Outcome Report of the Self-Assessment Related to Entities' Preparation for DORA

Directorate-General for Strategic Policy and International Affairs

Department of Strategy, Innovation, and Sustainable Finance

4 December 2024

Table of contents

1 Introduction

In December 2022, the DORA Regulation on digital operational resilience was published as part of the digital finance package. This regulation will come into effect on 17 January 2025.

While several level 2 and 3 regulatory measures are still awaiting approval by the European Commission, the final drafts of all these measures have already been published.

The CNMV has introduced a self-assessment form, which is not intended as a supervisory exercise, with two main goals:

— To assess how prepared investment firms and management companies are for DORA.

— To promote self-assessment, enabling institutions to identify gaps in compliance with the Regulation and plan their implementation accordingly.

Throughout this document, you will find highlighted boxes containing recommendations (indicated by), expectations ( ), key regulations ( ), and references to more technical guidance materials. These may be particularly useful for **small and medium-sized companies**.

The data in this report are based on an analysis of responses from companies to the questionnaire developed by the CNMV. This constitutes a self-assessment exercise conducted by the companies, and their responses have not been verified by the CNMV.

The report offers recommendations to the sector, but it should not be considered regulatory in nature under any circumstances.

2 Questionnaire on DORA readiness

The number and content of questions in the questionnaire have been tailored according to the size of the organisation.[1]

The questionnaire is divided into the following sections:

— **General section** for data collection on the organisation and its current DORA implementation status.

— **Risk management related to information and communication technologies (ICT).** This section includes the following areas:

  - Governance and organisation.
  - ICT risk management framework.
  - Policies and procedures.
  - Identification, detection, protection, response, and recovery.

— **ICT incident management, classification, and reporting.**

— **Digital operational resilience testing.**

— **Management of ICT-related third-party risk.**

To evaluate the level of maturity, many questions offered three possible answers: i) a very comprehensive implementation of the DORA requirements, ii) a partial implementation, and iii) whether the Regulation is yet to be implemented.

In other questions, organisations needed to select applicable options from a list of elements (e.g., contract clauses with providers, types of resilience testing conducted, protection measures, etc.).

1 For instance, micro-enterprises are exempt from certain requirements such as Article 5.3, and small, non-interconnected investment firms follow a simplified ICT risk management framework outlined in Article 16, instead of the requirements set out in Articles 5 to 15 (see recitals 42 and 43 of DORA).

Financial institutions are advised to review the final drafts of the RTS and ITS[2] once they are approved. Updates on regulatory developments can be found on the CNMV website under the "Cybersecurity"[3] section and on the websites of the European Supervisory Authorities (ESAs).[4]

2 RTS: regulatory technical standards, ITS: implementing technical standards.

3 https://www.cnmv.es/portal/ciberseguridad.aspx?lang=en

4 https://finance.ec.europa.eu/digital-finance/cyber-resilience_en

3 Participation of financial institutions

The CNMV acts as the competent authority under DORA for the following types of financial institutions (Articles 2 and 46 of DORA):

— Investment firms (excluding national financial advisory firms [EAFNs]).

— Management companies.

— Alternative investment fund managers (except those specified in Article 2.3.a)).

— Crowdfunding service providers.

— Crypto-asset service providers.

— Administrators of critical benchmarks.

— Market infrastructures (including central securities depositories, central counterparties, and trading venues).

However, this questionnaire was targeted only at investment firms (IFs), management companies, and crowdfunding service providers (PSFPs). These entities could submit their responses **during June and July 2024**.

The participation rate was 74%. In total, responses were received from **245 entities**: 142 from investment firms (IFs), 94 from fund managers, and 9 from crowdfunding service providers (PSFPs).

— Among the 190 investment firms, 81 responses came from broker-dealers and brokers (SAV), while 61 were from financial advisory firms (EAF).

— Out of the 112 management companies subject to DORA, 89 collective investment scheme management companies (CISMC) and 5 venture capital management companies (SGECR) provided responses.

Participation of financial institutions

TABLE 1

	IFs	Management companies	Crowdfunding platforms	Total
Number of institutions	190	112	26	328
Participation	142	94	9	245
%	74.74	83.93	34.62	74.70

Source: CNMV.

Participation by investment firms and management companies

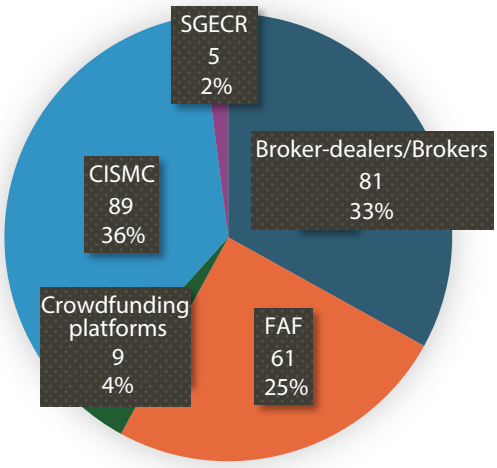
TABLE 2

	IFs		Management companies	
	FAF	Broker-dealers/ brokers	CISMC	SGECR
Number of institutions	89	101	101	11
Participation	61	81	89	5
%	68.54	80.20	88.12	45.45

Source: CNMV.

Participation by institution type

FIGURE 1



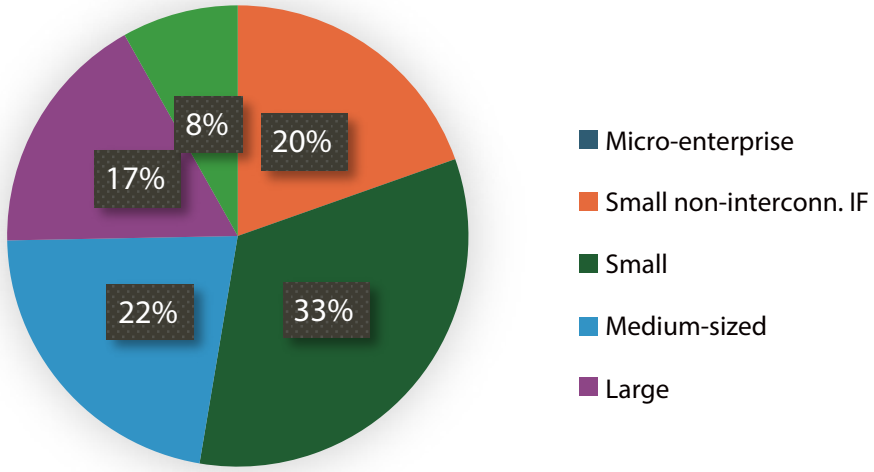
Source: CNMV.

It is important to note that 152 fund managers (16 CISMCs and 136 SGECRs) did not take part in this survey because they are outside DORA's scope, managing only alternative funds and not exceeding the thresholds specified in Article 3.2 of Directive 2011/61 on alternative investment fund managers.

Fund management companies excluded from DORA's scope are advised to voluntarily adopt the regulation if they anticipate exceeding these thresholds in the short or medium term.

Among those who responded to the questionnaire, using the size classification in Article 3 of DORA, only 8% (20) are **large companies**. The majority are **SMEs**, with a significant number of **micro-enterprises** (20%, or 48 in total), and 33% (81) benefit from the **simplified risk management framework.**[5]

Size of institutions FIGURE 2



Source: CNMV.

Since DORA establishes a unified regulatory framework for all financial entities – from large banks, insurance companies, and market infrastructures to small financial advisory firms – the principle of **proportionality** is crucial within the regulation and its RTS.

Specifically, Article 4 of the regulation addresses this principle:

> 1. Financial entities **shall apply the rules** set out in Chapter II (risk management framework) in accordance with the principle of proportionality, **taking into account their size, overall risk profile, and the nature, scale, and complexity of their services, activities, and operations**.
>
> 2. Furthermore, the **application** by financial entities of Chapters III and IV (incident reporting and testing) and Chapter V (ICT risks from third parties), Section I, shall be **proportionate to their overall size and risk profile, as well as to the nature, scale, and complexity of their services, activities, and operations,** as specifically established in the relevant provisions of those Chapters.

In essence, when applying the requirements set out in these chapters, consideration will be given to the size and other characteristics of the entity and its operations, in addition to the general risk profile inherent in its business.

5 Among other things, section 16 of DORA applies to them instead of sections 5 to 15.

Furthermore, DORA considers different exemptions and flexibilities based on the type and size of the entity. For instance, micro-enterprises are exempt from certain requirements, and small, non-interconnected investment firms benefit from a simplified risk management framework.[6] Conversely, more stringent requirements apply to more critical entities, such as central counterparties.

As a general principle, DORA advocates a risk-based approach, taking into account critical or important functions.

As a general question, entities have been asked about the **degree of adaptation with respect to DORA**:

— 18% had already reviewed their compliance and allocated the necessary resources.

— 58% were in the process of review and implementing a plan.

— 24% had planned to start the review process but had not yet done so. Among these, 83% do not belong to a corporate group and 95% are composed of micro or small enterprises.

The conclusion is that there is a substantial percentage (24%) of institutions that have yet to undertake this review. As expected, the most prepared are the larger entities and those that are part of a group, as they generally have more resources to manage these compliance review processes for the new regulations.

 Before DORA comes into effect, financial institutions should have conducted a **compliance gap analysis** and developed an implementation plan with assigned resources and responsibilities.

6 Recitals 42 and 43 of DORA.

4 ITC risk management

The questionnaire included a section covering Articles 5 to 16 of DORA and the RTS concerning the ICT risk management framework and its simplified version.

This section contained the most questions, as it forms the foundation for organisations to build adequate cyber resilience. Institutions should integrate this management approach into their business processes, governance structures, and responsibility assignments. It should also be incorporated into the integration with other risks (primarily operational risk), the standardisation and maturity of processes (including strategies, policies, and procedures), and the continuous review and improvement, which should be overseen by the internal control or audit function and reported to the management body.

Generally, financial institutions were already required to practise effective risk management.[7] With DORA, they must also address ICT-related risks. This management demands specific attention due to factors such as the need to protect the availability, authenticity, integrity, and confidentiality of data, the complexity of systems and processes, exposure to cyber threats, the evolving landscape of technology and threats, and the significant reliance on third-party providers.

4.1 Governance and organisation

DORA highlights the critical role of governance and organisation in ensuring cyber resilience,[8] assigning ultimate responsibility for managing technology risk to the entity's management body.

Effective cyber resilience management must be well-governed and backed by leadership support. The National Institute of Standards and Technology (NIST) has introduced a "Governance" section in version 2.0 of its cybersecurity framework,[9] which is vital for prioritising and achieving other functions: identification, protection, detection, response, and recovery.

7 Rule 4 of Circular 6/2009 concerning internal control of CISMCs, and Rule 6 of Circular 1/2014 regarding internal organisation and control functions of IFs, are relevant here.

8 Article 5 of DORA and Article 28 of the RTS, which deal with the simplified risk management framework.

9 https://www.nist.gov/cyberframework

For Spanish investment firms and fund managers, the **Board of Directors** serves as the institution's highest decision-making authority. It is responsible for defining, approving, and overseeing all aspects of the ICT risk management framework. Although the board retains ultimate responsibility, it can delegate operational management to a committee or similar body.

Most respondents have already implemented governance and organisational measures comprehensively, notably approving the business continuity policy (55% of respondents), internal audit plans (45%), and budget allocation (44%). However, the responses indicate that some fundamental elements are still not fully in place. For example, 29% of institutions reported lacking a **digital operational resilience strategy**, and 38% had not yet appointed **someone to monitor third-party agreements**.

Similarly, there is considerable room for improvement in some key areas for entities using the simplified risk management framework. Specifically, in governance and organisation, 69% did not arrange for **regular reporting to the management body**, and 44% had not implemented **regular approval and review of the ICT risk management framework**. Most institutions reported that their management body set security objectives (69%), implemented policies and processes (68%), and defined responsibilities (64%).

The management body should regularly receive updates on the main ICT-related risks and the review of its management framework for approval.

A common issue in cyber resilience is the lack of communication between management and ICT leaders. DORA emphasises the need for management training and effective communication processes,[10] as these are crucial for maintaining a constructive dialogue with senior management.

The **Good Governance Code for Cybersecurity**,[11] developed by the National Cybersecurity Forum, is available for consultation. This code provides general recommendations on operational resilience for the governing bodies of companies, organised into principles that can be adopted by any organisation seeking to ensure robust cybersecurity governance.

10 Articles 5.4 and 14 of DORA, respectively.

11 https://foronacionalciberseguridad.es/index.php/documentacion/publico/124-good-governance-code-on-cybersecurity/file

4.2 ICT risk management framework

Articles 6 and 16 of DORA require entities to establish an ICT risk management framework.

This framework generally comprises the following stages:

— Risk identification: identifying assets, threats, and vulnerabilities.

— Risk assessment: calculating and evaluating risks.

— Risk treatment: implementing safeguard measures or mitigation controls and calculating residual risk.

— Risk monitoring: assessing the effectiveness of measures and ongoing risk monitoring.

Various standard management frameworks exist in cybersecurity, and each entity should select the one that best fits its needs, ensuring compliance with DORA requirements. For SMEs, resources from INICBE,[12] the CCN,[13] and guides from ENISA[14] and NIST[15] can serve as useful references.

DORA specifies that the **simplified** ICT risk management **framework** does not apply to management companies.

Instead, this simplified framework is relevant for entities classified as "**small, non-interconnected investment firms**".[16]

Data from the questionnaire reveal that 37% of institutions do not have an ICT **risk management framework** in place, and only 22% implement it comprehensively. 18% have not separated their **control and management functions**, while 54% employ the three lines of defence: management, control, and internal audit.[16]

Small and independent entities often find it challenging to implement the second line of defence, so they typically establish management and combined control/internal audit lines instead. Most institutions with a management framework **do review it**, but 45% do not do so with the frequency or level of detail required by DORA. A significant number of institutions (43%) conduct **regular audits** of their management framework and track the outcomes. In addition, 45% have not clearly defined a **strategy** for digital operational **resilience**.

12 https://www.incibe.es/empresas/blog/analisis-riesgos-pasos-sencillo
13 https://pilar.ccn-cert.cni.es/en/risk-analysis/what-is-risk-analysis
14 https://www.enisa.europa.eu/publications/archive/RMForSMEs
15 https:/nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf
16 According to Article 12.1 of Regulation (EU) 2019/2033 of the European Parliament and of the Council.

For entities subject to the **simplified framework**, 63% engage in **identifying** and assessing their ICT risks. However, 62% have not established risk tolerance levels, 63% neither define nor **monitor risk mitigation** in relation to these levels, and 60% do not **regularly review their risk assessments** (although 58% produce some form of regular report on the **framework's review**).

All financial institutions are required to **document and review their ICT risk management frameworks**.[17] The review should occur at least annually or as needed based on the type of institution and the occurrence of serious ICT-related incidents.

The CNMV may request a **report on this review**. The content and format of this report are detailed in the RTS on risk management.[18]

4.3 Policies and procedures

Articles 5 to 16 of DORA, along with the RTS, specify numerous policies and procedures that must be part of the ICT risk management framework. This includes areas such as operations management, cryptography, vulnerability and patch management, and data security.

DORA expects organisations to have a sufficient level of maturity in their cyber resilience management, supported by clearly defined strategies, policies, and procedures.[19]

Only 23% of institutions lack a formally approved security policy.

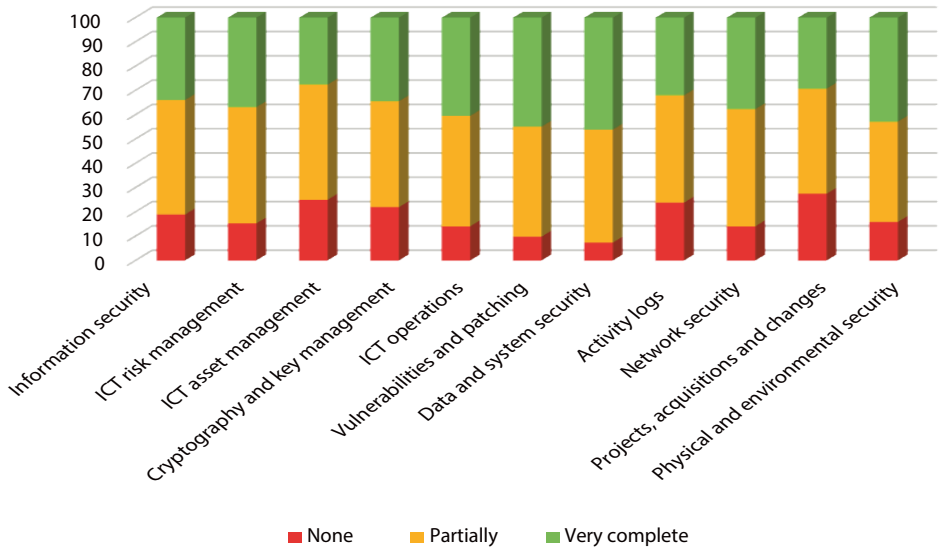
The questionnaire enquired about the various policies and procedures outlined in DORA and the RTS relevant to the risk management framework. Notably, 93% of organisations had implemented a policy on data and systems, 90% on vulnerability management and security patching, and 86% on ICT operations. However, there were notable gaps in project, procurement, and change management policies (27%), asset management policies (25%), and cryptography and key management (22%).

17 Articles 6.2 and 16.2.

18 Articles 27 and 41 of the RTS on the risk management framework (RD EU 2024/1772).

19 At least level L3 or similar of the maturity model (CMM). Available at: https://www.ccn-cert.cni.es/publico/herramientas/Pilar-5.4.8/web/help/html/niveles_de_madurez.html

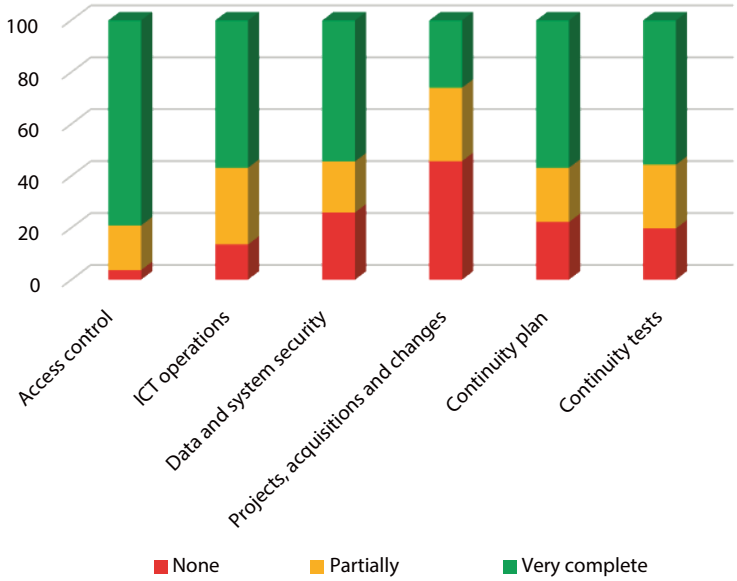
Risk management framework policies and procedures FIGURE 3



Source: CNMV.

Among the entities subject to the **simplified framework**, 76% had robust access control measures in place. Additionally, 49% managed their ICT assets throughout their lifecycle, not just at acquisition. Basic security measures for data, systems, and networks were implemented by 26%, while 78% had a continuity plan, and 80% conducted tests on their recovery mechanisms.

Simplified risk management framework procedures FIGURE 4



Source: CNMV.

Institutions that already have security, continuity, and backup policies are advised to assess whether they comply with DORA or need to be adapted or supplemented with additional policies and procedures. These should be approved by the management body and reviewed regularly.

4.4 Identification, detection, protection, response, and recovery

Similar to NIST,[20] Section II of Chapter II of DORA (Articles 8 to 14 and 16) is organised around the functions of ICT risk management: identification, protection and prevention, detection, response and recovery, learning, and evolution and communication.

i) The **identification** phase is crucial for managing cyber resilience. Institutions must identify, classify, and document their business functions and ICT assets, along with their interdependencies, as well as the sources of risks to which they are exposed.

To **identify risk sources**, threat catalogues are available within risk management framework standards. Examples include Pilar/Magerit v3[21] and the Secure Controls Framework.[22]

About 21% of organisations reported not having a documented process for identifying and classifying ICT functions and assets, while 44% only did so partially. A process for identifying threats and vulnerabilities was not conducted by 14% of respondents.

When major changes occurred in ICT services, 86% reassessed the risks. Of these, 49% did so comprehensively, including legacy systems.

Without proper **identification**, an institution's ability to manage risks is reduced, as systems, assets, or threats may remain unmanaged.[23] **Classification** helps to focus on the most critical ICT systems and assets for the institution.

ii) Regarding **detection and response**, 88% had monitoring and alert systems for their services, with 51% employing automated early warning mechanisms. In terms of responsiveness, 85% had proactive monitoring resources, and 46% had automated response processes.

It is recommended to **automate** detection and response processes as much as possible, tailored to each institution's capacity, to minimise incident response times. Measures can range from automatic email alerts or EDR/XDR protections to more advanced solutions like SIEM for correlating activity logs and SOAR for orchestrating responses.

20 https://www.nist.gov/itl/smallbusinesscyber
21 https://pilar.ccn-cert.cni.es/docman/documentos/2-magerit-v3-libro-ii-catalogo-de-elementos
22 https://securecontrolsframework.com/risk-management-model/#threat-catalog
23 https://www.incibe.es/en/incibe-cert/blog/shadow-it-exposed-risks-and-best-practices

iii) Based on risk management, each institution should implement appropriate **protections** to limit or mitigate the impact of potential threats, ensuring that business functions are carried out in line with its policies and procedures. Key measures include:

- Identity protection: unique identities, strong password policies, two-factor authentication (MFA), password managers, and so on.
- Authorisation: principle of least privilege, need-to-know basis, and robust processes for user onboarding, offboarding, and modifications.
- Protection of the attack surface: safeguarding services exposed to the internet or third parties.
- Protection of workstations and user devices: antivirus software, hardening, removable storage, encryption, etc.
- Data protection: ensuring data availability, integrity, and confidentiality.
- Network and system security: high availability, hardening, zero trust, VPNs, and more.
- Secure code development, environment separation, and change management.
- Protection of system administration: management of privileged users, network segmentation, monitoring, and handling of activity logs and alerts, among other measures.

The survey inquired about various protection systems. Institutions reported using a range of solutions, with the most common being anti-spam systems, internet communication encryption, antivirus software, firewalls, and high-availability systems.

The extensive array of security products and solutions available on the market can complicate the decision-making process. Furthermore, it is essential to remember that simply purchasing a product is insufficient; it must be configured to suit the institution's specific needs. Therefore, risk management analysis is crucial **to prioritise and tailor mitigation measures** according to the institution's capacity. Additionally, the solutions implemented must be **maintained over time, and their effectiveness** in mitigating risks should be regularly **tested**. To ensure these tasks are carried out effectively, the roles responsible for monitoring, internal auditing, and resilience testing are vital. Several guidelines exist for securely configuring products, such as those provided by the CCN[24] and the CIS.[25]

24 https://www.ccn-cert.cni.es/en/guides.html
25 https://www.cisecurity.org/cis-benchmarks

Security and resilience measures implemented by institutions must be correctly configured and regularly maintained, incorporating the latest security updates.

iv) Regarding **recovery**, Article 11 of the DORA incorporates ICT business continuity plans[26] to ensure the continuity of an institution's critical or important functions.

A total of 81% of institutions already had a business continuity policy in place, and 86% tested it, although 34% did so only occasionally. Additionally, 77% conducted business impact analyses (BIA).[27] A crisis management function was assigned in 88% of cases.

Furthermore, 93% had implemented ICT response and recovery plans and procedures, with 70% conducting internal audits of these plans.

All institutions performed backups: 67% used highly robust mechanisms, while the rest employed more basic methods.

ICT **business continuity plans** must comply with the recovery levels and timelines approved by the management body, aligning with the institution's characteristics, such as size, general risk profile, and the nature, scale, and complexity of its services, activities, and operations.

v) **Learning and evolution** are crucial elements of cyber resilience under DORA. As technology rapidly evolves, it brings new business opportunities (like cloud services, artificial intelligence, and 5G technologies) and increasing cyber threats (such as malware-as-a-service, deepfakes and other uses of AI, quantum cryptography, nation-state actors, etc.).

Cyber resilience in an institution needs to develop and mature over time, becoming a process of continuous improvement. The management body should understand the technological risks they face, users must be well-trained in cyber hygiene and awareness, and technical staff should adhere to cyber resilience procedures and best practices.

26 https://www.incibe.es/empresas/que-te-interesa/plan-contingencia-continuidad-negocio
27 https://www.incibe.es/empresas/blog/pasos-seguir-realizar-analisis-impacto-negocio

For **identifying vulnerabilities, cyber threats, and ICT-related incidents** as mentioned in section 1 of article 13 of DORA, the following measures are recommended:

— Subscribe to security alerts from INCIBE, CCN-CERT, or similar bodies.[28]

— Review and update to the latest versions of security patches and release notes from major manufacturers or products used or subscribe to their bulletins.

— Regularly review threat landscape reports, such as those from ENISA, or incident dashboards.[29]

— Collaborate with other institutions and participate in cybersecurity forums and events (refer to section 8 on information-sharing agreements).

— Consult other sources such as Mitre, which documents the tactics and techniques used by cybercriminals,[30] or OWASP's list of the top 10 security risks in web applications.[31]

DORA should not lead to uncontrolled changes in institutions that, due to the complexity of new systems or procedures, could threaten their operations because of insufficient knowledge or capacity.

Implementing high-risk changes gradually and in a controlled manner is recommended, taking into account each institution's capabilities and prioritising critical and important functions.

Various cyber resilience tests, monitoring and auditing mechanisms, and detection and alert systems should assist in updating the institution's ICT-related risks.

DORA should not be seen as a one-time effort to meet regulatory requirements. Financial institutions need to establish procedures to **maintain and enhance their cyber resilience** over time.

For **smaller institutions**, which have fewer resources to meet the new DORA requirements, and **applying the principle of proportionality**, even if they do not have all the required measures fully implemented when the Regulation comes into effect, they are expected to have defined and budgeted an implementation plan to develop their cyber resilience within a reasonable timeframe.

28 https://www.incibe.es/en/incibe/suscripciones and https://www.ccn-cert.cni.es/en/updated-security.html

29 https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends and https://ciras.enisa.europa.eu/

30 https://attack.mitre.org/

31 https://owasp.org/www-project-top-ten/

Although it is preferable to anticipate incidents, those that do occur should be used to enhance processes and mitigation measures and to analyse which controls were ineffective or which safeguards need reinforcement against specific threats.

vi) **Communication** is also a crucial element in managing cyber resilience. Institutions should have a crisis communication plan to responsibly disclose serious ICT-related incidents or vulnerabilities to the relevant parties (internal staff, customers, counterparties, or the public), as outlined in article 14 of DORA.

5 Management of ICT-related incidents

Incident management has a life cycle and doesn't start when an incident is detected. Preparations such as gathering the necessary management tools, and establishing classification and alert criteria, as well as defining roles and responsibilities, should be made in advance. Institutions must be as prepared as possible to prevent improvisation when incidents occur; consulting guidelines like those from INCIBE can be helpful).[32]

The questions in this section of the questionnaire relate to articles 17 to 20 of DORA, the RTS on ICT-related incident classification criteria, the Guidelines on costs and losses, and the RTS and ITS on major incident reporting.

Generally, institutions were found to be least prepared in this area. 35% lacked a defined **incident management policy**, and in 36% of cases, the policy was generic. 36% had not implemented an **incident classification and logging** mechanism. 29% of respondents had not assigned **roles and responsibilities** or defined **communication plans**. 22% had not made the necessary preparations to **notify the CNMV** of serious incidents.

Financial institutions under the CNMV's jurisdiction are required to **report major ICT-related incidents** to the CNMV, including the initial notification, interim reports, and final reports, as specified in article 19 of DORA and its RTS.

For details on how to report serious incidents and significant cyber threats, please visit the "Cybersecurity" section of the CNMV's website.[33]

Additionally, if a serious incident impacts **customers' financial interests**, financial institutions must inform them of the incident and any measures taken.[34]

The RTS outline **criteria and thresholds for classifying** an incident as serious.[33] An **incident is deemed major** if it meets any of the following criteria regarding the critical nature of the affected services:

32 https://www.incibe.es/en/incibe-cert/incidents/incident-handling and https://www.incibe.es/index.php/en/incibe-cert/publications/guides-and-studies/guides/spanish-national-guidelines-reporting-and-managing-cyber-incidents

33 Commission Delegated Regulation (EU) 2024/1772 on criteria for the classification of ICT-related incidents.

i) Impacts ICT services that support the institution's critical or important functions.

ii) Affects financial services provided by the institution that require authorisation, registration, or supervision.

iii) Results in effective, malicious, and unauthorised access to the institution's ICT systems.

Additionally, the incident must meet one of the following conditions:

i) The malicious access (mentioned in point iii above) could lead to data loss.

ii) If at least two of the criteria specified in Article 9 of the RTS are met:

   a. Impact on customers, financial counterparties, and transactions (paragraph 1).

   b. Reputational impact (paragraph 2).

   c. Duration of the incident and service interruption (paragraph 3).

   d. Geographical spread (paragraph 4).

   e. Data loss (paragraph 5).

   f. Financial consequences (paragraph 6).

iii) If more than one non-serious incident occurs within six months and the following conditions are met:

   a. The financial institution is neither a microenterprise nor a small non-interconnected investment firm.

   b. The incidents have the same underlying cause.

   c. Collectively, the incidents meet the preconditions' requirements.

Digital operational resilience, especially regarding incidents, covers more than just cyberattacks, even though these pose a significant, high-impact threat. It also addresses non-malicious failures, such as system faults (whether hardware or software) and human errors in process execution.

The **timelines specified** in the RTS and ITS on incident reporting (Article 6 of the RTS)[34] are as follows:

— **Initial notification**: within 4 hours after classifying it as serious or 24 hours from becoming aware of the incident.

— **Intermediate report**: within 72 hours of the initial notification, with updates when relevant information arises and when normal activity is resumed.

— **Final report**: within one month of the last update to the interim report.

Besides notifying the CNMV of major incidents, institutions can **voluntarily** report cyber threats they deem significant to the financial system, service users, or customers.

Experiencing a serious incident is often a complex and stressful situation. Adequate preparation beforehand is crucial for a swift recovery. Institutions are advised to establish procedures for classification and ensure they can **notify the CNMV within the required deadlines**, including all necessary information.

It is also advisable to implement procedures related to the **communication plan for customers**, which should include responsibilities, communication criteria, notification templates, and channels to be used.

Competent authorities will then pass on these incidents to the European Supervisory Authority and other relevant bodies, such as CSIRTs and NIS single points of contact.[35] By collecting and sharing this information, authorities can gather valuable threat intelligence to improve their response to incidents and support other financial institutions and authorities in achieving a stronger collective defence.

34 Exceptions apply if an incident occurs during the weekend or if the institution encounters difficulties in reporting, but it must still inform the authority of these issues.

35 Article 19.6 of DORA.

6 Digital operational resilience testing

Institutions should implement policies to test their **ICT systems** for vulnerabilities, assess the **people** using those systems (e.g., through phishing campaigns or crisis simulations), and evaluate related **processes** (such as parameter validation, error checking, and monitoring). It is important to verify that systems operate as expected, mitigation measures are effective, and change processes do not lead to incidents.

Each financial institution should conduct regular digital operational resilience tests that suit its characteristics, including size, overall risk profile, and the nature, scale, and complexity of its services, activities, and operations, to achieve a high level of resilience, including **testing of continuity plans**.

Small non-interconnected investment firms must develop an ICT **security testing plan** (Article 36 of the RTS on the simplified risk management framework).

Institutions other than microenterprises must establish and maintain a **testing programme** (Article 24 of DORA).

Microenterprises will conduct tests more flexibly (Article 25.3 of DORA).

The questionnaire included questions related to articles 24 and 25 of DORA. Articles 26 and 27 were not considered as they focus on advanced threat-based penetration testing for highly mature institutions, which is beyond the scope of this document aimed at smaller institutions.

The data collected indicate that only 34% had a robust testing plan in place, meaning one with a defined frequency and a process for addressing identified deficiencies. In 43% of the institutions, although a test plan existed, tests were not conducted at regular intervals, and results were not formally followed up. Furthermore, 23% of the institutions did not have a defined test plan.

The questionnaire inquired about the types of tests the institutions carried out in various areas. The most common were data restoration (84%), system restoration (72%), environmental (60%), performance (53%), and penetration tests (52%). Only 26% conducted crisis simulations.[36]

36 https://www.incibe.es/empresas/formacion/juego-rol-pyme-seguridad

DORA identifies various resilience tests, including:[37]

— Vulnerability assessments and scans.

— Open source analysis.

— Network security evaluations.

— Gap analysis.

— Physical security reviews.

— Questionnaires and scanning software solutions.

— Source code reviews, where feasible.

— Scenario-based tests.

— Compatibility tests.

— Performance tests.

— End-to-end tests.

It is crucial to analyse and **monitor the results** of digital operational resilience tests to integrate them into the institution's ICT risk management.

37 Recital 56 of DORA.

7 Management of ICT-related third-party risk

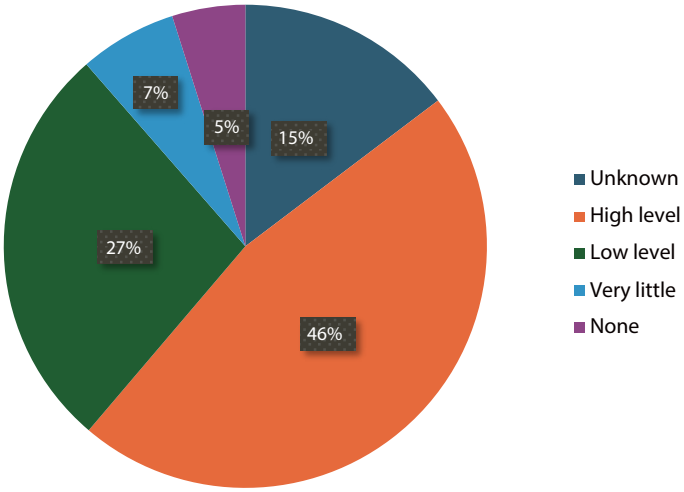
ICT services are broadly defined and include digital and data services provided continuously through ICT systems to internal or external users. Likewise, DORA encompasses a diverse range of third-party ICT service providers.[38]

The questionnaire included questions on Articles 28 to 30 of DORA, RTS on outsourcing, RTS on policies concerning agreements with ICT service providers, and ITS on provider's register of information.

Only 31% of the institutions had implemented a **strategy** for managing third-party **risk**. Meanwhile, 33% did not maintain a **contract register** to manage associated technology risks, and only 23% kept a comprehensive information register. **Before signing a contract**, just 20% conducted due diligence, while 35% had no procedures in place.

Financial institutions generally have a high dependency on various service providers due to the nature of their work. This was evident in the questionnaire responses, showing that 46% relied on providers that were difficult or costly to replace. In 34% of cases, institutions could switch providers at an acceptable cost, with 7% having minimal dependency. Notably, 15% were unaware of their level of dependency on their providers.

Dependence on ICT service providers FIGURE 5



Source: CNMV.

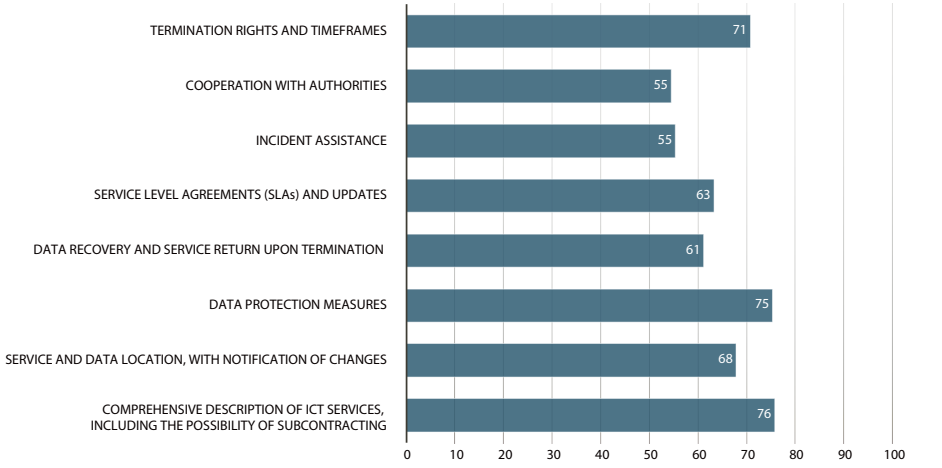
38 Recitals 35 and 63 of DORA.

In December 2020, the **ESMA Guidelines on outsourcing to cloud service providers** were approved.[41] These guidelines aim to provide a reference for institutions to manage these services and for authorities to integrate them into the supervisory framework.

They are currently being revised to align with DORA.

Below is the percentage of institutions that have generally identified whether the following elements were included in their ICT[40] service provider contract terms:

Clauses in contracts with ICT service providers FIGURE 6



Source: CNMV.

The percentage of contracts with providers supporting the institution's critical or important functions that included more specific clauses[41] is as follows:

Clauses in contracts with ICT service providers that support critical or important functions FIGURE 7

Source: CNMV.

39 https://www.esma.europa.eu/sites/default/files/library/esma_cloud_guidelines.pdf
40 Article 30.2 of DORA.
41 Article 30.2 of DORA.

In the first section, the least adhered-to aspects are cooperation with authorities and assistance in case of incidents. In the second section, the lowest level of compliance is found in access, inspection, and audit rights.

Questions about **outsourced business functions** revealed that the most common are internal control (67%), financial intermediary services and platforms, and transaction processing (50%), along with information security, document management, and business repositories (47%).

Regarding **digital and data services from providers** supporting critical or important functions, apart from internet lines (88%), data services (80%), communications and networks (68%), and ICT security (64%) are prominent. For other types of services (IaaS, SaaS, hardware, infrastructure hosting, ICT operations management, etc.), the data indicate that over 40% of institutions used them.

Financial institutions with contractual arrangements for using ICT services in their business operations are **fully responsible** at all times for complying with all DORA obligations and applicable financial services law.[44]

Like other processes, third-party risk management follows a lifecycle, which should be thoroughly documented in the institution's policies for critical or important services:

— Pre-assessment of risks.

— Due diligence.

— Contracting the agreement.

— Monitoring the service.

— Terminating the service.

It is recommended that institutions prepare a **register of ICT service providers**, including the detailed information specified in the ITS on provider register of information.[45]

All financial institutions should have a Legal Entity Identifier (LEI)[46] code for identification purposes,[47] although European providers might be required to have a different identification code once the ITS on registration is approved.

42 Article 28.1.a) of DORA applies. Although point b) adds the principle of proportionality.

43 https://www.esma.europa.eu/press-news/esma-news/esas-announce-timeline-collect-information-designation-critical-ict-third

46 https://cnmv.es/docportal/mifidii_mifir/codigolei.pdf

47 At the date of writing of this document, providers had yet to define their identifier, LEI or EUID. See ITS annex. Available at: https://www.esma.europa.eu/press-news/esma-news/esas-respond-european-commissions-rejection-technical-standards-registers

The management of technological risk arising from third-party providers presents several challenges:

— Identifying ICT service providers, given the broad scope of the definition.

— Including the necessary contractual clauses and renegotiating them if they are incomplete.

— Obtaining the information required for record-keeping and meeting other requirements (such as the relevant supply chain and monitoring).

— Many providers are large entities and are often reluctant to adapt to the needs of smaller institutions.

Intra-group ICT service providers are subject to the same regulatory framework. However, their higher level of control must be considered in the overall risk assessment.[48]

DORA aims to ensure that reliance on third parties is managed in a controlled way, ensuring the institution's cyber resilience. It seeks to avoid unfair contractual terms that provide little assurance of service quality, prevent disorderly termination of the provider's activities, and ensure transparency in their resilience procedures. Additionally, it calls for an evaluation of alternative providers.

DORA is expected to enable smaller institutions to more easily access clauses that assist in managing ICT provider risk. A common framework is anticipated, in which larger financial institutions and the authorities encourage providers to offer these clauses. Greater **harmonisation and alignment** of criteria are expected, aided by the publication of Q&A documents, and the practice of including financial addenda in contracts and renegotiations should become standardised.

The sector would also benefit from EU-level **oversight** of providers classified as critical and the ability of national authorities to supervise the most significant domestic providers.

For existing ICT service contracts, particularly those supporting critical or important functions, a **revision of the terms** is anticipated to align them with the Regulation's requirements.[49] Applying proportionality, if renegotiating agreements or changing providers is not feasible, institutions should consider these risks when renewing contracts.

48 Recital 31 of DORA.

49 Recital 69 of the Regulation.

The European supervisory authorities – the European Securities and Markets Authority (ESMA), the European Banking Authority (EBA), and the European Insurance and Occupational Pensions Authority (EIOPA) – have organised a dry-run exercise on reporting the registers of information in 2024. This involved conducting quality checks on the data provided by the institutions that opted to participate.[48] The most significant aspects of this exercise have been summarised in a Frequently Asked Questions (FAQ) document available on their websites.

This provider register will enable the authorities to monitor institutions' exposure to certain risks, such as provider concentration in the sector. It will also be utilised to identify and designate critical providers that will be jointly overseen by the ESAs.

Financial institutions must report to the competent authorities at least once a year, providing **information about the number of new agreements** related to the use of ICT services, the categories of third-party ICT service providers, the types of contractual arrangements, and the ICT services and functions provided.

Institutions are also required to promptly inform the competent authority **when they plan to enter into any contractual agreements** for ICT services that support critical or important functions, as well as when a function becomes critical or important.[51]

50 https://www.eba.europa.eu/activities/direct-supervision-and-oversight/digital-operational-resilience-act/preparation-dora-application

51 Article 28.3 of DORA.

8 Information sharing agreements

As cyber criminals continue to act in an increasingly organised manner (with forums for malware trading and sharing, selling stolen credentials, hacktivism, etc.), financial institutions need to bolster collaboration among themselves to gain a better understanding of the threat landscape and to share cyber resilience strategies at strategic, tactical, and operational levels.[50]

To explore this issue, related to Article 45 of DORA, a questionnaire included some relevant questions.

From the responses received, less than 20% of institutions had collaborations with industry stakeholders (such as manufacturers and consultancy firms), other financial institutions (notably those within their own banking group, sector associations like Inverco, or collaboration groups such as FS-ISAC and FIRST),[51] or governmental agencies (notably INCIBE[52] and CCN-CERT).[53]

Financial institutions must notify the competent authorities of their participation in information-sharing arrangements with other financial institutions. This is in line with the conditions outlined in Article 45.1 of DORA, at the time their membership is confirmed, or upon the termination of their participation, once it becomes effective.[56]

52 Recital 34 of DORA.
53 https://www.fsisac.com/ and https://www.first.org/
54 https://www.incibe.es/empresas/blog/que-es-el-reglamento-dora and https://www.incibe.es/empresas
55 https://www.ccn-cert.cni.es/en
54 Article 45.3 of DORA.

9 Conclusions

The self-assessment questionnaire has increased awareness among financial institutions about the main requirements of DORA and provided insight into their current preparedness ahead of the Regulation coming into effect.

Additionally, while processing the responses, the CNMV has supported the sector by addressing queries on topics where there was significant uncertainty, responding to numerous questions via the cybersecurity mailbox).[55]

Overall, a detailed analysis of the responses shows that, generally, institutions have strong governance, cybersecurity, and business continuity measures. However, many lack regular reviews or follow-up on these measures.

More significant gaps have been identified in incident management, test management, and ICT service provider risk management. Smaller institutions not part of a larger group are the least prepared.

Thus, it can be concluded that financial institutions face the challenge of adapting to the new regulation but also have the opportunity to enhance their resilience. Specifically, they will need to consider how to implement the regulation within their organisation in a way that is proportionate to their size, risk profile, and complexity.

The CNMV will work with the industry to ensure efficient implementation but will also monitor the process to assess whether the measures have been appropriately implemented.

57 https://www.cnmv.es/portal/ciberseguridad.aspx?lang=en

Annex Legislative references in different areas

The following regulations will be referenced throughout this annex (status as of the date of writing of this document):

ID	Regulation
DORA	Digital Operational Resilience Regulation
RTS1	Commission Delegated Regulation (EU) 2024/1772 on criteria for the classification of ICT-related incident
RTS2	Commission Delegated Regulation (EU) 2024/1773 on ICT TPP polic
RTS3	Commission Delegated Regulation (EU) 2024/1774 on ICT risk management framework and on simplified ICT risk management framework
RTS4	Final Report on draft RTS specifying elements related to threat led penetration tests
RTS5	Final report on the draft RTS and ITS on incident reporting
RTS6	Final Report on draft RTS on harmonisation of conditions enabling the conduct of the oversight activities
RTS7	Final Report on the draft RTS on the composition of the joint examination team JET
RTS8	Final report on the draft RTS on subcontracting
ITS1	Final report on draft ITS on Register of Information (rejected by the European Commission, subject to changes)
GL1	Guidelines on the estimation of aggregated costs/losses caused by major ICT-related incidents
GL2	Guidelines on oversight cooperation

References to the articles of the most relevant rules regulating the following aspects are included below:

a) Roles and responsibilities

	Ref.
Management body (Board of Directors)	DORA 5 DORA 13.5 DORA 17.3.e) DORA 28.2 RTS2 3.1 RTS3 2.2.b) RTS3 15.5 RTS3 25.5 RTS3 27.2.b) RTS3 28.2 RTS3 29.2.a) RTS3 40.3 RTS3 41.2.b)
Position for monitoring agreements with third party ICT service providers (or members of senior management)	DORA 5.3
ICT risk management function	DORA 6.4
Control function	DORA 6.4
Internal audit function	DORA 6.4 DORA 6.6
Crisis management function	DORA 11.7
Spokesperson's role with the public and the media	DORA 14.3

b) Strategies

	Ref.
Digital operational resilience strategy	DORA 6.8 DORA 13.4
Global multi-supplier strategy (optional)	DORA 6.9
Communication strategy on ICT-related incidents	DORA 14.3
Strategy for third-party ICT-related risk	DORA 28.3

c) Policies and procedures

	Ref.
Information security policy	DORA 9.4.a) RTS3 29
Overall ICT business continuity policy (or as an integral part of the overall business continuity policy)	DORA 11.1, 2, 5 and 6 RTS 3 24
Backup policies and procedures and restoration and recovery procedures and methods	DORA 12
Communication policies	DORA 14.2
Policies and procedures for following up on problems discovered during the testing process	DORA 24.5
Policy on the use of ICT services provided by third-party providers that support critical or important functions	DORA 28.2 RTS2 RTS8
ICT asset management policy and procedure	RTS3 4 and 5
Encryption policy and cryptographic controls	RTS3 6
Cryptographic key management policy	RTS3 7
Policies and procedures related to ICT operations	RTS3 8
Capacity and performance management procedures	RTS3 9
Vulnerability and patch management procedures	RTS3 10
Data and system security procedures	RTS3 11
Logging procedures	RTS3 12
Policies and procedures for network security management	RTS3 13
Policies and procedures for protecting information in transit	RTS3 14
ICT project management policy	RTS3 15 RTS3 38
Policy governing the acquisition, development and maintenance of ICT systems	RTS3 16 RTS3 37
ICT change management procedures	RTS3 17 RTS3 38
Physical and environmental security policy	RTS3 18
Human resources policy	RTS3 19
Identity management policies and procedures	RTS3 20
Access control policy and account management procedure	RTS3 21
ICT incident management policy	RTS3 22
ICT asset management policy and procedure	RTS 3 23.5
Procedures for controlling logical and physical access	RTS3 33
Backup and restore procedures	RTS3 39 and 40

d) Plans

	Ref.
Response and recovery plan	DORA 5.e) DORA 11.6 DORA 11.8 DORA 13.3 DORA 15.f) RTS3 26
Audit plan	DORA 5.f) DORA 6.6 RTS2 3.8 RTS3 28
Business continuity plan	DORA 11.6 DORA 11.7 DORA 11.8 DORA 13.3 DORA 15.e DORA 16.1.f) and 16.1.g) RTS3 25 RTS3 39
Crisis communication plan	DORA 11.6.b) DORA 14.1
Test plan	DORA 11.6 RTS3 36
Exit and transition plan for ICT services from providers	DORA 28.8

e) Reports and records

	Ref.
Report on the review of the ICT risk management framework	DORA 6.5 RTS3 27
Report on the review of the simplified ICT risk management framework	DORA 16.2 RTS3 41
Report on major ICT-related incidents	DORA 17.3.e) DORA 19.4 RTS5
Report on the estimated total annual costs and losses caused by major ICT incidents	DORA 11.10 GL1
ICT service provider information register	DORA 28.3 ITS1
ICT asset register	RTS3 4.2.b)
Register of all certificates and certificate storage devices	RTS 3 7.4
Logging of detected vulnerabilities and tracking their resolution	RTS3 10.2.h)
Logs of activity, access control, and identity	RTS3 12 RTS3 20 RTS 3.21

f) Periodic reviews

	Ref.
Implementation of the **ICT business continuity policy** and the ICT **response and recovery plans**	DORA 5.2.e) DORA 11.6
Internal ICT audit plans and the financial institution's ICT audits, including any significant changes	DORA 5.2.f)
Policy on agreements for the use of ICT services provided by third-party providers	DORA 5.2.h)
ICT **security** policies, procedures, protocols, and tools	RTS3 2.2.j)

g) Annual reviews

(In some cases, periodic reviews for micro-enterprises)	Ref.
Budget needed to meet digital operational resilience requirements	DORA 5.2.g) RTS3 28.2.e)
ICT **risk management framework**	DORA 6.5 DORA 16.2 RTS3 31.2
Appropriateness of the **classification and documentation** of all ICT-supported business functions, tasks, and responsibilities, the information assets and ICT assets supporting these functions, and their roles and dependencies concerning ICT risk	DORA 8.1
ICT **risk scenarios** affecting them	DORA 8.2
Specific assessment of ICT-related **risk** in all **legacy ICT systems**	DORA 8.7
Testing business continuity and ICT response and recovery plans related to ICT systems supporting all functions	DORA 11.6.a)
Report **findings** to the management body referred to in section 3 (lessons learnt from testing and actual ICT-related incidents) and make recommendations	DORA 13.5
Ensure that all ICT systems and applications supporting critical or important functions undergo **appropriate testing**	DORA 24.6
Report to the relevant authorities information regarding **new agreements** on the use of ICT services, the categories of third-party ICT service providers, the types of contractual arrangements, and the ICT services and functions delivered	DORA 28.3
Acceptance of **residual ICT-related risks**	RTS3 3.d).iv
Network **architecture and security design**	RTS3 13.i)
Access rights (review every six months for ICT systems supporting critical or important functions)	RTS 21.e).iv
Test **backup and restore** procedures	RTS3 40
Policy on the use of ICT services provided by third-party providers that support critical or important functions	RTS2 3.1

h) Obligations to the CNMV

	Ref.
Provide, on request, comprehensive and current information on **ICT-related risks** and the ICT risk **management framework**	DORA 6.3
Submit, on request, a report **reviewing** the ICT risk **management framework**	DORA 6.5 DORA 16.2
Central securities depositories must provide copies of the **results from ICT business continuity tests** or similar exercises	DORA 11.9
(Where applicable to non-micro-enterprises). Report, on request, an **estimate of the total annual costs and losses** resulting from significant ICT incidents	DORA 11.10 GL1
Report **significant ICT incidents** according to paragraph 4 of this Article (initial, interim, and final reports)	DORA 19.1 DORA 19.4 RTS5
Report **significant cyber threats** on a voluntary basis when deemed relevant to the financial system, service users, or customers	DORA 19.2 RTS5
At least once a year, provide information about the **number of new agreements related to ICT services**, the categories of third-party ICT service providers, the types of contractual arrangements, and the ICT services and functions provided	DORA 28.3
Promptly inform when **entering into any contractual arrangements for ICT services** that support critical or important functions, or when a function becomes critical or important	DORA 28.3
Upon request, provide the **full register of information** for ICT service providers	DORA 28.3 ITS1
Notify **participation in information-sharing arrangements** as soon as membership is validated, or termination of participation once effective	DORA 45.3
If outsourcing the obligation to report serious incidents, as outlined in Article 19.5 of DORA, ensure compliance with relevant procedures	RTS5 6

i) Exemptions for micro-enterprises or small non-interconnected investment firms

They are not required to:	Ref.
Create a senior management position or designate a member to monitor agreements with third-party providers	DORA 5.3
Assign ICT risk management and oversight to a specific control function	DORA 6.4
Document and review the ICT risk management framework annually (although periodic reviews are still required)	DORA 6.5
Subject the ICT risk management framework to regular internal audits	DORA 6.6
Conduct comprehensive assessments after major changes to network or information systems processes and infrastructure	DORA 8.3
Perform regular risk analyses on legacy ICT systems	DORA 8.7
Audit the implementation of ICT response and recovery plans with independent internal audits	DORA 11.3
Establish a crisis management function	DORA 11.7
Extend testing of business continuity, response, and recovery plans to cover scenarios involving switching between primary ICT infrastructure and backup facilities	DORA 11.6
Provide estimates of the total annual costs and losses due to major ICT-related incidents to relevant authorities upon request	DORA 11.10
Maintain redundant ICT capabilities	DORA 12.4
Report changes to national competent authorities that have been made following reviews conducted after ICT incidents	DORA 13.2
Continuously monitor relevant technological developments	DORA 13.7
Develop a comprehensive programme for digital operational resilience testing as an integral part of the ICT risk management framework	DORA 24 DORA 25.1
Adopt and periodically review a strategy to manage ICT-related risks arising from third parties	DORA 28.2
Perform advanced testing of ICT tools, systems, and processes using threat-based penetration testing	DORA 26.1
Assess whether recurring incidents qualify as major incidents	RTS1 8.2

Additional concessions to micro-enterprises:	Ref.
Micro-enterprises should evaluate their need to maintain redundant ICT capabilities based solely on their risk profile.	DORA 12.4
(In digital operational resilience testing programs). When designing digital operational resilience testing programmes, they should balance the goal of maintaining high digital operational resilience, the resources available, and their overall risk profile when determining the type and frequency of tests to be conducted	DORA 25.3
They can agree with third-party ICT service providers to delegate the financial entity's rights of access, inspection, and auditing to an independent third party, appointed by the third-party ICT service provider	DORA 30.3