Forthcoming Irish and EU Operational Resilience Regulatory Frameworks - Time to Act!

Flavien Corolleur, Senior Legal Counsel/ Director and Data Protection Officer at SS&C Financial Services (Ireland) Limited and member of Compliance Institute's DP&IS Working Group.

Operational resilience, the EU and Irish regulatory frameworks: DORA and CBI Operational Resilience Guidance

At EU level, an EU regulation in the form of *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience Digital Operations Resilience Act*[1] (DORA) was published on 27 December 2022 in the Official Journal of the EU. As a regulation, DORA will apply directly in each of the 27 EU Member States. DORA is perhaps one of the most significant EU regulations affecting the financial sector since the EU General Data Protection Regulation (GDPR), which came into effect on 25 May 2018.

In Ireland, the Central Bank of Ireland (CBI) published in December 2021 the *Cross Industry Guidance on Operational Resilience*[2] (CBI Operational Resilience Guidance). Conscious the EU regulatory framework is developing with, for instance, the forthcoming DORA which will also apply in Ireland, the CBI clarified that the CBI Operational Resilience Guidance *"is in line with international best practice and compatible with/ complementary to DORA and the Directive on Security of Network and Information Systems (NIS2)"*.

Time is ticking!

DORA, entered into force in January 2023, will apply in full from 17 January 2025. The CBI Operational Resilience Guidance will itself apply as early as December 2023. Regulated Financial Service Providers (RFSPs) with respect to the CBI Operational Resilience Guidance on one hand and, financial entities caught under DORA on the other hand, should create a task force as soon as possible, if not already done, to prepare an implementation project plan.
DORA, as an EU regulation, is as important to read, understand and implement as GDPR was in 2018, taking account of DORA's operational resilience, outsourcing, privacy and cyber impact.

Objective and Scope of DORA / CBI Operational Resilience Guidance

Objective of DORA

In simple terms, DORA aims at *"closing the door to cyber-attacks and enhancing oversight of outsourced services"*[3]. While "*increased digitalisation and interconnectedness [...] amplify ICT risk, making society as a whole, and the financial system in particular, more vulnerable to cyber threats or ICT disruptions...*"[4], DORA aims at creating an EU harmonised regulatory framework so that all relevant financial entities which are increasingly reliant on information and communications technology (ICT) have the necessary safeguards in place to mitigate cyber-attacks and other risks. DORA, therefore, lays down enhanced uniform requirements concerning the security of network and information systems supporting the business processes of financial entities.[5]

Objective of CBI Operational Resilience Guidance

The CBI Operational Resilience Guidance has the following specific objectives:

1. Communicate to the boards and senior management of RFSPs, the Central Bank's expectations with respect to the design and management of operational resilience;
2. Emphasise board and senior management responsibilities when considering operational resilience as part of their risk management and investment decisions; and
3. Require boards and senior management to take appropriate action to ensure that their operational resilience frameworks are well designed, are operating effectively, and are sufficiently robust. This action should ensure that the risks to the firm's operational continuity do not transmit into the financial markets and that the interests of the customers and market participants are safeguarded during business disruptions.

Scope of DORA and CBI Operational Resilience Guidance

Both DORA and the CBI Operational Resilience Guidance will apply to RFSPs and financial entities respectively such as credit institutions, investment firms, fund services providers (management companies[6], depositaries, fund administrators), payment institutions, crypto-asset service providers, and insurance and reinsurance undertakings. DORA, in addition, will also apply to the so-called "ICT third-party service providers"[7], as defined below.

DORA however excludes certain financial entities from its application such as certain smaller managers of alternative investment funds, insurance and reinsurance undertakings excluded from the Solvency II Directive, insurance intermediaries, reinsurance intermediaries and ancillary insurance intermediaries which are microenterprises or small or medium-sized enterprises and "post office giro institutions".[8]

The importance to adopt a holistic approach during implementation

When implementing DORA and the CBI Operational Resilience Guidance, the impacted financial entities and RFSPs should adopt **a holistic approach**. In other words, the compliance and governance programme enhanced to adopt and implement both DORA and the CBI Operational Resilience Guidance should ensure interconnectivity between the various applicable regulatory regimes, including for instance, GDPR, outsourcing, cyber security, (digital) operational resilience and NIS2.

The CBI has also clarified that: "*The Guideline should be read in conjunction with the Central Bank's "Cross Industry Guidance on Outsourcing" and the forthcoming DORA in relation to ICT outsourced service providers*". In particular, under DORA, contractual arrangements on the use of ICT services should include at least certain elements such as "*provisions on availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data*".[9]

The importance of understanding some key terminology

Some key defined terms under DORA and the CBI Operational Resilience Guidance include the following terms. While broadly consistent, the CBI considers operational resilience as a matter for "*the financial services sector as a whole*", in addition to being a matter for the relevant firm or RFSP.

	DORA	CBI Operational Resilience Guidance
"critical or important function" (DORA) versus "Critical or Important Business Service" (CBI Operational Resilience Guidance)	A function, the disruption of which would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law	A service provided by a firm to an external end user or market participant where a disruption to the provision of the service could cause material customer detriment; harm market integrity; compromise policyholder protection; or threaten a firm's viability, safety and soundness, or financial stability
"digital operational resilience" (DORA) versus "operational resilience" (CBI Operational Resilience Guidance)	The ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions	The ability of a firm, and the financial services sector as a whole, to identify and prepare for, respond and adapt to, recover and learn from an operational disruption
"ICT services"	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	Note that Guideline 9 of the CBI Operational Resilience Guidance requires RFPs to have "ICT and Cyber Resilience strategies that are integral to the operational resilience of its critical or important business services"
"ICT third-party service provider" (DORA) versus "Outsourced Service Provider" (CBI Operational Resilience Guidance)	An undertaking providing ICT services	A third-party entity that is undertaking an outsourced process, service or activity, or parts thereof, under an outsourcing arrangement. This refers to both external third party service providers and intra/inter group service providers

There is a plan in everything, and we love it when a plan comes together, or key considerations during implementation?

A short overview of the "plan"

At high level, the "plan" may include the following primary steps:

1. Identification and data mapping
   - Financial entities and RFSPs may wish to leverage their existing GDPR / outsourcing data mapping and update it for DORA and CBI Operational Resilience purposes
   - Important to undertake this step as early as possible, to identify for instance, the "critical or important" functions (under DORA) and services (under CBI Operational Resilience)

2. Governance
   - From a CBI perspective, the CBI *"sees the management of a firm's operational risk and resilience as an aligned approach that is integrated into the firm's governance structures"*. Even made clearer under Guidelines 1 and 3 of the CBI Operational Resilience Guidance, the Board is expected to have a proactive role in the firm's operational resilience framework compliance. For instance, the Board *"has ultimate responsibility for the Operational Resilience of a firm" or again "reviews and approves the criteria for critical or important business services"*.
   - From a DORA perspective, financial entities are expected to have in place an internal governance and control framework ensuring an *"effective and prudent management of ICT risk"*.[10]

3. Technical Measures
   - From a CBI perspective, the CBI expects regulated firms, when conducting the initial due diligence review in respect of outsourced service providers, to consider the effectiveness of risk management and internal controls, including IT and cybersecurity in providing appropriate technical and organisational measures to protect the data in accordance with the firm's data management strategy.[11]
   - From a DORA perspective, certain specific technical measures are expected from financial entities. Those include *"appropriate tests, such as 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 testing and penetration testing"*.[12] Furthermore, financial entities will need to assess which critical or important functions need to be covered by threat-led penetration testing (TLPT). TLPT will be expected to be performed on live production systems supporting such functions.

4. Contracts
   - As a first rule of engagement, do not underestimate time needed for contractual uplift.
   - From a DORA perspective, Article 30.2 of DORA sets out the key contractual provisions the contractual arrangement between the financial institution and the ICT third-party service provider should include. Additional contractual terms set out under Article 30.3 of DORA will need to be documented in relation to the use of ICT services supporting "critical or important functions".

- From a CBI perspective, RFSPs should take account of the CBI Cross-Industry Guidance on Outsourcing[13]. In addition, the CBI Operational Resilience Guidance provides that a firm should ensure legally binding written agreements are in place with third parties, detailing how the critical or important services will be maintained during a disruption and an exit strategy if/when the service cannot be maintained.

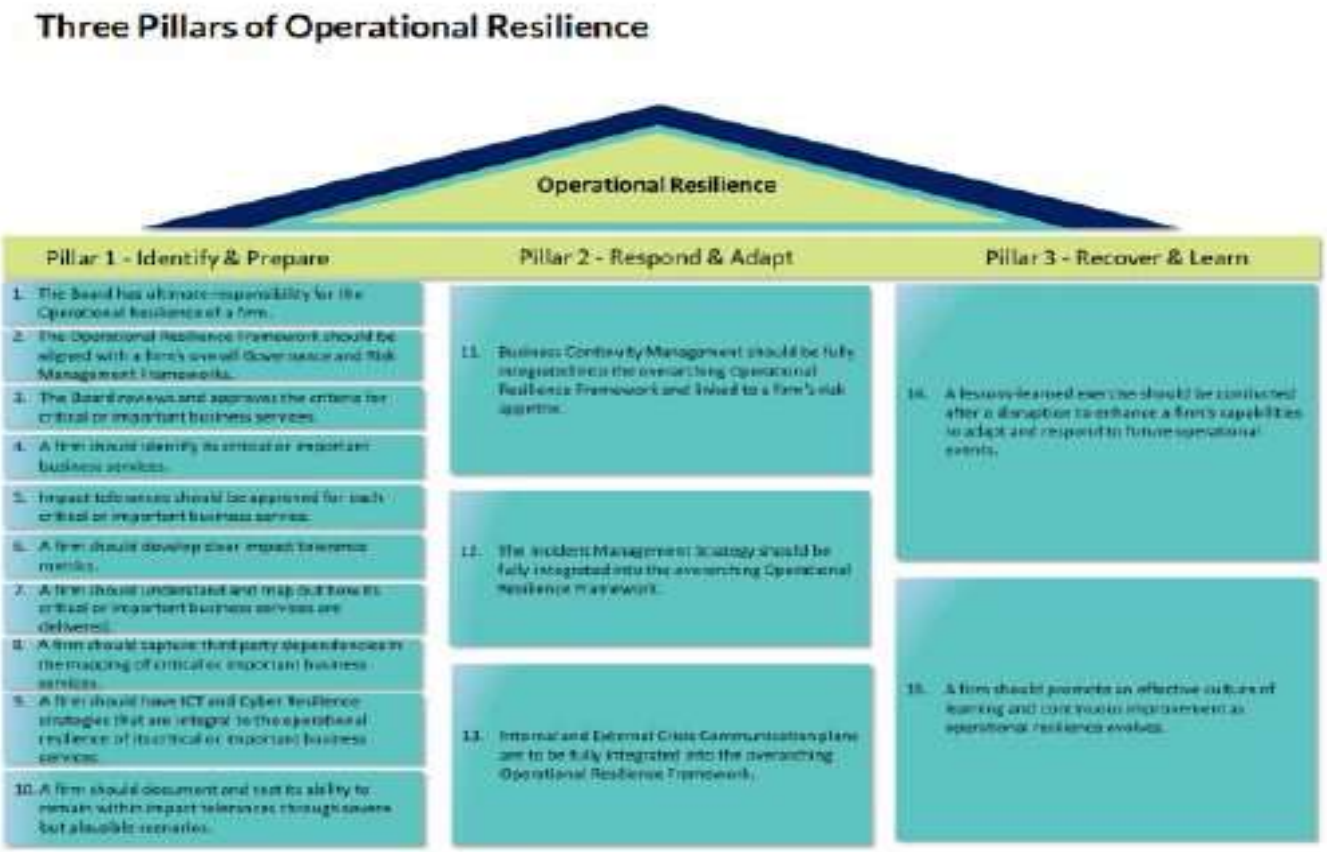
5. Documentation or "document, document and document!"
   - Leverage to the extent possible existing policies and procedures.
   - Update or implement new documentation for accountability purposes.
   - When updating and implementing, do engage with all stakeholders, to include senior management, board members, business, operations, compliance, risk, legal, data protection office, information security, and IT.
   - As clearly stated in the CBI Operational Resilience Guidance, the CBI, when assessing the firm's implementation, will *"look for evidence" that the board is seeking the required information to enable it to understand the risk and resilience profile of the firm and make targeted investment decisions to support on-going resilience efforts.*
   - Under DORA, financial entities are expected to have *"a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system, which enables them to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience"*[14].

More details of the "plan" within DORA and CBI Operational Resilience Guidance

The CBI Operational Resilience Guidance is built around 3 pillars of operational resilience:

1. Identify and prepare,
2. Respond and adapt and
3. Recover and learn,

each of these pillars with requirement subsets are set out under the following pyramid:



DORA is itself built around 5 primary pillars, namely:

1. **ICT risk management**[15] (covering among other things, governance and organisation, ICT risk management framework, detection, response and recovery, and learning and evolving)
2. **ICT-related incident management**, classification and reporting[16] (including among other things, classification of ICT-related incidents and cyber threats, and reporting of major ICT-related incidents and voluntary notification of significant cyber threats)
3. **Digital operational resilience testing**[17] (including among other things, general requirements for the performance of digital operational resilience testing, testing of ICT tools and systems, advanced testing of ICT tools, systems and processes based on TLPT, and requirements for testers for the carrying out of TLPT)
4. **Managing of ICT third-party risk**[18] (including among other things, oversight Framework of critical ICT third-party service providers)
5. **Information-sharing arrangements**[19] (financial entities are expected to comply with their obligations under GDPR)

DORA / CBI Operational Resilience Guidance: key takeaways for Compliance Officers?

Act now! Relevant financial entities/ RFSPs caught under DORA and/or the CBI Operational Resilience Guidance should create a task force as soon as possible, if not already done, to prepare an implementation project plan.

While implementing the CBI Operational Resilience Guidance and DORA, financial entities/ RFSPs should both (i) closely monitor any developments and related communications from the CBI, EU Commission, or other European Supervisory Authorities and (ii) consider any other EU legislative act, which may overlap with either DORA or the CBI Operational Resilience Guidance.

For instance, in addition to DORA, **Directive** (EU) 2022/2556 of the European Parliament and of the Council was published on 14 December 2022[20]. This EU Directive has the effect to amend several EU Directives such as AIFMD and UCITS as regards digital operational resilience for the financial sector.

Furthermore, several European Supervisory Authorities (EBA, EIOPA and ESMA or collectively ESAs) published on 29 September 2023 their joint response to the European Commission's Call for Advice on the forthcoming DORA regime. In particular, the **ESAs technical advice report** aimed at specifying further criteria for critical ICT third-party service providers (CTPPs) and determining oversight fees levied on such providers, this in order to assist the EU Commission in the drafting of delegated EU legislation to address these technical matters.[21]

Lastly, Directive (EU) 2022/2555 of the European Parliament and of the Council was published on 14 December 2022 on measures for a high common level of cybersecurity across the EU **(Directive NIS 2)**. Directive NIS 2 aims to enhance cybersecurity across EU Member States. Directive NIS 2 is expected to be incorporated into EU Member States national law by 17 October 2024, with corresponding measures implemented by 18 October 2024.

REFERENCES
1 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554
2 https://www.centralbank.ie/docs/default-source/publications/consultation-papers/cp140/cross-industry-guidance-on-operational-resilience.pdf
3 https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1684
4 Recital 1, DORA
5 Article 1 of DORA
6 Including managers of alternative investment funds
7 See full list of financial entities caught under DORA under Article 2.1 of DORA
8 See full list of financial entities exempted from DORA in Article 2.3 of DORA
9 Article 30.2.c of DORA
10 Article 5 of DORA
11 See section 6 of the CBI Cross-Industry Outsourcing Guidance at https://www.centralbank.ie/docs/default-source/publications/consultation-papers/cp138/cross-industry-guidance-on-outsourcing.pdf
12 Article 25 of DORA
13 See section 7 of the CBI Cross-Industry Outsourcing Guidance at https://www.centralbank.ie/docs/default-source/publications/consultation-papers/cp138/cross-industry-guidance-on-outsourcing.pdf
14 Article 5.1 of DORA
15 Chapter II of DORA
16 Chapter III of DORA
17 Chapter IV of DORA
18 Chapter V of DORA
19 Chapter VI of DORA
20 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2556&from=EN
21 https://www.esma.europa.eu/sites/default/files/2023-09/Joint-ESAs__response_to_the_Call_for_advice_on_the_designation_criteria_and_fees_for_the_DORA_oversight_framework_final.pdf