ICT RISK MANAGEMENT FRAMEWORK

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

[FIRM NAME]

[DATE]

This is the ICT Risk Management Framework prepared by [FIRM NAME] (the "**Firm**") as at [DATE] under Chapter II (ICT Risk Management) of DORA.

This ICT Risk Management Framework was approved by the Firm's Board on [DATE] (the "**Adoption Date**").

It comprises the following sections:

1. Governance and Organisation;
2. ICT Risk Management Framework;
3. ICT Systems, Protocols and Tools;
4. Identification;
5. Protection and Prevention;
6. Detection;
7. Response and Recovery;
8. Backup Policies and Procedures, Restoration and Recovery Procedures and Methods;
9. Learning and Evolving; and
10. Communication.

It will be reviewed by the Firm annually with effect 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 – GOVERNANCE AND ORGANISATION

	Question/Answer
1.	**Please confirm that the Firm has in place an internal governance and control framework that ensures an effective and prudent management of ICT risk, in accordance with Article 6(4) of DORA, in order to achieve a high level of digital operational resilience.**[2]
	[YES/NO]
2.	**Please confirm that the management body of the Firm defines, approves, oversees and is responsible for the implementation of all arrangements related to the ICT risk management framework referred to in Article 6(1) of DORA.**[3]
	[YES/NO]
3.	**Please confirm that the management body of the Firm has accepted to bear the ultimate responsibility for managing the Firm's ICT risk.**[4]
	[YES/NO]
4.	**Please confirm that the management body of the Firm has put in place policies that aim to ensure the maintenance of high standards of availability, authenticity, integrity and confidentiality of data.**[5]
	[YES/NO]
5.	**Please confirm that the management body of the Firm has set clear roles and responsibilities for all ICT-related functions and established appropriate governance arrangements to ensure effective and timely communication, cooperation and coordination among those functions.**[6]
	[YES/NO]
6.	**Please confirm that the management body of the Firm has accepted to bear the overall responsibility for setting and approving the digital operational resilience strategy as referred to in Article 6(8) of DORA, including the determination of the appropriate risk tolerance level of ICT risk of the Firm, as referred to in Article 6(8)(b) of DORA.**[7]
	[YES/NO]

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

7.	**Please confirm that the management body of the Firm approves, oversees and periodically reviews the implementation of the Firm's ICT business continuity policy and ICT response and recovery plans, referred to, respectively, in Article 11(1) and (3) of DORA, which may be adopted as a dedicated specific policy forming an integral part of the Firm's overall business continuity policy and response and recovery plan.**[8]
	[YES/NO]
8.	**Please confirm that the management body of the Firm approves and periodically reviews the Firm's ICT internal audit plans, ICT audits and material modifications to them.**[9]
	[YES/NO]
9.	**Please confirm that the management body of the Firm allocates and periodically reviews the appropriate budget to fulfil the Firm's digital operational resilience needs in respect of all types of resources, including relevant ICT security awareness programmes and digital operational resilience training referred to in Article 13(6) of DORA, and ICT skills for all staff.**[10]
	[YES/NO]
10.	**Please confirm that the management body of the Firm approves and periodically reviews the Firm's policy on arrangements regarding the use of ICT services provided by ICT third-party service providers.**[11]
	[YES/NO]
11.	**Please provide an overview of how the management body of the Firm has put in place, at corporate level, reporting channels enabling it to be duly informed of the following: (i) arrangements concluded with ICT third-party service providers on the use of ICT services; (ii) any relevant planned material changes regarding the ICT third-party service providers; and (iii) the potential impact of such changes on the critical or important functions subject to those arrangements, including a risk analysis summary to assess the impact of those changes, and at least major ICT-related incidents and their impact, as well as response, recovery and corrective measures.**[12]
	[FIRM TO INSERT ANSWER]
12.	**Please confirm whether the Firm has:** **a) established a role in order to monitor the arrangements concluded with ICT third-party service providers on the use of ICT services; or** **b) designated a member of senior management as responsible for overseeing the related risk exposure and relevant documentation.**[13] **If (a), please provide details of the relevant role, including the name of the individual who undertakes such role.**

[8] Article 5(2) of DORA.
[9] Article 5(2) of DORA.
[10] Article 5(2) of DORA.
[11] Article 5(2) of DORA.
[12] Article 5(2) of DORA.
[13] Article 5(3) of DORA.

	If (b), please provide the name of the member of senior management who has been designated for such purposes.
	[FIRM TO INSERT ANSWER] [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][14]
13.	**Please provide an overview of how the management body of the Firm actively keeps up to date with sufficient knowledge and skills to understand and assess ICT risk and its impact on the operations of the Firm, including by following specific training on a regular basis, commensurate to the ICT risk being managed.**[15]
	[FIRM TO INSERT ANSWER]

[14] Article 3(60) of DORA.
[15] Article 5(4) of DORA.

SECTION 2 – ICT RISK MANAGEMENT FRAMEWORK

14.	**Please confirm that the Firm has put in place a sound, comprehensive and well-documented ICT risk management framework as part of its overall risk management system, which enables it to address ICT risk quickly, efficiently and comprehensively and to ensure a high level of digital operational resilience.**[16]
	[YES/NO]
15.	**Please provide an overview of the Firm's strategies, policies, procedures, ICT protocols and tools that are necessary to duly and adequately protect all information assets and ICT assets, including computer software, hardware, servers, as well as to protect all relevant physical components and infrastructures, such as premises, data centres and sensitive designated areas, to ensure that all information assets and ICT assets are adequately protected from risks including damage and unauthorised access or usage.**[17]
	[FIRM TO INSERT ANSWER]
16.	**Please provide an overview of how the Firm minimises the impact of ICT risk by deploying appropriate strategies, policies, procedures, ICT protocols and tools. The Firm must provide complete and updated information on ICT risk and on its ICT risk management framework to the competent authorities upon request.**[18]
	[FIRM TO INSERT ANSWER]
17.	**Please provide an overview of how the Firm assigns the responsibility for managing and overseeing ICT risk to a control function and ensures an appropriate level of independence of such control function in order to avoid conflicts of interest. The Firm must ensure appropriate segregation and independence of ICT risk management functions, control functions, and internal audit functions, according to the three lines of defence model, or an internal risk management and control model.**[19]
	[FIRM TO INSERT ANSWER] [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][20]
18.	**Please confirm how often the Firm's ICT risk management framework is documented and reviewed.**[21]
	[FIRM TO INSERT ANSWER] [THE FIRM'S ICT RISK MANAGEMENT FRAMEWORK MUST BE DOCUMENTED AND REVIEWED AT LEAST ONCE A YEAR, OR PERIODICALLY IN THE CASE OF A MICROENTERPRISE, AS WELL AS UPON THE OCCURRENCE OF MAJOR ICT-RELATED

[16] Article 6(1) of DORA.
[17] Article 6(2) of DORA.
[18] Article 6(3) of DORA.
[19] Article 6(4) of DORA.
[20] Article 3(60) of DORA.
[21] Article 6(5) of DORA.

	INCIDENTS, AND FOLLOWING SUPERVISORY INSTRUCTIONS OR CONCLUSIONS DERIVED FROM RELEVANT DIGITAL OPERATIONAL RESILIENCE TESTING OR AUDIT PROCESSES. IT MUST BE CONTINUOUSLY IMPROVED ON THE BASIS OF LESSONS DERIVED FROM IMPLEMENTATION AND MONITORING. A REPORT ON THE REVIEW OF THE ICT RISK MANAGEMENT FRAMEWORK MUST BE SUBMITTED TO THE COMPETENT AUTHORITY UPON REQUEST]
19.	**Please confirm how often the Firm's ICT risk management framework is subject to internal audit.[22] Please also provide a description of any formal follow-up process following such audit.**[23]
	[FIRM TO INSERT ANSWER] [THE FIRM MUST BE SUBJECT TO INTERNAL AUDIT BY AUDITORS ON A REGULAR BASIS IN LINE WITH THE FIRM'S AUDIT PLAN. THOSE AUDITORS MUST POSSESS SUFFICIENT KNOWLEDGE, SKILLS AND EXPERTISE IN ICT RISK, AS WELL AS APPROPRIATE INDEPENDENCE. THE FREQUENCY AND FOCUS OF ICT AUDITS MUST BE COMMENSURATE TO THE ICT RISK OF THE FIRM] [BASED ON THE CONCLUSIONS FROM THE INTERNAL AUDIT REVIEW, THE FIRM MUST ESTABLISH A FORMAL FOLLOW-UP PROCESS, INCLUDING RULES FOR THE TIMELY VERIFICATION AND REMEDIATION OF CRITICAL ICT AUDIT FINDINGS] [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][24]
20.	**Please confirm that Firm's ICT risk management framework includes a digital operational resilience strategy ("DORS") setting out how the framework is implemented.** [25]
	[YES/NO]
21.	**Please confirm that the Firm's DORS includes methods to address ICT risk and attain specific ICT objectives.** [26] **Please provide details.**
	[FIRM TO INSERT ANSWER]
22.	**Please provide an overview of how the Firm's ICT risk management framework supports the Firm's business strategy and objectives.**[27]
	[FIRM TO INSERT ANSWER]

[22] Article 6(6) of DORA.
[23] Article 6(7) of DORA.
[24] Article 3(60) of DORA.
[25] Article 6(8) of DORA.
[26] Article 6(8) of DORA.
[27] Article 6(8) of DORA.