SUPERVISION CHECKLIST

DORA Checklist

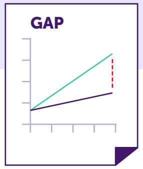
The Digital Operational Resilience Act is a European regulation that aims to increase the cyber resilience of financial companies. These companies have until 17 January 2025 to comply with the requirements. This DORA checklist serves to gain clarity on what is needed in terms of policies and procedures to meet the regulation based on ten key themes. Please note: given the scope of DORA, the checklist is not exhaustive. We refer to the regulation and associated RTS and ITS for a further explanation of the requirements. Please see the AFM website for further information.

Possible answers

✗ No

↓

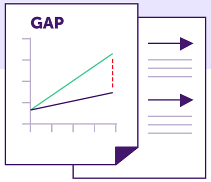
Recommendation to initiate a DORA GAP analysis



⊘ Partly

↓

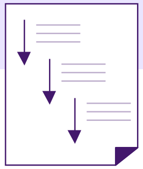
Recommendation to translate the DORA GAP analysis into action



✓ Yes, drawn up

↓

Recommendation to initiate the implementation programme and to adjust any relevant business processes



✓ Yes, drawn up and implemented

↓

Recommendation to monitor adequate functioning of policies and procedures on an ongoing basis

Please note: a simplified ICT risk management framework applies to a number of smaller parties, as explained in Article 16(1) and AFM DORA update 3.

AFM

SUPERVISION CHECKLIST

Questions

Governance (Article 5)

1/10

Has the management body established a governance and control framework for the management of ICT risks?

Such a framework should include clear duties and responsibilities of ICT-related functions, such as the set up of an ICT-related risk function; budget allocation; periodic assessments and reporting channels; and an internal ICT audit plan.

No	Partly	Yes, drawn up	Yes, drawn up and implemented
✗	⊘	✓	✓
□	□	□	□

ICT risk management (Article 6)

2/10

Have you established a framework for ICT risk management, as part of your company-wide risk management system?

Such a framework should include a risk-analysis methodology, a risk register (including action plans) and periodic assessments, among other things.

No	Partly	Yes, drawn up	Yes, drawn up and implemented
✗	⊘	✓	✓
□	□	□	□

See RTS15 and 16(3) for further explanation

ICT Asset inventory (Article 8)

3/10

Do you have an inventory of all information assets and ICT assets, including all company processes that rely on ICT third-party service providers?

This should be kept in a register which clearly indicates whether the assets support critical processes.

No	Partly	Yes, drawn up	Yes, drawn up and implemented
✗	⊘	✓	✓
□	□	□	□

See section III of RTS15 and 16(3) for further explanation

Questions

Information security policy (Article 9)

4/10

Have you established an ICT security policy providing policies and procedures aimed at protecting the availability, integrity and security of ICT systems?

This document should include policies and procedures on technical measures, such as the physical or logical access control; management of ICT changes; encryption; network security; and the implementation of patches and updates.

No	Partly	Yes, drawn up	Yes, drawn up and implemented
✗	⊘	✓	✓
□	□	□	□

See RTS15 and 16(3) for further explanation

Business continuity (Articles 11-12)

5/10

Have you put in place an ICT Business Continuity Plan, providing the implementation of business impact analyses, a communication plan, periodic testing, and a review of events?

This should be tested, among other things, on the basis of realistic test scenarios that attempt to simulate potential disruption.
The testing must also include the testing of ICT services provided by third parties, if possible. Test results must be documented and any identified deficiencies resulting from the tests must be analysed, addressed and reported to the management body.

No	Partly	Yes, drawn up	Yes, drawn up and implemented
✗	⊘	✓	✓
□	□	□	□

See RTS15 and 16(3) for further explanation

Back-up data and recovery (Article 12)

6/10

Do you have backup policies and procedures, including restoration and recovery procedures and methods?

No	Partly	Yes, drawn up	Yes, drawn up and implemented
✗	⊘	✓	✓
□	□	□	□

See RTS15 and 16(3) for further explanation

Awareness and training (Article 13)

7/10

Have you developed ICT security awareness programmes and digital operational resilience training as compulsory modules in staff training schemes commensurate to the remit of employees' duties?

No	Partly	Yes, drawn up	Yes, drawn up and implemented
✗	⊘	✓	✓
□	□	□	□

Questions

ICT-related incident management (Articles 17-23)

8/10

Have you established an ICT-related incident management process to detect and handle ICT-related incidents, including the use of an incident register and templates to support the notification duty?

No	Partly	Yes, drawn up	Yes, drawn up and implemented
✗	⊘	✓	✓
□	□	□	□

See RTS18(3), RTS20(a) and ITS20(b) for further explanation

Digital operational resilience testing (Articles 24-27)

9/10

Have you established a risk-based digital operational resilience testing programme, including policies and procedures to follow up on findings?

✗	⊘	✓	✓
□	□	□	□

See RTS26(11) for further explanation

Management of ICT risk for third-party providers (Articles 28-30)

10/10

Have you adopted policies on the use of ICT services supporting critical or important functions provided by third-party service providers?

These policies should include a register of information in relation to all contractual arrangements with ICT third-party service providers, exit strategies for ICT services supporting critical and/or important functions, and contract templates based on requirements from the RTS, such as service levels and audit rights.

✗	⊘	✓	✓
□	□	□	□

See RTS28(1), RTS30(5) and ITS28(9) for further explanation

Publications

In anticipation of DORA coming into force, the AFM will regularly share informative updates and other publications to prepare companies for DORA.