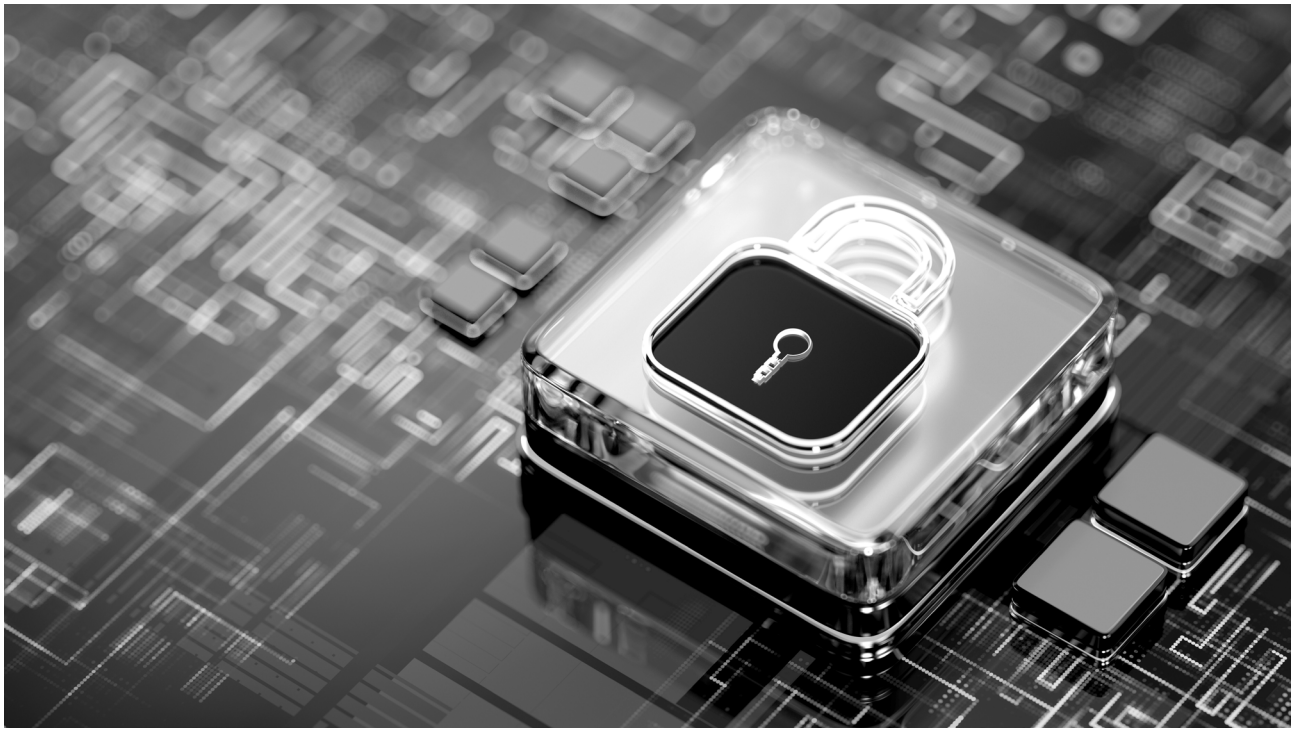
A&O SHEARMAN



# ECB requires significant institutions to address AI-enabled cybersecurity threats

CLIENT BRIEFING

**JULY 2026**

# Key Aspects

On 7 July 2026, Claudia Buch, Chair of the European Central Bank's (**ECB**) Supervisory Board, addressed a letter to the CEOs of all significant institutions (**SIs**) supervised under the Single Supervisory Mechanism (**SSM**), calling for immediate and proactive measures to address the escalating cybersecurity threats enabled by frontier artificial intelligence (**AI**) models. The letter, published simultaneously with a warning from the European Systemic Risk Board (**ESRB**) on systemic cyber risks stemming from frontier AI models, marks a material escalation of supervisory expectations regarding information and communication technology (**ICT**) resilience and cyber risk management. Significant institutions are required to submit a comprehensive action plan to their Joint Supervisory Team (**JST**) by 31 October 2026. While the letter is addressed exclusively to SIs, similar requirements are widely anticipated to follow for less significant institutions supervised by national competent authorities (NCAs), including the German Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht*; **Bafin**).

## AI REGULATION AND CYBERSECURITY: AN ACCELERATING SUPERVISORY FOCUS

The regulatory focus on AI-related cybersecurity risks for financial institutions has intensified markedly in recent months, driven by rapid advances in the capabilities of frontier AI models – the most advanced versions of general-purpose AI. The emergence of highly capable new models (including Anthropic's Claude Mythos model) has marked a step change in the speed and sophistication of AI-enabled threat vectors, compressing the timeline between vulnerability discovery and exploitation and enabling adversaries to operate at unprecedented scale. Multiple supervisory authorities across jurisdictions have identified these developments as a material driver of heightened cyber risk for financial institutions, triggering a wave of coordinated regulatory responses of which the ECB's letter is the most direct expression within European banking supervision to date. Bafin has also significantly raised its supervisory focus on cybersecurity (as highlighted in our May 2026 client briefing on Bafin's reinforcement of its supervisory activities in the anti-financial crime and cyber areas) and the authority has issued warnings regarding AI-enabled threats and has allocated additional supervisory resources to cyber risk oversight. The ECB's latest action, requiring SIs to develop and submit a comprehensive cybersecurity action plan within months, represents a logical and anticipated supervisory response to the evolving threat landscape, and it is reasonable to expect that Bafin and other EU NCAs will issue comparable obligations for the banks and other institutions they directly supervise in the near to medium term.

## THE ECB'S LETTER OF 7 JULY 2026: BACKGROUND AND CORE MESSAGE

The ECB's letter identifies rapid advancements in AI systems as a "pivotal change" to the cybersecurity landscape. Emerging AI models are capable of identifying software vulnerabilities and generating "functioning exploits" (i.e., code which exploits a vulnerability) at unprecedented speed, compressing the timeline between vulnerability discovery and exploitation. The ECB stresses that this is a long-term structural shift in the threat landscape, not a temporary phenomenon or a risk tied to any single tool or model, and that, while these developments do not introduce entirely new risk categories, they significantly increase the speed and scale at which existing risks materialise. Responsibility for responding to this evolving environment lies primarily with banks' management board (for German purposes, in line with the general prudential requirements under Section 25a and 25c of the German Banking Act (*Kreditwesengesetz*)) and requirements under Regulation (EU) 2022/2554 (*Digital Operational Resilience Act*; **DORA**), which are expected to revisit strategic ICT decisions, resource allocation and risk tolerance frameworks where necessary.

The letter further underscores the continued relevance of DORA and calls on institutions to address, without delay, any open supervisory findings related to ICT and security risks identified in previous activities, including on-site inspections, targeted reviews and the 2024 cyber-resilience stress test. Last month, the European Supervisory

Authorities (**ESAs**) published a report on major ICT-related incidents under DORA, which found a relatively low number of cybersecurity-related incidents suggesting systems were currently working well. Nevertheless, the ESAs urged firms to maintain high cybersecurity standards to keep pace with the potential threat from highly capable AI-driven tools – a position they reiterated yesterday in response to the ESRB's warning. Similarly, Bafin has repeatedly highlighted the escalating cyber risks facing banks in connection with new and highly capable frontier AI models, noting that tools such as Anthropic's Claude Mythos, OpenAI's GPT-5.5, and Microsoft's MDASH can discover and exploit vulnerabilities at unprecedented speed and scale, potentially threatening the stability of individual financial institutions and the financial system as a whole.

## ECB EXPECTATIONS AND ACTION PLAN REQUIREMENTS

Each SI's comprehensive cyber resilience action plan should outline concrete measures to strengthen relevant controls, allocate necessary resources, assign clear roles and responsibilities, and define implementation timelines. The ECB will conduct a horizontal analysis of the plans and share conclusions with SIs:

In this context, the following is worth noting:

- In the short term, three priority areas are identified: (i) accelerating vulnerability and patch management at scale; (ii) enhancing monitoring, detection and AI-enabled defensive capabilities; and (iii) verifying that third-party risk management is fit for purpose given the critical role of ICT service providers in supply chains.
- Over the longer term, structural measures should include reinforcing defence-in-depth and modernising infrastructure, in particular by replacing or updating legacy technologies, and improving operational resilience through crisis management, recovery mechanisms and information-sharing arrangements.

To enable institutions to focus resources on these priorities, the ECB will extend the deadline for the annual IT Risk Questionnaire from September 2026 to February 2027. More specifically, the ECB's letter requests that SIs' action plans address the following six focus areas, with separate objectives for the short and medium term:

In the short term:

- **Prioritise protection of attack surfaces:** Identify and monitor all ICT assets (including third-party software and open-source components), minimise internet-facing and externally exposed assets (including cloud environments), and prioritise perimeter technologies in remediation efforts.
- **Accelerate vulnerability and patch management at scale:** Conduct prioritised vulnerability scanning, prepare for more frequent and higher-volume patching cycles, and ensure that ICT change management arrangements support rapid, risk-based remediation — including through appropriate contractual terms with ICT service providers.
- **Enhance monitoring, detection and AI-enabled defensive capabilities:** Strengthen monitoring of application and access logs, network traffic and indicators of compromise, with a focus on internet-facing applications, cloud repositories and critical internal systems. AI-based defensive tools may be used where preceded by appropriate risk assessment and human oversight.
- **Strengthen governance, training and supply chain assurance:** Management bodies should assess the adequacy of ICT budgeting, staffing, tooling and change capacity. Training and awareness measures should be risk-commensurate and adjusted to the evolving threat landscape. Institutions remain fully accountable for risks stemming from outsourced ICT services and should maintain adequate supply chain assurance.

In the medium term:

- **Reinforce defence-in-depth and modernise infrastructure:** Apply segmentation and zero-trust principles, maintain strong baseline controls (including multi-factor authentication, least-privilege access and comprehensive logging), and replace or update legacy, unsupported or end-of-life ICT systems. AI-native and AI-assisted defensive tools should be deployed with appropriate governance and human oversight.
- **Improve operational resilience, crisis management and information-sharing:** Maintain robust and regularly tested incident response, backup, failover and recovery arrangements aligned with DORA. Conduct exercises covering high-speed, high-volume attack scenarios and supply chain or cloud service

disruption. Participate in secure information-sharing frameworks for exchanging threat intelligence and defensive strategies across the sector.

The detailed focus areas set out in Annex 1 to the ECB's letter are provided as an Annex to this briefing.

## IMPLICATIONS FOR BANKS

For SIs, compliance with the letter is an immediate priority. The **31 October 2026 deadline for submitting a comprehensive action plan** is fast approaching, and institutions should begin their gap assessment and remediation planning without delay. The requirements build on the existing DORA framework and reinforce the expectation that ICT governance, vulnerability management and third-party risk arrangements are not merely compliant on paper, but substantively effective in practice. Institutions with open supervisory findings in ICT-related areas should treat closure of those findings as particularly urgent in light of the ECB's explicit call to that effect. A range of further requirements will also need to be considered from a broader prudential perspective, including the intersection of AI deployment with data protection and operational resilience obligations.

For non-SIs (i.e., "Bafin-supervised" institutions), which fall outside the direct scope of the ECB's letter, the developments are nonetheless a clear signal. Supervisory expectations regarding cyber and AI risks are converging across European regulators. As highlighted in our May 2026 Client Briefing on Bafin's reinforcement of its anti-financial crime and cyber supervision, Bafin has already devoted significant additional resources to cyber risk oversight and has issued warnings regarding AI-enabled threats.

That said, in our view the ECB's letter forms part of a broader European regulatory trajectory in relation to AI, and in particular to AI-related cyber risks. Relevant workstreams and legal aspects include, by way of example, prudential requirements, outsourcing rules, DORA, cybersecurity requirements under the AI Act (Regulation (EU) 2024/1689), requirements for data security under the General Data Protection Regulation (GDPR, Regulation (EU) 2016/679, including GDPR requirements for deploying AI-enabled defensive tools), the CERT-EU Threat Landscape Report 2025 and the European Commission's Action Plan on Cybersecurity and AI. Beyond these immediate priorities, medium-term resilience planning should also account for emerging challenges such as post-quantum cryptography, which the ECB has signaled it will address in the future. The ECB's letter, while primarily directed at ICT resilience and cyber risk, further raises a number of issues that sit at the intersection of cybersecurity, data protection under the GDPR and emerging AI regulation.

We recommend that all institutions, not just SIs, undertake the following actions as set out in more detail in the Annex:

1. A **targeted gap analysis** of their cyber resilience posture, benchmarked against both the supervisory expectations outlined above (mapping existing ICT resilience measures, vulnerability management processes and third-party arrangements against each of the six focus areas set out below and in Annex 1 to the ECB's letter) and other applicable regulatory requirements in a wider sense.
2. **ICT budget.** The ECB expects management bodies to evaluate whether current ICT budgeting, staffing, tooling and change capacity are sufficient to support.
3. **Evaluate AI tool governance.** Where institutions are deploying or considering AI-enabled defensive tools, ensure that deployment is preceded by a thorough risk assessment covering both the cybersecurity benefits and any associated data protection, EU AI Act compliance and model risk considerations. Establish appropriate human oversight mechanisms and document the governance framework.
4. **Begin post-quantum cryptography planning.** Although the ECB will address this in a separate communication, it has signaled that the adoption of post-quantum cryptography must start now. Institutions should begin scoping the impact on their cryptographic estate and develop a roadmap for transition.

Please feel free to contact us to discuss what these developments mean for your institution, or how we can assist with the development of a tailored action plan or a preparatory health check.

# Annex
# ECB Focus Areas – Summary (ECB Letter of 7 July 2026, Annex 1)

**Details on relevant focus areas to prepare for increasing AI-enabled cybersecurity threats**

As mentioned above, the requested action plan should address short and long-term areas. The requested action plan should provide information on the following focus areas (specific actions for each area are provided for consideration):

In the short term:

a) Prioritise the protection of potential attack surfaces

- Identification of ICT assets, including third-party software and open-source components, is key to prioritising remediation efforts.
- 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.
- Prioritising perimeter technologies in the remediation efforts helps safeguard the most exposed assets, and can be followed by cloud and on-premises environments, with a particular focus on ICT critical internal systems and ICT security infrastructure.
- In remediation planning, it is beneficial to take into account the fact that threat vectors may originate not only from external networks but also from internal sources.

b) Accelerate vulnerability and patch management at scale

- Prioritised vulnerability scanning may help institutions cope better with the increasing speed and volume of vulnerability discovery. Where appropriate, this approach could be complemented by the use of AI-based tools, provided that their deployment is preceded by a thorough assessment of both their potential benefits and associated risks, and remains subject to adequate safeguards, human oversight and robust risk management.
- Preparation for more frequent and higher-volume patching may become increasingly important as vendors and open-source communities - as well as internally developed software - identify and remediate vulnerabilities faster, requiring ICT functions to be adequately staffed.
- ICT change management arrangements that enable rapid, risk-based remediation while maintaining operational stability can support the effective prioritisation of emergency changes, critical fixes, internet-facing systems and critical internal systems. These should also be reflected in contractual terms and service level agreements when an ICT service provider is involved.

c) Enhance monitoring, detection and AI-enabled defensive capabilities

- Strengthened monitoring of application and access logs, network traffic and other indicators can improve the detection of indicators of compromise and attempted exploitation, especially across internet-facing applications, cloud repositories and critical internal systems.

d) Strengthen governance, funding, awareness training and supply chain assurance

- Management bodies and senior management should assess whether current ICT budgeting, staffing, tooling and change capacity are sufficient to support accelerated patching, infrastructure updates, resilience testing, AI-enabled defence and sector-wide coordination.
- Training and awareness for all employees, customers, counterparties, third parties and other relevant stakeholders should be commensurate to the level of risk, appropriate for individual needs and adjusted to the evolving threat landscape in order to be relevant and useful as a protective tool, including, where relevant, training and awareness for ICT security personnel and members of the ICT lines of defence.
- Institutions remain exposed to, and fully accountable for, risks stemming from outsourced ICT services. Adequate supply chain assurance, including an understanding of third-party ICT service providers' preparedness for accelerated vulnerability disclosure and patching, remains relevant in this context.

Risk appetite frameworks should be reviewed in order to update and/or incorporate metrics, tolerance thresholds and control measures - including those related to increased patch management frequency - consistent with the evolving risk profile stemming both from the internal use of such models and from indirect exposure to them. The management body should actively provide appropriate direction and oversight to ensure the necessary consistency with the institution's strategy and risk management framework.

In addition to these short-term remediation actions, other structural measures can include the following:

e) Reinforce defence-in-depth and cyber hygiene, modernise infrastructure

- A prudent security posture assumes that perimeter defences will be breached, particularly as frontier AI systems increase the speed and scale of vulnerability discovery and exploitation, including potential zero-day exploitation.
- Segmentation and, where feasible, micro-segmentation, together with the adoption of zero-trust principles, including continuous verification of users, devices, applications, application programming interfaces (APIs) and service accounts, can support defence-in-depth.
- Strong baseline controls remain central to effective cyber hygiene. These include accurate asset inventories, secure configuration, robust access controls with least privilege, multi-factor authentication and comprehensive logging.
- Software development practices based on security-by-design, with appropriate consideration of secure code alongside delivery timelines, can reduce vulnerabilities before deployment.
- 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.
- Given the increased vulnerability exposure associated with legacy, unsupported or end-of-life technologies, replacing or updating these ICT systems, or providing comprehensive protection through additional controls where replacement is not feasible, can materially reduce risk.

f) Improve operational resilience (i.e. response and recovery), including crisis management, and information-sharing arrangements

- Robust and regularly tested crisis management, incident response, backup, failover, restoration and recovery arrangements aligned with DORA requirements and best practices for ICT risk management,

incident handling and operational resilience testing are essential in a context of higher probability of ICT-related incidents materialising.

- Exercises covering high-speed, high-volume attack scenarios, broad compromise through zero-day vulnerabilities, ransomware or destructive attacks and supply chain or cloud service disruption can help institutions validate preparedness under more demanding threat conditions.
- Secure frameworks for exchanging sensitive cyber information across institutions, including vulnerabilities, threat intelligence, defensive strategies and remediation approaches, can support collective resilience, leveraging existing trusted information-sharing arrangements.

While the actions outlined above focus on enhancing banks' cybersecurity and operational resilience, institutions could consider whether their broader risk appetite frameworks still adequately reflect the evolving risk landscape and inform decision-making processes related to risk acceptance, including origination policies.

# Key Contacts

## Germany


**Dr Alexander Behrens**
*Partner*

Tel +49 69 2648 5730
Alexander.Behrens@aoshearman.com



**Catharina Glugla**
*Partner*

Tel +49 211 2806 7103
Catharina.Glugla@aoshearman.com



**Niklas Germayer**
*Senior Associate*

Tel +49 69 2648 5973
Niklas.Germayer@aoshearman.com


## United Kingdom


**Chloe Barrowman**
*Senior Knowledge Lawyer*

Tel + 44 20 7655 5136
Chloe.Barrowman@aoshearman.com

# For more information, please contact:

**Frankfurt**

Allen Overy Shearman Sterling LLP
Große Gallusstraße 14
Frankfurt
60315
Deutschland

Tel +49 (0)69 2648 0000

## Global presence

A&O Shearman is an international legal practice with nearly 4,000 lawyers, including some 750 partners, working in 28 countries worldwide. A current list of A&O Shearman offices is available at aoshearman.com/en/global-coverage.

A&O Shearman means Allen Overy Shearman Sterling LLP and/or its affiliated undertakings. Allen Overy Shearman Sterling LLP is a limited liability partnership registered in England and Wales with registered number OC306763. Allen Overy Shearman Sterling (Holdings) Limited is a limited company registered in England and Wales with registered number 07462870. Allen Overy Shearman Sterling LLP (SRA number 401323) and Allen Overy Shearman Sterling (Holdings) Limited (SRA number 557139) are authorised and regulated by the Solicitors Regulation Authority of England and Wales.

The term partner is used to refer to a member of Allen Overy Shearman Sterling LLP or a director of Allen Overy Shearman Sterling (Holdings) Limited or, in either case, an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen Overy Shearman Sterling LLP's affiliated undertakings. A list of the members of Allen Overy Shearman Sterling LLP and of the non-members who are designated as partners, and a list of the directors of Allen Overy Shearman Sterling (Holdings) Limited, is open to inspection at our registered office at One Bishops Square, London E1 6AD.

A&O Shearman was formed on 1 May, 2024 by the combination of Shearman & Sterling LLP and Allen & Overy LLP and their respective affiliates (the legacy firms). This content may include or reflect material generated and matters undertaken by one or more of the legacy firms rather than A&O Shearman.



EUS1: 2006986336.2

aoshearman.com