FSB FINANCIAL STABILITY BOARD

Peer Review of the Netherlands

Review report

21 November 2025

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

Contact the Financial Stability Board

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

Table of Contents

Foreword

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

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

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

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

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

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

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

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

Abbreviations

1FTL	One Financial Threat Landscape
AFM	Autoriteit Financiële Markten (Authority for the Financial Markets)
ART	Advanced Red Teaming
CCP	Central Counterparty Clearing House
CROE	Cyber Resilience Oversight Expectations
CSIRT	Computer Security Incident Response Team
CTPP	Critical ICT Third-Party Service Providers
DDoS	Distributed Denial of Service
DNB	De Nederlandsche Bank
DORA	Digital Operational Resilience Act
ECB	European Central Bank
ESA	European Supervisory Authority
EU	European Union
FMI	Financial Market Infrastructure
FSAP	Financial Sector Assessment Program
FSB	Financial Stability Board
FI-ISAC	Financial Institutions Information Sharing and Analysis Centre
GTL	Generic Threat Landscape
ICAAP	Internal Capital Adequacy Assessment Process
ICT	Information, Communication and Technology
IMF	International Monetary Fund
LSI	Less Significant Institution
MoF	Ministry of Finance
NCSC	National Cyber Security Centre
NIS2	Network and Information Systems Security 2 Directive
NVB	Nederlandse Vereniging van Banken (Dutch Banking Association)
PFMI	Principles for Financial Market Infrastructures
RTO	Recovery Time Objective
SCSI	Standing Committee on Standards Implementation
SSM	Single Supervision Mechanism
TCO	Tripartite Crisis Management Operational
TCT	Test Cyber Team
TIBER	Threat Intelligence-Based Ethical Red-teaming
TLPT	Threat Led Penetration Testing
TTPs	Tactics, Techniques and Procedures
UK	United Kingdom

Executive summary

Background and objectives

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

Main findings

In line with global trends, the Dutch financial sector faces increasing cyber threats, including Distributed Denial of Service (DDoS) attacks, ransomware, and data breaches, driven by heightened geopolitical tensions and digitalisation. The sector's reliance on third-party service providers has also introduced supply chain vulnerabilities. Despite the maturity of cyber resilience practices, the interconnectedness of the financial system and the continued evolution of cyber threats necessitates a continued focus.

The Netherlands has made significant progress in enhancing cyber resilience within its financial sector, reflecting its strong commitment over many years. The Netherlands has developed several market-leading practices such as the Threat Intelligence-Based Ethical Red-teaming (TIBER) framework, the modular voluntary Advanced Red Teaming (ART) framework and the incorporation of cyber resilience into the Internal Capital Adequacy Assessment Process (ICAAP) for banks. Comprehensive threat intelligence gathering and dissemination occurs with substantial industry input and engagement. Robust supervision programs are in place with substantial cross sectoral coordination and a focus on implementation of the European Union (EU) Digital Operational Resilience Act. There is a comprehensive national level crisis management structure, known as the Tripartite Crisis management Operational structure (TCO) in place. Within the TCO, as well as on a national level (under the name ISIDOOR), crisis management exercises are conducted.

The rapidly evolving threat landscape continues to pose challenges, necessitating further enhancements. These include (i) regularly reviewing information sharing mechanisms, (ii) continuing to support the take-up of ART testing, and (iii) considering national analysis of third-party risks.

Regularly review information sharing mechanisms

Comprehensive information is gathered and shared including threat intelligence landscapes and risk landscapes. There is strong collaboration between the industry, financial authorities and the National Cyber Security Centre (NCSC) to dynamically aggregate available information. The authorities facilitate many meetings and working groups, both formal and informal with a large and sometimes overlapping membership. Given the confidential and sensitive nature of these discussions, there may be some hesitancy disclosing all possibly relevant information to a large group. During an incident, the authorities may be hesitant to share all information quickly due to information sharing barriers and the need to balance speed with accuracy. Authorities should periodically review the purpose and membership of information-sharing forums, both in peace time and in crisis mode, to ensure their efficiency and effectiveness. During incidents, authorities

could consider providing more timely information to assist defensive actions while balancing speed and accuracy.

Continue to support the take-up of ART testing

The ART framework is an innovation to broaden the range of financial institutions ready and able to conduct advanced ethical red teaming testing, driven by high-level threat intelligence. The ability to customise and select the modules allows entities to tailor the test to align with their needs. While the ART framework provides a valuable opportunity for (smaller) firms to enhance their cyber resilience, some firms remain unprepared for such tests. DNB could develop strategies to help these entities build the resources and mature the necessary capabilities to participate in cyber resilience testing.

Consider national analysis of third-party risks

Third-party service providers are identified as one of the major threat transmission channels. DORA introduces an EU-level framework for oversight of Critical ICT Third-Party Service Providers (CTPPs), based on a register of information of all contractual agreements on the use of ICT services provided by third-party providers. At a national level, the completed information registers can facilitate assessments of concentration risk, where shortcomings in the provider's cyber resilience or disruption or failure at the provider could have systemic consequences impacting multiple institutions simultaneously. Supervisory strategies leveraging the additional comprehensive insights the information registers can provide could be developed to mitigate this risk. Analysis of the interdependencies in the register of information can also be a valuable source of information during an incident to determine the full set of firms potentially impacted and systemic vulnerabilities.

Recommendations

In response to these main findings, the peer review has identified the following recommendations to the Dutch authorities:

1. The purpose and membership of each of the working groups and information exchange meetings between the authorities and industry could be periodically validated and communicated to ensure their efficiency and effectiveness. During an incident, the authorities could consider together with industry how to share more information quickly to assist in defensive actions and try to prevent sectoral consequences.

2. De Nederlandsche Bank (DNB) could consider developing strategies aimed at advancing cyber resilience capabilities to prepare (smaller) entities to get to a position to be able to conduct a form of cyber resilience testing such as ART.

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

1. Introduction

The Netherland's first peer review, published in 2014,[3] examined steps taken or planned by the Dutch authorities to implement reforms to the macroprudential policy framework and tools, and crisis management and bank resolution. The review found that the Netherlands was at the forefront of international reforms in these areas, but there was scope for additional steps in some areas covered by those recommendations.

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

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

Box 1: Recommendations of the FSB

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

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

---

3 FSB (2014), *Peer Review of the Netherlands*, November.

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

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

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

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

Box 2: Digital Operational Resilience Act (DORA)

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

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

The testing programme should be proportional and as such can encompass tests ranging from vulnerability assessments / scans, open-source analyses, network security assessments, gap analyses, physical security reviews, source code reviews and scenario-based tests to more advanced testing by means of Threat Led Penetration Testing (TLPT).

At a national level the only remaining FSB monitored reforms yet to be completed are those subject to EU legislation. Annex 1 provides an overview of the Netherlands' implementation status of G20 financial reforms as of July 2025, including the steps taken to date and actions planned by the authorities in core reform areas (not covered in this peer review) where implementation has not yet been completed.

2. Framework for monitoring cyber risks

2.1. Cyber threat environment in the Dutch financial sector

The Dutch financial sector has been persistently targeted in cyber-attacks amid increasing geopolitical risk. Cyber-related operational losses reported by Dutch banks doubled between 2018 and 2020,[8] and DDoS and ransomware attacks on Dutch financial institutions, including their third-party service providers, have increased substantially as last reported.[9] The Dutch Data Protection Authority received over 300 cyberattacks reports from financial services firms in between 2021 and 2023.[10]

A boost in digitalisation alongside shifting working cultures gave impetus to the sector's increased exposure to cyber risks. As over half of the Dutch population adopt homeworking practices,[11] authorities noted the increased likelihood of employees disregarding digital hygiene practices,[12] and added pressure to banks' networks thus making them more prone to DDoS

8 DNB (2022), *Occasional Studies - A macroprudential perspective on cyber risk*, June.

9 DNB (2023), *Financial Stability Report - Autumn 2023*, October.

10 Autoriteit Persoonsgegevens (2024), *Report Data Breaches 2023*, April.

11 Centraal Bureau voor de Statistiek (2024), *Over half of Dutch people work from home sometimes*, March.

12 DNB (2023), *How effectively do banks and payment institutions manage cyber risk?*, June.

attacks.[13] As such, actions have been undertaken to enhance supervisory activities in the area, while better coordination mechanisms between authorities and sectors were also introduced to enhance cyber resilience. Alongside defending against attacks, supply chain risks have become a key concern. Authorities flagged that the increasing reliance on third party service providers may create operational vulnerabilities especially under heightening geopolitical tensions.[14]

Despite having a financial sector that is relatively mature in its cyber resilience practices, the rapidly evolving risk landscape still poses significant risks to the Dutch financial sector. As a result, cyber resilience has continually been on authorities' priority list when developing their supervisory plans.[15]

2.2. Roles and Responsibilities of Authorities

The Dutch financial sector framework for monitoring cyber risks, ensuring operational resilience, and addressing emerging threats involves several authorities and government departments, each with distinct responsibilities and activities.

- **The Ministry of Finance** (MoF) is the primary legislator for financial markets policy in the Netherlands. It plays a central role in the implementation of European cyber risk legislation, such as DORA and the Network and Information Security Directive (NIS2). The MoF is also actively involved in governmental crisis management and sectoral operational crisis management structures. It collaborates with DNB and the Authority for the Financial Markets (AFM) within the Tripartite Crisis Management Operational (TCO) structure to address imminent operational disruptions or threats in the payments and capital market systems. Additionally, the MoF contributes to broader national crisis infrastructures, working closely with the NCSC and other government bodies to ensure a coordinated response to cyber incidents.

- **De Nederlandsche Bank** (DNB) has a dual role as both the central bank and the prudential supervisor in the Netherlands. In its role as the central bank, DNB plays a leading role in the TCO structure, serving as the first point of contact for imminent operational disruptions or threat in the payments and capital market systems and ensuring the smooth operation of this framework. This role includes education, training and organising specific crisis exercises. The central bank part of DNB also coordinates advanced cyber resilience tests, including TIBER exercises, to assess and improve the sector's resilience to cyber threats. This work is complemented by a team that conducts strategic sectoral threat intelligence. DNB also has oversight of Financial Market Infrastructures (FMIs), focusing on operational and ICT risks and the oversight of international payment systems. In its supervision function DNB supervises, amongst others, banks,[16] payment institutions, insurers, and pension funds through both vertical and horizontal supervisory teams.

---

13 DNB (2022), *Overzicht Financiele Stabiliteit - Najaar 2020*, April.

14 DNB (2024), *Resilience in turbulent times*, November.

15 DNB (2025), *Cyber resilience in an age of geopolitical tensions*, February.

16 Within the framework of the EU Single Supervisory Mechanism

- **The Authority for the Financial Markets** (AFM) is responsible for market conduct supervision across the financial sector and is the primary regulator of investment firms, asset managers, trading venues, FMIs and collective investment schemes. Key responsibilities include supervising financial entities' compliance with cyber resilience and broader operational resilience requirements and facilitating TIBER for trading venues and other market participants.

- **The National Cyber Security Centre** (NCSC), part of the Ministry of Justice and Security, serves as the national Computer Security Incident Response Team (CSIRT) for vital sectors, including the banking sector, and central government and cross-sectoral coordinator for cybersecurity in the Netherlands. Its responsibilities include monitoring cyber threats, vulnerabilities, and incidents at the national level; providing early warnings and disseminating information about cyber risks to essential and important entities, including financial institutions and participating in the TCO structure through the Advisory Group Cyber, contributing to the coordination of responses to cyber incidents through information sharing and by taking part in the discussions. The NCSC also plays a key role in organising national cyber exercises, such as the ISIDOOR national cyber exercises, to strengthen cross-sectoral preparedness for cyber crises. As cyber security risks increase so too has staffing, with resources at the NCSC growing from 25 to 400 staff.

3. Steps taken and actions planned

3.1. Monitoring the cyber landscape and threat intelligence gathering

In an increasingly interconnected and digitised financial ecosystem, the ability to anticipate, detect, and respond to cyber threats is critical to maintaining trust, operational continuity, and systemic stability. Cyber threat intelligence has emerged as a foundational capability for regulated entities, governments and regulators, enabling informed decision-making across strategic, operational, and technical domains. The typology of cyber threat intelligence reflects a broad range of uses and audiences. Some of the common forms of cyber threat intelligence are included in Table 1 below.

Dutch authorities are very active in developing and sharing threat intelligence documents amongst authorities and the industry**.** DNB has participated in and contributed to the development of cyber threat intelligence for many years, grounded in the desire to enhance industry-wide situational awareness through fostering a shared understanding of developments in the cyber threat landscape. A dedicated team in the Data and Information Technology division continues to innovate in threat intelligence gathering by enhancing databases to intensify knowledge sharing between departments in authorities whilst respecting information sharing barriers. The Dutch version of TIBER includes general insights into common attack vectors and malicious actors, as well as real-time intelligence on cyber-attacks and adversary behaviour, encompassing technical details such as TTPs. This ensures that TIBER can meet its objective to strengthen financial system incident response capabilities and support more informed, risk-based security decision-making.

Table 1: Common forms of cyber threat intelligence

Type	Description	Primary Use Cases
Strategic threat intelligence	High-level overview of the broad cyber threat landscape, including adversary motivations, capabilities, and long-term trends.	Board-level risk posture, investment prioritisation, red team test approaches.
Operational threat intelligence	Real-time insights into specific attacks, campaigns, or incidents. Granularity designed to support rapid identification of vulnerabilities and threats.	Incident response, threat correlation, vulnerability management.
Tactical threat intelligence	Focused on threat actor Tactics, Techniques and Procedures (TTPs) and indicators of compromise (e.g. internet protocol address, domains, file hashes) at a level of detail to enable detection and response.	Security Operations Centre tuning, threat hunting, alert triage.
Technical threat intelligence	Deep technical details of threats, including exploits, malware, and vulnerabilities.	Patch management, secure configuration, vulnerability remediation, red team test techniques, tooling and tactics.

Consolidating the various inputs from internal sources and the industry, the Dutch authorities have developed two key artefacts to document cyber risk landscapes:

- **Generic Threat Landscape (GTL)** - DNB's dedicated test cyber team responsible for organising industry cyber resilience testing develops and distributes this threat landscape document to entities entering into a TIBER exercise. It outlines which threat actors are most likely relevant for the exercise and reflects on the motivations of these actors to attack the critical functions of the entity. The GTL is created annually using various internal and external sources and enriched with information from government intelligence agencies.[17] The GTL is also an input into the industry focused One Financial Threat Landscape. From the 2026 version onwards, the AFM will join the development team to make the GTL applicable for their TLPT institutions as well.

- **One Financial Threat Landscape (1FTL)** – The national level Financial Institutions Information Sharing and Analysis Centre (FI-ISAC), together with DNB central bank's policy and sector threat intelligence team and NVB (Dutch Banking Association) security team, develops and distributes a threat landscape for more general purposes, aiming to provide actionable strategic intelligence to participants in the Dutch financial system in reinforcing their defences. The 1FTL is developed with various sources of public and proprietary information, including a closed survey of cyber experts amongst the FI-ISAC's member institutions. It represents a partnership between the public and private sector and is published twice a year.

[17] The General Intelligence Agency, the Military Intelligence Agency, Team High Tech Crime of the Dutch National Police and the National Cyber Security Centre.

These threat landscapes provide valuable information for scoping penetration testing exercises and preparing the industry to respond to evolving risks. Within DNB the 1FTL is shared with internal affairs, as well as supervision and oversight. The GTL, however, is not currently used for developing supervisory priorities. Although GTL is developed specifically for penetration testing, and therefore has a restricted circulation, some of the information, complemented with more specific intelligence, is shared through dedicated interagency coordination mechanisms. For example, following a particular cyber incident that occurred several years ago, DNB and AFM collaborated to create an internal approach to share information relating to technology and cyber. This has seen the creation of the 'Cyborg' forum comprised of representatives from DNB's horizontal Information Technology (IT) specialist teams, the crisis management team, the intelligence and testing team, the supervision IT expertise centres, the oversight team, AFM's dedicated horizontal IT team and cyber staff that are responsible for managing DNB's and AFM's own cyber risks. Since 2025, strategic intelligence gathered by the team that develops the GTL is used in a quarterly strategic intelligence overview that is shared with all those in cyborg. At a supervisory level, DNB and AFM maintain individual institution risk overviews alongside sector specific cyber dashboards comprised of cohorts of institutions, based on institutional self-assessments and supervisory information.

The authorities facilitate or participate in many important forums for engagement with the industry. These forums provide an environment in which authorities and industry can work together to combat rapidly evolving threats. Periodic touchpoints with the industry can be a valuable two-way flow of information for the authorities, CSIRT, ISACs, industry and other participants. These forums have large and sometimes overlapping membership and depending on the attendees those engaged may be hesitant to share information in as open a manner, particularly when it can include confidential information or reveal a potential vulnerability.

The NVB also plays an active role to facilitate industry forums in addition to its role as a founding member of the local FI-ISAC and member of the global FS-ISAC. Eight staff are dedicated to security topics including cyber risk with a dedicated liaison officer embedded in the NCSC to work on banking sector issues.

At a national level, the NCSC plays an important role when it comes to monitoring the cyber landscape and threat intelligence gathering. With its tasks of monitoring the incidents, disseminating information about risks and incidents and participating in the international network of CSIRTs, the NCSC has a unique information position which is beneficial to all vital sectors including the financial sector.

3.2. Supervision of cyber resilience in the financial sector

Following significant DDOS attacks in 2012, cyber security oversight has grown into a mature and well-connected supervisory framework with primary coverage by DNB and strong connection between the authorities. In terms of DORA, DNB is the primary prudential supervisor with responsibility over banks that are Less Significant Institutions (LSIs), payment institutions, electronic money institutions, insurers, pensions funds, clearing institutions, and issuers of asset-referenced tokens. Supervisors are split between horizontal and vertical teams with a dedicated horizontal team focused on digital operational resilience for LSIs and Significant Institutions, as well as a dedicated horizontal team focused on the digital operational resilience of insurers and pension funds. In the context of cyber and operational resilience, DNB assumes sector-wide roles

such as crisis management, threat intelligence, cyber resilience testing, and oversight as part of its banking function, while also incorporating supervisory functions within its organisational structure. DNB also emphasises education and transparency in their supervisory approach including organising seminars for the industry, publishing supervisory expectations and the general results of large-scale supervisory exercises. In terms of DORA, the AFM has direct supervisory oversight of, among others, trading venues and investment firms. For the FMIs which fall under the purview of both AFM and DNB the agencies collaborate and the exchange of information necessary for supervision is permitted via a covenant. AFM primarily focuses on supervision through monitoring. With the implementation of DORA, both AFM and DNB have a legal mandate to include TLPT as part of the supervision approach. While DNB and AFM both oversaw Threat Intelligence Based Ethical Red teaming (TIBER) tests before DORA, in which large financial institutions participated voluntarily, the DORA legal framework makes TLPT obligatory for the largest financial institutions. The TIBER-EU framework is used to guide TLPT testing.

Third-party service providers are identified as one of the major threat transmission channels under 1FTL. The Dutch authorities are facilitating the collation and submission to the ESAs the register of information on all contractual agreements on the use of ICT services provided by third-party providers. The ESAs will determine from these registers EU level designated CTPPs[18] which will be subject to direct oversight by the relevant ESA through Joint Examination Teams. The Dutch authorities do not currently have a structured approach to interact with third-party service providers, although ad-hoc discussions and inspections have taken place.

A technology tool is under development to analyse the concentration risk in outsourced activities with completion expected in early 2026. The initial plans for this tool should be supplemented with the completed information registers required by DORA. This tool could then facilitate assessments of concentration risk where shortcomings in the provider's cyber resilience or disruption or failure at the provider could have systemic consequences impacting multiple institutions simultaneously. Supervisory strategies could be developed to mitigate this risk. Analysis of the interdependencies in the register of information can also be a valuable source of information during an incident to determine the full set of firms potentially impacted and systemic vulnerabilities.

Cooperation and information sharing are systematically embedded within the overall approach to supervision which enhances the quality of supervisory practices across the financial sector. Regular meetings are held between the IT experts from LSI and Significant Institution account supervision teams and the horizontal IT support team to facilitate the exchange of knowledge on IT and cyber-related matters and to promote consistency in supervisory practices. Coordination on DORA implementation and supervision is supported through established meetings with cross-sectoral DORA coordinators.

DNB has been a pioneer in intelligence led red team testing. In 2016, building on a framework from the UK, DNB developed the TIBER framework to simulate cyber-attacks in a controlled manner to test and help improve financial institutions' detection and response capabilities. As the framework matured, the European Central Bank (ECB) and several other central banks in the EU evolved this framework into an EU-wide framework called TIBER-EU. Under DORA large financial entities (across all sectors) will be required to undergo a TLPT every three years, which

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

leverages the principles of TIBER-EU. While developed before the introduction of DORA, TIBER-EU is a well-adopted testing framework that could fulfill the requirements of DORA. As such, DNB aims to leverage the TIBER-EU testing framework as the TLPT requirement for financial entities subject to DORA and collaborate with other national competent authorities for joint exercises. A dedicated Test Cyber Team (TCT) in the central banking function of DNB oversees the TIBER tests for LSIs and, where required, supports or oversees, tests for Single Supervisory Mechanism (SSM) entities. The team is also responsible for promoting learning and knowledge sharing between red team and threat intelligence providers by hosting annual conferences and maintaining a trusted community, called Resilience testing Community, between financial entities for exchanging knowledge and learnings regarding resilience testing.

To complement TIBER, DNB launched the ART framework in 2024 as a flexible and potentially smaller scope option for cyber resilience testing aimed at firms that want to improve their cyber maturity and are looking to undergo periodic cyber resilience tests based on their size, maturity and learning appetite. Around 50 firms have the potential to conduct an ART test, ten tests have been undertaken so far in 2025, and DNB anticipates between five and seven tests can be prepared a year per test manager. ART allows institutions to select from a range of modules encompassing physical intrusion, incident response and network and application security. [19] The optional Gold Team module facilitates a crisis management exercise to evaluate organisational resilience in the aftermath of a cyber crisis. This flexible choice of modules allows entities to select those most relevant to their cybersecurity posture, maturity level and available resources, thereby optimising their cybersecurity efforts and investments. This also allows the TCT at DNB to expand their test offering to a wider set of entities, supporting the goal of allowing firms without the resources to conduct a TIBER test to perform cyber resilience testing in such a way as to advance their maturity of resources and capabilities to a level ready for TIBER. To ensure appropriate use of DNB resources, there is a mechanism in place to identify readiness for ART by firms, with some firms within the target group not yet mature enough for the test. DNB could consider developing strategies aimed at advancing cyber resilience capabilities to prepare (smaller) entities to get to a position to be able to conduct a form of TLPT such as ART.

DNB also commits substantial resources into developing sector- and ecosystem-wide business recovery drills. DNB continuously assesses the outcomes of penetration tests, red team exercises, and supervisory activities to evaluate the level of cyber resilience and identify where further work is required. Within the TCO, the education, training and exercising program is used to keep participants up-to-date and to evaluate the approach. One of the areas identified was the importance of cross-sectoral coordination in times of crisis, and hence in addition to exercises specifically designed for the financial sector, a comprehensive nationwide periodic exercise program is in place to improve the country's overall preparedness for cyber crises. This program, ISIDOOR[20] organised by the NCSC, is designed not only to test response capabilities but also to strengthen coordination and collaboration across public and private institutions. It also provides a practical platform for rehearsing crisis management procedures in realistic scenarios with financial institutions among the key participants.

---

19 DNB, (2024), *Advanced Red Teaming (ART) Framework*, April.

20 NCSC, *ISIDOOR - What does the NCSC do for you?*

Banking

DNB integrates cyber risk management into different aspects of their supervisory and regulatory frameworks. A targeted sample based horizontal review on cyber hygiene was undertaken in 2024 to identify common issues in the banking and payment service providing sectors. All institutions, including those not sampled, have been requested to explicitly address the common issues within their risk management processes. DNB has also taken the innovative step of integrating cyber resilience assessments into the ICAAP. In 2024 banks were required to conduct scenario analyses and stress tests on cyber scenarios as part of their Pillar 2 evaluation and hold capital accordingly. Going forward DNB will be looking at ways to improve ICAAP submissions and operational risk scenarios including how cyber risk should be incorporated into ICAAP expectations.

Financial Market Infrastructures

DNB and AFM have shared responsibilities for oversight over the various types of FMIs; however, DNB has primary cyber security responsibility for all FMIs. The cyber security supervisory program for FMIs follows a risk-based approach including periodic self-assessments, follow up supervisory activities and an annual on-site inspection. A risk profile for each FMI is determined based on the risk scores in categories aligned to the Principles for Financial Market Infrastructure (PFMI).[21]

The ECB built upon the PFMI to develop further expectations in the Eurosystem's Cyber Resilience Oversight Expectations (CROE) which DNB relied on to conduct risk-based cyber-related assessments of payments systems and FMIs. The oversight of FMIs is now focused on preparation for DORA. A gap assessment questionnaire based on guidance from the European Securities and Markets Authority was distributed to FMIs and followed by bilateral discussions. In general DNB observed that prior compliance to the CROE offered a strong basis for compliance with DORA with any identified gaps requiring mitigation plans.

Onsite reviews of Central Counterparty Clearing Houses (CCPs) are conducted on a rotating basis. DNB's participation in the internal cyber working groups supports these reviews. The Dutch Authorities conducted 'Project Prometheus', an innovative assessment of the resilience of a few FMIs against hybrid attacks by state actors. The assessment leveraged information obtained through survey and subsequent discussions with the institutions and has assisted the authorities gain insight where further work is warranted.

DNB and AFM incorporate a risk-based review of business continuity planning into their supervisory oversight. Under DORA, financial entities are required to establish a comprehensive cyber security business continuity policy within their risk management framework. This includes tailored plans, procedures, and technologies for containment and triage of cyber security-related incidents to ensure continuity of critical functions. DNB requires FMIs to review and test their business continuity and recovery plans, which may include cyber and hybrid scenarios, on at least an annual basis**.** FMIs are responsible for identifying their own critical processes (via Business Impact Assessments) and determining their relevant discontinuity scenarios. DNB

[21] BIS (2012), *Principles for financial market infrastructures*, April and see also CPMI and IOSCO (2016), *Guidance on cyber resilience for financial market infrastructures*, June

reviews the outcomes of testing of the plans and requires any lessons learns to be incorporated. The PFMI requires that FMIs are able to resume operations within two hours (2h Recovery Time Objective (RTO)) for their critical activities following disruptive events, and for CCPs to settle all transactions by end of business day. DNB ensures that these specific requirements are tested during the regular business continuity and disaster recovery tests, and the results are assessed against the 2-hour RTO.

Trading Venues

The Dutch financial sector has experienced significant growth following Brexit, as many financial institutions and trading venues have relocated or established operations in the Netherlands to maintain access to the EU's single market**.** This expansion has strengthened the Netherlands' role as a key financial hub within the EU. However, it has also introduced new complexities for local supervisory authorities. The 2024 IMF FSAP reports that several large trading platforms have established themselves in the Netherlands since Brexit, increasing Dutch platforms' share of European trading (including the United Kingdom (UK)) to over 30 percent from 5-10 percent pre-Brexit, with daily turnover volumes of EU-listed shares exceeding those in London.[22]

A proportion of the trading venues operating in the Netherlands are subsidiaries of parent companies based overseas, particularly in the UK, and cyber security operations are largely consolidated in the parent jurisdiction. Dutch supervision and access to cyber security operations may therefore depend on cooperation and support from the institution's home office and local home authorities. While this may not pose a clear identifiable risk to supervision of the domestic Dutch entities, the *FSB Recommendations to Achieve Greater Convergence in Cyber Incident Reporting* identifies legal and confidentiality concerns as potential barriers to effective international cooperation.[23] Also, an ESMA peer review report of National Competent Authorities (NCAs) identifies cooperation across NCAs as crucial to ensure effective supervision of firms' cross-border activities.[24] Cross-border arrangements are often shaped by individual authorities' willingness to share information and their historical relationships, resulting in a fragmented network of bilateral agreements. The recently released FIRE consultation paper further identifies that cooperation among authorities supports firms' incident response and recovery. Partnerships and engagement with home authorities becomes all the more important as the Netherlands' role as an EU passporting hub for international operations continues to grow.

The AFM has primary responsibility for the supervision of trading venues. Cyber security supervision is largely performed through monitoring of the cyber resilience functions of some of the supervised entities located in their home jurisdictions. The AFM assesses qualitative and quantitative information such as the asset classes, trading volumes, market share, risk management arrangements and the ESMA risk heatmap to set individual oversight priorities and determine supervision intensity. The eight largest trading venues receive enhanced supervisory focus as they are materially more significant than the remainder of the portfolio. To meet DORA expectations, AFM hired additional staff dedicated to trading venue and proprietary traders'

---

22 IMF (2024), *Kingdom of the Netherlands–The Netherlands: Financial System Stability Assessment,* April. This percentage is for EU-listed shares and will be different for other asset classes.

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

24 ESMA (2022), *Peer review on supervision of crossborder activities of investment firms*, March

supervision and has developed a specific DORA supervision programme. Based on DORA's qualitative requirements three trading venues have been designated to complete a TLPT and the DNB has designated an additional two entities to conduct a TLPT. DORA represents a significant increase in expectations of the management of ICT, consequently AFM conducted two pilot assessments in 2024 to assess readiness to comply. AFM has also undertaken regular public outreach to familiarise institutions with the expectations of DORA. Additionally, the large trading venues are incorporated into the TCO structure through the capital markets advisory group and are included in the ISIDOOR exercise.

The AFM interprets the TIBER-EU program as a strategic tool to enhance the cyber resilience of the Dutch financial sector, particularly trading venues. It applies the framework both for mandatory TLPT under the European DORA regulation and for voluntary tests offered to supervised entities. By consistently using the TIBER-EU framework, the AFM aims to ensure a uniform approach to resilience testing, foster collaboration between financial institutions and regulators, and build a community focused on sharing knowledge and improving learning outcomes in cybersecurity.

3.3. Incident reporting, communication and coordination of response

The NCSC operates an incident reporting system that supports a wide range of organisations, including financial institutions, allowing for both mandatory and voluntary reporting of cyber incidents. While financial institutions must report major ICT-related incidents directly to the sectoral supervisors (DNB or AFM), financial entities within scope of NIS2 are also required to notify the NCSC with the same information. The NCSC's reporting process is designed to capture detailed incident information, facilitate secure communication, and, where necessary, provide advice or coordinate with other authorities. For most financial sector incidents, the primary reporting responsibility remains with the relevant financial supervisors, with the NCSC acting as a central point for incidents that have broader national cross – sectoral or critical implications.

During an incident, the supervisory authority is constrained by an information sharing barrier intended to protect confidential supervisory information. DNB central bank team or NCSC, if involved, must verify the information received and consider to what extent they can assist the affected institution and the industry more broadly. Within DNB Cyborg and the Core Group Cyber (consisting of managers from IT supervision, central bank and the CISO office) are leveraged where possible, sharing threats and incidents if an incident covers multiple core tasks of DNB. Whilst significant efforts are made across the NCSC and the supervisory authorities to share knowledge and support in a crisis, there could be additional focus on providing relevant information during an incident to assist in taking defensive action. This must balance the requirements of information sharing barriers and the benefits of speed against accuracy.

The Netherlands has developed the TCO structure, comprising DNB, AFM and the MoF, with NCSC as a participant, to ensure coordination and collaboration in safeguarding financial stability during major operational disruptions, particularly those affecting critical financial core infrastructure. It contains a permanent secretariat staffed by DNB, AFM and MoF, that is supported by five specialised Advisory Groups, including one focused on cybersecurity. Financial Core Infrastructure designated institutions report operational disruptions to DNB permanent secretariat staff in the case of imminent external effects, major operational or financial problems or extensive media attention. The TCO structure maintains an active network, holds

an annual conference and conducts regular preparedness activities, including participating in ISIDOOR cyber exercises, organised by NCSC. It also conducts its own annual crisis management exercises as part of its Educate-Train-Exercise programme, which emphasises refining crisis plans through scenario-based "playbooks" (eg ransomware response protocols).

The NCSC's services have expanded to include operational coordination during major ICT crises and serving as a cybersecurity collaboration platform and the sectoral CSIRT for both public and private sectors, with a particular focus on vital infrastructures**.** Recent initiatives have further increased its role by intensifying cooperation with other government cybersecurity organisations; establishing a unified reporting platform for threats and vulnerabilities; and preparing for integration into a single national cyber organisation in early 2026. These steps aim to ensure timely alerts and support for organisations of all sizes and sectors in the face of evolving cyber threats. In view of its expanding role, the authorities should continually consider how crisis support services can be provided effectively and efficiently.

DORA requires reporting to the competent authority of major ICT-related incidents according to a standardised timeline with common information fields. There is also the ability to report significant cyber threats voluntarily. As more incident data is collected, DNB plans to share high-level observations with financial entities through supervisory dialogue. At the EU level, DNB participates in the SSM IT Risk Network, where cyber incidents, root cause analyses, and lessons learned are shared bimonthly to enhance the incident reporting lifecycle.

4. Conclusions and recommendations

The Dutch authorities have long had a strong commitment to enhancing cyber resilience and have developed several market leading practices such as the TIBER framework, the modular ART framework and incorporation of cyber resilience into the ICAAP for banks. The opportunity to participate in crisis management exercises such as ISIDOOR (multi-sectoral test) for the TCO structure and the Gold Teaming module (an individual exercise as part of an ART test) facilitates hands-on resilience testing. The TCO framework is comprehensive, clear, and well understood by its members. Although only launched in 2024, there has also been take up of the Gold Team module, also by firms not part of the TCO structure. Additionally, the authorities and government agencies demonstrate high levels of cooperation and information sharing with each other and with the industry. The NCSC plays an extensive role across information gathering, disseminating, crisis management testing and direct support in a crisis under specific circumstances. The active role of NVB and the creation of a national FI-ISAC provide a range of opportunities and forums to share information formally and establish networks for informal information sharing. Formal information sharing includes comprehensive threat intelligence documents such as the 1FTL.

At the same time, steps can be taken to further enhance cyber resilience. These include regularly reviewing relevant information sharing mechanisms; continuing to develop strategies to increase maturity across the industry; and considering a national analysis of third-party risks.

4.1. Regularly review information sharing mechanisms

The Dutch authorities have established a wide range of information sharing mechanisms including various standing and ad-hoc working groups and meetings, with large and sometimes

overlapping membership. It is important that the mandates and membership of these groups are regularly reviewed and shared with members, such that participants are aware of the respective positioning and purposes of different groups. This way, members can ensure the right experts are included in the appropriate forums, and more importantly, gain more confidence in sharing potentially confidential or sensitive information. Additional consideration could be given to how best to share relevant information quickly to both the impacted institution and the industry during a crisis to assist in taking defensive steps.

Recommendation 1: The purpose and membership of each of the information exchange meetings between the authorities and with industry could be periodically validated and communicated to ensure their efficiency and effectiveness. During an incident, the authorities could consider how to provide more information quickly to both the impacted institution and the industry to assist in defensive actions.

4.2. Continue to support the take-up of ART testing

The development of ART targeted firms to support the maturing of their cyber resilience capabilities. Around 50 firms are eligible for ART, with some still not of sufficient maturity to be eligible to conduct an ART test. This leaves vulnerabilities in these firms untested, and a lost opportunity for building their capabilities which the DNB could address with additional supervisory focus.

Recommendation 2: DNB could consider developing strategies aimed at advancing cyber resilience capabilities outside of penetration testing to prepare entities to get to a position to be able to conduct a form of cyber resilience / red teaming testing such as ART.

4.3. Consider national analysis of third-party risks

Whilst DORA introduces a register of information on third-party ICT contracts, the analysis under DORA is limited to identifying critical third-parties at an EU level to then be subject to direct supervision. The Dutch authorities are developing a technology tool to analyse concentration risk at a national level. The initial plans should be supplemented with the new information available under DORA. When the information registers are of good quality, there will be a rich source of information for national authorities to analyse at a national level for concentration risk, interdependencies and possible channels of systemic risk. This analysis could be done using parameters such as service provider dependency, geographical and intra-group concentration, supply chain overlaps, and substitutability.[25] Supervisory strategies could be developed to mitigate this risk. Analysis of the interdependencies in the register of information can also be a valuable source of information during an incident to determine the full set of firms potentially impacted and systemic vulnerabilities.

Recommendation 3: The authorities should progress plans to establish a national analysis of information including the DORA registers of information to identify critical third-party providers for the Netherlands. When the collection of the DORA register of information matures, authorities should be in a better position to assess concentration risk and define a supervisory strategy to address domestically critical third-parties.

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

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

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

IMPLEMENTATION STATUS OF REFORMS IN PRIORITY AREAS

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

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

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

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

IMPLEMENTATION STATUS OF REFORMS IN **OTHER AREAS**

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

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

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

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

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

Other information	Latest IMF-World Bank FSAP: April 2024	Latest FSB Country Peer Review: 2014	Home jurisdiction of G-SIBs: yes	Signatory of IOSCO MMoU: yes	Signatory of IAIS MMoU: yes

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

Reform area	Steps taken to date and actions planned (including timeframes)
Final Basel III framework	
Risk-based capital	In the Netherlands, the implementation of the Final Basel-III framework is taking place in accordance with the EU legislative process. The reforms of the Capital Requirements Regulation (CRR3), which transpose the Final Basel III reforms into the EU regulatory framework, have entered into force starting January 1st, 2025. Moreover, the implementation of the 6th Directive on Capital Requirements (CRD VI) is currently taking place and will complement CRR3. The provisions of CRD VI are expected to have been implemented and to have entered into force on January 1st, 2026. Completing the Final Basel III framework also requires implementation of the market risk capital requirements, known as the Fundamental Review of the Trading Book. These provisions will be implemented in accordance with the EU legislative process as well. The European Commission has, through an implementing act, decided to postpone implementation of these provisions until January 1st, 2027, subject to approval by co-legislators.
Resolution	
Resolution planning for systemic CCPs in more than one jurisdiction	A CMG is established, resolution planning has commenced, a CCP-specific cooperation Agreement is signed and in the resolution plan of the previous resolution planning cycle a first resolvability assessment has been performed. These steps complete implementation in this area.
Non-Bank Financial Intermediation	
Securities financing transactions	The minimum standards for cash collateral re-investment, regulations on re-hypothecation of client assets and minimum regulatory standards for collateral valuation and management have been implemented in sector-specific EU-legislation. With regards to the numerical haircut floors on bank to non-bank transactions: according to Article 519d of the CRR3, the European Banking Authority, in close cooperation with the European Securities and Markets Authority, shall, by 10 January 2027, report to the Commission on the appropriateness of implementing in Union law the minimum haircut floor framework for securities financing transactions. On the basis of the report referred to in paragraph 1 and taking due account of the FSB recommendation to implement the minimum haircut floor framework for securities financing transactions, as well as the related internationally agreed standards developed by the Basel Committee for Banking Supervision, the Commission shall, where appropriate, submit to the European Parliament and to the Council a legislative proposal by 10 January 2028.