OVERVIEW

No. RADAR
4444

Responsible level
EU

Competent authority
EU Commission

Standard designation
Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience in 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

Title of Standard
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

Abbreviation (standard)
Regulation (EU) 2022/2554

Short Title
Regulation (EU) 2022/2554

Abbreviation (standard)
DORA

Abbreviation
DORA

Implementation status of the standard
published

Industry relevance
Banking, insurance

category
01. Banking and banking supervisory law

Document type
Regulation

Management Summary
In the context of the digitalisation of the financial sector, this Regulation aims to ensure uniform

Regulatory and supervisory requirements for the operational resilience of information and communication technology (ICT) in the financial sector are to be created. The DORA Regulation (Digital Operational Resilience Act) can be used as a response to the*Joint Recommendations of the European Supervisory Authorities to the European Commission on the need for legislative improvements regarding the requirements for the management of ICT risks in the EU financial sector (JC 2019 26, Dataset 3592*). It takes into account recognized international standards and includes, among other things, the following components:

- Governance and responsibility of the management body;
- ICT risk management (identification, protection and prevention of ICT risks, anomaly detection, emergency and recovery planning, evaluation, further development and communication);
- Monitoring, documenting and reporting ICT-related incidents and cyber threats;
- internal review of the resilience of ICT capacities and functions;
- Monitoring ICT third-party service provider risks;
- Exchange of information.

Supervisory monitoring will be implemented for certain critical ICT third-party service providers.

The regulation contains numerous mandates for the European Supervisory Authorities (ESAs) to specify certain requirements, including their scope. Regulatory standards are intended to specify, for example, which financial institutions must conduct regular penetration tests and the extent to which certain institutions can apply simplified procedures.

Management Summary

In the context of growing digitalization of finance, this regulation creates common regulatory and supervisory standards for digital operational resilience in the industry, especially Information and Communication Technologies (ICT). The DORA Regulation (Digital Operational Resilience Act) can be understood as a response to the*Joint Advice of the European Supervisory Authorities to the European Commission on the need for legislative improvements relating to ICT risk management requirements in the EU financial sector (JC 2019 26, data set 3592)*. It takes into account recognized international standards and includes the following elements, others among:

- Governance and responsibility of the management body;
- ICT risk management (identification of, protection from and prevention on ICT risks, detection of anomalous activities, business continuity policies and recovery plans, learning and evolving and communication);
- monitoring, documentation and reporting of ICT-related incidents and cyber threats;
- internal resilience testing of ICT capabilities and functions;
- monitoring of ICT third-party risk;
- information sharing.

Supervisory monitoring is implemented for certain critical ICT third-party service providers.

The regulation contains several mandates for the European Supervisory Authorities (ESAs) to specify certain requirements, including their scope. For example, level 2 guidance will determine which financial entities need to regularly conduct threat-led penetration tests and to what extent certain companies can apply simplified procedures.

CONTENTS

Main content

A. Overview

I. General provisions (Chapter I)

II. ICT risk management (Chapter II)

III. Treatment, classification, and reporting of ICT-related incidents (Chapter III)

IV. Testing digital operational resilience (Chapter IV)

V. Managing ICT third-party service provider risk (Chapter V)

VI. Agreements on the exchange of information (Chapter VI)

VII. Competent authorities (Chapter VII)

VIII. Transitional and final provisions (Chapter IX)

B. Essential content

I. General provisions (Chapter I)

1. Scope (Article 2)

a) This Regulation is addressed to all entities in the financial sector subject to broader supervision, as well as to other entities such as rating agencies, administrators of critical benchmarks and securitisation repositories, in accordance with paragraph 1. With the exception of third-party service providers of information and
Communication Technology (ICT), the companies covered by this Regulation are referred to as financial companies (see source for details).

b) The *Regulation on managers of alternative investment funds within the meaning of Article 3 (2) of Directive 2011/61/EU (AIFMD, dataset 136*), (re-)insurance undertakings within the meaning of Art. 4 of the *Directive 2009/138/EC (Solvency II Directive)*, certain institutions for occupational retirement provision, to natural or legal persons who, in accordance with Articles 2 and 3 of the *Directive 2014/65/EU (MiFID II, dataset 615)* are exempt from its application, certain insurance intermediaries and post office giro offices within the meaning of Article 2 paragraph 5 no. 3 of the *Directive 2013/36/EU (CRD, dataset 550)*.

c) Member States may also exempt the institutions and companies listed in Article 2(5)(4) to (23) of the CRD within their respective territories (e.g., in Germany, state development banks and non-profit housing companies). The EU Commission shall publish the relevant exemptions.

2. Principle of proportionality (Article 4)

Financial institutions implement the provisions for the introduction of ICT risk management (Chapter II) taking into account their size and overall risk profile, as well as the nature, scope, and complexity of their services, activities, and processes, as well as their general risk profile (proportionality principle). The requirements of Chapters III (Handling ICT-related incidents), IV (Digital operational resilience assessment), and V, Section I (Managing ICT third-party service provider risk) are applied taking into account the proportionality principle, to the extent provided for in these chapters.

II. ICT risk management (Chapter II)

1. Governance and Organization (Article 5)

Financial institutions must have internal governance and control frameworks for the effective and prudent management of ICT risks in accordance with Article 6(4) in order to achieve a high level of digital operational resilience. The management body is responsible for implementing all regulations related to the ICT risk management framework described in Article 6(1) (including policies for maintaining data integrity, development and approval of the digital operational resilience strategy, regular review of contingency plans, audit reviews, budgets, and policies for the use of third-party service providers) (see source for details).

Financial institutions, with the exception of micro-enterprises within the meaning of the Commission Recommendation concerning the definition of micro, small and medium-sized enterprises (2003/361/EC), are required, in accordance with paragraph 3, to establish a function to monitor agreements with third-party ICT service providers or to assign this task to a senior manager. In addition, members of management are required to undergo regular training to understand and assess ICT risks.

2. ICT risk management framework (Article 6)

With the help of an ICT risk management framework (as part of the overarching overall risk management system), ICT risks should be addressed quickly and efficiently and a high level of digital operational resilience should be ensured. Particular attention should be paid to the protection of information and ICT assets, including software and relevant physical components and infrastructure such as premises, data centers, and areas designated as sensitive. Financial institutions, with the exception of micro-enterprises, should delegate the management and monitoring of ICT risks to an independent control function and ensure an appropriate separation of functions between ICT management, control, and audit functions. The framework should also contain a digital operational resilience strategy, including methods for determining ICT risks and specific ICT objectives, which sets out how the framework will be implemented (see source for details). The framework must be reviewed regularly (at least annually, except for micro-enterprises) and on an ad hoc basis, and subject to regular internal audits by expert and independent auditors. The audit reports must be submitted to the competent authority

To be made available upon request. Monitoring compliance with risk management requirements may be outsourced. Responsibility for verifying compliance with ICT risk management requirements remains with the outsourcing financial institution. (See source for details).

3. ICT systems, protocols and tools (Article 7)

Financial institutions should always use up-to-date, appropriate and reliable ICT systems, protocols and tools that must meet certain minimum requirements (including sufficient capacity for peak periods and in stress situations) (see source for details).

4. Identification (Article 8)

The ICT-related business functions, the roles and responsibilities, the information assets and ICT assets supporting these functions, and their dependencies on ICT risks must be identified, classified, and documented in the ICT risk management framework. Sources of ICT risks, particularly from other financial institutions, must be continuously identified, and the resulting cyber risks and ICT vulnerabilities assessed. Classification and risk scenarios must be reviewed at least annually. A risk assessment must be conducted in accordance with paragraph 3, among other things, in the event of significant changes to the network and information system infrastructure. Furthermore, the physical equipment considered critical and the processes that depend on third-party ICT service providers must be identified. Existing ICT systems must be reviewed regularly. Micro-enterprises are exempt from certain requirements (see source for details).

5. Protection and prevention (Article 9)

The security and proper functioning of ICT systems and instruments must be continuously monitored and ensured with the help of appropriate security mechanisms. The ICT security strategy, corresponding policies and procedures, as well as modern ICT technology and procedures, should ensure secure information transmission and the protection, integrity, authenticity, confidentiality, and availability of data, particularly for ICT systems supporting critical or important functions (see source for details). According to paragraph 4, the ICT risk management framework also includes, among other things, an information security policy with comprehensive regulations for the protection of ICT assets, data, and information values. Furthermore, procedures for access restrictions and authentication mechanisms as well as documented change management procedures must be considered (see source for details). The network infrastructure should be capable of being immediately disconnected or segmented so that contagion risks, especially in interconnected financial processes, are avoided or minimized as far as possible.

6. Recognition (Article 10)

Financial institutions have detection mechanisms in place to promptly detect anomalous activities in accordance with Article 17 and to identify all potential material sources of error. These mechanisms must, among other things, enable multiple levels of control and trigger automatic alerts to enable a prompt response to ICT-related incidents. Approved disclosure systems (APAs) and approved reporting mechanisms (ARMs) within the meaning of Article 2(1) Nos. 34 and 36 of Regulation (EU) No. 600/2014 (MiFIR, dataset 613) must maintain systems that implement completeness checks in trading reports.

identify missing and incorrect data and initiate resubmission of the reports (see source for details).

7. Response and Recovery (Article 11)

The ICT risk management framework also includes a dedicated and comprehensive ICT business continuity strategy and an ICT disaster recovery plan, which, among other things, ensure the continuation of critical functions in the event of an ICT-related incident and a tailored response to such an incident (see source for details). Essential functions that are outsourced or provided by third-party service providers should be included in the ICT business continuity plan and tested regularly in accordance with paragraph 4. The design and use of ICT resources and services should be consistent with the Business Impact Analysis (BIA) and ensure appropriate redundancy of all critical components. The ICT business continuity strategy and the ICT disaster recovery plan must be tested at least annually and after significant changes to the ICT systems. In addition, tests of the crisis communication plan within the meaning of Article 14 of this Regulation are required (see source for details). Financial undertakings (except micro-enterprises) should also, according to paragraph 7,

Establish a crisis management function that will handle communications in the event of an emergency, in accordance with Article 14 of this Regulation, and report costs and losses resulting from serious ICT incidents upon request from the competent authority, in accordance with paragraph 10. The ESAs will develop guidelines for this purpose together with the EU Commission (see source for details).

8. Backup policy and procedures, as well as recovery and restoration procedures and methods (Article 12)

As part of the ICT risk management framework, a data backup strategy and recovery procedures should be developed to minimize downtime (see source for details). If data backups are performed on separate systems, the ICT systems should be operated in a physically and logically separate IT environment in accordance with paragraph 3 (see source for details). By defining recovery times and time targets for each function, existing service level agreements should be ensured. During recovery, appropriate coordination should ensure the highest possible data integrity (see source for details).

9. Learning processes and further development (Art. 13)

Financial institutions should maintain sufficient capacity and staff to gather and analyze information on vulnerabilities, cyber-attacks, and other ICT-related incidents. Following serious ICT incidents, the causes must be investigated and the necessary improvements to ICT operations identified. Changes made following such incidents must be reported to the competent supervisory authority upon request (micro-enterprises are exempt from this). The review following ICT incidents should include response times and the quality of forensic analysis, as well as the effectiveness of escalation and communication (see source for details). Findings obtained, among other things, from the testing of ICT tools, systems, and processes pursuant to Articles 26 and 27 of this Regulation, from actual ICT incidents, and from corresponding market information, must be continuously considered in the ICT risk assessment process pursuant to paragraph 3 (see source for details). The digital

Operational stability within the meaning of Article 6 (8) should be monitored with regard to effective implementation (see source for details).

Senior ICT staff must inform management of the findings and resulting recommendations at least annually.

In addition, awareness-raising programs and training measures on digital operational resilience should be included in the training programs for employees and managers. Where appropriate, ICT third-party service providers should also be included in the relevant training within the meaning of Article 30(2)(i) of this Regulation. Financial institutions (with the exception of micro-enterprises) should also continuously inform themselves about technological developments, ICT risk management processes, and forms of cyberattacks (see source for details).

10. Communication (Article 14)

Communication plans as part of the ICT risk management framework should, at a minimum, facilitate the disclosure of significant ICT incidents or vulnerabilities to customers, counterparties, and, if applicable, the public. Communication strategies for employees and external stakeholders should be provided within the risk management framework. A press officer must also be appointed (see source for details).

11. Further harmonisation of tools, methods, processes and guidelines for ICT risk management (Art. 15)

EBA, ESMA, and EIOPA (ESAs), in consultation with the European Union Agency for Cybersecurity (ENISA), are to define further details on ICT risk management through technical regulatory standards within one year of the entry into force of this Regulation. These include, for example, requirements for the inclusion of security controls as a fundamental component in systems, for monitoring access rights, and requirements for testing ICT business continuity plans and ICT disaster recovery plans, as well as the audit report on the ICT risk management framework (see source for details).

12. Simplified ICT risk management framework (Article 16)

For small, non-interconnected investment firms, payment institutions exempted under Directive 2015/2366/EU (PSD2, dataset 1036), credit and financial services institutions exempted from the CRD at national discretion,*Directive 2009/110/EC (data set 48)*A simplified ICT system applies to exempt e-money institutions and small institutions for occupational pensions.
Risk management framework (see source for details). Documentation and review requirements also apply to the simplified ICT risk management framework. The ESAs publish regulatory technical standards that specify, for example, the essential elements, requirements for systems and networks, and emergency planning.

III. Treatment, classification, and reporting of ICT-related incidents (Chapter III)

1. Process for handling ICT-related incidents (Article 17)

Financial institutions must define and implement an ICT incident management process that governs the detection, reporting, and handling of incidents. All ICT-related incidents and significant cyber threats must be recorded. Appropriate policies and processes should prevent the recurrence of such incidents. Expected procedures include, for example, the establishment of early warning indicators; processes for identifying, tracking, logging, categorizing, and classifying incidents; the definition of responsibilities; communication plans; and reporting (see source for details).

2. Classification of ICT-related incidents and cyber threats (Article 18)

ICT-related incidents must be classified and assessed in terms of their impact based on the criteria specified in paragraph 1 (e.g., number and/or relevance of affected customers or counterparties, value or number of affected transactions, duration, geographical spread, type of data loss, criticality of affected services) (see source for details). Cyber threats must be classified as significant based on the criticality of the services at risk, including the transactions and business, the number and/or relevance of affected customers or counterparties, and the geographical extent of the affected areas. Further details (e.g., thresholds for determining serious ICT incidents and cyber threats) will be specified by regulatory technical standards.

3. Reporting of serious ICT-related incidents and voluntary reporting of significant cyber threats (Article 19)

Serious ICT-related incidents must be reported to the competent authority using the forms yet to be published. Significant credit institutions within the meaning of Article 6 (4) of the *Regulation (EU) No. 1024/2013 (SSM Regulation, dataset 815)* report the incidents to the competent national authority. Member States may establish additional reporting obligations, including reporting to the national computer emergency response team as defined in Articles 8 and 9 of the *Directive (EU) 2016/1148 (NIS Directive, dataset 910)*. If financial institutions consider significant cyber threats relevant to the financial system or customers, they may voluntarily report them to the competent authority. Users and customers whose financial interests are affected by serious ICT-related incidents must also be informed. Customers who may be affected by protective measures against significant cyber threats may be informed if deemed appropriate (see source for details).

Paragraph 4 sets out requirements for reporting to the competent authority, with the exact deadlines being defined in Article 20, subparagraph 1a, no. 2. An initial report is required; an interim report must be submitted in the event of significant changes and updated regularly. A final report must be submitted after the root cause analysis has been completed (see source for details). Transferring the reporting obligations to a third-party service provider is permissible.

4. Harmonisation of the content and templates of reports (Article 20), centralisation of reporting on serious ICT-related incidents (Article 21), feedback from supervisory authorities (Article 22)

Further details on the reporting obligation and reporting deadlines will be specified by means of regulatory or implementing technical standards within 18 months of the entry into force of this Regulation, and uniform reporting formats for the reporting obligation on serious ICT incidents and for the notification of significant cyber threats will be published. The ESAS should, in principle, follow the proposal for a Directive of the European Parliament and of the Council on measures for a high common level

on cybersecurity throughout the Union and repealing Directive (EU) 2016/1148 (NIS 2, dataset 4614) and justify a different approach (details see source Art. 20).

In addition, the supervisory authorities should examine the possible centralisation of reporting on significant ICT incidents through the establishment of an EU platform (for details see source Art. 21).

Upon receipt of a report regarding a relevant ICT incident, the competent authorities will promptly provide feedback to the financial institution on the procedure, if necessary, in accordance with Article 19(4). Irrespective of this, the financial institution remains responsible for handling the incident (for details, see Article 22).

5. Payment-related operational or security incidents affecting credit institutions, payment institutions, account information service providers and e-money institutions (Article 23)

The requirements of Chapter III also apply to payment-related operational or security incidents (including serious ones) affecting credit institutions, payment institutions, account information service providers and e-money institutions (see source for details).

IV. Testing digital operational resilience (Chapter IV)

1. General requirements for testing digital operational resilience (Article 24)

As part of the ICT risk management framework, a comprehensive and robust program must be implemented to assess digital operational resilience and identify corrective actions. The audit program should follow a risk-based approach and address both the evolving ICT risks and the specific characteristics of the financial institution. Audits should be conducted at least annually by independent parties. For internally conducted audits, sufficient resources must be allocated and conflicts of interest avoided. Internal validation procedures should ensure that all identified vulnerabilities, deficiencies, and gaps are appropriately addressed. Micro-enterprises are exempt from these requirements (see source for details).

2. Extended testing of ICT tools, systems and processes based on TLPT (Article 26)

At least every three years, certain financial institutions must conduct threat-led penetration tests (TLPTs) to test critical functions and services on live production systems. The competent authority may require a different frequency. For this purpose, the relevant ICT processes, systems, and technologies must be identified, taking into account any outsourcing. In the case of outsourcing, externally conducted pool tests may be carried out, for which specific requirements apply (see source for details). Appropriate risk management controls should minimize any risks resulting from the tests. Upon completion of the tests, the supervisory authority must demonstrate that they were carried out correctly by submitting the relevant documentation. The competent authority will issue a confirmation after reviewing the documents.

The financial entities required to conduct TLPTs are determined by the competent authorities in accordance with paragraph 8. The key factors are, among others, the criticality of the financial entity's business activities, its impact on financial stability, and its ICT risk profile (see source for details).

Further details will be provided by regulatory technical standards to be published no later than 18 months after the entry into force of this Regulation.

3. Requirements for testers regarding the implementation of TLPT (Article 27)

The individuals tasked with conducting TLPTs must meet certain standards regarding their reputation and competence, be certified by a relevant authority in a Member State, or be subject to a formal code of conduct. Auditors must provide independent confirmation or an audit report on their risk management and handling of confidential information, and be adequately insured (see source for details).

According to paragraph 2, the use of internal auditors must be approved by the competent authority. The competent authority must also ensure that sufficient resources are available and that no conflicts of interest exist. In this case, the provision of threat intelligence must also be provided by third parties.

According to paragraph 3, the agreements with external auditors must be designed in such a way that no risks arise for the financial institution from the handling of the audit results (see source for details).

V. Management of ICT third-party risk (Chapter V)

1. Key principles for sound ICT third-party risk management (Section I)

a) General principles (Article 28)

ICT risks related to third parties must be treated as an essential component of ICT risks within the ICT risk management framework. The financial institution remains fully responsible for compliance with legal regulations at all times, even if ICT services are used to conduct its operations. The resulting risk management is carried out according to the principles of proportionality in accordance with paragraph 1b; in particular, the degree of dependence on the service and its criticality must be considered at the individual and group levels (see source for details).

According to paragraph 2, a strategy for ICT risks related to third-party ICT service providers and policies for the use of such services must be implemented at the individual and group levels. The risks associated with outsourcing critical or important functions must be regularly reviewed by senior management, taking into account the overall risk profile and the scope and complexity of the business model. Micro-enterprises and financial institutions that are permitted to apply a simplified ICT risk management framework are exempt from these requirements (see source for details).

According to paragraph 3, the contractual agreements should be recorded in a corresponding information register, distinguishing between critical/important and other functions. Newly entered into agreements should be reported to the competent authority at least annually. Furthermore, the authority should be informed of planned measures related to critical or important functions (see source for details).

According to paragraph 4, even before concluding an ICT service contract, an assessment should be made as to whether critical or important functions are affected. The material risks associated with the contract, including a potential increase in ICT concentration risk, as well as potential conflicts of interest, must be evaluated (see source for details).

Furthermore, third-party service providers must meet appropriate information security standards. For critical or essential functions, it must be ensured before the contract is concluded that the ICT third-party service providers apply the most current and highest quality standards for information security (see source for details).

According to paragraph 7, contracts with ICT service providers must be able to be terminated under certain conditions (e.g. non-compliance with essential agreements, weaknesses in ICT risk management, restrictions on supervisory oversight) (see source for details).

Appropriate exit strategies and plans for ICT services that affect critical or essential functions are intended to prevent disruptions and deterioration in business quality, as well as limitations in compliance with regulatory requirements. Exit plans must be regularly reviewed and tested as necessary. Transition plans should ensure alternative solutions, while ensuring business continuity in all cases (see source paragraph 8 for details).

Specifications for a register within the meaning of paragraph 3 and for its filling as well as further details on internal guidelines are to be published within the framework of technical implementing standards / regulatory standards (see source for details).

b) Preliminary assessment of ICT concentration risk at company level (Article 29)

When assessing ICT concentration risk, financial institutions should consider the substitutability of the ICT third-party service provider and the scope of contracts already in place with the respective ICT third-party service provider and its affiliates to support critical or essential functions (see source for details).

According to paragraph 2, possible sub-outsourcing of critical or important functions should be considered, particularly if these are provided by companies based in a third country. Factors such as data protection under EU law, legal enforceability, insolvency law provisions, the possibility of effective supervision by the competent authority, and outsourcing chains should be taken into account (see source for details).

c) Essential contractual provisions (Article 30)

The contractual provisions with the third-party ICT service provider, including service level agreements, should be contained in a written document and include the minimum content listed in paragraphs 2 and 3. In addition to a description of the services, these include provisions regarding subcontracting, reporting obligations, support in the event of an ICT incident, monitoring rights, training, determination of termination rights, and cooperation with third parties. Micro-enterprises may enter into different agreements regarding ongoing monitoring (see source for details).

According to paragraph 4, standard wording developed by public authorities for specific services should be used when drafting contracts.

Further details on the sub-outsourcing of critical or important functions shall be published through regulatory technical standards within 18 months of the entry into force of this Regulation.

2. Monitoring framework for critical ICT third-party service providers (Section II)

a) Classification of critical ICT third-party service providers (Article 31)

On the recommendation of a new supervisory forum to be established pursuant to Article 32(1), the ESAs will determine which ICT third-party service providers are to be classified as critical for financial undertakings and will designate a primary supervisory authority (EBA, ESMA or EIOPA) for each critical ICT third-party service provider (see source for details).

When classifying third-party service providers, according to paragraph 2, the systemic importance of the services provided by the third-party service provider and the contractually bound financial institutions, their market position, and potential substitutability – if applicable, at the group level – are assessed. Critical ICT third-party service providers belonging to a corporate group must appoint a legal entity as a coordinating body, which assumes the representative function and communicates with the lead supervisory authority. Following the corresponding classification by the supervisory authority, critical ICT service providers must inform their customers (see source for details).

The classification is only possible after the adoption of a delegated regulation by the EU Commission specifying the criteria described and does not apply to financial undertakings that provide ICT services to other financial undertakings, to third-party service providers that are subject to the European supervisory framework, to ICT services within a group of companies, or to third-party service providers that offer ICT services in only one Member State exclusively to financial undertakings that are only active in that Member State (see source for details).

The ESAs' list of critical ICT third-party service providers is updated annually. Third-party service providers can apply for inclusion on the list. Service providers based in a third country that have been classified as critical under paragraph 1 should only be used by financial institutions if they have established a subsidiary in the EU within 12 months of this classification (see source for details).

b) Structure of the monitoring framework (Article 32), tasks of the lead supervisory authority (Articles 33 - 43)

The Oversight Forum for critical ICT third-party service providers will be established as a subcommittee of the ESAs' Joint Committee with the participation of national supervisory authorities (Article 32).

It is the responsibility of the lead supervisory authority to examine whether a critical ICT third-party service provider has taken the necessary precautions to address potential ICT risks to which it may expose financial undertakings (see source Article 33 for details). To this end, it may request information from a critical ICT third-party service provider, impose fines on it, and conduct audits and investigations.
– including on-site and, if necessary, in third countries – and issue recommendations. The type and scope of the information, as well as the report content, are specified within the framework of technical regulatory standards (for details, see Articles 35 et seq.). If a critical ICT service provider fails to comply with the recommendations, the competent authority can, as a last resort, prohibit the financial institution from fulfilling its obligations and, if necessary, demand the termination of existing contracts (for details, see Article 42). The costs of supervision are charged to critical ICT service providers in the form of fees (Article 43).

VI. Agreements on the exchange of information (Chapter VI)

Agreements on the exchange of information and intelligence on cyber threats (Article 45)

Financial institutions may share cyber threat information and intelligence, including indicators of impairment, tactics, techniques and procedures, alerts, and configuration tools, for the purpose of improving digital operational resilience, provided this occurs within trusted circles and based on appropriate confidentiality agreements (see source for details). The competent authorities must be notified of both the initiation and termination of such agreements (see source for details).

VII. Competent authorities (Chapter VII)

Compliance with the requirements of this Regulation is monitored in accordance with Article 46 by the authority responsible for the respective type of institution or company under existing EU law (see source for details).

According to Article 50, the competent authorities are granted the appropriate rights of access, inspection, questioning, and action. According to Article 50(3) and (4), Member States should establish appropriate administrative sanctions and remedial measures for violations of this Regulation and provide the competent authorities with at least the specified powers to implement these measures. These include, for example, fines and the publication of violations and the identity of the companies responsible (see source for details).

Pursuant to Article 54, imposed sanctions must be published immediately on the official website of the competent authorities, stating the company concerned, and retained for a maximum of five years. Personal data may be stored and used by the ESAs and the competent authorities pursuant to Article 56 exclusively for specific purposes and in compliance with the principles of data protection under European law. (See source for details).

VIII. Transitional and final provisions (Chapter IX)

The requirements for rating agencies (*Regulation (EC) No 1060/2009 of the European Parliament and of the Council on credit rating agencies (Dataset 83)*), for central counterparties and trade repositories (*Regulation (EU) No. 648/2012 (EMIR, dataset 396)*), for central securities depositories (*Regulation (EU) No. 909/2014 (CSDR, Dataset 701)*), for data provision services (*Regulation (EU) No. 600/2014 (MiFIR, dataset 613)*) as well as for benchmarks and their administrators (*Regulation (EU) 2016/1011 (Benchmark Regulation, dataset 1069)*) will be adjusted (details see source Art. 58 ff).

CATEGORIZATION

Keywords

BIA, Business Impact Analysis, Governance, ICT Risk Management Framework, Financial Institutions, Risk Management, Information and Communication Technology, ICT, Digital Operational Resilience, ICT Risk, Threat-Led Penetration Test, TLPT, Critical Function, ICT Third Party Service Provider, Sanction, Fine,

Information exchange, cyber risk, cyber threat, service provider, outsourcing, critical ICT third-party service provider, sub-outsourcing, outsourcing, ICT concentration risk, auditor, resilience, digitalization, ICT system, ICT incident, test, development bank, proportionality principle, micro-enterprises, ICT information value, ICT asset, simplified ICT risk management framework, security-relevant incident, payment transactions, outsourcing, threat-oriented penetration testing, thread intelligence, ICT third-party service provider risk

Legal and information bases

- Proposal for a Directive of the European Parliament and of the Council concerning measures for a high common level of cybersecurity across the Union and repealing Directive (EU) 2016/1148 (NIS 2) (Dataset 4614)
- ESAs: Joint Recommendations (JC 2019 26) (Dataset 3592)
- Regulation (EU) 2016/1011 (Benchmark Regulation) (Dataset 1069)
- Directive 2015/2366/EU (PSD2) (Dataset 1036)
- Directive (EU) 2016/1148 (NIS Directive) (Dataset 910)
- Regulation (EU) No 1024/2013 (SSM Regulation) (Dataset 815)
- Regulation (EU) No. 909/2014 (CSDR) (Dataset 701)
- Directive 2014/65/EU (MiFID II) (Dataset 615)
- Regulation (EU) No. 600/2014 (MiFIR) (Dataset 613)
- Directive 2013/36/EU (CRD IV) (Dataset 550)
- Regulation (EU) No. 648/2012 (EMIR) (Dataset 396)
- Directive 2011/61/EU (AIFMD) (Dataset 136)
- Regulation (EC) No 1060/2009 of the European Parliament and of the Council on credit rating agencies (Dataset 83)
- Directive 2009/110/EC (data set 48)
- Directive 2009/138/EC of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (Solvency II)

Related Standards

- ESAs: Joint Recommendations (JC 2019 26) (Dataset 3592)

Target group – credit institutions

Yes

Target group – financial services institutions

Yes

Target group – Other companies in the financial sector
Yes

Target group – payment institutions
Yes

Target group – insurance companies
Yes

Target group – supplement

Comments

Statement by (date)

Implementation status Explanation

Status – Further Details

Date of entry into force/publication
January 16, 2023

Entry into force estimated?
No

Date of first application
January 17, 2025

Application appreciated?
No

Date Standard repealed

Remark (Entry into force/Publication)
This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union (publication on 27 December 2022).
It will apply from 17 January 2025.
The Regulation is binding in its entirety and directly applicable in all Member States.

Comments
This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union (publication on 27 December 2022).
It shall apply from 17 January 2025.
The Regulation shall be binding in its entirety and directly applicable in all Member States.

Sources
The sources are not shown in this working paper.