DORA: Exemptions for simplified ICT risk management and beyond

By Emilios Charalambous at Elias Neocleous & Co. LLC

The Digital Operational Resilience Act (DORA) is set to come into effect soon, reflecting the European Union (EU) regulators' efforts to strengthen the IT security of financial entities. This move addresses the finance sector's growing dependence on technology and on tech companies to deliver their services.

In our previous article, we explored how each financial entity is defined within DORA in order to better understand which firms fall under its scope. When reviewing these definitions, it is also vital to understand the exemptions under DORA—whether certain entities are entirely excluded from compliance or subject to simplified ICT risk management requirements.

Entities subjected to simplified ICT risk management:

Under the simplified ICT risk management framework, Articles 5-15 of the regulation do not apply. Instead, the provisions of Article 16 enter into play, allowing finance firms to still implement an ICT risk management framework and minimize ICT risks through simplified requirements, along with other provisions.

Through this process, the firms listed below will be able to avoid various aspects of the regulations including, but not limited to, the internal governance and organization structures required, an extensive ICT risk management framework, the protection and prevention provisions and the response and recovery operations.

Such simplifications apply to entities defined as:

1. small and non-interconnected investment firms;
2. payment institutions exempted pursuant to Directive (EU) 2015/2366;
3. institutions exempted pursuant to Directive 2013/36/EU in respect of which Member States have decided not to apply the option referred to in Article 2(4) of DORA;
4. electronic money institutions exempted pursuant to Directive 2009/110/EC;
5. small institutions for occupational retirement provisions which may be excluded from the scope of Directive (EU) 2016/2341 under the conditions laid down in Article 5 of that Directive by the Member State concerned and operate pension schemes which together do not have more than 100 members in total;
6. institutions exempted pursuant to Directive 2013/36/EU;
7. microenterprises.

The entities that fall under the simplified risk management framework benefit from reduced compliance burdens while maintaining robust operational safeguards. The streamlined requirements simplify risk management processes, reduce administrative costs, and enhance operational efficiency, offering a more tailored approach to their compliance.

Entities falling outside the scope of the regulation:

There are a limited number of entities that do not have to comply at all with DORA, the inclusion of which was not considered as proportional to the scope of the Regulation.

These entities are:

1. managers of alternative investment funds referred to in Article 3(2) of Directive 2011/61/EU of the European Parliament and of the Council;
2. insurance and reinsurance undertakings referred to in Article 4 of Directive 2009/138/EC of the European Parliament and of the Council;
3. institutions for occupational retirement provision which operate pension schemes which together do not have more than 15 members in total

Entities excluded from the scope of the Digital Operational Resilience Act (DORA) benefit from greater flexibility in managing their digital operational risks. Without the need to follow prescriptive regulatory requirements, these entities can tailor their risk management strategies to align with their specific business models, focusing on growth and operational priorities while voluntarily adopting best practices for cybersecurity and resilience.

Entities falling outside the scope of the regulation upon discretion of their Member State:

As long as they are located within their respective territories, Members states are able to choose to exempt from the application of DORA the entities referred to in Article 2(5), points (4) to (23) of Directive 2013/36/EU, as below:

1. in Belgium, the Institut de Réescompte et de Garantie/Herdiscontering- en Waarborginstituut
2. in Denmark, the Eksport Kredit Fonden, the Eksport Kredit Fonden A/S, the Danmarks Skibskredit A/S and the KommuneKredit;
3. in Germany, the Kreditanstalt für Wiederaufbau, undertakings which are recognised under the Wohnungsgemeinnützigkeitsgesetz as bodies of State housing policy and are not mainly engaged in banking transactions, and undertakings recognised under that law as non-profit housing undertakings;
4. in Estonia, the hoiu-laenuühistud, as cooperative undertakings that are recognised under the hoiu-laenuühistu seadus;
5. in Ireland, credit unions and the friendly societies;
6. in Greece, the Ταμείο Παρακαταθηκών και Δανείων (Tamio Parakatathikon kai Danion);
7. in Spain, the Instituto de Crédito Oficial;
8. in France, the Caisse des dépôts et consignations;
9. in Italy, the Cassa depositi e prestiti;
10. in Latvia, the krājaizdevu sabiedrības, undertakings that are recognised under the krājaizdevu sabiedrību likums as cooperative undertakings rendering financial services solely to their members;
11. in Lithuania, the kredito unijos other than the Centrinė kredito unija;
12. in Hungary, the MFB Magyar Fejlesztési Bank Zártkörűen Működő Részvénytársaság and the Magyar Export-Import Bank Zártkörűen Működő Részvénytársaság;
13. in the Netherlands, the Nederlandse Investeringsbank voor Ontwikkelingslanden NV, the NV Noordelijke Ontwikkelingsmaatschappij, the NV Industriebank Limburgs Instituut voor Ontwikkeling en Financiering and the Overijsselse Ontwikkelingsmaatschappij NV;
14. in Austria, undertakings recognised as housing associations in the public interest and the Österreichische Kontrollbank AG;
15. in Poland, the Spółdzielcze Kasy Oszczędnościowo — Kredytowe and the Bank Gospodarstwa Krajowego;
16. in Portugal, the Caixas Económicas existing on 1 January 1986 with the exception of those incorporated as limited companies and of the Caixa Económica Montepio Geral;
17. in Slovenia, the SID-Slovenska izvozna in razvojna banka, d.d. Ljubljana;
18. in Finland, the Teollisen yhteistyön rahasto Oy/Fonden för industriellt samarbete AB, and the Finnvera Oyj/Finnvera Abp;
19. in Sweden, the Svenska Skeppshypotekskassan;
20. in the United Kingdom, the National Savings Bank, the Commonwealth Development Finance Company Ltd, the Agricultural Mortgage Corporation Ltd, the Scottish Agricultural Securities Corporation Ltd, the Crown Agents for overseas governments and administrations, credit unions and municipal banks.

In summary, it is crucial for financial entities to determine whether they are required to comply with DORA. This understanding allows them to effectively plan their compliance operations and stay ahead of regulatory requirements.

If you are interested in evaluating how compliant your organisation is with DORA, our team of experts can conduct a gap assessment and support you in your compliance requirements.