

# Ania

Associazione Nazionale  
fra le Imprese Assicuratrici

2023 Edition

## ANIA Exploring Digital Regulation

**Focus on** artificial intelligence, digital  
finance and cybersecurity



Associazione Nazionale  
fra le Imprese Assicuratrici

# INDEX

- 1.** Introduction to the Digital Operational Resilience Act
- 2.** Scope of application of DORA
- 3.** Relationship with other relevant pieces of law and regulation
- 4.** General overview of the new obligations applicable to financial entities
- 5.** ICT risk management - governance and organization measures
- 6.** ICT risk management – duty to adopt the relevant framework
- 7.** Management and classification of ICT-related incident
- 8.** Communicating and reporting obligations. Exchange of information
- 9.** Digital operational resilience testing
- 10.** Management of ICT third-party risk: main principles
- 11.** Management of ICT third-party risk: key contractual provisions
- 12.** Competent authorities, powers and sanctions

Newsletter **ANIA**

Contacts:

**Umberto Guidoni,  
Benedetta Carducci,  
Alessandra Diotallelli,  
Anna Giulia Ghislanzoni**

[exploringdigital@ania.it](mailto:exploringdigital@ania.it)

All rights are reserved by ANIA

## Foreword

ANIA's commitment to explore the evolution of **digital regulation** and the relevant impacts on the insurance market continues in 2023 with a new edition of the "ANIA Exploring Digital Regulation" newsletter.

This year's focus will be the analysis of the recently introduced **Regulation (EU) no. 2022/2554** of the European Parliament and of the Council of December 14, 2022 on **digital operational resilience for the financial sector**, so-called "**DORA**" ("**Digital Operational Resilience Act**").

DORA sets forth an harmonized legal framework within the EU, applicable to financial entities (**including insurance and reinsurance companies**), aimed at mitigating risks deriving from the increasing use of **information and communication technologies (ICT)** in financial markets.

In this perspective, DORA requires financial entities to implement comprehensive capabilities to enable a strong and effective ICT risk management, as well as specific mechanisms and policies for handling and reporting ICT-related incidents. This will have a **strong impact** on the Regulation's recipients, including under a corporate governance, organizational and operational perspective.

Therefore, each number of this newsletter will focus on the main aspects of the new Regulation, by providing a brief overview of the most relevant provisions and implications arising from it for market operators.

Such as the 2022 edition, also the 2023 newsletters will be issued on a regular basis, in a one-page format, and will be collected in a single volume to form a practical – and easy to use – reference guide in view of the forthcoming application of DORA.

Newsletter **ANIA**

Contacts:

**Umberto Guidoni,**  
**Benedetta Carducci,**  
**Alessandra Diotallevi,**  
**Anna Giulia Ghislanzoni**

[exploringdigital@ania.it](mailto:exploringdigital@ania.it)

# Introduction to the Digital Operational Resilience Act

1 FEBRUARY, 8  
2023

On **December 27, 2022**, the **Regulation (EU) no. 2022/2554** of the European Parliament and of the Council of December 14, 2022 on **digital operational resilience for the financial sector**, so-called “**DORA**” (“**Digital Operational Resilience Act**”), was published in the Official Journal of the European Union.

This Regulation is based on the **European Commission’s proposal (COM (2020) – 595 final)** issued on **September 24, 2020** as part of the so-called “*Digital finance package*”, and namely a set of measures aimed at further enabling and supporting the potential of digital finance within the EU in terms of innovation and competition while mitigating the relevant risks.

The main purpose of DORA is to **consolidate and upgrade information and communication technology (ICT) risk requirements** that have been addressed separately in various EU legal acts so far.

In this perspective, DORA operates an important **change in the applicable paradigm** to ensure **operational resilience**: so far, operational risk rules favoured a **traditional quantitative approach** to addressing the relevant risks (namely setting a capital requirement to cover ICT risk) rather than establishing **targeted qualitative rules** for the protection, detection, containment, recovery and repair capabilities against ICT-related incidents, or for reporting and digital testing capabilities.

Differently, for the first time DORA aims at bringing together in one single legislative act all provisions addressing digital risks in the financial sector in a consistent manner and filling-in the existing gaps and inconsistencies by explicitly setting forth **targeted rules on ICT risk-management capabilities, incident reporting, operational resilience testing and ICT third-party risk monitoring**.

Moreover, DORA raises awareness of ICT risk and acknowledges that ICT incidents and a **lack of operational resilience may jeopardize the soundness of financial entities**. This is true also for the **insurance sector**, which has been transformed by the use of ICT and the increasing offer by insurance intermediaries of their services online operating with **InsurTech** as well as the use of digital insurance underwriting.

In order to reach the aforementioned objectives, DORA requires financial entities to follow the same approach and the same principle-based rules when addressing ICT risk, taking into account their **size and overall risk profile**, and the **nature, scale and complexity** of their services, activities and operations in line with the **proportionality principle**.

DORA entered into force on **January 16, 2023** and its provisions will become enforceable starting from **January 17, 2025**.

Therefore, before DORA’s enforceability all financial entities included in its scope of application shall be ready to implement its provisions, which incorporate the best practices, recommendations, guidelines and approaches for a comprehensive management of ICT-related risk, whose responsibility lies within the **management body**.

## Ania

Associazione Nazionale  
fra le Imprese Assicuratrici

←---- [BACK TO THE INDEX](#)



Newsletter **ANIA**

Contacts:

**Angelo Doni,**  
**Umberto Guidoni,**  
**Benedetta Carducci,**  
**Alessandra Diotallevi,**  
**Anna Giulia Ghislanzoni**

[exploringdigital@ania.it](mailto:exploringdigital@ania.it)

All rights are reserved by ANIA



# Ania

Associazione Nazionale  
fra le Imprese Assicuratrici

←---- [BACK TO THE INDEX](#)

The Digital Operational Resilience Act (so-called “**DORA**” - Regulation (EU) no. 2022/2554, hereinafter the “**Regulation**”) aims at establishing a **common legal framework** for the **digital operational resilience** of financial entities; for this purpose, it has a **wide scope of application**.

**Subjectively**, DORA applies to **all financial entities** such as, in particular, “*insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries*” as well as “*ICT third-party service providers*”.  Art. 2, letter from a) to t), DORA

For these purposes, DORA refers to the notions of “*insurance undertaking*”, “*reinsurance undertaking*”, “*insurance intermediary*” and “*ancillary insurance intermediary*” provided, respectively, by Directive 2009/138/EC and Directive (EU) 2016/97.

Without prejudice to the above, DORA expressly takes into account that certain financial entities - including insurance and reinsurance undertakings - benefit from **exemptions or are subject to a very light regulatory framework** under the relevant sector-specific Union law when the relevant conditions occur. In addition, DORA expressly acknowledges the **specificities of the insurance intermediation market structure** and the exemptions applicable to microenterprises or as small or medium-sized enterprises.

Therefore, in application of the **proportionality principle** underpinning the entire DORA, **the Regulation does not apply to, *inter alia*, insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries which are microenterprises or small or medium-sized enterprises.**

 Art. 2, par. 2 of DORA and Art. 4 Directive 2009/138/EC

As regards the **objective scope of application of DORA**, the Regulation relates to **all types of ICT services for operators of the whole financial sector**.

In this perspective, DORA defines “**ICT services**” as “*digital and data services provided through ICT systems to one or more internal or external users on an ongoing basis, including hardware as a service and hardware services which includes the provision of technical support via software or firmware updates by the hardware provider, excluding traditional analogue telephone services*”.

Therefore, the Regulation imposes specific obligations binding upon all financial entities relating to **prevention, management, monitoring and communication** of risks connected to the provision of ICT services.

Newsletter **ANIA**

Contacts:

**Angelo Doni,**  
**Umberto Guidoni,**  
**Benedetta Carducci,**  
**Alessandra Diotallevi,**  
**Anna Giulia Ghislanzoni**  
[exploringdigital@ania.it](mailto:exploringdigital@ania.it)

# Relationship with other relevant pieces of law and regulation

**3** APRIL, 6  
2023

## Ania

Associazione Nazionale  
fra le Imprese Assicuratrici

The Digital Operational Resilience Act (so-called “**DORA**” - Regulation (EU) no. 2022/2554) aims at consolidating and upgrading ICT risk requirements as part of the operational risk requirements that have been addressed separately in several Union legal acts so far.

Reference shall be made, first of all, to **Directive (EU) 2016/1148** of the European Parliament and of the Council (concerning measures for a high common level of security of network and information systems across the Union), **now repealed**, which was the first horizontal cybersecurity framework enacted at Union level, and which used to apply to three types of financial entities, namely **credit institutions, trading venues and central counterparties**.


As of today, **NIS 2 Directive (Directive (EU) 2022/2555** on measures for a high common level of cybersecurity across the Union) repealed Directive (EU) 2016/1148 and sets forth a uniform criterion to determine the entities falling within its scope of application (size-threshold rule).

In this perspective, DORA further increases the level of harmonization of the various digital resilience components by introducing **requirements on ICT risk management and ICT-related incident reporting that are more stringent** than those laid down in the current Union financial services law, including under NIS2 Directive.

In addition, the obligations laid down in Chapters III (*Resilience of critical entities*) and Chapter IV (*Critical entities of particular European significance*) of **Directive (EU) 2022/2557 on the resilience of critical** entities should not apply to **financial entities** falling within the scope of that Directive, as the **physical resilience** of financial entities is now governed by the ICT risk management and the reporting obligations covered by **DORA**:

 **whereas no. 19 of DORA**

Moreover, considering that DORA - together with **Directive (EU) 2022/2556 on digital operational resilience for the financial sector** - entails a consolidation of the provisions for the management of ICT risks, DORA **amends and limits** the scope of Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 accordingly.

Finally, it shall be pointed out that DORA leaves unaffected the responsibility of Member States with regard to essential State functions concerning **public security, defence and the protection of national security**, including as regards the supply of information which would be contrary to the protection of each Member State's strategic interests:  **whereas no. 17 of DORA**

[←---- BACK TO THE INDEX](#)



Newsletter **ANIA**

Contacts:

**Angelo Doni,**  
**Umberto Guidoni,**  
**Benedetta Carducci,**  
**Alessandra Diotallevi,**  
**Anna Giulia Ghislanzoni**  
[exploringdigital@ania.it](mailto:exploringdigital@ania.it)

All rights are reserved by **ANIA**

# General overview of the new obligations applicable to financial entities

# Ania

Associazione Nazionale  
fra le Imprese Assicuratrici

←---- [BACK TO THE INDEX](#)

Digital Operational Resilience Act (so-called “DORA” - Regulation (EU) no. 2022/2554) sets forth **several obligations applicable to the financial entities falling within its scope of application**. These obligations are aimed at harmonizing key digital operational resilience requirements for all financial entities and at contributing to ensure a high level of protection of investors and consumers in the Union.

In general, reference shall be made to the provisions set out under:

(i) **Chapter II (“ICT risk management”),**



Artt. 6, 7, 8, 9, 10 DORA (“ICT risk management framework”; “ICT systems, protocols and tools”; “Identification”; “Protection and prevention”; “Detection”)


(ii) **Chapter III (“ICT-related incident management, classification and reporting”)**



Artt. 18, 19 DORA (“Classification of ICT-related incidents and cyber threats”; “Reporting of major ICT-related incidents and voluntary notification of significant cyber threat”)

(iii) **Chapter IV (“Digital operational resilience testing”),** and (iv) **Chapter V (“Managing of ICT third-party risk”).**

More specifically, particular attention shall be paid to, among others, the provisions regarding (a) the adoption of an **internal governance and organization framework**; (b) the adoption of an **ICT risk and related incidents management system**, including those derived from or caused by third parties; and (c) the **creation of information sharing protocols**.

Financial entities are required to **assign specific tasks and powers to the management body** which, thus, shall be entitled to approve and enforce all ICT risk management provisions and shall be fully responsible in relation to their implementation.  **whereas no. 45 and 46 of DORA**

In addition, financial entities must also adopt an **ICT Risk Management Framework** aimed at harmonizing the risk management rules related to ICT risks, including those arising from third parties, at each stage of their life cycle, with an end-to-end view of business processes. This includes the **classification** of cyber incidents and threats and the establishment of an appropriate **reporting system**.

In fact, DORA requires the establishment of procedures to identify, track, record, categorize, and classify ICT related incidents according to their priority, severity, and criticality as well as assigning **roles and responsibilities to internal personnel** in order to **notify** such incidents to the relevant authorities. In this respect, the recipients of DORA shall also adopt **information sharing protocols** aimed at encouraging the exchange of cyber threat information between them.

Newsletter **ANIA**

Contacts:

**Angelo Doni,**  
**Umberto Guidoni,**  
**Benedetta Carducci,**  
**Alessandra Diotallevi,**  
**Anna Giulia Ghislanzoni**  
[exploringdigital@ania.it](mailto:exploringdigital@ania.it)



# ICT risk management - governance and organization measures

5 JUNE, 12  
2023

Ania

Associazione Nazionale  
fra le Imprese Assicuratrici

Financial entities falling within the scope of application of the Digital Operational Resilience Act (so-called “**DORA**” – Regulation (EU) no. 2022/2554) are required to adopt specific **policies and corporate governance measures** in order to ensure a full and effective control over ICT risks, including those deriving from third parties in case of outsourcing of ICT services.

In particular, DORA imposes on its recipients to have in place an **internal governance and control framework** that ensures an effective and prudent management of ICT risk, provided that the relevant provisions are characterized by a gradual application on the basis of the size of the financial entities concerned, consistently with the **proportionality principle**.

 whereas n. 38 DORA; Art. 5, par. 1, DORA (“Governance and organization”)

The **management body** has the responsibility to define, approve and monitor the implementation of all measures related to the ICT management framework. It must, among others: (a) bear the ultimate **responsibility for managing** the financial entity’s ICT risk; (b) put in place policies that aim to ensure the maintenance of **high standards** of availability, authenticity, integrity and confidentiality of data; (c) set clear **roles and responsibilities** for all ICT-related functions and establish appropriate **governance arrangements** in this regard; (d) bear the overall responsibility for setting and approving the digital **operational resilience strategy**; (e) approve, oversee and periodically review the implementation of the financial entity’s **ICT business continuity policy and ICT response and recovery plans**; (f) approve and periodically review the financial entity’s ICT internal **audit plans**; (g) allocate and periodically review the appropriate **budget** to fulfil the financial entity’s digital operational resilience needs; (h) approve and periodically review the financial entity’s policy on arrangements regarding the use of **ICT services provided by ICT third-party service providers**; (i) put in place reporting channels between the relevant functions at corporate level.


 Art. 5, par. 2, DORA (“Governance and organization”)

Without prejudice to the above, financial entities other than microenterprises shall allocate the responsibility for managing and overseeing ICT risk on an **independent control function** in order to avoid conflicts of interest.

 Art. 6, par. 4, DORA (“ICT risk management framework”)

Moreover, larger financial entities shall **establish a role** in order to monitor the arrangements undertaken with ICT third-party service providers on the use of ICT services or shall designate a member of **senior management** as responsible for monitoring the related risk exposure and relevant documentation.

 Art. 5, par. 3, DORA (“Governance and organization”)

In any case, all financial entities are required to ensure appropriate **segregation and independence** of ICT risk management functions, control functions, and internal audit functions.  Art. 6, par.4, DPRA “ICT risk management framework”)

[←--- BACK TO THE INDEX](#)



Newsletter **ANIA**

Contacts:

**Umberto Guidoni,  
Benedetta Carducci,  
Alessandra Diotallevi,  
Anna Giulia Ghislanzoni**

[exploringdigital@ania.it](mailto:exploringdigital@ania.it)

All rights are reserved by **ANIA**




# ICT risk management - duty to adopt the relevant framework


# Ania


Associazione Nazionale  
fra le Imprese Assicuratrici


←--- [BACK TO THE INDEX](#)

Financial entities falling within the scope of application of the Digital Operational Resilience Act (so-called “**DORA**” – Regulation (EU) no. 2022/2554) are required to adopt a specific **legal framework** in order to manage ICT risks, by applying ICT strategies, policies, procedures, protocols and tools **to protect their information assets and their IT and physical infrastructure**. In essence, DORA defines a set of obligations that financial entities are **mandatorily** required to perform in order to ensure a high level of digital operational resilience.

In particular, DORA requires its recipients to **prevent and reduce the impact of cyber risk** by establishing “*methods to address cyber risks and achieve specific ICT objectives*”.  **art. 6, par. 8, DORA**

As a general principle, when allocating resources and capabilities for implementing the ICT risk management framework, financial entities should find the right **balance** between **their own ICT needs**, on the one hand, and **their overall risk**, as well as the nature, scope and complexity of their services, activities and operations on the other.  **whereas n. 36, DORA**

In this perspective, DORA requires that responsibilities for managing and overseeing cyber risks be assigned to a “Level II” independent oversight function and, among others, that the ICT risk management framework shall be: (a) **documented and reviewed** at least annually or periodically; and (b) **periodically audited internally**. Moreover, on the basis of the audit activity, financial entities shall establish a formal **process to follow up on it**, including rules for timely verification of critical findings and adoption of remedies.  **Whereas N. 43; Art. 6, parr. 4, 7, DORA**

In order to ensure full alignment and overall consistency between the business strategies of financial entities, on the one hand, and IT risk management, on the other, **management bodies** of financial entities are required to maintain an **active and key role** in guiding and adapting the framework for managing of cyber risks and the overall digital operational resilience strategy.  **whereas n. 45, DORA**

Furthermore, the ICT risk management framework shall include a digital operational resilience strategy that defines how the relevant framework is **implemented**; in this context, financial entities may establish a holistic ICT strategy at the group or entity level.

In accordance with EU and national sectoral regulations, financial entities may also entrust companies within or outside the group with the tasks of **verifying compliance with ICT risk management requirements**; even in case of outsourcing, financial entities remain fully responsible for the verification of compliance.  **Art. 6, parr. 8, 9, 10, DORA**

Newsletter **ANIA**

Contacts:

**Umberto Guidoni,  
Benedetta Carducci,  
Alessandra Diotallevi**


[exploringdigital@ania.it](mailto:exploringdigital@ania.it)

# Management and classification of ICT-related incident

7 AUGUST, 4  
2023

Ania


Associazione Nazionale  
fra le Imprese Assicuratrici

Financial entities falling within the scope of application of the Digital Operational Resilience Act (so-called “**DORA**” - Regulation (EU) no. 2022/2554) are required to establish and implement an **ICT-related incident management process to detect, manage and notify ICT-related incidents**.  [art. 17, par. 2, DORA](#)


This implies the adoption of appropriate **processes and procedures** to ensure a consistent and integrated monitoring, handling and follow-up of ICT-related incidents to ensure that root causes are identified, documented and addressed in order to prevent the occurrence of such incidents.

 [art. 17, par. 3, DORA](#)

Such procedures shall include, among others: the identification of **early warnings indicators**, the attribution and of **roles and responsibilities** within the entity's organization, the establishment of **communications plans** to staff, external stakeholders and media, the establishment of ICT-related incident **response procedures** to mitigate impacts and ensure that services become operational and secure in a timely manner, etc.

For these purposes, DORA sets forth **common criteria for the classification of ICT-related incidents and cyber threats**, including: (i) the number and/or relevance of clients/financial counterparties/transactions affected by the disruption caused by the ICT incident and whether or not this incident caused a reputational impact; (ii) the duration of the ICT incident, including the period of service downtime; (iii) the geographical spread of the ICT incident; (iv) the data losses resulting from the ICT incident, in relation to availability, authenticity, integrity, or confidentiality of data; (v) the criticality of the affected services and (vi) the economic impact of the ICT incident (in particular direct and indirect costs and losses).  [art. 18, DORA](#)

In addition, the ESAs shall develop further common draft regulatory technical standards for the purposes of such classification.

Moreover, financial entities shall **report** - through **initial notification, interim and final reports** - major ICT-related incidents to the relevant **competent authority**. Upon receipt of such documents, details on the major ICT-related incidents are provided (depending on the case and including the nature of the financial entity concerned) to EBA, ESMA, EIOPA, ECB and/or other relevant public authorities under national law, in order to allow a discussion on the **remedies** applied at the level of the financial entity and ways to **minimise and mitigate adverse impact** across the financial sector.  [artt. 20 & subs; art. 46, DORA](#)

[← BACK TO THE INDEX](#)



Newsletter **ANIA**

Contacts:

**Umberto Guidoni,**  
**Benedetta Carducci,**  
**Alessandra Diotallevi**

[exploringdigital@ania.it](mailto:exploringdigital@ania.it)

All rights are reserved by **ANIA**


# Communicating and reporting obligations. Exchange of information


# Ania

Associazione Nazionale  
fra le Imprese Assicuratrici


←--- [BACK TO THE INDEX](#)


Among the main aspects regulated by the Digital Operational Resilience Act (so-called “**DORA**” – Regulation (EU) no. 2022/2554), **discipline of communication, sharing of information and reporting of cyber risks and threats** plays a key role.



Communication and sharing of information on threats and vulnerabilities between financial entities contributes to (i) create increased **awareness** of cyber threats and (ii) enhance the capacity of financial entities to **prevent** cyber threats from becoming real ICT-related incidents and (iii) enables financial entities to contain more effectively the impact of ICT-related incidents and to **recover** faster.  [whereas n. 32, DORA](#)

Therefore the Regulation fosters mechanisms for **voluntary information-sharing**, in order to help financial operators prevent and collectively respond to cyber threats by quickly limiting the spread of ICT risks and impeding potential contagion throughout the financial channels.  [whereas n. 34, DORA](#)

Article 14 of DORA regulates **the disclosure profile of information on ICT risks**: it requires financial entities, within the ICT risk management framework, **to prepare and implement (i) crisis communication plans and (ii) communication policies for internal staff and external stakeholders**.  [Art. 14, par. 1 & 2, DORA](#)

Article 45 of DORA recognises the possibility to exchange cyber threat information and analysis among financial entities, provided that such sharing (i) enhances their digital operational resilience; (ii) takes place within what DORA identifies as “trusted communities of financial entities” and (iii) is carried out in full protection of potential sensitive information, of business confidentiality and of personal data protection under Regulation (EU) 2016/679 (GDPR) and of competition policy guidelines.  [Art. 45, par. 1, letters a\), b\) & c\), DORA](#)

**Information-sharing mechanisms must also provide for the possible involvement of public authorities and third-party ICT service providers, as well as for the operational elements set up for this purpose** (such as, for instance, the use of IT platforms).  [Art. 45, par. 2, DORA](#)

Finally, **DORA** requires the notification to the relevant authorities of the willingness to participate in sharing mechanisms and **encourages the European Supervisory Authorities (ESAs) to set up mechanisms to facilitate the sharing of effective practices across financial sectors**, in order to improve awareness and identification of cyber risks and vulnerabilities common to all sectors.  [Art. 45, par. 3, DORA](#)  [Art. 49, par. 1, DORA](#)

Newsletter **ANIA**


Contacts:


**Umberto Guidoni,  
Benedetta Carducci,  
Alessandra Diotallevi**



[exploringdigital@ania.it](mailto:exploringdigital@ania.it)


All rights are reserved by ANIA



The Digital Operational Resilience Act (so-called “**DORA**” - Regulation (EU) no. 2022/2554) provides that financial entities shall establish, maintain and review a sound and comprehensive **digital operational resilience testing programme as an integral part of the ICT risk-management framework** in order to assess preparedness for handling ICT-related incidents, identifying weaknesses, deficiencies and gaps in digital operational resilience.  Art. 24, par. 1, DORA

In particular, this implies the creation of a system that shall include a range of assessments, tests, methodologies, practices and tools to be applied in accordance with Articles 25 and 26 of DORA, rather than a mere “functional test”.  Art. 24, par. 2, DORA

For the above purposes financial entities, other than microenterprises shall execute appropriate **tests of ICT tools and systems** (i.e. vulnerability assessments and scans, open source analyses, network security assessments, gap analyses, physical security reviews, questionnaires and scanning software solutions, source code reviews where feasible, scenario-based tests, compatibility testing, performance testing, end-to-end and penetration testing), as well as at least every 3 years **advanced testing** by means of TLPT (**Threat-Led Penetration Testing**), the frequency of which may be modified by the competent Authority according to the operational circumstances of the financial entity.  Art. 25, par. 1 & 2, DORA  Art. 26, par. 1, DORA

In particular, as per the carrying out of TLPT, financial entities shall only use testers, that: (i) are of the highest suitability and reputability; (ii) possess technical and organisational capabilities and demonstrate specific expertise in threat intelligence, penetration testing and red team testing; (iii) are certified by an accreditation body in a Member State or adhere to formal codes of conduct or ethical frameworks; (iv) provide an independent assurance, or an audit report, in relation to the sound management of risks associated with the carrying out of TLPT, including the due protection of the financial entity’s confidential information and redress for the business risks of the financial entity and (v) that are duly and fully covered by relevant professional indemnity insurances, including against risks of misconduct and negligence.  Art. 27, par. 1, DORA

**Microenterprises shall perform the tests referred to in Article 25, paragraph 1** (see above), by combining a risk-based approach with a strategic planning of ICT testing, by duly considering the need to maintain a balanced approach between the scale of resources and the time to be allocated to the ICT testing provided for in Article 25 of DORA, on the one hand, and the urgency, type of risk, criticality of information assets and of services provided, as well as any other relevant factor, including the financial entity’s ability to take calculated risks, on the other hand.

 Art. 25, par. 3, DORA

[←--- BACK TO THE INDEX](#)



Newsletter **ANIA**

Contacts:

**Umberto Guidoni,  
Benedetta Carducci,  
Alessandra Diotallevi**

[exploringdigital@ania.it](mailto:exploringdigital@ania.it)

# Management of ICT third-party risk: main principles



# Ania


Associazione Nazionale  
fra le Imprese Assicuratrici


←---- [BACK TO THE INDEX](#)

The Digital Operational Resilience Act (so-called “DORA” - Regulation (EU) no. 2022/2554) sets forth in Chapter V (“**Managing of ICT third-party risk**”) – Section I (“**Key principles for a sound management of ICT third-party risk**”) key principles to guide financial entities’ management of ICT third-party risk, which are of particular importance when financial entities resort to ICT third-party service providers to support their critical or important functions.

 [whereas n. 29, DORA](#)

According to DORA, those principles should be accompanied by a set of **core contractual rights** in relation to several elements in the **performance** and **termination** of **contractual arrangements**. This in order to provide certain minimum safeguards and to strengthen financial entities’ ability to effectively monitor all ICT risk emerging at the level of third-party service providers. In this perspective **financial entities may define a holistic ICT multi-vendor strategy**, at group or entity level, **showing key dependencies** on ICT third-party service providers and **explaining the rationale** behind the procurement mix of ICT third-party service providers. In this regard, DORA’s aim is also to give greater prominence to the potential systemic risks arising from **concentration under the same ICT service provider** (or corporate group).  [whereas nn. 29, 30 & 31, DORA](#)  [Art. 6, par. 9, DORA](#)

Thus, in the context of the ICT cyber risk management framework, financial entities shall adopt and periodically review a **strategy for cyber risks arising from third parties**, taking into account the strategy based on a variety of providers referred to in Article 6 paragraph 9, when applicable. This strategy shall include a **policy for the use of ICT services** to support essential or important functions provided by third-party vendors and shall be applied on an individual and, where appropriate, sub-consolidated and consolidated basis. Based on an assessment of the financial entity’s overall risk profile and the scope and complexity of operational services, the management body shall periodically review the risks identified in relation to contractual arrangements for the use of ICT services to support essential or important functions.  [Art. 28, par. 2, DORA](#)

Moreover, according to the **strategic importance of ICT service providers** in the day-to-day performance of financial entities’ activities, whether they are entrusted with services that qualify as outsourcing or not, **DORA emphasises the need to regulate in detail the relevant contracts** (which must be properly documented) **and the effects of their termination**. In particular, **DORA requires financial institutions to report annually to the relevant authorities the number of agreements entered into and to have exit plans** (to be reviewed periodically) **in the event of well-identified regulatory or contractual breaches or supervening circumstances** that change risks and/or alter the provider’s ability to perform assigned functions and/or impair its ability to ensure availability, authenticity, integrity and confidentiality of data and information, or an inability of the competent authority to supervise the financial entity effectively due to the terms of the contractual agreement at hand.  [Art. 28, parr. 3 & subs., DORA](#)

Newsletter **ANIA**

Contacts:

**Umberto Guidoni,  
Benedetta Carducci,  
Alessandra Diotallevi**


[exploringdigital@ania.it](mailto:exploringdigital@ania.it)

# Management of ICT third-party risk: key contractual provisions

11 NOVEMBER, 22  
2023


Ania

Associazione Nazionale  
fra le Imprese Assicuratrici

**Financial entities** falling within the scope of application of the Digital Operational Resilience Act (so-called “**DORA**” – Regulation (EU) no. 2022/2554) are required to comply with certain **requirements** in order to ensure control of their operational risks, information security and business continuity throughout the whole duration of contractual agreements with third-parties.  **Art. 28, DORA**


In particular, financial entities (i) shall maintain and update at entity level, and at sub-consolidated and consolidated levels, a **register of information** in relation to all **contractual arrangements** on the use of ICT services provided by ICT third-party service providers, distinguishing between those that cover ICT services supporting critical or important functions and those that do not and (ii) shall pay attention to the so-called **lock-in mechanisms** that may result from entering into a contract with a particular supplier.

 **Art. 28, par. 3, DORA; Art. 29, DORA**

The latter implies a **preliminary assessment** in order to evaluate whether the envisaged conclusion of a contractual arrangement in relation to ICT services supporting critical or important functions would lead to: (i) contracting an ICT third-party service provider that is **not easily substitutable**; or (ii) having in place **multiple contractual arrangements** in relation to the provision of ICT services supporting critical or important functions with **the same** ICT third-party service provider or with **closely connected** ICT third-party service providers.  **Art. 29, par. 1, DORA**

In this perspective, DORA also identifies **key contractual provisions** that must be included in the contractual arrangements on ICT services use such as, among others: (i) a clear and complete **description** of all functions and ICT services to be provided by the ICT third-party service provider; (ii) the obligation of the ICT third-party service provider to **provide assistance** to the financial entity; (iii) the obligation of the ICT third-party service provider to fully **cooperate** with the competent authorities and (iv) the resolution authorities of the financial entity and the termination rights and related minimum notice periods for the termination of the contractual arrangements.

 **Art. 30, par. 2, letters a), b), f), g), DORA**

That being said, additional provision will need to be set out for **termination of the contract** in case of well-identified regulatory or contractual breaches, supervening circumstances that change the risks and/or affect the supplier's ability to perform assigned functions and/or impair the supplier's ability to ensure the availability, authenticity, integrity and confidentiality of data and information, or a supervening inability on the part of the competent authority to effectively supervise the financial entity due to the terms of the contractual agreement in question.  **Art. 28, par. 8, DORA**

[←--- BACK TO THE INDEX](#)

Newsletter **ANIA**

Contacts:

**Umberto Guidoni,  
Benedetta Carducci,  
Alessandra Diotallevi**

[exploringdigital@ania.it](mailto:exploringdigital@ania.it)

All rights are reserved by **ANIA**



# Competent authorities, powers and sanctions

# Ania

Associazione Nazionale  
fra le Imprese Assicuratrici

←--- [BACK TO THE INDEX](#)

Without prejudice to the provisions on the Oversight Framework for critical ICT third-party service providers referred to in Chapter V, Section II, of the Digital Operational Resilience Act (so-called “**DORA**” - Regulation (EU) no. 2022/2554), **compliance with DORA** shall be ensured by the competent authorities in accordance with the powers granted by the respective legal acts listed under **Article 46 of DORA**.

Competent authorities shall have all **supervisory, investigatory and sanctioning powers** necessary to fulfil their duties under DORA and in particular at least the following: (i) to have **access** to or take a copy of any relevant document or data held in any form; (ii) to carry out on-site **inspections** or **investigations**, which shall include but shall not be limited to (a) summoning representatives of the financial entities for oral or written explanations on facts or documents relating to the subject matter and purpose of the investigation and to record the answers and (b) interviewing any other natural or legal person in order to collect information relating to the subject matter of an investigation; and (iii) to require corrective and remedial **measures for breaches** of the requirements of DORA.

🔍 Art. 50, par. 1 & 2, DORA

In this perspective, without prejudice to the right of Member States to impose **criminal penalties** in accordance with Article 52, Member States shall lay down rules establishing appropriate **administrative penalties and remedial measures** (which shall be effective, proportionate and dissuasive) for breaches of DORA and shall ensure their effective implementation.

In particular, Member States shall confer on competent authorities the power to apply at least the aforementioned administrative penalties or remedial measures for breaches of DORA. Also, where Article 50 applies to legal persons, Member States shall grant competent authorities with the power to apply the administrative penalties and remedial measures - subject to the conditions provided for in national law - **to members of the management body and to other individuals who under national law are responsible for the breach**. 🔍 Art. 50, par. 5, DORA

Consequently, competent authorities shall exercise the powers to impose administrative penalties and remedial measures in accordance with their national legal frameworks, taking into account whether **the breach is intentional or results from negligence**, and all other relevant circumstances and **publishing on their official websites**, without undue delay, any decision imposing an administrative penalty against which there is no appeal after the addressee of the penalty has been notified of that decision. 🔍 Art. 51, par. 1 & 2; Art. 54, par. 1, DORA

Newsletter **ANIA**

Contacts:

**Umberto Guidoni,  
Benedetta Carducci,  
Alessandra Diotallevi**

[exploringdigital@ania.it](mailto:exploringdigital@ania.it)

**ANIA**, the Italian Insurance Association,  
founded in 1944, is a voluntary non-profit association.  
Its main purpose is to develop and spread the culture of safety  
and prevention in our country, so as to protect both people  
and companies, and society as a whole, more and better.

Moreover, ANIA represents its members and the Italian insurance market  
vis-à-vis the main political and administrative institutions, including the  
Government and Parliament,  
trade unions and other social bodies.

The Association studies and cooperates in the resolution  
of technical, economic, financial, administrative, fiscal, social, juridical and  
legislative issues concerning the insurance industry.  
It supports and provides technical assistance to members,  
promotes the education and professional training of those  
working in the insurance sector.

Ania

Associazione Nazionale  
fra le Imprese Assicuratrici

Via di S. Nicola da Tolentino, 72 | 00187 Roma | Tel. 06.326881

[www.ania.it](http://www.ania.it)