

The European Central Bank's (ECB) AI Cyber Warning Explained

What this 2026 supervisory call to action means for banks, their cybersecurity strategies, and the third parties they rely on.



What's *inside*

00	Introduction
----	--------------

01	Breaking Down the ECB's Cyber Risk Warning
----	--

02	AI-Driven Attacks and the Defense Gap
----	---------------------------------------

03	AI's Impact on Third-Party Exposure
----	-------------------------------------

04	Preparing the October 31 JST Action Plan
----	--

05	Building Continuous Cyber Resilience
----	--------------------------------------

06	Conclusion
----	------------

AI is Changing How Banks Operate

AI has gone from a technology financial institutions were cautiously experimenting with to one that is increasingly embedded in how they operate.

Banks are applying AI across IT operations, software development, customer support, legal and document analysis, and the list goes on. On October 1, 2026, European Central Bank (ECB) President Christine Lagarde said that nearly nine out of ten significant euro area banks (specifically the ones the ECB directly supervises) already use generative AI. ECB supervisors describe AI adoption as accelerating, particularly with the rapid emergence of generative and agentic AI. As AI agents begin to operate across systems, they're entering workflows that involve sensitive data and external providers. This creates more ways for AI to interact with a bank's systems and data, expanding its potential exposure to risk. Lagarde also warned that AI is changing how quickly vulnerabilities in financial institutions can be identified and exploited, leaving banks with less time to detect and contain an attack.

AI is changing what banks can do, but it's also changing the technology environments they need to secure. As AI becomes more embedded in banking, questions are emerging about whether existing cybersecurity and third-party risk practices can keep pace. For banks, the stakes are particularly high. They operate within highly interconnected technology ecosystems and face strict security and accountability requirements. While AI is changing how risks emerge, responsibility for managing them remains with the bank.

The ECB has already taken steps to address these concerns. In a July 7, 2026, letter (SSM-2026-0301) to the CEOs of banks it directly supervises, ECB Banking Supervision warned that AI models can identify software vulnerabilities and generate working exploits at unprecedented speed. This could compress the time between a vulnerability being discovered and an attack being launched. The ECB describes this as a long-term shift in the threat landscape and calls on banks to strengthen their existing ICT resilience measures accordingly.

AI is amplifying existing risks and increasing the speed and scale at which they can materialize. Vulnerabilities that remain unresolved could become far more serious as a result. The ECB has asked each significant bank to submit an action plan to its supervisors by October 31, 2026. One short-term priority the ECB names is verifying that third-party risk management is fit for purpose, particularly given the role ICT service providers play in critical supply chains.

The question is whether third-party risk practices can
keep pace with AI.

The ECB is pushing banks to prepare for faster AI-enabled threats

AI is accelerating the speed at which cyber threats can develop, and the ECB is making clear that banks cannot afford to treat this as a problem for later.

On July 7, 2026, European Central Bank Supervisory Board Chair Claudia Buch sent a supervisory letter to the CEOs of the banks the ECB directly supervises, warning of the growing cybersecurity risks linked to increasingly capable artificial intelligence. The letter was published alongside a warning from the European Systemic Risk Board that frontier models could create systemic cyber risks, reinforcing that the issue extends beyond individual institutions to the wider financial system.

The ECB has adjusted its own supervisory calendar to give banks room to respond. The deadline for its annual IT Risk Questionnaire has been extended from September 2026 to February 2027, giving banks' ICT teams more time to prioritize resources on the AI threat environment. Banks are also expected to submit an action plan to their Joint Supervisory Team (JST) by October 31, 2026.

The letter frames that work in terms of pace. It says these developments significantly amplify the speed and scale at which existing risks materialize, and that the increased pace and breadth of cyber threats "underscore the importance of strengthening existing ICT resilience measures and accelerating efforts to mitigate vulnerabilities."

"Emerging AI models are capable of identifying software vulnerabilities and generating functioning exploits at unprecedented speed, compressing the timeline between vulnerability discovery and exploitation."

Claudia Buch, Chair of the ECB Supervisory Board · ECB letter SSM-2026-0301, 7 July 2026

74%

of banks responding to the EBA's spring 2026 risk assessment questionnaire named cyber risk and data security as a key driver of operational risk, down from 82% a year earlier, though still more than any other driver. The EBA also describes AI as "a material risk amplifier."

Source: European Banking Authority, Risk Assessment Report, June 2026.

The ECB will discuss each action plan with the bank and monitor its progress, then compare plans across institutions and share what it finds.

AI is moving faster than security processes were built for

In cybersecurity, the pace at which threats emerge is becoming a challenge in itself. AI is accelerating how quickly threats develop, putting growing pressure on financial institutions to identify and address risks before they outpace their response.

AI can shorten multiple stages of the threat lifecycle, from identifying vulnerabilities to developing new attack techniques.

The result is a mismatch between the speed at which threats can develop and the time organizations have to identify and address them, and the capability behind it is climbing quickly.

"In a simulated 32-step attack, models released at the end of 2025 completed about a third of the steps on average, with the remaining steps proving too difficult for them. The latest models, however, completed every step."

Christine Lagarde, President of the ECB, 1 October 2026, citing independent tests reported by the UK's AI Security Institute and the ESRB

For banks, the challenge is that security measures cannot always move at the same speed. Before a change reaches a critical system, it is risk-assessed and tested so it can be deployed safely. A remediation process can therefore work exactly as designed, but still move too slowly. As AI shortens that window, practices such as periodic patch cycles become harder to rely on.

Days or weeks → minutes or hours

Crafting a weaponized exploit used to take human experts days or weeks. Frontier AI models can now do it in a matter of minutes or hours, which the ESRB calls "a collapse of defensive time buffers."

Source: European Systemic Risk Board, Warning ESRB/2026/3, 25 June 2026.

"Prioritised vulnerability scanning may help institutions cope better with the increasing speed and volume of vulnerability discovery."

ECB letter SSM-2026-0301, Annex 1 · Focus area 2

A bank's security perimeter extends far beyond the systems it directly controls

Banks increasingly operate through a complex web of external technology providers. Cloud infrastructure, SaaS applications, open-source components, and other third parties are embedded across critical operations, creating layers of dependency that can extend several providers deep.

AI is putting new pressure on an already complex ecosystem. As vulnerabilities and threats emerge faster, a bank's risk profile can change through a provider it does not directly manage. Knowing who the vendors are is the starting point, and the harder part is seeing how risk changes across those relationships as it happens.

The ESRB's June 2026 warning makes the same point for the system as a whole. It notes that incidents "may also propagate rapidly across financial institutions and markets if critical third-party providers, shared technological ecosystems, or widely used open source components are affected." An incident that starts outside a bank's own systems can still become the bank's problem.

DORA register

In 2025, the ECB ran its first collection of banks' DORA registers of ICT third-party arrangements. The data confirmed increased reliance on ICT third-party providers, concentration in a small number of them, particularly cloud service providers, and low substitutability.

Source: European Central Bank, Annual Report on supervisory activities 2025, March 2026.

AI also makes traditional vendor assessments age faster. A provider may introduce a new AI tool, integrate a new model, change how data is processed, or become exposed to a newly identified vulnerability between formal reviews. A vendor that met a bank's security requirements at its last review may therefore present a materially different risk profile today.

A more adaptive approach matches the depth of each assessment to the relationship: what the vendor does, what data or systems it can reach, where it uses AI, and the further dependencies that use creates. Pairing targeted questionnaires with continuous monitoring can reduce duplicated documentation and show when a vendor's exposure changes, so teams can see where action is needed most.

Responsibility for third-party risk stays with the bank. Under DORA (Regulation (EU) 2022/2554), a bank that relies on ICT services from third parties remains fully responsible for complying with all of its obligations under the regulation and applicable financial services law, and it has to manage ICT third-party risk as an integral component of ICT risk within its ICT risk management framework. The ECB's letter also points to understanding whether third-party ICT providers are prepared for accelerated vulnerability disclosure and patching.

As attack timelines shrink, a provider's ability to respond becomes part of the bank's own resilience. Panorays maps a bank's third parties and the providers behind them, and tailors each assessment to what the relationship involves.

The ECB wants banks to show how their cyber strategy will keep pace

By October 31, 2026, banks directly supervised by the ECB are expected to submit an action plan to their JST addressing the evolving threat landscape. The response does not need to start from scratch. The ECB expects it to build on each bank's existing cyber-risk strategy and to cover both immediate priorities and longer-term resilience.

The letter starts with the attack surface. It asks banks to prioritize protecting internet-facing and externally exposed assets, and it counts third-party software, open-source components, cloud environments and VPN connections to third parties as part of that attack surface.

"Minimisation and continuous monitoring of all internet-facing and externally exposed assets, including cloud environments, and other VPN connections to third parties, remain important elements of an effective defensive posture."

ECB letter SSM-2026-0301, Annex 1 · Focus area 1

On patching, the ECB says preparing for more frequent, higher-volume updates may become increasingly important as vendors and open-source communities fix vulnerabilities faster, and it points to prioritized vulnerability scanning as one way to cope with the volume. It also describes change management that allows rapid, risk-based remediation while maintaining operational stability, so that emergency changes, critical fixes, internet-facing systems, and critical internal systems can be prioritized.

Those arrangements extend into the supply chain, since Annex 1 says they should also be reflected in contractual terms and service level agreements when an ICT service provider is involved. When a provider sits between a vulnerability and its fix, its patch speed sets the bank's.

76%

of financial services organizations plan to increase their cyber budgets in 2026, with AI as their top priority. Yet only 24% are spending significantly more on proactive than on reactive security measures.

Source: PwC, Global Digital Trust Insights 2026, Cybersecurity outlook: Financial services.

The letter also points to stronger monitoring of application and access logs, network traffic, and other signs of attempted attack or compromise. It adds that AI-native and AI-assisted defensive tools can help institutions keep pace with AI-enabled threats, provided they are deployed with appropriate governance, validation and human oversight. Annex 1 says management bodies should assess whether ICT budgets, staffing, tooling and change capacity are sufficient, and that risk appetite frameworks should be reviewed to include metrics and tolerance thresholds, including those tied to more frequent patching. Over the longer term, it points to replacing or updating legacy systems and strengthening response and recovery planning.

Frank Elderson, Vice-Chair of the ECB Supervisory Board, previewed the letter in early June. He described AI-enabled threats as a firm-wide strategic challenge, with management bodies taking clear ownership and multi-year investment in people, systems and governance. He also warned that the critical infrastructure banks depend on, including cloud providers, telecommunications networks, payment systems, and electricity and water supplies, could become targets.

"Scenarios that were once considered tail risks may become more likely."

Frank Elderson, Vice-Chair of the ECB Supervisory Board · Reuters, 3 June 2026

The October deadline is a test of whether banks can turn awareness of AI-related cyber risks into a strategy that keeps pace. It starts with visibility: knowing where exposure sits and which third parties could affect operations helps security teams decide where action is most urgent. Panorays continuously monitors vendors' external attack surfaces and flags cyber events that involve them, so a provider's new exposure shows up when it happens.

Annual vendor reviews struggle when risk can change every day

For security teams, the challenge goes beyond where a third party's risk stands today to knowing when it has changed. That makes third-party risk a continuous question, one that stays open between reviews. The sooner teams can see those changes, the more time they have to respond before exposure becomes a broader resilience issue.

As banks rely on outside vendors to support critical operations, third-party risk becomes harder to isolate. A supplier can change its infrastructure, connect new AI tools or agents, expand access to sensitive systems, or become exposed to a new vulnerability between reviews.

That is pushing security teams toward continuous visibility into third-party risk, so a change in a vendor's posture surfaces when it happens. Monitoring a vendor's external-facing assets for new vulnerabilities is one input, alongside changes in what the vendor does, the data and systems it can reach, and where it uses AI. Together they show how a vendor's exposure is changing over time.

"Institutions remain exposed to, and fully accountable for, risks stemming from outsourced ICT services."

ECB letter SSM-2026-0301, Annex 1 · Focus area 4

Third-party risk keeps changing long after a vendor clears review, and it is becoming a management-level resilience issue. The ECB's letter reinforces that shift by listing third-party risk management among its short-term priorities. Panorays gives teams continuous visibility into third-party risk, combining assessments that reflect each vendor relationship with ongoing monitoring of external exposure, so changes surface between formal reviews.

The October Deadline is Only the First Step

The ECB's 2026 letter puts cybersecurity and third-party risk on the same short-term agenda, with patch management and supply chain assurance in a single action plan.

Financial institutions operate across interconnected technology environments, where weaknesses in vendors, service providers, and supporting infrastructure can become operational risks. No institution can predict every disruption or cyber incident, but it can strengthen the conditions that determine how well it responds. In practice, that comes down to visibility across third parties and the critical dependencies behind them, and to continuous monitoring of how AI-related threats are emerging across the wider technology ecosystem.

Continuous monitoring gives organizations a more accurate, up-to-date view of the vulnerabilities and exposures across their environment. It keeps risk management active, helping institutions identify changes earlier, respond more effectively to disruption, maintain critical operations, and demonstrate stronger resilience to supervisors and boards.

The October 31 deadline is an important milestone. The larger challenge is a third-party risk program that keeps assessing and monitoring AI-related risk as technology and regulatory expectations continue to evolve.

Every figure and quotation, *at its source*

- **European Central Bank** · Letter SSM-2026-0301, "Addressing AI-enabled cybersecurity threats", 7 July 2026, including Annex 1. Quotation from Supervisory Board Chair Claudia Buch, the 31 October 2026 action-plan deadline, the IT Risk Questionnaire deadline extended to February 2027, and the focus areas described in Sections 2 to 5.
- **European Systemic Risk Board** · Warning ESRB/2026/3 on systemic cyber risks stemming from frontier artificial intelligence models, 25 June 2026, published 7 July 2026.
- **European Central Bank** · Christine Lagarde, "Where AI risks meet", welcome address at the tenth annual conference of the ESRB, 1 October 2026. Generative AI use among significant euro area banks, and the AI Security Institute and ESRB test results she cites.
- **European Central Bank** · Pedro Machado, "Technology is neutral, governance is not: AI adoption in the banking sector", keynote speech at the KPMG RiskTech Conference, 24 February 2026. AI adoption trends and generative AI use cases in banks.
- **European Central Bank** · Annual Report on supervisory activities 2025, March 2026. First collection of DORA registers of information on ICT third-party arrangements.
- **European Banking Authority** · Risk Assessment Report, June 2026. Cyber risk and data security as a driver of operational risk (74% agreement), and AI as a material risk amplifier.
- **Reuters** · "ECB to ask banks for targeted measures to counter AI risk", 3 June 2026. Remarks by Frank Elderson, Vice-Chair of the ECB Supervisory Board.
- **European Central Bank** · Frank Elderson, "Strengthening operational resilience for the age of AI", keynote speech at the Goldman Sachs European Financials Conference 2026, Zurich, 3 June 2026.
- **PwC** · Global Digital Trust Insights 2026, Cybersecurity outlook: Financial services, February 2026.
- **DORA** · Regulation (EU) 2022/2554 on digital operational resilience for the financial sector.

FROM ACTION PLAN TO ACTION

Know where your exposure is changing, and *where to act first*

Panorays gives banks continuous visibility into third-party risk across their vendor ecosystem, so security teams can see where a vendor's risk is changing and where action is needed most.

[See what Panorays can uncover](#)[Talk to our team](#)