

DORA critical ICT third-party checklist

29 checks across contracts, monitoring, registers and
exit plans

Based on Articles 28 to 35 of the Digital Operational Resilience Act

A	Know your exposure	☐ ☐ ☐ ☐	p. 2
B	Article 30(2) contract provisions	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	p. 2
C	Article 30(3) additional provisions	☐ ☐ ☐ ☐ ☐ ☐	p. 3
D	Monitor and escalate	☐ ☐ ☐	p. 3
E	Exit planning	☐ ☐ ☐ ☐	p. 3
F	Oversight readiness	☐ ☐ ☐	p. 3

CHECKLIST · PART 1

Most firms have the contract. Fewer can evidence the governance around it.

Use this to find the gaps before a supervisor does.

☐ Tick what you can evidence **GAP** Flag what you cannot _____ Note the gap and its owner

A Know your exposure Art. 28		GAP / OWNER
☐	Identify every ICT service that supports a critical or important function	_____ GAP
☐	Keep the Register of Information granular enough for supervisory review	_____ Art. 28(3) GAP
☐	Hold a consolidated group view of provider exposure across all legal entities	_____ GAP
☐	Map the subcontracting chain behind each critical provider	_____ GAP

B Article 30(2) contract provisions Art. 30(2)		GAP / OWNER
All ICT third-party contracts		
☐	Full description of services and subcontracting	_____ Art. 30(2) (a) GAP
☐	Service locations and data processing locations, with change notification	_____ Art. 30(2) (b) GAP
☐	Data availability, authenticity, integrity and confidentiality, including personal data	_____ Art. 30(2) (c) GAP
☐	Data access, recovery and return on insolvency, resolution or termination	_____ Art. 30(2) (d) GAP
☐	Service level descriptions, including updates	_____ Art. 30(2) (e) GAP
☐	Incident assistance at no extra cost, or at a pre-agreed cost	_____ Art. 30(2) (f) GAP
☐	Cooperation with competent and resolution authorities	_____ Art. 30(2) (g) GAP
☐	Termination rights and minimum notice periods	_____ Art. 30(2) (h) GAP
☐	Participation in security awareness and resilience training	_____ Art. 30(2) (i) GAP

Article 30(3) additional provisions

C

Art. 30(3)

Critical or important functions

GAP / OWNER

☐	Quantitative and qualitative service level targets, with reporting	Art. 30(3)(a)		GAP
☐	Notice periods and reporting on material developments	Art. 30(3)(b)		GAP
☐	Business continuity and ICT security implemented and tested	Art. 30(3)(c)		GAP
☐	Participation in threat-led penetration testing	Art. 30(3)(d)		GAP
☐	Unrestricted access, inspection and audit rights, including for competent authorities and the Lead Overseer	Art. 30(3)(e)		GAP
☐	Exit strategy provisions: transition periods and migration cooperation	Art. 30(3)(f)		GAP

D

Monitor and escalate Art. 28

GAP / OWNER

☐	Continuous monitoring against SLAs and ICT risk indicators		GAP
☐	Escalation paths to the management body defined and used		GAP
☐	Concentration risk assessed and reported into enterprise risk management		GAP

E

Exit planning Art. 28

GAP / OWNER

☐	Exit strategy documented for every critical dependency		GAP
☐	Exit plan tested as an operational process, not a paper exercise		GAP
☐	Constraints and substitutability addressed honestly		GAP
☐	Named owner and review cadence for each exit plan		GAP

F

Oversight readiness Art. 31 to 35

GAP / OWNER

☐	Checked whether any of your providers are on the ESA list of designated critical ICT third-party providers		GAP
☐	Contracts enable Lead Overseer information requests, investigations and on-site inspections, including at material subcontractors		GAP
☐	Evidence pack ready for competent authority requests		GAP

Every unticked box is a question your supervisor can ask.



of 29 ticked

Count your ticks across sections A to F

Tick fewer than 20?

Start with your Register of Information and exit plans.

Contracts can be renegotiated at renewal; gaps in monitoring and evidence cannot be fixed overnight.

See how SureCloud covers DORA →

Book a DORA demo →

surecloud.com/dora

This checklist is a guide, not legal advice. Check requirements against the regulation text and your competent authority's guidance.