EUROPEAN
COMMISSION

Brussels, 10.3.2026
COM(2026) 119 final

REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT

on the preparedness in the EU financial sector

1. Introduction

The European Union is facing growing risks and unprecedented threats in multiple sectors. These risks range from heightened uncertainty, geopolitical tensions and conflicts, cybersecurity and information manipulation risks, to climate change and increasing risks of natural hazards. To boost the EU's ability to anticipate, prevent and respond to these threats, the Commission and the European External Action Service (EEAS) jointly presented on 26 March 2025 the preparedness union strategy[1]. The EU's financial sector plays a key role in maintaining vital societal functions under all circumstances. This is why, as part of the preparedness union strategy, and delivering on action 25 of the annex of the joint communication, the Commission is undertaking a comprehensive assessment of the level of preparedness in the financial sector. In particular, it is assessing the sector's capacity to continue to carry out its critical functions, such as making payments and funding the economy, under all circumstances.

The EU's financial services legislation is built on a solid tradition of prudence, precaution, resilience and anticipation. The objectives are clear: to preserve financial stability, the orderly resolution of any failing financial institutions, crisis management and deposit insurance, investor protection and market integrity. The EU completed a comprehensive overhaul of its prudential rules and of the banking supervision architecture following the Great Financial Crisis initiated in 2007. These reforms have strengthened the EU's financial institutions, its capital markets and financial market infrastructure providers.

Today the EU's financial sector has achieved a high level of resilience by consolidating three pillars: (i) risk-based capital for banks and financial institutions, (ii) governance and transparency requirements and (iii) supervisory cooperation mechanisms across Member States and across sectors. The EU has put in place policies and principles that produce continued assessments of the risks of extreme events in operational risk frameworks, business continuity and contingency plans.

The EU framework has been tested by several episodes of crises in recent years, such as the COVID-19 pandemic, Russia's aggression of Ukraine, the US regional banking crisis and Credit Suisse crisis in 2023, power blackouts, cyberattacks and hybrid incidents. In the face of these crises, the EU financial sector has demonstrated robustness and resilience. Authorities at EU and national levels have acted swiftly and effectively.

In general, preparedness is not static; it is a dynamic, forward-looking state. It requires a continuous cycle of planning, training, equipping, testing, evaluating and improving. It requires a focus on readiness to deal with all hazards by anticipating risks, developing capabilities, coordinating across sectors (government, private, public) and learning from past events to build resilient communities that can prevent, protect and recover when a crisis hits. This applies equally to the financial sector.

[1] The Commission and the EEAS issued a joint communication on the preparedness union strategy.

This report provides an overview of the current state of preparedness of the EU financial sector, building on continued discussions with the European Central Bank, the European Supervisory Authorities, the European Systemic Risk Board, the Single Resolution Board, Member States and the financial services industry.

2. Preparedness in the EU single market

At EU level, preparedness in the financial sector has improved over the past few years through legislative measures and by creating governance structures at EU level that reflect the cross-border nature of the EU financial sector. Governance is based on two pillars: EU regulation and EU authorities. This structure is complemented by a suite of measures taken at euro area, regional (involving several Member States) and Member State level.

2.1 EU legislation governing the financial sector

The financial sector is regulated by both sector-specific and cross-cutting legislation.

Sector-specific legislation

Sector-specific legislation includes the Capital Requirements Directive and Regulation (CRD/CRR)[2], Solvency II[3], the Markets in Financial Instruments Directive II (MiFID II)[4], the European Market Infrastructure Regulation (EMIR)[5] and the Central Securities Depositories Regulation (CSDR)[6]. These pieces of legislation put in place prudential requirements to ensure the resilience, stability and sound functioning of financial institutions, financial infrastructure and the financial system.

From the preparedness angle, several pieces of sector-specific legislation set out requirements governing operational risk management, operational resilience, ICT resilience, business continuity and crisis management. For example, in the banking sector, the CRR/CRD, the Bank Recovery and Resolution Directive (BRRD)[7], the Single Resolution Mechanism Regulation

---

2 Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (CRD);
Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and amending Regulation (EU) No 648/2012 (CRR).

3 Consolidated text: Directive 2009/138/EC of the European Parliament and of the Council of 25 November 2009 on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II).

4 Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (MiFID II).

5 Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (EMIR).

6 Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012.

7 Directive 2014/59/EU of the European Parliament and of the Council of 15 May 2014 establishing a framework for the recovery and resolution of credit institutions and investment firms and amending Council Directive 82/891/EEC, and Directives 2001/24/EC, 2002/47/EC, 2004/25/EC, 2005/56/EC, 2007/36/EC, 2011/35/EU, 2012/30/EU and 2013/36/EU, and Regulations (EU) No 1093/2010 and (EU) No 648/2012, of the European Parliament and of the Council (BRRD).

(SRMR)[8] and the Deposit Guarantee Schemes Directive (DGSD)[9] ensure that banks have the resilience to withstand a broad range of potential risks, including extreme events. Banks are expected to implement robust governance and risk management frameworks, including enhanced business continuity, communication and recovery plans, to address a wide range of risks effectively. Key features of the measures to address the risk scenarios, both precautionary and reactive, include specific *ex ante* requirements for banks such as recovery plans and resolution plans, as mandated under the SRMR and the BRRD.

In addition to banks, insurance undertakings regulated under Solvency II, investment firms under MiFID II, and market infrastructures such as central counterparties (CCPs) and central securities depositories are subject to similar requirements to ensure operational resilience, ICT risk, business continuity and crisis management. These are complemented by requirements to enhance recovery and resolution planning where needed. Asset management and non-bank financial intermediation are also subject to a broad and increasingly comprehensive EU regulatory framework, including the Undertakings for Collective Investment in Transferable Securities Directive, the Alternative Investment Fund Managers Directive and the Money Market Funds Regulation. These instruments impose requirements on risk management, liquidity management, leverage, valuation and transparency, to foster the stability of the sector. Action to develop the Savings and Investments Union (SIU) by building up the EU financial sector's capability to connect savings with productive investments, thus improving risk sharing and diversification across the EU financial sector, will improve its overall resilience and preparedness.

The European Central Bank (ECB) – the single supervisor for banks in 21 Member States – and national competent authorities within and outside the euro-area place the financial and operational resilience of banks at the centre of their supervision priorities. Banks are notably encouraged to duly take account of geopolitical risks and integrate them into their risk management processes. Exposures to counterparties in non-EU countries, potential impacts of foreign sanctions on exposures and dependencies on external service providers and infrastructures should be considered by banks in that context. In addition, banks should develop a robust governance framework and protection against cyber threats and other threats that can affect their operational resilience. This includes measures to increase safety and protect against physical damage. Beyond institution-specific measures, the EU banking prudential framework also addresses broader system-wide and cross-border risk channels.

The crisis management framework creates a toolkit available to use when the viability of the provider of a critical function is under threat. The revised Crisis Management and Deposit Insurance framework for banks, on which a political agreement was reached in June 2025,

---

8 Regulation (EU) No 806/2014 of the European Parliament and of the Council of 15 July 2014 establishing uniform rules and a uniform procedure for the resolution of credit institutions and certain investment firms in the framework of a Single Resolution Mechanism and a Single Resolution Fund and amending Regulation (EU) No 1093/2010 (SRMR).

9 Directive 2014/49/EU of the European Parliament and of the Council of 16 April 2014 on deposit guarantee schemes (DGSD).

marks an important step in making the EU's crisis management system even more effective, in particular for smaller and medium-sized banks.

One important aspect of preparedness in the financial sector is to have payment instruments available for the public, both cash and electronic payments. To ensure **cash** is available under all circumstances, at Eurosystem level, a key measure is to maintain common strategic stocks of euro banknotes. The ECB is the central coordination and decision-making body and runs periodic crisis management exercises, including potential crisis communication. At national level, national central banks (NCBs) maintain business continuity plans to ensure that cash withdrawals and deposits remain available.

In parallel, the proposal on the legal tender of euro banknotes and coins, put forward by the Commission on 28 June 2023, seeks to ensure that euro cash remains widely accepted for payments and easily accessible for people, businesses and public entities across the euro area. Requirements to maintain a healthy cash infrastructure in normal times support the availability of cash in contingency situations. The Commission proposal did not include a provision on resilience, but the Council added this in its negotiating mandate, which requires Member States to have in place a cash resilience plan or combination of equivalent measures.

In addition, the Payment Services Directive 3 (PSD3), on which a political agreement was reached in November 2025, aims to boost cash access in shops by allowing retailers to offer cash withdrawals without a purchase (i.e. cash-in-shops), up to a certain limit. This makes the use of cash more convenient, especially in rural areas, by clarifying rules for retailers and ATM operators.

In addition to cash availability, it is critical to maintain the continuity of **payment services** including card payments, account-to-account transfer-based payments (including via mobile phones), access to payment accounts and the ability to make deposits, in order to maintain public confidence in the financial system, maintain public order and ensure the basic functioning of the economy in the event of a widespread disruption by providing the public with continued access to basic services.

The current Payment Services Directive 2 (PSD2) regulates other aspects including the management of operational and security risks and the reporting of major incidents. The aim is to strengthen the security and resilience of payment systems across the EU.

The Eurosystem promotes the safety and efficiency of payment systems. It has put in place oversight requirements to address the key risk scenarios identified for the European payment ecosystem. The frameworks set out a comprehensive set of requirements for managing operational risks. These include measures for business continuity management and timely recovery, along with specific provisions for information security, cyber resilience, physical security, outsourcing, IT risk management and other related areas. The framework covers electronic payment instruments (like cards, direct debits, credit transfers, e-money and digital wallets), as well as the schemes (e.g. card networks) and applications (e.g. e-wallets) that enable their use.

To provide greater protection, Article 15 of the ECB Regulation for Systemically Important Payment Systems (SIPS) sets out other requirements. For example, it requires systems to ensure recovery within two hours (including via the use of secondary sites) and that SIPS operators are able to complete the settlement of all payments due on a day by the end of the business day when the incident occurred.

The project to create a digital euro – a digital form of cash, complementing physical cash and private payment solutions – would give the public an additional method of payment, while simultaneously fostering digital and financial inclusion. As the first unified pan-European payment system, the digital euro would also help safeguarding the international role of the euro. By strengthening the EU's open strategic autonomy and expanding the range of available payment instruments, the digital euro project aims at further bolstering the overall resilience of payment services. As for the proposal on the legal tender, the Council added additional provisions to further boost the resilience of the digital euro. In this context, EU Digital Identity (EUDI) wallets will be interoperable with digital euro user interfaces, ensuring secure and seamless user authentication.[10]

Cross-sectoral legislation in the financial sector

To complement the financial legislation highlighted above, the Digital Operational Resilience Act (DORA) is a financial sector-specific piece of legislation that applies across the entire EU financial sector. It covers 20 different types of financial entities including credit institutions, payment service providers, financial market infrastructures, insurance companies, credit-rating agencies and asset managers.

DORA puts a strong focus on the resilience of financial entities, on their level of preparedness to withstand potential disruptions in the ICT field, and on managing risks arising from the dependence of financial entities on ICT third-party service providers, including systemic and concentration risks posed by ICT providers that are critical to the EU financial sector. DORA establishes a harmonised and robust framework for strengthening the EU financial sector's ability to prevent, withstand, respond to and recover from ICT-related disruptions. Financial entities must put in place a comprehensive framework for managing ICT risk – covering governance, asset inventory, risk identification, protection, detection, response, recovery and continuous improvement. This ensures that vulnerabilities and resilience in systems and processes are managed proactively. Financial entities are also required to detect, classify and report major ICT-related incidents to competent authorities using agreed definitions, thresholds and timelines to enable coordinated responses across jurisdictions. It mandates regular testing and assessments of their resilience and preparedness processes, tools and arrangements.

[10] The European Digital Identity Framework establishes a secure and trustworthy ecosystem for digital identification and authentication and the use of digital evidence which will be available to all EU citizens by the end of 2026. European Digital Identity Wallets will directly benefit the resilience and preparedness of the EU's financial sector against crisis, protecting against fraud and identity theft in payments, customer onboarding and other financial services.

Financial entities must also manage risks associated with the use of third-party ICT service providers, especially critical third-party providers (CTPPs). DORA mandates financial entities to perform due diligence on concentration risks before entering into new contracts with ICT third-party providers (TPPs). DORA has an oversight mechanism, where the three European Supervisory Authorities (ESAs)[11] oversee critical ICT third-party service providers (CTPPs) on a pan-European scale, enhancing overall digital operational resilience across the EU's financial sector. In November 2025, the ESAs published the list of designated critical ICT third-party providers under DORA. The DORA framework is particularly well suited to manage cybersecurity, connectivity, preparedness and operational risks with a strong international dimension.

Besides DORA, which is *lex specialis* for the financial sector, the financial sector is also covered by horizontal cooperation arrangements on physical and digital resilience under the Critical Entities Resilience (CER)[12] Directive and the NIS2 Directive.

The CER Directive creates an overarching framework that addresses the resilience of critical entities in respect of all hazards. It mandates risk assessments, national strategies and specific resilience measures for designated critical entities to ensure they are able to continue providing vital societal functions. Although the Directive includes the banking sector and financial market infrastructures as critical sectors, the financial sector is out of scope of all of the substantive requirements of the CER, as it is covered by much more specific requirements under DORA. Nonetheless, the financial sector remains in scope of the CER Directive for horizontal cooperation arrangements.

The NIS2 Directive provides a broader framework for cybersecurity across various critical sectors. DORA is considered *lex specialis* towards the NIS2 Directive meaning that the requirements concerning risk management and incident reporting set out in DORA apply as a sector-specific Union legal act instead of the NIS2 Directive. As communicated by the Commission in its guidelines on the application of Article 4 (1) and (2) of the NIS2 Directive[13], certain provisions laid down in the NIS2 Directive which are essential for ensuring preparedness and achieving a high level of resilience of financial entities continue to apply, including the requirements to adopt a cybersecurity strategy and establish a national cyber crisis management framework (with the obligation to designate cyber crisis management authorities and adopt national large-scale cybersecurity incident and crisis response plans) which cover the sectors banking and financial market infrastructures. Further, computer security incident response teams ('CSIRTs') and the EU cyber crisis liaison organisation network ('EU-CyCLONe') should carry out their tasks with regard to the sectors banking and financial market infrastructures.

---

11 The three ESAs are the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA); and the European Securities and Markets Authority (ESMA).

12 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Article 5(5) of the Directive provides for the Commission, in cooperation with the Member States, to develop a voluntary common reporting template for the purpose of complying with Article 5(4) of the Directive.

13 C(2023)6068.

The preparedness measures outlined for the financial sector are designed to balance the need for resilience with the principle of proportionality. Regulatory and supervisory requirements are tailored to the size, complexity and systemic importance of institutions to avoid putting a disproportionate burden on smaller entities. To avoid unnecessary administrative burden, harmonised frameworks like DORA streamline requirements across the sector, ensuring consistency while reducing duplication of effort.

2.2 EU authorities: tools and cooperation

EU authorities are entrusted with specific tools that may be activated in emergency situations and that maintain preparedness arrangements to ensure business continuity. For instance, the three ESAs have been attributed emergency powers under their founding regulations. Once an emergency situation has been formally recognised by the Council (under Article 18 of the ESA regulations), they may temporarily restrict financial activities under Article 9, through individual decisions. They also perform a general coordination function between national authorities and within the European System of Financial Supervision (ESFS) (Article 31).

As mentioned above, the ECB is the single supervisory authority for banks in the 21 Member States that participate in the Single Supervisory Mechanism, ensuring consistent prudential supervision across the area. The Single Resolution Board is the single resolution authority for these Member States, responsible for the orderly resolution of failing banks, thereby safeguarding financial stability and minimising costs to taxpayers.

To boost operational resilience, all the EU authorities have developed internal business continuity, preparedness arrangements and critical incident management proceedings to manage a variety of hazards. They regularly test these measures to ensure business continuity and to identify the most time-critical business processes to be carried out in an emergency and at what level.

Given the need to preserve the integrity and well-functioning of the single market and given the high degree of interconnectedness and risk of spillover effects in the EU financial sector, coordination among different EU authorities and involving Member States is essential in order to anticipate and manage crises that have the potential to affect multiple parts of the EU simultaneously. Early involvement and swift cooperation are essential both at the planning phase and at each stage of the crisis. To ease cooperation and exchange information that can be relevant also in a crisis, several EU authorities have concluded cooperation instruments among each other or with national competent authorities or national resolution authorities, or concluded memoranda of understanding, (e.g. Memorandum of Understanding between the ECB and the SRB), and are also conducting dry-runs to ensure adequate crisis preparedness.

One important milestone in this work is the European Union Systemic Cyber Incident Coordination Framework (EU-SCICF), established in January 2025 by the ESAs. This

framework provides a strategic foundation for cooperation during significant cyber incidents[14]. It aims to facilitate rapid information sharing and joint responses by putting in place protocols to evaluate and mitigate threats across EU Member States.

Moreover, the Council adopted in June 2025, a cyber crisis management Blueprint'[15] as an important guide for Member States to enhance their preparedness, detection capabilities and response to cyber security incidents, based on all relevant mechanisms including those created by the NIS2 Directive, DORA (EU-SCICF) and the Cyber Solidarity Act.

Regular exercises can be conducted under this framework to ensure that readiness and response capabilities remain robust and effective. In addition, at international level, the G7 Cyber Incident Response Protocol aims to unify global response efforts to cybersecurity threats impacting the financial sector and to ensure timely and coordinated responses across jurisdictions.

Each EU authority carries out regular risk assessments and other measures to identify the most relevant risks vis-à-vis each authority's mandate and functions. The risk assessments are conducted in cooperation with national authorities, contributing to develop a shared and more in-depth understanding of the risk landscape and the risks to be prioritised. Risk assessments often feed into early warning systems that in turn are part of the EU authorities' preparedness frameworks. Furthermore, the existing regulatory and supervisory arrangements between EU authorities and private-sector stakeholders allow for continued dialogue on reciprocal expectations vis-à-vis preparedness[16].

2.3 Frameworks at national and regional level

In addition to legislation at EU level, Member States have developed their own national preparedness schemes[17]. These schemes typically go beyond the financial sector and cover societal preparedness as a whole at national level. For this reason, national schemes differ among Member States, reflecting differing national governmental and administrative structures, and scope of competencies. At the same time, these national schemes operate within a consistent EU framework and increasingly interact with EU-level arrangements and cross-border coordination mechanisms.

The preparedness of the financial sector is always a key element in national preparedness strategies. The sector is in the lead on preparedness, a showcase for other sectors. National preparedness strategies for the financial sector go beyond the EU *acquis*, focusing on national operational issues. Differences across national financial systems (e.g. main features of the

---

14 The EU-SCICF also implements Article 49 of DORA with the aim of enhancing coordination with other EU crisis frameworks.

15 Council Recommendation of 6 June 2025 on an EU blueprint for cyber crisis management, *OJ C, C/2025/3445, 20.6.2025*, http://data.europa.eu/eli/C/2025/3445/oj

16 The EU preparedness union strategy recognises the importance of such partnerships. Key actions 36 and 37 aim to establish a public-private preparedness task force and develop public-private emergency protocols in all sectors.

17 As part of its work to deliver on the mandate of action 25 of the annex of the joint communication on the preparedness union strategy, the Commission also built on continued discussions with Member States on preparedness schemes.

national banking sector, extent of cash use, adoption of the euro, participation in the Banking Union) are naturally reflected in how the level of national preparedness of the financial sector is assessed and ensured.

Given the pivotal role played by public authorities, especially in the event of a crisis or major incident, reliable short-term funding functions must remain available to avoid liquidity or funding shortages at the level of the sovereign and the public sector more broadly and to avoid broader repercussions for society in terms of public trust and financial stability. However, this does not apply to all crisis frameworks in the same way: in particular, bank resolution is designed to limit reliance on public funds, through bail-in and industry-financed resolution mechanisms.

To ensure the resilience of governments' short-term funding functions, national debt management offices (DMOs) have developed contingency and business continuity planning to continue operating also in the event of a crisis. These arrangements are increasingly complemented by exchanges of best practices and coordination at both EU and regional level.

In addition, the European Stability Mechanism (ESM) offers several financial assistance instruments designed to safeguard financial stability by providing assistance to ESM Members, to enhance the euro area's capacity to manage sovereign and banking distress. These instruments are intended to address systemic crises and complement national and EU operational preparedness for more tangible disruption scenarios. Some Member States have developed bilateral arrangements to ensure the availability of short-term financing in the event that any of the basic DMO functions become unavailable. Finalising the pending ESM Treaty change would further strengthen the safety net of the euro area.

In parallel, there are regional coordination fora, such as the Nordic Baltic Cooperation Mechanism, an important regional initiative focused on the Baltic Sea countries. These fora foster collaboration on financial supervision and crisis management, exchanges of information on risk assessments and strategic planning. They illustrate how regional cooperation can enhance preparedness.

Several Member States have developed dedicated private-public partnerships or fora in the context of their national preparedness schemes (encompassing private-sector representatives from several sectors).

Overall, these EU-level, regional and national arrangements are part of a layered preparedness framework, where coordination and cooperation at EU and regional level is complemented by national action.

3. Stress testing

Stress testing is a key aspect of preparedness, as recognised in the Council Recommendation on strengthening the resilience of critical infrastructures[18]. In the financial sector, stress testing is already an integral and essential part of the supervision of financial institutions and financial market infrastructure providers. Stress tests strengthen financial sector preparedness by simulating severe crises (like recessions, climate shocks or cyberattacks) to uncover vulnerabilities in financial institutions' capital and liquidity. This forces institutions and providers to improve risk management, boost capital buffers, refine strategic planning and build resilience against future shocks, enhancing overall financial stability and building market confidence.

Stress testing also supports preparedness by capturing system-wide and cross-border risk channels, including sources of global financial instability, geopolitical tensions, cyber incidents and disruptions to critical infrastructure.

In the **banking system**, the European Banking Authority (EBA) has a mandate to initiate and coordinate EU-wide stress tests for the banking sector. Based on this mandate, the EBA carries out an EU-wide stress test every two years covering around 75% of the banking sector. The CRD also mandates competent authorities to carry out supervisory stress tests on the institutions they supervise, as appropriate but at least once a year. In addition, the EBA has issued guidelines to ensure that the authorities use a common methodology when conducting annual supervisory stress testing.

Within the Banking Union, the ECB regularly carries out stress tests, scenario analyses and simulations to inform the Supervisory Review and Evaluation Process. The ECB also conducts targeted reviews of cyber resilience and outsourcing arrangements.

In the **insurance and occupational pension funds sector**, the EIOPA regularly runs EU-wide stress tests for insurance and reinsurance undertakings and for occupational pension funds (IORPs)[19], every three years, including a cyber risk and climate risk component.

The European Securities and Markets Authority (ESMA) conducts regular EU-wide stress tests of CCP resilience, in the framework of the assessments in accordance with Article 32 of the ESMA Regulation and Article 24a of the EMIR. Although these tests focus on CCP resilience to withstand adverse market developments, the ESMA includes other types of exogenous risks too.

The European Systemic Risk Board (ESRB) draws up adverse scenarios for the EBA (banks), for EIOPA (insurance, pension funds) and for ESMA (CCPs) stress tests.

---

[18] Council Recommendation of 8 December 2022 of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure (2023/C 20/01).

[19] In several Member States, occupational pension funds do not fall under the scope of the IORP II Directive and are therefore not regulated under EU rules. Such pension funds are not subject to EIOPA's stress testing exercises.

Directive 2014/49/EU on the Deposit Guarantee Scheme Directive (DGS) requires Member States to perform their tasks under the Directive. The results of those tests are then used by the EBA to conduct peer reviews to examine the resilience of DGS.

4. Outlook

The EU financial sector is underpinned by a solid and multi-dimensional preparedness framework. The framework is made up of specific sectoral legislation, cross-cutting legislation and cooperation mechanisms across sectors and across Member States. The preparedness of the EU financial sector also has an external dimension, by which the EU strengthens not only its financial stability, but also its role as a reliable and credible financial sector at global level.

The EU's financial sector has proven its resilience during past crises. It has proven its ability to weather the storms of the COVID-19 pandemic, the aggression by Russia of Ukraine, financial crises in other jurisdictions, cyberattacks and many more episodes.

Nonetheless, given the unprecedented threats and the more uncertain geopolitical environment that the EU faces, it is important to continuously assess the level of preparedness of the EU financial sector. The EU is taking this work forward and may set in motion any adjustments needed to ensure rapid, concerted and proportionate preventive and reactive actions, both at EU and Member State level, with a view to maintaining a steadfast course and preserving the EU financial sector's vital functions. Going forward, the development of the SIU and the introduction of the digital euro is expected to improve the overall resilience of the EU financial sector and to further improve its level of preparedness.