Steptoe

This table is an extract from our client alert "Stay Resilient: EU Reaches Agreements to Improve the Cybersecurity of Businesses Operating in Critical Sectors of the Economy", available on our website (link here)

Table below sets out some of the key differences between the three proposed legislations that businesses should be aware of.

Key changes	DORA	NIS 2	UK NIS
Reporting obligations	Any major ICT-related incident must be reported in a centralized and harmonized manner. An ICT-related incident is major when it has the potential to adversely impact on the network and information systems that support the critical functions of a financial entity. The impact is determined by considering various criteria such as the number of users, the duration, the geographical spread, the type of data loss, the severity of the impact, the criticality of the services and the economic impact. Financial entities must notify the competent authority without undue delay but no later than the end of the business day ('EOB'). However, if the incident occurred two hours before EOB, the notification must be done no later than four hours before the beginning of the next business day. Should reporting channels not be available, then as soon as they become available. In some cases, flexible timelines will be justified. In addition to the above, an intermediate report, relevant status updates, and a final report must be provided using the template commonly drafted by European Supervisory Authorities.[1]	Any significant incidents must be reported i.e., when it (potentially) causes severe operational disruption of the service or financial losses for the entities concerned or affects other natural or legal persons by causing considerable material or non-material losses. EEs must notify the competent authority within 24 hours of becoming aware of the incident and provide a more detailed report within 72 hours. A report containing minimal requirements must also be submitted.	OES and DSPs must report any incident which has a significant impact on the availability, integrity, or confidentiality of networks and information systems, and which may cause, or threaten to cause, substantial disruption to the service. DSPs must notify the competent authority without undue delay, but no later than 72 hours after being aware of the incident having a substantial impact on the provision of specific digital services.
Testing requirements	Every three years, designated financial entities must carry out advanced testing of their critical	Although NIS 2 provides measures that must be implemented to assess the	Similar to NIS2, DSPs must consider 'testing' as a measure to manage their security risks.

[1] There are three European Supervisory Authorities (ESAs): the European Banking Authority, the European Securities and Markets Authority, and the European Insurance and Occupational Pensions Authority.

	functions and services by means of threat led penetration testing (performed live). Additionally, internal and external tests will need to be implemented (with one in three tests carried out by an external provider).	effectiveness of cybersecurity risk management measures, the latter is less precise (i.e., refers to ('testing' in general).	
Service providers	Financial entities may only enter into contracts with ICT service providers that comply with high, appropriate and the latest information security standards. Critical ICT service providers will be subjected to an oversight framework which empowers Lead Overseers (appointed within EBA, ESMA or EIOPA) to request information and reports, conduct investigations, and address recommendations. If not complied with, the Lead Overseers may impose a periodic penalty payment. Additionally, critical ICT service providers which are established in a third country are required to establish a subsidiary in the EU.	There are not yet any equivalent compliance requirements under NIS 2.	There are not yet any equivalent compliance requirements under the UK NIS. However, the government is currently consulting on whether to expand the definition of "digital services" so that service providers which manage essential digital services on behalf of digital providers are also subject to same requirements of the NIS as digital providers. Additionally, in April 2022, the UK announced its intention to consult on the risks posed by critical third-party entities in the financial sector.[2]
Sharing obligations	Subject to EU data protection and competition laws, DORA encourages entities to set up information sharing arrangements on cyber threat information and intelligence.	Subject to EU data protection laws, NIS 2 proposals will enable entities to participate in information sharing arrangements.	While there are no such requirements under UK NIS, information sharing is one of the improvements proposed by the UK government in its new strategy.

Authors: Diletta De Cicco, James Downes, Naomi Capelle, Leigh Mallon, Charles Helleputte

[2] The UK Financial Authorities announced the publication of a joint discussion paper on Operational Resilience in the course of 2022. More information available here.