5. Digital operational resilience

Odile Petitfrère, Christophe Segers and Thomas Plomteux

Threat landscape

Over the past decade, the financial sector has become increasingly dependent on digital processes, critical infrastructure, ICT services, standardised information system components and partnerships. As a result, ICT and cyber risks pose a growing challenge to the operational resilience, performance and stability of the financial system. Cyber threats continue to evolve and are expected to become increasingly sophisticated, fuelled by geopolitical tensions, the rapid development of artificial intelligence and quantum computing. Malicious actors are often well funded, organised and technically agile. It is a major challenge for financial entities to keep pace with this rapidly changing threat landscape, ensure they dispose of the necessary tools, expertise and financial resources to adequately protect their assets, and cope with a range of extreme yet plausible scenarios. The importance of a proper understanding (and anticipation) of emerging threats, detection mechanisms, response and recovery solutions, forensics, the mapping of critical or important functions and their dependencies on third-party service providers is therefore constantly increasing. **The CrowdStrike incident on 19 July 2024 illustrated how even an unintentional error by a single service provider can cause widespread disruption to the economy, including the financial sector.** Other large-scale or high-profile ICT crises in recent years have been caused by, for example, supply chain problems, cyber-attacks, zero-day vulnerabilities, [1] geopolitical tensions, and poorly prepared ICT changes.

The assessment and promotion of cyber and IT risk management are top priorities for the Bank and by extension the Single Supervisory Mechanism (SSM). Various activities are carried out to assess compliance with the regulatory framework and the adequate management of cyber and IT risks. In addition to more traditional tools such as on-site inspections, IT risk questionnaires, incident notifications, third-party registers, and threat information, the Bank also relies on its ethical hacking programme, TIBER-BE, internal and sector-wide crisis simulation exercises, and European coordination mechanisms. One initiative worth mentioning, to which the Bank made a substantial contribution, was the cyber resilience stress test organised by the ECB in the first half of 2024, to gauge the effectiveness of the response and recovery plans of significant credit institutions during a simulated cyber crisis. [2]

Digital Operational Resilience Act

The Digital Operational Resilience Act (DORA) [3] entered into force on 16 January 2023. Its provisions have applied to a wide range of financial entities since 17 January 2025, including central securities

1 A zero-day vulnerability in software or hardware is one that is typically unknown to the vendor and for which no patch or other fix is available. The vendor thus has zero days to prepare a patch, as the vulnerability has already been described or exploited.

2 ECB concludes cyber resilience stress test.

3 Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.

depositories, credit institutions, insurance and reinsurance undertakings, stockbroking firms, payment institutions and electronic money institutions. DORA sets out important principles and requirements for financial entities as regards: [1]

- ICT governance and risk management,
- the management, classification and reporting of ICT-related incidents,
- the testing of digital operational resilience,
- the management of ICT risks originating from third parties, etc.

DORA is considered a *lex specialis* and thus prevails over the EU directives on measures for a high common level of cybersecurity across the Union (NIS2) [2] and on the resilience of critical entities (CER). [3]

The Bank is making various efforts to ensure the successful implementation of DORA. For instance, it actively contributed in 2024 to the development of level 2 regulatory and technical standards relating to:

- the ICT risk management framework to be implemented by financial entities,
- the criteria to be used when classifying ICT-related incidents and the applicable provisions on the reporting of such incidents to the competent authorities,
- the policies to be adopted by financial entities regarding ICT services provided by third parties that support critical or important business functions,
- the factors to be assessed when subcontracting such services,
- the templates to be used to report ICT dependencies to the competent authorities,
- the criteria and requirements for advanced threat-led penetration testing, and
- standards to guide the oversight of critical third parties.

Most of these standards have since been adopted and published by the European Commission.

The Bank is also raising awareness of DORA in the financial sector through the organisation of various seminars and communications, carrying out work to facilitate the integration of DORA into the Belgian legal order, preparing the necessary IT tools and processes, adapting its supervisory methodologies, and anticipating, to the extent possible, the impact that the oversight of critical third parties will have on its activities. Box 8 explains how the Bank expects to meet DORA's advanced resilience testing requirements through adaptations to TIBER-BE.

1 For more information, please see the article on digital operational resilience in last year's FMI Report (fmi-2024_dor.pdf).

2 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148 (NIS2 Directive).

3 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

BOX 8

TIBER-BE and threat-led penetration testing under DORA

Since 2018, the Bank has been supporting systemically important financial entities through so-called threat intelligence based ethical red teaming (TIBER), referred to as threat-led penetration testing (TLPT) in DORA, to foster robust ICT-systems and applications. With the introduction of DORA, this type of advanced cyber resilience testing is now mandatory. The TIBER-BE cyber team represents the TLPT authority responsible for identifying in-scope systemically important financial entities in Belgium. **It should be noted that TLPT is an evolution rather than a revolution. As was previously the case, an important objective remains to enable a learning experience for the financial entity concerned.** While DORA determines the formal criteria and requirements of what is to be tested, the TIBER-EU framework very much continues to guide how to assess whether financial entities are able to withstand an advanced cyber-attack. The experience acquired by the Bank, more specifically the TIBER-BE cyber team, will guarantee a smooth transition and the continuation of best practices.

Monitoring compliance with DORA

The Bank launched a survey in July 2024 to gain insight into the extent to which financial entities had made progress in implementing DORA and, more importantly, whether they expected to be compliant with the regulation by 17 January 2025. Responses were received from 132 financial entities (see Figure 13). Analysis of the responses revealed that financial entities appeared to be making significant efforts to comply with DORA and its accompanying standards as soon as possible. This was for instance illustrated by the expected substantial increase in self-assessed compliance[1] for the period between 30 September 2024 and 17 January 2025 (Figure 14). Moreover, for each item surveyed, a majority of financial entities believed that they would be compliant by 17 January 2025 (Figures 15, 16, 17 and 18), possibly because DORA's requirements are often an extension of pre-existing sectoral regulations.

Nevertheless, a substantial proportion of financial entities indicated that they did not expect to achieve full compliance, including operational effectiveness, in 2025. This was particularly the case in the following areas:

- **ICT risk management framework** (Figure 16): Respondents indicated in some cases that the relevant policy documents and procedures were still being developed or had not yet been effectively implemented. Some financial entities stated that they had not yet succeeded in mapping the dependencies between their ICT assets and ICT service providers, on the one hand, and their (critical or important) business functions, on the other. Also, in the areas of business impact analysis, encryption of data in transit, network segmentation,

1 The survey asked respondents to assess their compliance with DORA and its level 2 regulatory and implementing technical standards (RTS and ITS):
- the regulation itself (level 1),
- the RTS on the ICT risk management framework,
- the RTS and ITS on third-party risk management, and
- the RTS and ITS on incidents.

access management, vulnerability management, monitoring and detection, and software development and testing, some respondents indicated that they were experiencing difficulties complying in a timely manner.

- **Management of risks arising from dependencies on ICT third-party service providers** (Figure 17): Given the large number of contracts that need to be renegotiated, some respondents indicated that they were using a phased approach, prioritising services that support critical or important business functions. They specifically mentioned that clauses on audits, monitoring, reporting and contract termination were not yet present in every contract. Respondents also considered the visibility and management of dependencies on subcontractors to be major challenges, along with the concrete development and testing of exit strategies.

- **Testing of digital resilience:** A number of respondents indicated that they assumed they would need part of 2025 to operationalise their testing strategy and supporting governance. They noted that testing for severe but plausible scenarios (such as cyber-attacks or the failure of an ICT service provider) was not yet sufficiently established and that the imposed testing frequency was a challenge, as was the formalisation of response and recovery plans.

The Bank reminded financial entities that they were expected to have implemented DORA in full by 17 January 2025.

Figure 13

Number of responses to the DORA self-assessment survey per type of financial entity

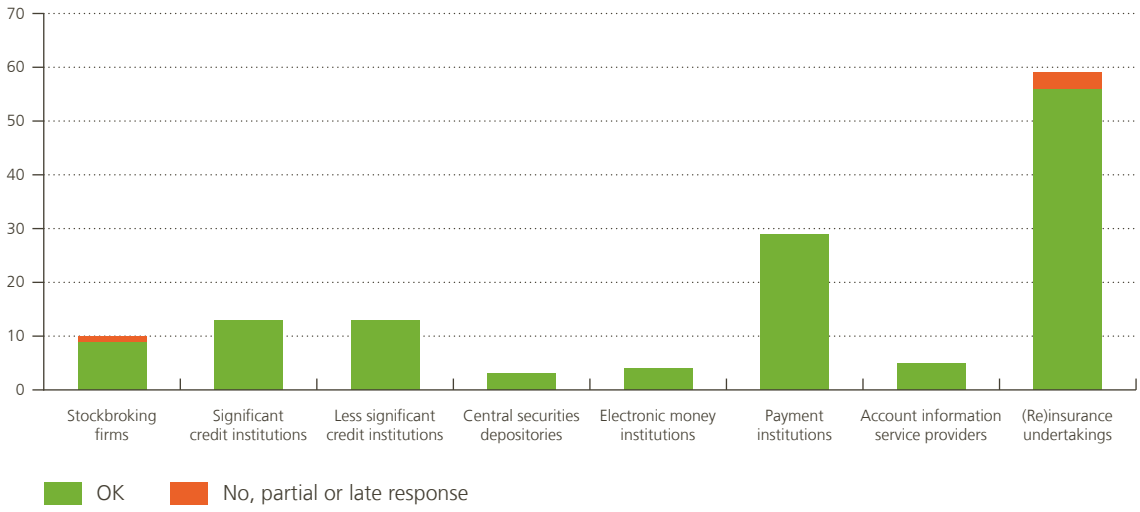


Figure 14

Self-assessed/projected compliance with the DORA Level 1 text and its RTS and ITS (the technical standards on ICT risk management, third-party risk management and incidents) on 30/9/2024 and 17/1/2025

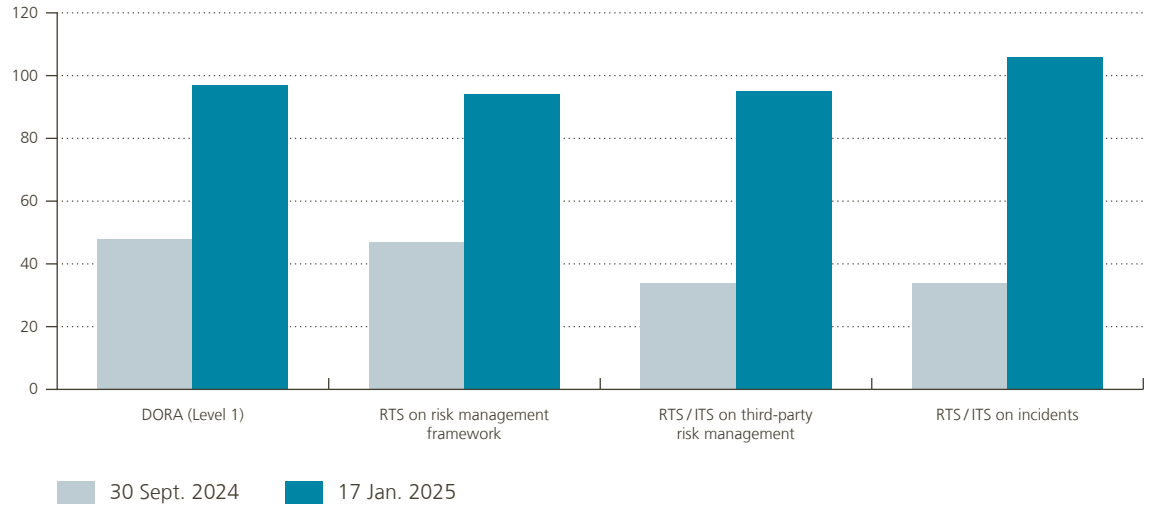


Figure 15

Projected compliance with DORA (Level 1) on 17/1/2025 (blue: Chapter II – ICT risk management; red: Chapter III – ICT-related incident management, classification and reporting; black: Chapter IV – Digital operational resilience testing; green: Chapter V – Management of ICT third-party risk)

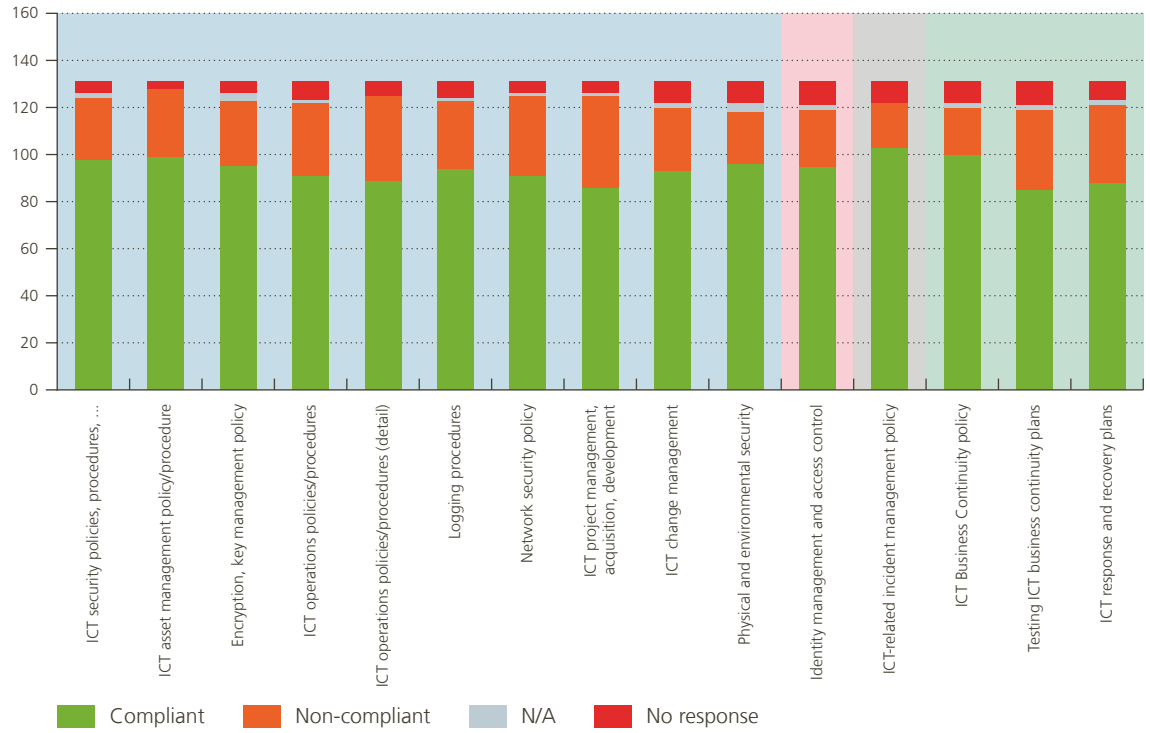


Figure 16

Projected compliance with the DORA RTS on the ICT risk management framework on 17/1/2025 (blue: Chapter I – ICT security policies, procedures, protocols and tools; red: Chapter II – Human resources policy and access control; black: Chapter III – ICT-related incident detection and response; green: Chapter IV – ICT business continuity management)

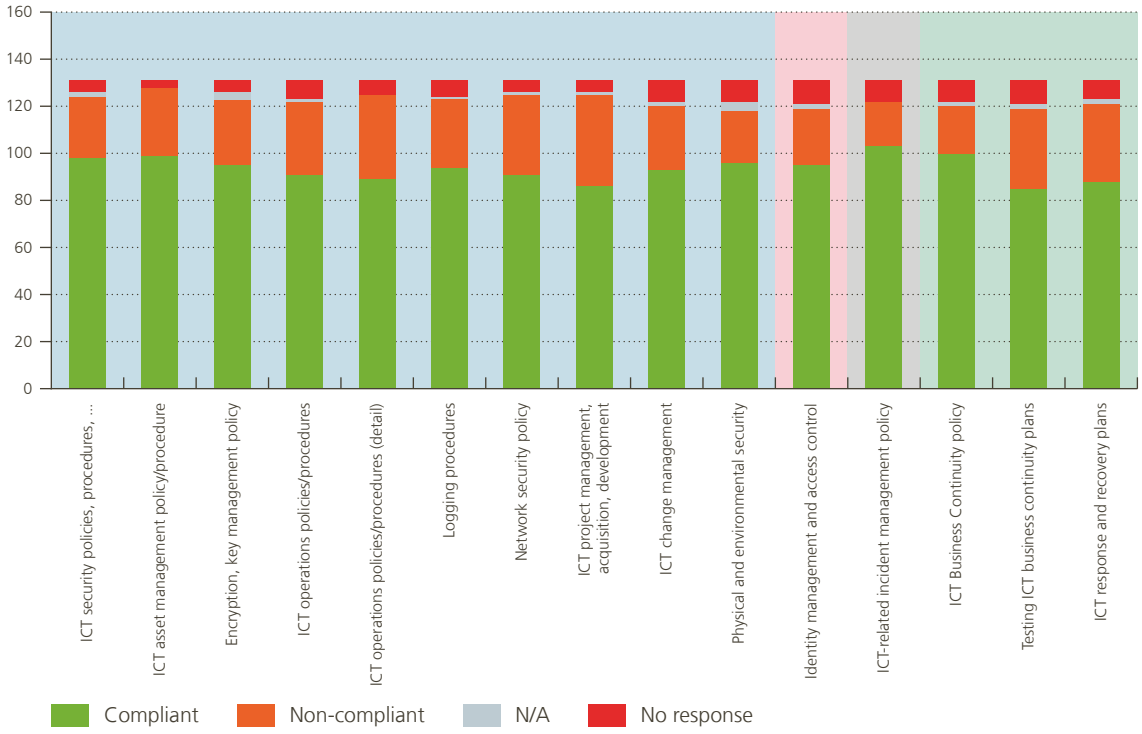
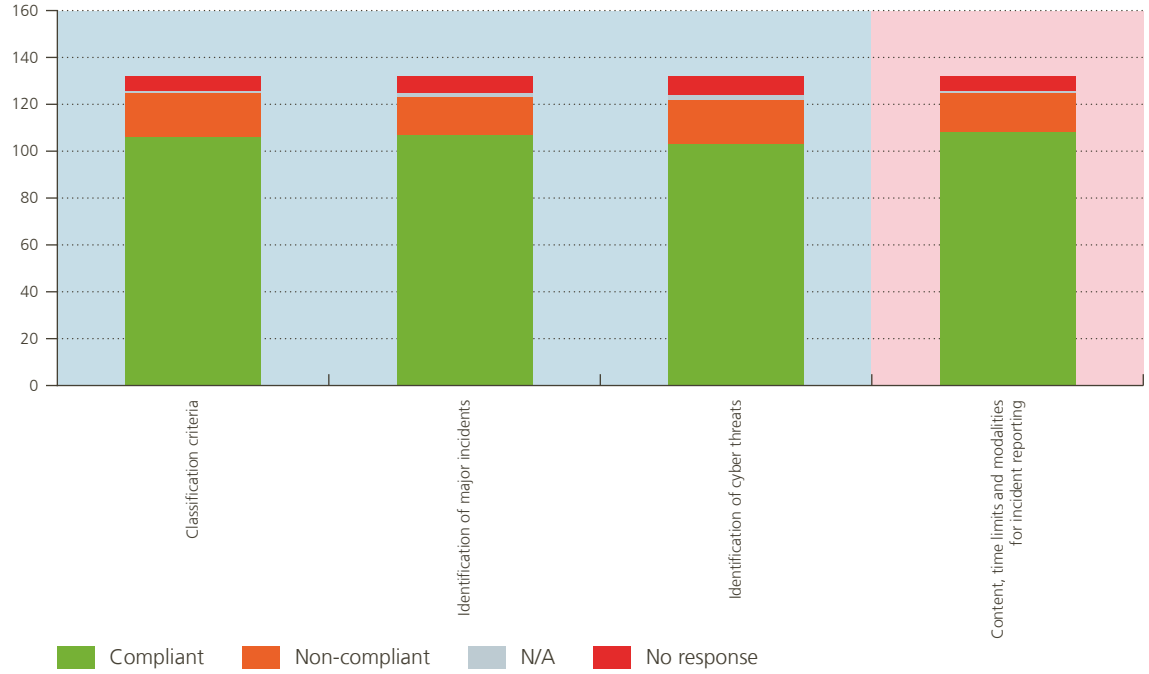


Figure 17

Projected compliance with the DORA technical standards on third-party risk management on 17/1/2025 (blue: RTS on the policy on third-party ICT services; red: Chapter II – RTS on subcontracting of ICT services; black: Chapter III – ITS on the register of information)

Figure 18

Projected compliance on 17/1/2025 with the DORA technical standards on incident management (blue: RTS on ICT-related incident classification; red: RTS/ITS on incident reporting)



Physical components and infrastructure

For a financial entity to be resilient, it is essential that its physical infrastructure, such as data centres and offices, be adequately secured. Physical security consists of all measures and systems designed and implemented to protect an institution against, for example, destruction, damage, theft, unauthorised access and natural disasters. DORA integrates physical security so as to address resilience in a holistic manner, in coherence with the Critical Entities Resilience Directive (CER)[1] and the Network and Information Systems Directive (NIS2).[2]

Recognising the importance of physical security for institutions subject to its supervision, the Bank launched a self-assessment survey on this matter in early 2025. Based on the results of this survey, the Bank will map the risks to which the Belgian financial sector is exposed, allowing supervisory actions in this area to be defined and prioritised. The survey will also contribute to raising awareness of the need to ensure an adequate degree of operational resilience, in keeping with the applicable European legislation.

1 Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

2 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.