THE ECB CYBER-DIRECTIVE MATURITY GUIDE

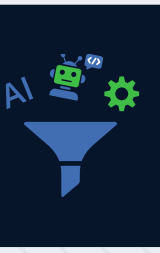
Frontier AI models can now find and exploit vulnerabilities faster than any human-paced process can respond to, a risk that now threatens the resilience of European banks. The European Central Bank (ECB) requires every significant euro area bank to submit a concrete action plan addressing these threats.

Our Maturity Guide walks you through the six focus areas an ECB plan will be measured against, and the questions your Joint Supervisory Team (JST) is likely to ask. It also includes a preparation path to help you assess where you stand today. Positioning your bank honestly is the fastest way to assess the current and target state sections of your plan.

Every bank's action plan will be read against a set of concrete supervisory questions. Three of them warrant an especially rehearsed answer. Each one carries an evidence expectation attached to it.

Three Questions Your Joint Supervisory Team Will Ask

How quickly can you determine whether a new vulnerability materially affects your bank?



How do you prevent risky or untrusted software, including AI models, MCP servers, and agent skills, from entering production?

How fast can you remediate an exposed component and produce a proven record of the fix?

The ECB's Six Focus Areas at a Glance

1. PRIORITIZE PROTECTION OF ATTACK SURFACES

Full inventory of ICT assets, third-party and open-source components, with internet-facing systems monitored first.

2. ACCELERATE VULNERABILITY AND PATCH MANAGEMENT AT SCALE

Prioritized scanning and near real-time, risk-based change management.

3. ENHANCE AI-ENABLED MONITORING AND DETECTION

Detection and logging that match the speed of AI-driven attacks.

4. STRENGTHEN GOVERNANCE AND SUPPLY CHAIN ASSURANCE

Budget, staffing, and third-party readiness that match the risk, including AI models, MCP servers, and agent skills.

5. REINFORCE DEFENSE IN DEPTH AND MODERNIZE INFRASTRUCTURE

Zero trust, security by design, retirement of legacy technology.

6. IMPROVE OPERATIONAL RESILIENCE AND INFORMATION SHARING

Crisis management, recovery testing, cross-institution intelligence sharing.

Addressing these six areas is the foundation. What strengthens a submission further is identifying how mature each area is today and acting now to close the distance to the next level, and that’s exactly what the preparation path below is built to show you.

Where Does Your Bank Stand? A Preparation Path in Five Levels

Under the ECB directive, cyber resilience is a maturity progression, not a checklist. Five capabilities compound on each other, and positioning your bank honestly on this ladder is the fastest way to write the current and target state sections of your plan.

Level 1. Visibility: Know exactly what software you run.

Frontier AI reduces the value of any inventory that is incomplete or refreshed only on a periodic schedule. Prepare a comprehensive component inventory covering applications, containers, binaries, cloud workloads, and every AI model, MCP server, and agent skill in production, with SBOM coverage across open source and third-party dependencies and every asset mapped to a critical business service.

✅ *Measure: percent of production software with known component provenance.*

Level 2. Context: Know what actually matters.

Move beyond prioritization based on CVSS alone to contextual risk: applicability, exploitability, reachability, asset criticality, internet exposure, runtime context, and active exploitation. The target is to resolve a vulnerability disclosure to a bounded set of materially affected production instances within hours, not weeks.

✅ *Measure: time required to identify materially affected assets.*

Level 3. Control: Reduce risk before vulnerable software reaches production.

Finding vulnerabilities faster is insufficient if risky software keeps entering the environment. Strengthen controls at the supply chain entry point: trusted repositories, curated open source, automated policy gates, secure-by-design development, verifiable build and release processes, and governed exceptions. Treat AI models, MCP servers, and agent skills as first-class components inside this control plane.

✅ *Measure: percent of risky components stopped before production.*

Level 4. Response Velocity: Compress the threat exposure window.

Traditional patching follows Discover, Ticket, Prioritize, CAB, Patch Window, Deploy. Frontier AI compresses the attacker side, so the defender side must compress too, without destabilizing production. Prepare an emergency change path with automated rebuild, test, and release, and track Mean Time to Applicability and Mean Time to Remediation as first-class KPIs alongside patch capacity and legacy system constraints.

✅ *Measure: time from material vulnerability disclosure to trusted remediation.*

Level 5. Resilience: Respond at machine speed while preserving trust, governance, and evidence.

For a regulated bank, speed alone is not resilience. Actions taken at machine speed must remain policy controlled, auditable, and demonstrably compliant. Evidence must connect what was affected to the policy decision, to the artifact and its provenance, to testing and approval, to what was deployed, and to whether the resulting state complies with policy.

✅ *Measure: percent of critical remediation actions with verifiable provenance, policy decision, approval, deployment traceability, and machine-readable compliance evidence.*

How JFrog Can Help

Meeting the ECB directive at machine speed comes down to five capabilities working together across the software supply chain:

- A single governed system of record for every binary, with full lineage
- Security embedded in every lifecycle stage, from prevention to signed release evidence
- Governance of AI models, MCP servers, and agent skills as first-class components
- Reachability validation that suppresses roughly 90% of CVEs as not applicable
- Remediation automation that keeps humans on the loop, rather than in it

JFrog delivers all five, and was named a Leader in the inaugural Gartner® Magic Quadrant™ for Software Supply Chain Security, positioned highest for Ability to Execute. That trust runs deep across the industry, with **83% of Fortune 100 companies relying on JFrog.**

Ready to See Where You Stand?

Reach out for a tailored evaluation of your environment and a readiness plan that carries you into your submission to the Joint Supervisory Team and beyond, so you're ready to keep pace with frontier AI and protect your bank and your customers. **Contact us.**