ANSSI would not be able to share them unless financial supervisors request specific accreditations to get access to this information. However, it is generally accepted practice within the EU to consult the financial authorities in establishing the sectoral criteria and economic impact factors and then also involve them in evaluating the resilience of the critical infrastructures. The new CER directive requires the determination of economic impact for service disruptions and market share to identify critical infrastructures and defines what are vital operators, essential services and critical infrastructure.

E. Conclusions and Recommendations

93. The cyber security testing practice of the supervisory authorities is in line with good practices, and the TIBER-FR framework has been implemented. In future, the TLPT required by DORA will allow mature financial institutions to perform more sophisticated tests.

94. Formal crisis management roles and procedures must be defined for cyber crisis, as they may potentially escalate to systemic crisis. The escalation thresholds, communication chains and precedence of overlapping responsibilities should be established, with clearly defined interfaces to other tools or bodies responsible for financial stability. The ENISA Best Practices of Cyber Crisis Management[26] is a useful resource that emphasizes the need for national procedures and agreements between the competent national authorities. The United Kingdom Authorities' Response Framework is also a proven model for collaboration and cooperation among the authorities. While the PRG is an excellent and mature voluntary initiative, which should be further developed and utilized to ensure private sector involvement, it does not replace the need for a public body or a

[26] https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management

specific framework involving only the public authorities in order to prepare for formalized intervention from the financial authorities.

95. Information sharing about specific incidents and general cybersecurity trends should be formalized and improved both within the authorities and among BdF, ACPR, AMF and ANSSI. All concerned authorities should be able to receive timely critical incident information data from the other authorities, when necessary, in line with the objectives of DORA.[27] Once the information sharing is operational, it may also simplify double incident reporting on behalf of the supervised entities. Incident information should be used to inform risk management decisions and identify common trends or modus operandi. Data should also be channeled and incorporated into financial stability reports and macroprudential monitoring.

96. Supervisors should increase the use of automated tools for the evaluation of documents, reports and questionnaires, and trigger actions on red flags. Even basic tools such as macros or database triggers can make the evaluation of questionnaires more efficient and eliminate potential human errors. With the increased reporting requirements under DORA, and the use of self-assessment questionnaires for offsite supervision and licensing, automation can bring efficiency gains and save valuable human resources which can be deployed elsewhere. More advanced technologies such as artificial intelligence or large language models may also be potentially utilized for more sophisticated analytical needs. Apart from some experiments with artificial intelligence to analyze or compare documents, the authorities do not use any automated tools to facilitate cyber risk supervision. Questionnaires are evaluated by supervisors without any technical aid or triggers to identify red flags. Innovative suptech developments are also carried out independently by BdF/ACPR and AMF. ACPR uses macros to evaluate LSIs' IT questionnaires and has an ongoing project with an internally developed tool for banking supervision which aims to help them process documentation.

97. An increased onsite supervisory presence should be planned for the upcoming years. Onsite supervision gives the best level of assurance about the control framework and operations of entities, and it is not possible to replace it with purely offsite activities. Therefore, the workplans and resources should be developed accordingly. The final DORA text was published in 2022, and the financial entities had time to prepare for most of the new requirements, though some of the delegated acts with the more detailed requirements were published only in July 2024. The intention of the European regulator was to raise the level of digital operational resilience by implementing and enforcing the unified requirements, so the French authorities should consider this in their annual planning.

[27] The simplification of incident reporting obligations was one of the original aims of the new regulation, requested by the Joint Technical Advice of the ESAs (JC 2019 26).