DORA Incident Response Readiness Checklist

Questions to test whether your firm could manage and report a major ICT-related incident under the EU Digital Operational Resilience Act (DORA). Work through them with your ICT, risk, compliance and business continuity leads.

The reporting clock

Initial notification	Within 4 hours of classifying the incident as major, and no later than 24 hours after becoming aware of it.
Intermediate report	Within 72 hours of the initial notification, with updates when the status changes significantly.
Final report	No later than one month after the latest intermediate report.

Governance	Yes	Partly	No
The management body has approved the ICT risk management framework and understands its role in a major incident.			
Named people own incident classification, reporting and communication, with deputies.			

Detection and classification	Yes	Partly	No
We can detect, log and track all ICT-related incidents from a single record.			
Our classification process applies the DORA criteria, including impact on critical or important functions, clients affected, duration, data losses and economic impact.			
We can classify a serious incident quickly enough to meet the 4-hour notification window.			

Reporting	Yes	Partly	No
We hold the competent authority's reporting templates and know how to submit them.			
Someone is available to classify and report incidents outside business hours.			
We have a process to inform affected clients where required.			

Response and recovery	Yes	Partly	No
ICT business continuity and response plans exist for critical or important functions and have been tested.			
Backup and restoration have been tested against realistic recovery objectives.			

Third parties	Yes	Partly	No
Our register of information on ICT third-party arrangements is complete and current.			
Contracts with critical ICT providers require them to notify us of incidents promptly.			

Testing and learning	Yes	Partly	No
We run a digital operational resilience testing programme, including scenario-based exercises.			
Post-incident reviews identify root causes, and actions are tracked until closed.			

Check reporting thresholds, templates and channels against the current regulatory technical standards and your competent authority's guidance. General guidance only. Adapt it to your organisation's own policies, procedures and legal or regulatory requirements before use.