CYBERSECURITY READINESS · EU FINTECH · 2026

The DORA & EU AI Act Readiness Playbook for EU Fintech

A board-level checklist for the people who carry ICT risk. Run it on your own firm in fifteen minutes.

CEO | CISO | CTO | Head of Compliance | CRO

WHY THIS PLAYBOOK

A regulator does not wait for a convenient quarter. Neither does an attacker.

EU fintech runs on three things a single incident can take away in an afternoon: a working trading or payment system, a licence in good standing, and the trust of the banks and partners that keep your rails open. When one breaks, the loss is not an IT line item. It is revenue you cannot bill, client funds you have to explain, and a supervisor who now wants answers in writing.

$5.56M

Average cost of a data breach in financial services, the second-highest of any sector (IBM, 2025).

92%

Of EU financial firms are not yet fully compliant with DORA resilience testing and third-party risk management (Deloitte, 2025).

€35M / 7%

Maximum EU AI Act penalty for the most serious breaches, of global annual turnover.

€20M / 4%

Maximum GDPR fine: €20 million or 4% of global annual turnover, whichever is higher.

In Deloitte's 2025 survey, only 25% of financial institutions said they were confident in their DORA compliance, and just 8% reported full compliance on third-party risk management, the area examiners look at first. DORA has applied since January 2025; the EU AI Act's high-risk obligations land in August 2026.

> **One honest note up front.** This playbook helps you build and evidence the technical controls your obligations rest on. The formal sign-off, the legal interpretation and the audit opinion stay with your compliance function and your auditors.

BUSINESS IMPACT

ICT and AI risk is not a cost to defend. It is a position to use.

Security stopped being an IT topic the moment a single outage could move your revenue and your licence at the same time.

The trading floor goes dark

An infrastructure outage takes a broker offline during market hours. The lost order flow does not come back, and the incident report goes to the regulator either way.

The rails close

A breach at a payment firm puts the banking and PSP relationships that carry its volume at risk. The partner's own risk team now has a file open on you.

The deadline becomes a finding

A supervisor that spots a third-party risk gap does not send a warning and move on. It sets a remediation deadline and watches.

There is an upside most firms underuse. Demonstrable ICT maturity is a sales asset. It is the difference between a year-long onboarding with an institutional counterparty and a fast one, and the answer a CISO hands to a partner's due-diligence questionnaire without a three-week scramble. Firms that can **show** their controls, not just describe them, win trust from clients, banking partners and investors, and they win it faster.

THE METHOD

Readiness in five steps

Resilience is not a project the IT team owns in a corner. It is a way of running the company that an examiner, a partner and an investor can all read. These five steps build it in the order that holds up under scrutiny.

1 Put ICT and AI risk on the board agenda

Under DORA, accountability sits with the people who run the firm, and that has to be visible, not implied. Assign ownership, review it on a fixed cadence, and treat it with the same seriousness as liquidity or market risk.

- A named owner for ICT, third-party and AI risk, with authority and budget
- A current ICT asset and third-party register, mapped to the DORA areas examiners review first
- An AI system inventory, each system classified against the EU AI Act categories
- A risk picture ranked by likelihood and financial impact

2 Build the evidence architecture

Good resilience identifies, protects, detects, responds and recovers, and it produces evidence at every step. The goal is an architecture where proof of a control is a by-product of running it, not a document written the week before an audit.

- Detection written as code, versioned and reviewable
- Logging and asset coverage that answers "what did we see, and when"
- Continuity and recovery plans that are current and tested, with defined RTO and RPO
- Reports a non-technical board member and a technical examiner both understand

3 Build awareness and role clarity at the management level

Controls fail at the seams between people. Continuous training keeps the management team and high-exposure functions able to judge a risk and respond to one.

- Regular management briefings on current threats and the obligations that apply
- Awareness programmes for all staff: phishing, credentials, and reporting
- Deeper training for the functions that get targeted: IT, legal and finance
- One accountable person who reports to the board on a schedule

4 Get incident-response ready before you need it

A tested plan is the difference between an incident that costs a bad week and one that costs the relationship. DORA expects ICT incidents to be detected, managed and reported, and the evidence of that process is part of what gets reviewed.

- An incident-response plan, tested with tabletop exercises
- A reporting workflow aligned to DORA, with timeline and ownership decided in advance
- Crisis communication paths defined ahead of time: internal, clients, partners, authorities
- External response and forensics contracted before an incident, not during one

5 Monitor continuously and adapt

Threats and rules both keep moving, so the strategy is reviewed and adjusted, not set once.

- 24/7 detection or managed detection and response, tuned to your environment
- Regular vulnerability scanning and review, with priorities that shift
- Continuous monitoring of third-party ICT risk, not a once-a-year questionnaire
- A clear way to absorb new obligations: EU AI Act, MiCA, NIS-2

THE REGULATORY FLOOR

The obligations you have to address now

Across the EU, the rules that govern ICT and AI risk in financial services have hardened. They reach the value of the firm and the personal exposure of its leadership.

DORA

Applies since January 2025. Requires ICT risk management, third-party risk management, incident detection and reporting, and resilience testing. Accountability rests with the management body.

EU AI Act

Binding obligations for high-risk systems from August 2026: risk management, documentation, logging, human oversight. Credit, fraud and certain profiling use cases fall into scope.

MiCA

Governs crypto-asset service providers, with authorisation and operational requirements now in force.

GDPR & NIS-2

GDPR continues to govern personal data, including breach-notification duties. NIS-2 raises baseline cybersecurity and reporting duties for a wider set of entities.

> **The honest line.** These rules are the requirement. We build the technical controls and the evidence your compliance rests on. Your compliance function, your DPO and your auditors own the interpretation and the sign-off.

WHAT IS AT STAKE

The cost of getting it wrong

Financial penalties

GDPR up to €20M or 4% of global turnover. EU AI Act up to €35M or 7% for the most serious breaches. NIS-2 sets substantial penalties for essential entities; DORA empowers supervisors to act.

Supervisory measures

Reviews, audits, and in the extreme, restrictions on the business.

Reputational cost

A public finding erodes trust and shows up in valuations and lost partnerships.

Personal liability

Where leadership fails to implement required measures, the exposure reaches the management body, not just the budget.

Getting the controls right early protects you from sanctions and, just as usefully, builds trust with the partners and investors who ask to see them. The next two pages give you a way to measure where you stand today.

SELF-ASSESSMENT

The readiness traffic light

One rule: no "yes" counts without evidence. Only answers you can back with a document, a report, a configuration or a test result score a point.

1. A complete, current ICT asset and third-party (ICT TPRM) register, mapped to the DORA areas examiners review first.
   EVIDENCE — REGISTER + LAST REVIEW DATE

2. An incident-response plan that has actually been tested, with a reporting workflow aligned to DORA.
   EVIDENCE — PLAN + LAST EXERCISE PROTOCOL

3. 24/7 detection (security operations or MDR) is active, with documented detection logic.
   EVIDENCE — CONTRACT/SLA OR RUNBOOK + DETECTION-AS-CODE REPO

4. An inventory and risk classification of your AI systems against the EU AI Act categories.
   EVIDENCE — AI INVENTORY + CLASSIFICATION

5. A penetration test or threat-led test in the last 12 months.
   EVIDENCE — FULL REPORT INCLUDING FINDINGS

6. MFA in place, with automated joiner/mover/leaver identity lifecycle, across critical systems.
   EVIDENCE — IAM CONFIGURATION OR AUDIT REPORT

7	Network segmentation isolating critical trading and payment systems.	EVIDENCE — ARCHITECTURE DIAGRAM
8	Backup and recovery tested in the last 12 months, against defined RTO and RPO.	EVIDENCE — TEST PROTOCOL WITH RTO/RPO
9	Continuous, prioritised vulnerability management.	EVIDENCE — PROCESS + RECENT SCAN
10	ICT and AI risk reported to the management body on a regular cadence.	EVIDENCE — BOARD MINUTES OR QUARTERLY REPORT

How to read your score

- **Red · under 6** — critical exposure. Act now, before a deadline or incident sets the timing for you.
- **Yellow · 6 to 8** — real gaps, but addressable. Prioritise and close them over the next one to two quarters.
- **Green · 9 to 10** — strong, low exposure. Keep evidence current and the cadence running.

If you scored Red or Yellow on questions that map to a deadline you are already inside, those are the ones to fix first. The next page shows how.

FROM SCORE TO PLAN

The roadmap to readiness

A score tells you where you stand. A roadmap turns it into a plan with a budget and a sequence, so ICT and AI resilience becomes a controllable part of strategy rather than a recurring fire drill.

TYPICAL ENTRY POINT

AI Readiness Audit Sprint — €8,000, two weeks

Fully credited toward the implementation if you proceed. You get the score, the gaps and a sequenced plan, with no obligation to continue.

01 · ASSESS

A full review of where your controls actually are, with evidence, not assertions.

02 · REPORT

A standardised maturity picture and a prioritised set of next steps.

03 · PLAN

Measures and ownership agreed together, with cost laid out so it is plannable.

04 · ALIGN

A working session with your decision team, so the plan is owned inside the firm.

From there, engagements scale with scope, from a focused control build-out for a single high-priority gap through to full security-operations and identity programmes. Every step is framed as an implementation roadmap with clear cost and measurable indicators, not as a compliance opinion.

YOUR PARTNER

AI-native security operations, built in production

WingsGRC is a team of senior security engineers who have built, run and defended systems in one of the most demanding environments there is: online trading, where large sums move in real time and exposure never sleeps.

Security operations with an AI reasoning layer, built for the volume and speed of regulated fintech.

Identity, access and zero-trust automation across your access stack.

The detection, logging and evidence architecture your obligations depend on.

Incident-response readiness and the technical reporting evidence DORA expects.

Book a readiness session

We engineer the security, identity and detection systems whose continuous outputs map to DORA, GDPR and EU AI Act evidence requirements. Audit attestation remains with your compliance and audit partners.

SOURCES

References

- IBM. **Cost of a Data Breach Report 2025.** Financial-services average $5.56M; global average $4.44M.
- Deloitte. **DORA European Survey 2025.** 92% not fully compliant on resilience testing & third-party risk; 8% fully compliant on TPRM; 25% confident overall.
- ENISA. **Threat landscape for the financial sector.**
- European Supervisory Authorities (EBA, ESMA, EIOPA). **DORA regulatory and implementing technical standards.**
- Regulation (EU) 2022/2554 (DORA), official text.
- Regulation (EU) 2024/1689 (EU AI Act), official text.
- Regulation (EU) 2023/1114 (MiCA), official text.
- Regulation (EU) 2016/679 (GDPR), official text.