DIGITAL OPERATIONAL RESILIENCE TESTING PROGRAMME

UNDER CHAPTER IV OF THE DIGITAL OPERATIONAL RESILIENCE ACT (EU REGULATION 2022/2554) ("DORA")[1]

[FIRM NAME]

[DATE]

This is the Digital Operational Resilience Testing Programme prepared by [FIRM NAME] (the "**Firm**") as at [DATE] under Chapter IV (Digital Operational Resilience Testing) of DORA.

This Digital Operational Resilience Testing Programme was approved by the Firm's Board on [DATE] (the "**Adoption Date**").

It comprises the following sections:

1. General Requirements for the Performance of Digital Operational Resilience Testing (Article 24 of DORA);
2. Testing of ICT Tools and Systems (Article 25 of DORA);
3. Advanced Testing of ICT Tools, Systems, and Processes Based on Threat-Led Penetration Testing (Article 26 of DORA); and
4. Requirements for Testers for the Carrying Out of Threat-Led Penetration Testing (Article 27 of DORA).

This Digital Operational Resilience Testing Programme will be reviewed by the Firm annually from its Adoption Date.

[1] Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector.

SECTION 1 – GENERAL REQUIREMENTS FOR THE PERFORMANCE OF DIGITAL OPERATIONAL RESILIENCE TESTING

	Question/Answer
1.	**Please confirm that, for the purpose of assessing preparedness for handling ICT-related incidents, of identifying weaknesses, deficiencies and gaps in digital operational resilience, and of promptly implementing corrective measures, the Firm has established, maintains and periodically reviews a sound and comprehensive Digital Operational Resilience Testing Programme as an integral part of the Firm's ICT Risk Management Framework.**[2]
	[FIRM TO INSERT ANSWER. UNDER ARTICLE 4(2) OF DORA, THE FIRM'S DIGITAL OPERATIONAL RESILIENCE TESTING PROGRAMME MUST BE PROPORTIONATE TO THE FIRM'S SIZE AND OVERALL RISK PROFILE AND TO THE NATURE, SCALE AND COMPLEXITY OF THE FIRM'S SERVICES, ACTIVITIES AND OPERATIONS][3] [THIS SECTION DOES NOT APPLY TO A "MICROENTERPRISE", WHICH IS DEFINED IN SUMMARY AS A FINANCIAL ENTITY, OTHER THAN A TRADING VENUE, A CENTRAL COUNTERPARTY, A TRADE REPOSITORY OR A CENTRAL SECURITIES DEPOSITORY, WHICH EMPLOYS FEWER THAN 10 PERSONS AND HAS AN ANNUAL TURNOVER AND/OR ANNUAL BALANCE SHEET TOTAL THAT DOES NOT EXCEED EUR 2 MILLION][4]
2.	**Please confirm that the Firm's Digital Operational Resilience Testing Programme includes a range of assessments, tests, methodologies, practices and tools which are applied in accordance with Articles 25 and 26 of DORA (see Sections 2 and 3 of this Document).**[5] **Please provide details of such assessments, tests, methodologies, practices and tools.**
	[FIRM TO PROVIDE ANSWER]
3.	**When conducting its Digital Operational Resilience Testing Programme, please confirm that the Firm follows a risk-based approach duly considering the evolving landscape of ICT risk, any specific risks to which the Firm is or might be exposed, the criticality of information assets and of services provided, as well as any other factor the Firm deems appropriate.**[6] **Please provide details of the risk-based approach followed by the Firm.**
	[FIRM TO PROVIDE ANSWER. UNDER ARTICLE 4(2) OF DORA, THE FIRM'S RISK-BASED APPROACH MUST BE PROPORTIONATE TO THE FIRM'S SIZE AND OVERALL RISK PROFILE AND TO THE NATURE, SCALE AND COMPLEXITY OF THE FIRM'S SERVICES, ACTIVITIES AND OPERATIONS][7] [THIS SECTION DOES NOT APPLY TO A "MICROENTERPRISE", WHICH IS DEFINED IN SUMMARY AS A FINANCIAL ENTITY, OTHER THAN A TRADING VENUE, A CENTRAL COUNTERPARTY, A TRADE REPOSITORY OR A CENTRAL SECURITIES DEPOSITORY,

[2] Article 24(1) of DORA.
[3] Article 4(2) of DORA.
[4] Article 3(60) of DORA.
[5] Article 24(2) of DORA.
[6] Article 24(3) of DORA.
[7] Article 4(2) of DORA.