December 2024

Report on Internal Control
Annex on Information and Communication Technology (ICT) Risk Management

(Annex prepared in accordance with the *Arrêté du 3 novembre 2014*, as amended, and with Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector)

Introduction

The purpose of this annex is to supplement the template of the Report on Internal Control with the elements provided for under Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (hereinafter referred to as the "DORA Regulation"). This annex is applicable to entities submitting a Report on Internal Control, as laid down in Article 2 of the DORA Regulation. The elements required from entities relate to the framework for the management of information and communication technology (ICT) risk that is provided for in Article 6 of the DORA Regulation, the review rules of which are specified in Article 6(5). The obligations applicable to entities subject to the simplified ICT risk management framework provided for in Article 16 of the DORA Regulation are set out in a box in this annex.

This annex shall be sent to the ACPR in a computerised format, under the conditions laid down in amended Instruction No 2017-I-24 on the transmission of accounting and prudential documents and other information to the ACPR.
It shall be sent to the SGACPR by April 30 at the latest following the end of each financial year. For the first round of reporting, submission of this annex is expected by 30 June 2025 at the latest.

The report should be drafted in French. By way of exception, for institutions subject to the ECB's direct supervision, the report may be written in English.

Expected information on IT activities

Table of contents

1. IT strategy and governance

- Presentation of the institution's IT strategy (organisation, links with the overall strategy, priority objectives and action plans set, risk appetite framework...) and the resources allocated to implement it (procedures in place to ensure compliance, allocated budget and budget steering procedure, staff numbers and type of staff dedicated to IT operations management, information system security and business continuity);
- Presentation of the governance framework (roles of the effective managers, the supervisory body and, where applicable, the risk committee, in identifying, monitoring and reviewing the ICT risk management framework) (Article 5 of the DORA Regulation).

2. ICT risk management

- Presentation of the digital operational resilience strategy and the resources allocated to implement it (Article 6(8) of the DORA Regulation);
- Presentation of the ICT risk management policies and procedures containing all the elements referred to in Article 3 of Commission Delegated Regulation (EU) 2024/1774 of 13 March 2024 supplementing Regulation (EU) 2022/2554 of the European Parliament and of the Council with regard to regulatory technical standards specifying ICT risk management tools, methods, processes, and policies and the simplified ICT risk management framework ('Delegated Regulation 2024/1774')[1];
- Presentation of the organisation of the ICT risk management[2] framework (Articles 5(1), 6(1) and 16(1)(a) of the DORA Regulation) including the following elements:
    i) ICT risk profile assessment process and its results;
    ii) ICT risk tolerance threshold;
    iii) Audit process, ICT audit plan (Article 5(2)(f) and Article 6(6) of the DORA Regulation) and formal follow-up process based on the conclusions derived from the internal audit review (Article 6(7) of the DORA Regulation);

[1] Delegated Regulation 2024/1774 is based on the draft regulatory technical standards submitted to the Commission by the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority, in consultation with the European Union Agency for Cybersecurity.

[2] This management framework shall be reviewed at least once a year.

iv) The procedures used to report to the effective managers and the supervisory body on the institution's ICT risk exposure[3] and the frequency of these reports.

Do you have the following elements in place:	Yes/no/ partially	Comments
Risk reduction measures for major ICT risks and controls to monitor their effectiveness, a description of the procedures used to report to the effective managers and the supervisory body;	Choose an item.	
A description of the continuous monitoring and control of the security and functioning of ICT systems and tools (Article 9(1) of the DORA Regulation, cf. Part 2);	Choose an item.	
A presentation of ICT risks including risks to the resilience, continuity and availability of ICT systems, in particular those supporting critical or important functions (Article 9(2) of the DORA Regulation);	Choose an item.	

– For entities referred to in Article 16(1) of the DORA Regulation for which the simplified ICT[4] risk management framework applies, a presentation of:

i) the main shortcomings identified, any risks and anomalies detected;

ii) the remedial measures undertaken to address identified shortcomings, the expected date of implementation of these measures, and the state of progress of their implementation as at the date of drafting of this Report;

iii) the procedures used to follow up on recommendations issued as a result of ongoing monitoring (tools, persons in charge);

iv) the procedure used to verify that the remedial measures ordered within the institution are implemented by the appropriate persons within a reasonable timeframe (Articles 11(f) and 26(a) of the *Arrêté du 3 novembre 2014* on the internal control of companies in the banking, payment services and investment services sector subject to supervision by the *Autorité de contrôle prudentiel et de résolution*).

3. Security of ICT networks and systems

Do you have the following elements in place:	Yes/no/ partially	Comments
A security policy for information systems[5] - cf. Article 9(4)(a) of the DORA Regulation?	Choose an item.	
Date of creation or update		
Name of the head of IT security		

[3] Attach the most recent dashboard used to inform them.

[4] This framework shall be reviewed periodically.

[5] An information security policy defining rules to protect the availability, authenticity, integrity and confidentiality of data, information assets and ICT assets, including those of their customers, where applicable.

Do you have the following elements in place:	Yes/no/ partially	Comments
ICT security policies (Article 9(2) of the DORA Regulation)? Reminder: ICT security policies must comply with the provisions set out in Article 2 of Delegated Regulation 2024/1774	Choose an item.	
Network security management procedures, protocols, policies and tools (Article 13(1) of Delegated Regulation 2024/1774)?	Choose an item.	
Procedures, protocols, policies and tools to protect information in transit (Article 14(1) of Delegated Regulation 2024/1774)?	Choose an item.	

- Description of the procedures implemented to detect, prevent and respond to ICT-related incidents (Article 6(8)(a) and Article 11(2)(b) of the DORA Regulation) and major ICT-related[6] incidents;
- Presentation of the procedure used to report major ICT-related incidents to the competent authority and the procedure used for voluntary notification of significant cyber threats to the competent authority (Article 19 of the DORA Regulation);

Do you have the following elements in place:	Yes/no/ partially	Comments
ICT security awareness programmes (awareness programmes for staff and third-party ICT service providers where applicable) and digital operational resilience training (Article 13(6) of the DORA Regulation).	Choose an item.	
A physical and environmental security policy as per Article 18 of Delegated Regulation 2024/1774.	Choose an item.	
A logical security policy, a security policy to protect the integrity and confidentiality of data (specific measures set up for online banking, description of the penetration testing carried out during the year under review, IT contingency plan...).	Choose an item.	

4. Management of ICT operations

4.1. Presentation of information asset management

Do you have the following elements in place:	Yes/no/ partially	Comments
An ICT asset management policy (Articles 4(1) and 8(1)(2)(a) of Delegated Regulation 2024/1774);	Choose an item.	

[6] An ICT-related incident means a single event or a series of linked events unplanned by the financial entity that compromises the security of the network and information systems, and have an adverse impact on the availability, authenticity, integrity or confidentiality of data, or on the services provided by the financial entity (Article 3(8) of the DORA Regulation).

A record of ICT assets (Article 4(2)(b) points (i) to (ix) of Delegated Regulation 2024/1774)	Choose an item.	

4.2. Human resources policy and access control

- Description of the main principles of the human resources policy (Article 19 of Delegated Regulation 2024/1774)

In addition, do you have the following elements in place:	Yes/no/ partially	Comments
A policy comprising measures to control physical access to ICT assets (Article 21(g) of Delegated Regulation 2024/1774)	Choose an item.	
Identity management policies and procedures (Article 20 of Delegated Regulation 2024/1774)	Choose an item.	
A policy on the control of access management rights to ICT assets (Article 21 of Delegated Regulation 2024/1774)	Choose an item.	
Policies and protocols for strong authentication mechanisms (Article 9(4)(d) of the DORA Regulation and Article 21(f) of Delegated Regulation 2024/1774)	Choose an item.	

4.3. ICT operations management process: presentation of the procedures covering the operation, monitoring and control of ICT systems and services

Do you have the following security procedures in place for ICT operations:	Yes/no/ partially	Comments
Policies and procedures for ICT operations (Article 9(2) of the DORA Regulation and Article 8(1) of Delegated Regulation 2024/1774)	Choose an item.	
Capacity and performance management procedures (Article 9 of Delegated Regulation 2024/1774)	Choose an item.	
Vulnerability management procedures (Articles 10(1) and 10(2) of Delegated Regulation 2024/1774)	Choose an item.	
Patch management and update management procedures (Article 9(4)(f) of the DORA Regulation and Articles 10(3) and 10(4) of Delegated Regulation 2024/1774)	Choose an item.	
An ICT data and system security procedure (Article 11 of Delegated Regulation 2024/1774)	Choose an item.	
Logging procedures, protocols and tools (Article 12 of Delegated Regulation 2024/1774)	Choose an item.	

- Description of the digital operational resilience testing programme for the purpose of assessing preparedness for handling ICT-related incidents (Article 24 of the DORA Regulation)

4.4. Incident detection and management process for operational or security incidents, including:

Description of the main principles of the ICT-related incident management process and mechanisms in place to promptly detect anomalous activities (Articles 17 and 10 of the DORA Regulation).

More specifically, do you have the following elements in place:	Yes/no/ partially	Comments
A communication strategy in the event of ICT-related incidents the disclosure of which is required pursuant to Article 14 of the DORA Regulation (Article 6(8)(h)).	Choose an item.	
An ICT-related incident management policy (including a list of relevant internal/external contacts) (Article 22 of Delegated Regulation 2024/1774)	Choose an item.	
Technical, organisational and operational mechanisms to enable the prompt detection of anomalous activities and behaviours (including ICT network performance issues and incidents) and mechanisms to analyse significant and recurring incidents (Articles 22(c) and 22(e) of Delegated Regulation 2024/1774)	Choose an item.	
A procedure to retain all evidence relating to ICT-related incidents in compliance with the provisions set out by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (Article 22(d) of Delegated Regulation 2024/1774)	Choose an item.	
Tools generating alerts for anomalous activities and behaviour, at least for ICT assets and information assets supporting critical functions, and logging each anomalous activity (Articles 23(2)(b) and 23(4) of Delegated Regulation 2024/1774)	Choose an item.	
A procedure for the communication of changes implemented following post-incident reviews (Article 13(2) of the DORA Regulation).	Choose an item.	

4.5. Project and change management

- Description of the ICT change management policies (Article 9(4) of the DORA Regulation);
- Description of the management framework for IT projects and programs:

Do you have the following elements in place:	Yes/no/ partially	Comments
An ICT project management policy (Article 15 of Delegated Regulation 2024/1774)	Choose an item.	
A policy governing the acquisition, development and maintenance of ICT systems (Article 16 of Delegated Regulation 2024/1774)	Choose an item.	
ICT change management procedures (Article 17 of Delegated Regulation 2024/1774).	Choose an item.	

5. Business continuity management

5.1. Description of the business continuity management system required under the *Arrêté du 3 novembre 2014* on internal control

- Roles and responsibilities set for business continuity management;
- Business continuity policy, including its objectives and retained scenarios, the organisation to be implemented by the institution's business units or for the various operational processes;
- Mechanism used to conduct a business impact analysis of exposure to severe business disruptions (*Business impact analysis* - BIA), including the organisation adopted for its implementation within the institution. Presentation of the main conclusions derived from the analysis, and presentation of its results for critical or important processes;
- Presentation of the contingency and business continuity plan(s), scenarios retained, overall architecture (a single plan or a plan per business line or process, overall consistency where multiple plans are in place), responsibilities (scope of activities covered by the contingency and business continuity plan(s)), activities given priority in the event of a crisis, residual risks not covered by the contingency and business continuity plan, implementation time frames of the contingency and business continuity plan;
- Audit and results of the continuous monitoring of the contingency and business continuity plan.

5.2. Description of the operational continuity support for ICT systems and solutions (ICT continuity) (cf. Article 11 of the DORA Regulation)

- Roles and responsibilities assigned in relation to ICT continuity management;
- Presentation of the ICT continuity policy (as referred to in Article 11.2 of the DORA Regulation and Article 39 of Delegated Regulation 2024/1774), including:
  - i) Disruption scenarios covered (operational and security incidents),
  - ii) Ability to identify ICT assets supporting critical or important processes, including when they are managed by service providers.
  - iii) Objectives and procedures defined for ICT continuity testing.
- Presentation of the response plans associated with each of the different disruption scenarios defined for the various ICT assets supporting critical or important processes, including when they are managed by service providers. Indication of the maximum permissible service downtime and data loss;
- Presentation of IT continuity testing (Article 40 of Delegated Regulation 2024/1774) performed over the year under review (objective, scope, area covered, schedule), and explanation of the associated results and action plans.

- Audit and results of the continuous monitoring of the ICT response and recovery plan.

5.3. Crisis management framework (cf. Article 11 of the DORA Regulation)

- Roles and responsibilities assigned to the crisis management function[7] (cf. Article 11.7 of the DORA Regulation);
- Presentation of the crisis management system (organisation, triggers defined for the various activation stages);
- Description of recovery procedures and methods;
- Presentation of all instances of activation of the crisis management system during the year under review (e.g. influenza A virus [H1N1], Covid, IT failure or cyber-attack).

- Entities referred to in Article 16(1) of the DORA Regulation for which the simplified ICT risk management framework applies, shall ensure the continuity of critical or important functions, through business continuity plans and response and recovery measures (point f), which include, at least, back-up and restoration measures, and they shall test the plans and measures referred to in point (f) on a regular basis, as well as the effectiveness of the controls implemented in accordance with points (a) and (c) (point (g).

6. Outsourcing of ICT activities

- Establishment of a role in order to monitor the arrangements concluded with ICT third-party service providers (Article 5(3) of the DORA Regulation)[8];
- Concerning arrangements for the use of ICT services provided by ICT third-party service providers (Article 5(2)(h) and Article 28(2) of the DORA Regulation): presentation of the institution’s policy and strategy defined for ICT third-party risk, including in particular a description of existing provisions to inform outsourcing decisions *(prior analysis carried out on the criticality of the activity to be outsourced and on the assessment of associated risks, etc.)* before they become effective;
- adaptations made to comply with the requirement to maintain a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers (Article 28(3) of the DORA Regulation);
- description of the procedure used and assessments carried out before entering into a contractual arrangement with ICT third-party service providers;
- description of the permanent and periodic control system in place for outsourced activities;
- description of the methodology used for the assessment of service quality and frequency of review;
- description of the procedure used for the identification, management and monitoring of risks associated with outsourced activities;
- description of the procedures implemented by the institution to maintain the expertise required to effectively control outsourced activities and manage the risks associated with outsourcing;
- description of the procedures used to identify, assess and manage conflicts of interest related to the outsourcing mechanism of the institution, including between entities of the same group;
- description of the business continuity plans and exit strategy defined for critical or important outsourced activities: formalised retained scenarios and objectives as well as alternative measures considered, presentation of performed tests (frequency, results...), reporting to senior management (regarding tests and updates to the plans or exit strategy);

[7] Microenterprises are exempted.

[8] Microenterprises are exempted. A microenterprise is 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 (Article 3(60) of the DORA Regulation).

- description, formalisation and date(s) of update of the procedures guiding the permanent and periodic control of outsourced activities (including compliance review procedures);
- results of 2nd level permanent control actions carried out on outsourced activities: main shortcomings identified and corrective measures implemented to address them (provisional date of implementation and state of progress of their implementation at the time of drafting of this report), procedures used to follow-up on recommendations derived from permanent control actions *(tools, persons in charge)*;
- results of periodic control actions carried out on outsourced activities: main shortcomings identified and corrective measures implemented to address them (provisional date of implementation and state of progress of their implementation at the time of drafting of this report), procedures used to follow-up on recommendations derived from periodic control actions.