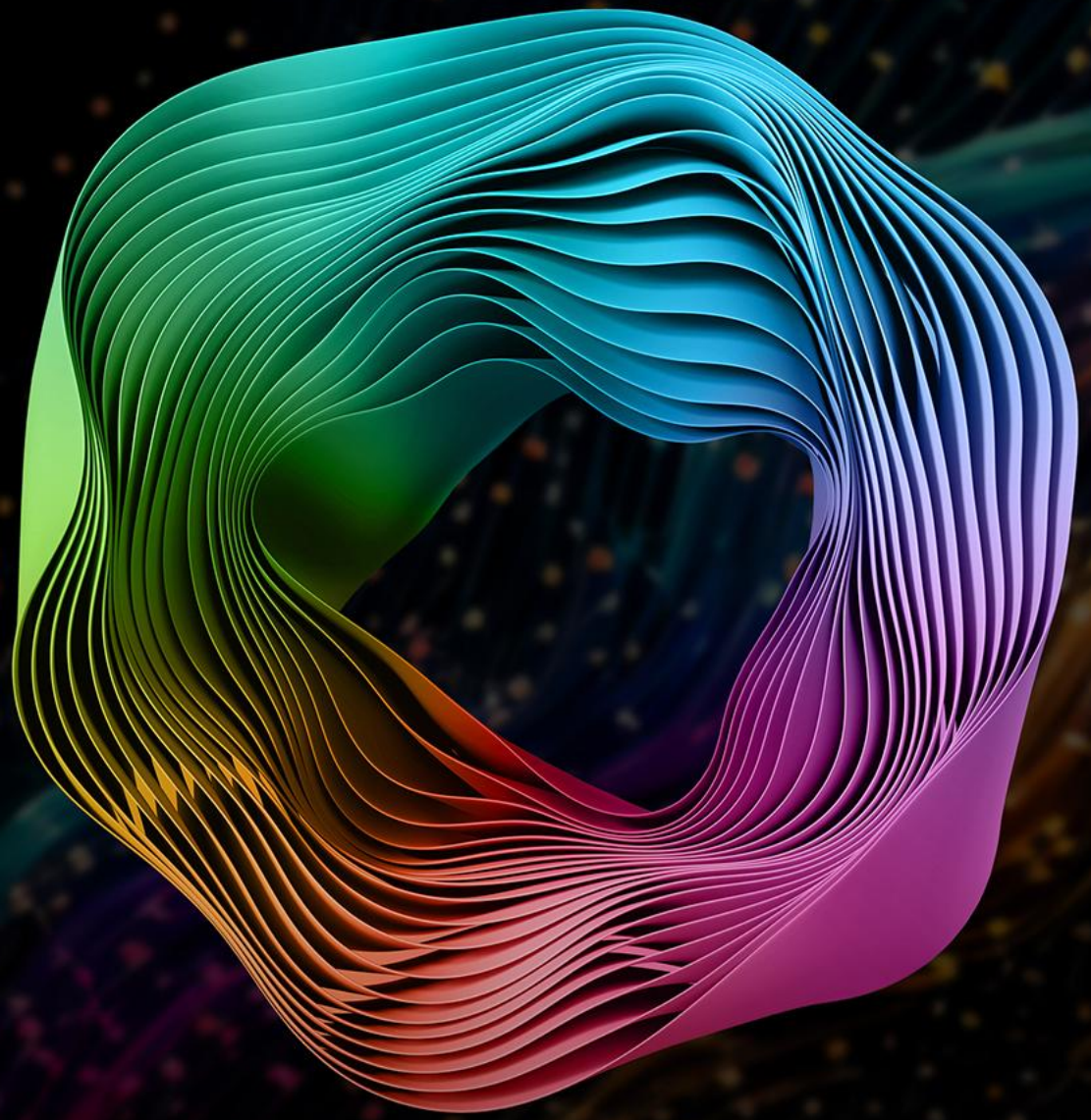
Deloitte.



AI enabled cybersecurity threats - Board briefing

MAKING AN IMPACT THAT MATTERS since 1845

AI enabled cyber risk is now a Board issue

AI-enabled cyber threats have become a strategic supervisory priority, requiring stronger Board oversight, governance and operational resilience.

CONTEXT

AI-enabled cyber risk is now a Board-level supervisory priority

AI can accelerate both vulnerability discovery and exploit generation. For banks, this compresses the response window and increases the materiality of unresolved cyber weaknesses.

SCOPE

- **Significant Institutions**
- All ECB supervised **significant banks**
- **Board and senior management oversight**
- Internal and third-party ICT environments

Management message:
Cyber resilience is a Board decision topic.

THREAT LANDSCAPE

AI does not create entirely new risks. It accelerates existing ones.

AI accelerated vulnerability discovery
Tools identify weaknesses and generate exploits faster.

Reduced time to attack
Banks have less time to assess, prioritise and patch.

Internet facing asset exposure
Cloud, perimeter and VPN assets face higher pressure.

Patch and remediation pressure
Higher volume patching requires more capacity and governance.

Third party and supply chain risk
Provider readiness and open-source exposure become critical.

AI governance and oversight gap
AI-driven risk acceleration may outpace governance, risk appetite, oversight and control frameworks.

Board takeaway: unresolved weaknesses become more material and supervisory-relevant.

31 October 2026: Action Plan Submission Deadline

The Board should understand this as a formal supervisory deliverable, not only a risk awareness message.

DEADLINE

31 OCTOBER 2026

What must be submitted

- Impact assessment of evolving AI threat landscape
- Comprehensive action plan with concrete measures
- Clear owners, resources and implementation timelines
- Short-term remediation and longer-term structural actions

ECB wording: act without delay

Board-level expectations

ECB focus areas require decisions, accountable owners and visible progress tracking.

#	ECB FOCUS AREA	BOARD ACTION	KEY ACTIVITIES / EVIDENCE
1	Attack surface protection	Prioritise exposed ICT assets	Focus perimeter, internet-facing, cloud, VPN, third-party software, AI-enabled services and OSS.
2	Vulnerability & patching	Accelerate patch management at scale	Scale scanning, prioritisation, Trustworthy AI design and emergency changes.
3	Monitoring & AI defence	Enhance detection capabilities	Strengthen logs, traffic monitoring and AI-enabled defence.
4	Governance & supply chain	Fund capacity and validate providers	Review budgets, RTFs, staffing, supplier readiness, AI governance, risk appetite and oversight frameworks.
5	Resilience & recovery	Prepare for faster, broader incidents	Test crisis management, backup and recovery and response to AI-driven incidents.

Supervisory follow-up: JST review, progress monitoring and ECB horizontal analysis.

Responding to the ECB Letter: How We Can Help

Our support is mapped directly to the exact ECB action-plan request below and the deliverables banks must prepare for JST review.

ASSESS

AI threat impact assessment

Assess impact of the evolving AI threat landscape across ICT assets, open findings, internet-facing exposures, providers and DORA resilience.

How we help: Board-ready gap view

PLAN

Supervisory-ready action plan

Define concrete measures, accountable owners, resources, milestones, governance arrangements, and implementation timelines for 31 October submission.

How we help: ready action plan

REMEDIATE

Short-term control uplift

Prioritise attack surfaces, accelerate vulnerability and patch management, enhance monitoring / AI defence, strengthen AI governance, help design trustworthy AI solutions and verify third-party readiness.

How we help: risk reduction roadmap

STRENGTHEN

Structural resilience measures

Reinforce defence-in-depth and cyber hygiene, modernise legacy tech, and test crisis response, backup, recovery and information sharing.

How we help: sustainable resilience

REQUIREMENT FROM ECB LETTER

"...the ECB is calling on significant institutions to assess the impact of the evolving threat landscape without delay, and to develop a comprehensive action plan outlining concrete measures to strengthen relevant controls, allocating the necessary resources, assigning clear roles and responsibilities, and defining timelines for implementation"

What banks must submit

Impact assessment + comprehensive action plan with concrete measures, resources, owners, and timelines for JST review.

- **Impact** — Assess AI threat landscape
- **Measures** — Concrete control actions
- **Owners** — Roles, resources, funding
- **Timeline** — Implementation milestones
- **Evidence** — JST progress tracking

Damir Vukotić
Partner | Deloitte Central Europe
Strategy, Risk & Transactions
FSI Risk & Regulatory Advisory
dvukotic@deloittece.com
M: +385995249000

Ratko Drča
Director | Deloitte Central Europe
Technology & Transformation
Cyber
rdrca@deloittece.com
M: +385916786091

Deloitte.