Basic information

2020/0266(COD) COD - Ordinary legislative procedure (ex-codecision procedure) Regulation	Procedure completed
Digital finance: Digital Operational Resilience Act (DORA) Amending Regulation 2009/1060 2008/0217(COD) Amending Regulation 2012/648 2010/0250(COD) Amending Regulation 2014/600 2011/0296(COD) Amending Regulation 2014/909 2012/0029(COD) **Subject** 2.50.03 Securities and financial markets, stock exchange, CIUTS, investments 2.50.04 Banks and credit 2.50.08 Financial services, financial reporting and auditing 2.50.10 Financial supervision 3.30.06 Information and communication technologies, digital technologies **Legislative priorities** Joint Declaration 2021 Joint Declaration 2022	

Key players

European Parliament

Committee responsible	Rapporteur	Appointed
ECON Economic and Monetary Affairs	KELLEHER Billy (Renew)	15/10/2020
	Shadow rapporteur FITZGERALD Frances (EPP) SANT Alfred (S&D) PEKSA Mikuláš (Greens/EFA) RZOŃCA Bogdan (ECR) BECK Gunnar (ID)	

Committee for opinion	Rapporteur for opinion	Appointed
ITRE Industry, Research and Energy	The committee decided not to give an opinion.	
IMCO Internal Market and Consumer Protection	The committee decided not to give an opinion.	

Council of the

European Union	
European Commission	**Commission DG** / **Commissioner** Financial Stability, Financial Services and Capital Markets Union / MCGUINNESS Mairead
European Economic and Social Committee	

Key events

Date	Event	Reference	Summary
24/09/2020	Legislative proposal published	COM(2020)0595	Summary
17/12/2020	Committee referral announced in Parliament, 1st reading		
01/12/2021	Vote in committee, 1st reading		
01/12/2021	Committee decision to open interinstitutional negotiations with report adopted in committee		
07/12/2021	Committee report tabled for plenary, 1st reading	A9-0341/2021	Summary
13/12/2021	Committee decision to enter into interinstitutional negotiations announced in plenary (Rule 71)		
15/12/2021	Committee decision to enter into interinstitutional negotiations confirmed by plenary (Rule 71)		
13/07/2022	Approval in committee of the text agreed at 1st reading interinstitutional negotiations	PE734.260 GEDA/A/(2022)005010	
09/11/2022	Debate in Parliament		
10/11/2022	Decision by Parliament, 1st reading	T9-0381/2022	Summary
10/11/2022	Results of vote in Parliament		
28/11/2022	Act adopted by Council after Parliament's 1st reading		
14/12/2022	Final act signed		
27/12/2022	Final act published in Official Journal		

Technical information

Procedure reference	2020/0266(COD)
Procedure type	COD - Ordinary legislative procedure (ex-codecision procedure)
Procedure subtype	Legislation
Legislative instrument	Regulation
Amendments and repeals	Amending Regulation 2009/1060 2008/0217(COD) Amending Regulation 2012/648 2010/0250(COD) Amending Regulation 2014/600 2011/0296(COD) Amending Regulation 2014/909 2012/0029(COD)
Legal basis	Treaty on the Functioning of the European Union TFEU 114-p1
Other legal basis	Rules of Procedure EP 165

Mandatory consultation of other institutions	European Economic and Social Committee
Stage reached in procedure	Procedure completed
Committee dossier	ECON/9/04230

Documentation gateway

European Parliament

Document type	Committee	Reference	Date	Summary
Committee draft report		PE689.801	17/03/2021	
Amendments tabled in committee		PE693.603	27/05/2021	
Committee report tabled for plenary, 1st reading/single reading		A9-0341/2021	07/12/2021	Summary
Text agreed during interinstitutional negotiations		PE734.260	07/07/2022	
Text adopted by Parliament, 1st reading/single reading		T9-0381/2022	10/11/2022	Summary

Council of the EU

Document type	Reference	Date	Summary
Coreper letter confirming interinstitutional agreement	GEDA/A/(2022)005010	29/06/2022	
Draft final act	00041/2022/LEX	14/12/2022	

European Commission

Document type	Reference	Date	Summary
Legislative proposal	COM(2020)0595	24/09/2020	Summary
Document attached to the procedure	SEC(2020)0307	24/09/2020	
Document attached to the procedure	SWD(2020)0198	24/09/2020	
Document attached to the procedure	SWD(2020)0199	24/09/2020	
Commission response to text adopted in plenary	SP(2022)688	17/01/2023	

National parliaments

Document type	Parliament /Chamber	Reference	Date	Summary
Contribution	CZ_CHAMBER	COM(2020)0595	16/12/2020	
Contribution	ES_PARLIAMENT	COM(2020)0595	22/02/2021	
Contribution	PT_PARLIAMENT	COM(2020)0595	09/03/2021	
Contribution	RO_SENATE	COM(2020)0595	10/05/2021	

Contribution	IT_CHAMBER	COM(2020)0595	27/10/2021	

Other institutions and bodies

Institution/body	Document type	Reference	Date	Summary
EESC	Economic and Social Committee: opinion, report	CES5040/2020	24/02/2021	
EDPS	Document attached to the procedure	N9-0035/2021 OJ C 229 15.06.2021, p. 0016	10/05/2021	

Additional information

Source	Document	Date
European Commission	EUR-Lex	

Final act

Regulation 2022/2554
OJ L 333 27.12.2022, p. 0001 Summary

Delegated acts

Reference	Subject
2024/3006(DEA)	Examination of delegated act
2025/2574(DEA)	Examination of delegated act
2025/2623(DEA)	Examination of delegated act

Digital finance: Digital Operational Resilience Act (DORA)

2020/0266(COD) - 27/12/2022 - Final act

PURPOSE: to strengthen the IT security of financial entities such as banks, insurance companies and investment firms to enable the European financial sector to maintain resilient operations in the event of a serious operational breaches.

LEGISLATIVE ACT: Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

CONTENT: the Digital Operational Resilience Regulation (**DORA Regulation**) **uniform requirements** for the security of network and information systems of companies and organisations operating in the financial sector as well as critical third parties which provide ICT (Information Communication Technologies)-related services to them, such as cloud platforms or data analytics services.

DORA creates a **regulatory framework on digital operational resilience** whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats. These requirements are homogenous across all EU member states. The core aim is to prevent and mitigate cyber threats.

Uniform requirements

DORA sets uniform requirements for the security of networks and information systems of companies and organisations operating in the financial sector, as follows:

- requirements for financial entities with regard to: (i) information and communication technology (ICT) **risk management**; (ii) reporting of major ICT incidents to the competent authorities and voluntary reporting of significant cyber threats to the competent authorities; (iii) reporting of major payment-related operational or security incidents by financial entities to the competent authorities; (iv) digital operational resilience testing; (v) information and intelligence sharing in relation to cyber threats and vulnerabilities; (vi) measures to ensure sound **risk management** of third-party ICT service providers;

- requirements in relation to the **contractual arrangements** concluded between ICT third-party service providers and financial entities;

- rules for the establishment and conduct of the **Oversight Framework** for critical ICT third-party service providers when providing services to financial entities;

- rules on **cooperation** among competent authorities, and rules on supervision and enforcement by competent authorities in relation to all matters covered by this Regulation.

Scope of application

The new Regulation will **apply to almost all financial entities**. It will not apply to insurance intermediaries that are micro, small or medium-sized enterprises. Auditors will not be subject to DORA but will be part of a future review of the regulation, where a possible revision of the rules may be explored.

Proportionality principle

The efforts asked from financial entities will be proportional to the potential risks. The Regulation states that financial entities will implement the rules on the principle of proportionality, taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations.

Governance and organisation

Financial entities will:

- have a **governance and internal control framework** that ensures effective and prudent management of ICT risk to achieve a high level of digital operational resilience;

- have a robust, comprehensive and well-documented **ICT risk management framework** that enables them to respond to ICT risk in a timely, efficient and comprehensive manner and to ensure a high level of digital operational resilience;

- put in place mechanisms to **promptly detect anomalous activities**. All detection mechanisms will be regularly tested.

Framework for the supervision of critical third-party ICT service providers

Critical third-country ICT service providers to financial entities in the EU will be required to establish a **subsidiary within the EU** so that oversight can be properly implemented.

To ensure that critical ICT third-party service providers are appropriately and effectively overseen on a Union level, this Regulation provides that any of the three European Supervisory Authorities (ESAs) will be designated as a Lead Overseer.

Lead Overseers will be granted the necessary powers to conduct investigations, to carry out onsite and offsite inspections at the premises and locations of critical ICT third-party service providers and to obtain complete and updated information.

To ensure a consistent approach to oversight activities and with a view to enabling coordinated general oversight strategies and cohesive operational approaches and work methodologies, the three Lead Overseers appointed will set up a **Joint Oversight Network** to coordinate among themselves in the preparatory stages and to coordinate the conduct of oversight activities over their respective overseen critical ICT third–party service providers.

The Lead Overseer will also exercise its supervisory powers in third countries.

Digital operational resilience testing

To assess preparedness to deal with ICT-related incidents, identify weaknesses, deficiencies and gaps in digital operational resilience and promptly implement corrective measures, financial entities, other than micro-enterprises, will establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework.

Under the Regulation, **penetration tests** will be carried out in functioning mode, and it will be possible to include several Member States' authorities in the test procedures. The use of internal auditors will be possible only in a number of strictly limited circumstances, subject to safeguard conditions.

ENTRY INTO FORCE: 16.1.2023. The Regulation will apply from 17.1.2025.

Digital finance: Digital Operational Resilience Act (DORA)

2020/0266(COD) - 24/09/2020 - Legislative proposal

PURPOSE: to lay down uniform requirements concerning the security of network and information systems supporting the business processes of financial entities with a view to achieving a high level of digital operational resilience for the financial sector.

PROPOSED ACT: Regulation of the European Parliament and of the Council.

ROLE OF THE EUROPEAN PARLIAMENT: the European Parliament decides in accordance with the ordinary legislative procedure and on an equal footing with the Council.

BACKGROUND: this proposal is part of the Digital Finance package, a package of measures to further enable and support the potential of digital finance in terms of innovation and competition while mitigating the risks. The digital finance package includes a new Strategy on digital finance for the EU financial sector with the aim to ensure that the Union's financial services legislation is fit for the digital age, and contributes to a future-ready economy that works for the people, including by enabling the use of innovative technologies. The Union has a stated and confirmed policy interest in developing and promoting the uptake of transformative technologies in the financial sector, including blockchain and distributed ledger technology (DLT).

This package also includes a proposal for a pilot regime on distributed ledger technology market infrastructures, a proposal on crypto-asset markets, and a proposal to clarify or amend certain related EU financial services rules.

The use of digital, or Information and Communication Technologies (ICT) has in the last decades gained a pivotal role in finance, assuming today critical relevance in the operation of typical daily functions of all financial entities. Digitalisation covers, for instance, payments, which have increasingly moved from cash and paper-based methods to the use of digital solutions.

However, digital, or Information and Communication Technologies (ICT), gives rise to opportunities as well as risks. Risks include an increased threat to cyber attacks and ICT disruptions.

ICT risks pose challenges to the operational resilience, performance and stability of the EU financial system. The absence of detailed and comprehensive rules on digital operational resilience at EU level has led to the proliferation of national regulatory initiatives (e.g. on digital operational resilience testing) and supervisory approaches (e.g. addressing ICT third-party dependencies).

This situation fragments the single market, undermines the stability and integrity of the EU financial sector, and jeopardises the protection of consumers and investors.

It is therefore necessary to put in place a detailed and comprehensive framework on digital operational resilience for EU financial entities.

CONTENT: this proposal aims to put into place a comprehensive framework which shall enhance digital risk management. In particular, it seeks to strengthen and streamline the financial entities' conduct of ICT risk management, establish a thorough testing of ICT systems, increase supervisors' awareness of cyber risks and ICT-related incidents faced by financial entities, as well as introduce powers for financial supervisors to oversee risks stemming from financial entities' dependency on ICT third-party service providers.

Scope of the Regulation

To ensure consistency around the ICT risk management requirements applicable to the financial sector, the proposed Regulation shall cover a range of financial entities regulated at Union level, namely inter alia: (i) credit institutions, (ii) payment institutions, (iii) electronic money institutions, (iv) investment firms, crypto-asset service providers, (v) central securities depositories, (vi) central counterparties, (vii) trading venues, (viii) trade repositories, (ix) credit rating agencies, (x) crowdfunding service providers.

Such a coverage facilitates a homogenous and coherent application of all components of the risk management on ICT-related areas, while safeguards the level playing field among financial entities in respect of their regulatory obligations on ICT risk.

Governance related requirements

As this proposed Regulation is designed to better aligning financial entities' business strategies and the conduct of the ICT risk management, the management body shall be required to maintain a crucial, active role in steering the ICT risk management framework and shall pursue the respect of a string cyber hygiene.

ICT risk management requirements

Digital operational resilience is rooted in a set of key principles and requirements on ICT risk management framework, in line with the joint ESAs technical advice. These requirements, inspired from relevant international, national and industry-set standards, guidelines and recommendations, revolve around specific functions in ICT risk management (identification, protection and prevention, detection, response and recovery, learning and evolving and communication). To keep pace with a quickly evolving cyber threat landscape, financial entities are required to set-up and maintain resilient ICT systems and tools that minimize the impact of ICT risk.

ICT-related incident reporting

The proposal shall create a consistent incident reporting mechanism that will help reduce administrative burdens for financial entities and strengthen supervisory effectiveness. The reporting shall be processed using a common template and following a harmonised procedure as developed by the ESAs.

Digital operational resilience testing

The capabilities and functions included in the ICT risk management framework need to be periodically tested for preparedness and identification of weaknesses, deficiencies or gaps, as well as the prompt implementation of corrective measures. This proposal allows for a proportionate application of digital operational resilience testing requirements depending on the size, business and risk profiles of financial entities.

Information sharing

To raise awareness on ICT risk, minimise its spread, support financial entities' defensive capabilities and threat detection techniques, the proposed Regulation shall allow financial entities to set-up arrangements to exchange amongst themselves cyber threat information and intelligence. All voluntary information sharing arrangements between financial entities that this Regulation promotes would be conducted in trusted environments in full respect of Union data protection rules.

Budgetary implications

As the current Regulation foresees an enhanced role for the ESAs by means of powers granted upon them to adequately oversee critical ICT third-party providers, the proposal would entail the deployment of increased resources, in particular to fulfil the oversight missions (such as onsite and online inspections and audits exercises) and the use of staff possessing specific ICT security expertise.

The scale and distribution of these costs will depend on the extent of the new oversight powers and the (precise) tasks to be performed by the ESAs.

The estimated total cost impact is approximately EUR 30.19 million for the period 2022 - 2027. Therefore, no impact on EU budget appropriations is foreseen (except for the additional staff), as these costs will be fully funded by fees.

Digital finance: Digital Operational Resilience Act (DORA)

2020/0266(COD) - 07/12/2021 - Committee report tabled for plenary, 1st reading/single reading

The Committee on Economic and Monetary Affairs adopted the report by Billy KELLEHER (Renew Europe, IE) on the proposal for a regulation of the European Parliament and of the Council on the digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014.

The Commission's proposal for a legislative act on digital operational resilience in the financial sector (DORA) aims to establish uniform requirements for the security of networks and information systems to provide a comprehensive framework that will improve the management of digital risks by financial entities.

The committee responsible recommended that the European Parliament's position adopted at first reading under the ordinary legislative procedure should amend the proposal as follows:

Uniform requirements

The requirements for financial entities will concern: (i) information and communication technology (ICT) risk management; (ii) reporting of major IT-related incidents to the competent authorities; (iii) reporting of major payment-related operational or security incidents by credit, payment and electronic money institutions to the competent authorities; (iv) digital operational resilience testing; (v) information and intelligence sharing in relation to cyber threats and vulnerabilities; and (vi) measures to ensure sound risk management of third-party ICT service providers by financial entities.

This Regulation would be without prejudice to the competences of Member States concerning the maintenance of public security, defence and national security.

Scope of application

The proposal should apply to insurance intermediaries, that are **not micro, small or medium-sized enterprises**, with the exception of undertakings which rely exclusively on organised automated sales systems. Statutory auditors and small and medium-sized audit firms would also be excluded from the scope of the Regulation, with some exceptions. The Regulation would apply to ICT intra-group service providers, with the exception of the supervisory framework in Chapter V.

Proportionality principle

The amended text clarifies that financial entities should implement the rules introduced by Chapters II (risk management), III (management, classification and reporting of IT incidents) and IV (resilience testing) in accordance with the principle of proportionality, taking into account their **size, the nature, scale and complexity** of their services, activities and operations and their overall risk profile.

The Regulation should not apply to small non-interconnected investment firms, credit institutions and electronic money institutions exempted under the relevant EU directives. It should also not apply to small institutions for occupational retirement pensions. However, these exempted firms and entities would have to put in place a sound and well-documented ICT risk management framework, which would be reviewed at least once a year.

Governance and organisation

Financial entities should have in place an **internal governance and a control framework** that ensures an effective and prudent management of all ICT risks, with a view to achieving a high level of digital operational resilience. The management body should bear the ultimate responsibility for managing the financial entity's ICT risks and put in place procedures and policies that aim to ensure the maintenance of high standards of security, confidentiality and integrity of data.

Risk identification, protection, prevention, detection

Financial entities should, *inter alia*, (i) review as needed, and at least yearly, the criticality or importance of ICT-related business functions; (ii) ensure that data is protected from internal ICT risks, including poor administration, processing-related risks and human error; (iii)

record all ICT-related incidents that have an impact on the stability, continuity or quality of financial services, including where the incident has or is likely to have an impact on such services.

The purpose of the **ICT business continuity policy** should be to manage and mitigate risks that may adversely affect the ICT systems and services of financial entities and to facilitate their rapid recovery if necessary.

ICT security awareness programmes should apply to all staff, while the digital operational resilience trainings should apply to, at least, all employees with rights of direct access to the ICT systems and to senior management staff.

Reporting major ICT-related incidents

Financial entities could notify, on a **voluntary basis**, significant cyber threats to the relevant competent authority where they deem the threat to be of relevance to the financial system, service users or clients.

The competent authority should be informed in any event within **24 hours** of becoming aware of an incident in respect of incidents that significantly disrupt the availability of services provided by the entity or that affect the integrity, confidentiality or security of personal data held by the financial entity. For incidents that have a significant impact other than on the availability of services provided by the financial entity, the competent authority should be informed within 72 hours.

Upon receipt of the incident report, the competent authority should provide details of the major IT incident to EBA, ESMA or EIOPA, and the ECB, as appropriate, as soon as possible. The Single Resolution Board (SRB) should be informed where the affected financial entity falls under the Single Resolution Mechanism Regulation, while the CSIRTs should be notified where the affected entities fall under the CRS Directive.

Testing

Threat led penetration testing should cover at least the critical or important **functions and services of a financial entity**. In addition, the text has been amended with regard to the involvement of an ICT third-party service provider. Where the involvement of ICT third-party service provider could potentially have an impact on the quality, confidentiality or security of the ICT third-party provider's services to other customers, the ICT third-party service provider may contractually agree that the ICT third-party service provider is permitted to enter directly into contractual arrangements with an external tester. ICT third-party service providers may also enter into such arrangements on behalf of all their financial entity service users in order to conduct pooled testing.

At the end of the test, once the reports and remediation plans have been approved, the financial entity and the external testers should provide the single public authority designated under the Regulation with a confidential summary of the test results and documentation confirming that the threat led penetration test was conducted in accordance with the requirements.

Sound management of ICT third-party risks by financial entities

Financial entities should maintain and update a register of information relating to all contractual arrangements for the use of IT services provided by third-party IT service providers that support critical or important functions. Contractual arrangements for the use of ICT services should allow financial entities to take appropriate remedial action, which could include wholly terminating the arrangements, if no rectification is possible, or partially terminating the arrangements, if rectification is possible, under applicable law.

With a view to reducing the risk of disruptions at the level of the financial entity, in duly justified circumstances and in agreement with its competent authorities, the financial entity may decide not to terminate the contractual arrangements with the ICT third-party service provider until it is able to switch to another ICT third-party service provider or change to in-house solutions consistent with the complexity of the service provided.

Lastly, where contractual arrangements for the use of ICT services that support critical or important functions are entered into with a **third-party ICT service provider established in a third country**, financial entities should also take into account compliance with data protection and the effective enforcement of the rules set out in this Regulation.

Digital finance: Digital Operational Resilience Act (DORA)

2020/0266(COD) - 10/11/2022 - Text adopted by Parliament, 1st reading/single reading

The European Parliament adopted by 556 votes to 18, with 38 abstentions, a legislative resolution on the proposal for a regulation of the European Parliament and of the Council on the digital operational resilience of the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648 /2012, (EU) No 600/2014 and (EU) No 909/2014.

The Digital Operational Resilience Regulation (DORA) aims to achieve a high level of digital operational resilience for all regulated financial entities, such as banks, insurance companies and investment firms.

DORA creates a regulatory framework on digital operational resilience in which all firms must ensure that they can withstand, respond to and recover from all types of ICT-related disruptions and threats. The new rules will provide a strong framework to strengthen IT security in the financial sector.

The European Parliament's first reading position under the ordinary legislative procedure amends the proposal as follows:

Uniform requirements

DORA sets uniform requirements for the security of networks and information systems of companies and organisations operating in the financial sector, as follows:

- requirements for financial entities with regard to: (i) information and communication technology (ICT) risk management; (ii) reporting of major ICT incidents to the competent authorities and voluntary reporting of significant cyber threats to the competent authorities; (iii) reporting of major payment-related operational or security incidents by financial entities to the competent authorities; (iv) digital operational resilience testing; (v) information and intelligence sharing in relation to cyber threats and vulnerabilities; (vi) measures to ensure sound risk management of third-party ICT service providers;

- requirements for contractual arrangements between third party ICT service providers and financial entities;

- rules on the establishment of the supervisory framework applicable to critical third-party ICT service providers when providing services to financial entities, as well as those related to the exercise of tasks within that framework.

Scope of application

The new regulation should apply to **almost all financial entities**. It should not apply to insurance intermediaries that are micro, small or medium-sized enterprises. **Auditors** will not be subject to DORA but will be part of a future review of the regulation, where a possible revision of the rules may be explored.

Proportionality principle

The amended text clarifies that financial entities should implement risk management rules in accordance with the proportionality principle, taking into account their size and overall risk profile as well as the nature, scale and complexity of their services, activities and operations.

Governance and organisation

Financial entities should have a **governance and internal control framework** that ensures effective and prudent management of ICT risk to achieve a high level of digital operational resilience. The management body of the financial entity should define, approve, oversee and be responsible for the implementation of all provisions of the ICT risk management framework.

Critical ICT third–party service providers

The **European Supervisory Authorities** (ESAs), through the Joint Committee and upon recommendation from the Oversight Forum established pursuant to the Regulation should designate the ICT third–party service providers that are critical for financial entities, following an assessment.

In order for supervision to be properly implemented, financial entities should only be able to use the services of an ICT third-party service provider and which has been designated as critical if it has established **a subsidiary in the EU** within 12 months of the designation.

Oversight framework

Lead Overseers should be granted the necessary powers to conduct investigations, to carry out onsite and offsite inspections at the premises and locations of critical ICT third–party service providers and to obtain complete and updated information. Those powers should enable the Lead Overseer (i.e. the ESA designated in accordance with the Regulation) to acquire real insight into the type, dimension and impact of the ICT third–party risk posed to financial entities and ultimately to the Union's financial system.

To ensure a consistent approach to oversight activities and with a view to enabling coordinated general oversight strategies and cohesive operational approaches and work methodologies, the three Lead Overseers appointed should set up a **Joint Oversight Network** to coordinate among themselves in the preparatory stages and to coordinate the conduct of oversight activities over their respective overseen critical ICT third–party service providers.

The Lead Overseer should also be able to exercise its supervisory powers in **third countries**. The exercise of these powers in third countries should enable the Lead Overseer to examine the facilities from which ICT or technical support services are actually provided or managed by the critical third party ICT service provider.

Digital operational resilience testing

In order to assess preparedness to deal with ICT-related incidents, identify weaknesses, deficiencies and gaps in digital operational resilience and promptly implement corrective measures, financial entities, other than micro-enterprises, should establish, maintain and review a sound and comprehensive digital operational resilience testing programme as an integral part of the ICT risk-management framework.

Under the amended Regulation, penetration tests should be carried out in functioning mode, and it should be possible to include several Member States' authorities in the test procedures. The use of internal auditors will be possible only in a number of strictly limited circumstances, subject to safeguard conditions.

Data protection

The ESAs and the competent authorities should be allowed to process personal data only where necessary for the purpose of carrying out their respective obligations and duties pursuant to this Regulation, in particular for investigation, inspection, request for information, communication, publication, evaluation, verification, assessment and drafting of oversight plans.