DORA ICT-RELATED INCIDENT MANAGEMENT PROCESS CHECKLIST

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

[FIRM NAME]

[DATE]

This checklist documents the compliance of the ICT-Related Incident Management Process adopted by [FIRM NAME] (the "**Firm**") on [DATE] with the provisions contained in Chapter III (ICT-Related Incident Management, Classification and Reporting) of DORA.

This checklist was approved by the Firm's [Compliance Officer/Head of Compliance] on [DATE] (the "**Adoption Date**").

It comprises the following sections:

1. ICT-Related Incident Management Process (Article 17 of DORA);
2. Classification of ICT-Related Incidents and Cyber Threats (Article 18 of DORA);
3. Reporting of Major ICT-Related Incidents and Voluntary Notification of Significant Cyber Threats (Article 19 of DORA); and
4. Operational or Security Payment-Related Incidents Concerning Credit Institutions, Payment Institutions, Account Information Service Providers and Electronic Money Institutions (Article 23 of DORA).

This checklist will be reviewed by the Firm on an annual basis 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 – ICT-RELATED INCIDENT MANAGEMENT PROCESS

	Question/Answer
1.	**Please confirm that the Firm has defined, established and implemented an ICT-related incident management process to detect, manage and notify ICT-related incidents.**[2]
	[YES/NO]
2.	**Please confirm that the Firm records all ICT-related incidents and significant cyber threats.**[3]
	[YES/NO. PLEASE PROVIDE IN YOUR RESPONSE DETAILS OF HOW THE ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS ARE RECORDED E.G. THEY ARE ENTERED INTO A REGISTER OF ICT-RELATED INCIDENTS AND SIGNIFICANT CYBER THREATS MAINTAINED BY THE FIRM'S IT DEPARTMENT]
3.	**Please confirm that the Firm has established appropriate procedures and processes to ensure:** **(a) a consistent and integrated monitoring, handling and follow-up of ICT-related incidents; and** **(b) that root causes are identified, documented and addressed in order to prevent the occurrence of such incidents.**[4]
	[YES/NO. PLEASE PROVIDE IN YOUR RESPONSE DETAILS OF SUCH PROCEDURES]
4.	**Please confirm that the Firm's ICT-related incident management process puts in place early warning indicators.** [5] **Please provide details of such early warning indicators.**
	[FIRM TO INSERT ANSWER. PLEASE PROVIDE DETAILS OF THE EARLY WARNING INDICATORS ADOPTED BY THE FIRM, THE CONDITIONS WHICH WOULD TRIGGER SUCH EARLY WARNING INDICATORS AND THE ACTIONS TO BE TAKEN BY THE FIRM AFTER SUCH EARLY WARNING INDICATORS HAVE BEEN TRIGGERED]
5.	**Please confirm that the Firm's ICT-related incident management process establishes procedures to identify, track, log, categorise and classify ICT-related incidents according to their priority and severity and according to the criticality of the services impacted, in accordance with the criteria set out in Article 18(1) of DORA (see Question 10 of this Checklist).** [6]
	[YES/NO. PLEASE PROVIDE IN YOUR RESPONSE DETAILS OF SUCH PROCEDURES].

[2] Article 17(1) of DORA.
[3] Article 17(2) of DORA.
[4] Article 17(2) of DORA.
[5] Article 17(3) of DORA.
[6] Article 17(3) of DORA.