ASCENDO ANALYTICS

Supervisory Addendum — From Frontier-AI Expectations to Action Authority

How dated supervisory expectations connect to one bounded defensive-action record

8 September 2026

Table of Contents

Purpose

Five European texts published between late June and the end of July 2026 point in the same direction without doing the same legal work. One is a systemic-risk warning, one is a direct supervisory letter to significant institutions, two set wider policy and supervisory expectations, and one is national supervisory guidance. Read together, they make frontier-AI cyber risk harder for a financial institution to leave as an unowned observation.

They do not, however, supply one new universal rule for automating defence. An action plan still has to answer a different question: what may one named defensive action do in production, to which controlled object, under whose authority, with what recovery path and with what consequence owner? This addendum connects that supervisory demand to the decision method in *Autonomous Defensive Action: How Buyers Decide Action Authority and Accountability*.

What arrived

Date and instrument	Direct applicability	What it asks for
25 June / 7 July — ESRB Warning ESRB/2026/3	Addressed directly to European and national authorities; it is not a firm-level action-plan instruction.	Monitor and reassess systemic cyber risk from frontier AI models, which the ESRB assessed as severe.
7 July — ECB Banking Supervision letter	Addressed directly to CEOs of significant institutions under ECB direct supervision. The 31 October 2026 submission date belongs to this route.	Assess the changed threat landscape without delay and submit a comprehensive action plan to the Joint Supervisory Team, with concrete measures, necessary resources, clear roles and responsibilities, and implementation timelines; the JST will discuss the plan and monitor progress.
7 July — European Commission Action Plan on Cybersecurity and AI	Union policy programme. The page reviewed for this addendum does not itself establish a firm-specific submission duty.	Improve prevention, preparedness, response and deterrence across the Union, building on the existing legal framework.
22 July — UKNF recommendations	Directed to market entities within the recommendation's stated scope in Poland; the named entity, service, duty and date still require review.	Review exposure and prepare or adjust action plans, including measures, resources, responsibilities and timelines. There is no fixed submission date; adequacy and effectiveness will be examined through ongoing supervision and inspections.
31 July — joint EBA, EIOPA and ESMA statement	Cross-sectoral supervisory statement; it does not itself create a standalone firm-specific submission duty.	Support a risk-based and consistent supervisory response and point firms back to existing governance and ICT-risk requirements and supervisory dialogue; it does not define an action-specific automation boundary.

The source and wording limits behind these summaries are recorded in the accompanying *Evidence Record — Supervisory Addendum*. That record is part of this addendum, not an optional bibliography.

Which supervisory or national clock reaches you

The 31 October deadline belongs to the ECB letter and therefore to the significant institutions it addresses. It does not automatically become a local legal deadline for every subsidiary or for every institution outside direct ECB supervision. A parent may translate it into a group requirement, but the local entity still needs a named owner, an applicable basis and its own delivery date.

Outside that direct route, the clock depends on the instrument and the duty. In Poland, the amended national cybersecurity act entered into force on 3 April 2026. Existing entities that qualify under its transitional rule have twelve months to implement the Chapter 3 obligations, and existing key entities have twenty-four months to complete the first audit; the registration request follows the ministerial schedule rather than one universal six-month date. For financial entities, DORA may operate as the sector-specific rule for equivalent duties, but it does not erase every NIS2 or national obligation by label alone.

In Czechia, Act 264/2025 Sb. entered into force on 1 November 2025. The reviewed official materials use a sixty-day service-notification clock and a one-year implementation period measured from delivery of the registration decision. The entity, regulated service and delivery event therefore have to be identified before anyone converts those periods into calendar dates.

Other jurisdictions are intentionally omitted from this edition. Their dates and applicability triggers require the same atomic legal record as Poland and Czechia; a signpost without that record would look more useful than it is.

The decision gap inside an action plan

The reviewed texts focus chiefly on how frontier models change the threat and on how institutions and supervisors should respond. None of the five reviewed texts expressly names the defender-side controlled object on which a production action would operate. That is a bounded finding about this declared five-text basket as reviewed on 4 September 2026, not a claim that no law, supervisor or contract addresses the issue anywhere.

The distinction matters. A plan can be fully responsive at programme level and still contain a measure that nobody can safely authorise: “automate containment”, for example, says nothing about the object, trigger, blast radius, approval path or restoration obligation. The report’s four decision questions and nine-field record turn that programme measure into a decision that can be monitored, challenged and reopened.

Mapping the expectation to the record

What the plan needs to show	Where the record supplies it
A concrete measure	Field 1 names the scenario, exposure evidence, controlled object and business service. A capability label is not yet a monitorable measure.
Its authority boundary	Fields 2 and 3 separate investigation, recommendation and production change, then name the trigger, authority grantor, escalation path and technically enforced scope.

What the plan needs to show	Where the record supplies it
Roles and responsibilities	Decision question III identifies the consequence owner; Fields 2 and 7 name the operational, rollback, recovery and restoration-cost owners. The programme-delivery block below separately names the owner of each implementation milestone.
Necessary implementation resources	The programme-delivery block below records people or capacity, funding or budget, dependencies, the confirming owner and any shortfall. Fields 5–7 allocate contractual, insurance, recovery and restoration consequences; they do not replace this resource plan.
An implementation timetable	The milestone table in the programme-delivery block below records implementation start, target completion, dependencies and status. Field 4 does not supply this timetable.
Completion evidence	The completion-evidence table below names the acceptance criterion, evidence artefact, reviewer and completion or sign-off date for each measure or milestone.
Third-party and exit treatment	Fields 5 and 8 record the relevant contractual allocation, governance classification and exit artefacts. Field 8 data may feed a separate DORA register of information; it neither replaces that register nor establishes its completeness or compliance.
Evidence for supervisory follow-up	Field 9 defines the action log and effectiveness measure; the separate completion-evidence table shows delivery against the plan. Annex A of the report defines the provenance, freshness and maximum-formulation discipline for the claims supporting it.
A decision state	Field 9 closes only on AUTHORISE, WITHHOLD or DEFER, each confined to the exact recorded action.

Programme delivery block required alongside the action record

The action record controls the authority for one production action. It does not by itself constitute the resource plan or implementation schedule requested in a programme-level action plan. Complete the following three blocks for every measure in that plan, or maintain equivalent fields in the institution’s programme system with a stable reference from the measure.

Field 4 clocks measure evidence freshness and decision validity; they are not an implementation timetable. Field 9 expiry, reopen conditions and decision date govern the action record and likewise do not show delivery progress. Implementation progress belongs in the milestones block below.

Resources

Field	Entry
Measure	
People or capacity	
Funding or budget	
Dependencies or procurement	
Confirming owner	
Confirmation date	
Shortfall and resolution	

Milestones and implementation timetable

Field	Entry
Measure	
Milestone or deliverable	
Accountable owner	
Start date	
Target completion	
Dependencies	
Status	

Completion evidence

Use one separate completion-evidence card for each measure or milestone.

Field	Entry
Measure / milestone	
Acceptance criterion	
Evidence artefact and location	
Reviewer	
Sign-off date	

A programme may share a threat assessment, policy owner or reporting cadence across measures. Its authority does not aggregate in the same way. Four production-changing measures normally require four action records, because each acts on a different object or carries a different trigger, scope or recovery path. Later records should become cheaper as common evidence is reused by reference, but no result widens itself.

The same applies when a security operations centre is outsourced. The provider may perform the operational role, but consent, escalation, recovery, restoration cost and the business-service owner remain interfaces the institution must be able to name. A contract does not dissolve the authority boundary; it makes the boundary more important.

Legitimate results that are easy to overlook

Incumbent sufficient — No action. Existing controls meet the same material threshold on the same scenario, object, population, clock and exclusions; no further action is warranted on the current evidence.

Unresolved is different. It means a measurement or condition needed to answer the question is still missing. The plan should name that item, its owner and the date on which the question reopens; if the action record cannot yet close, Field 9 records DEFER. Missing evidence must not be relabelled as No action simply to make the plan look complete.

No action is also legitimate where the question has been answered and nothing further is warranted under the current evidence. It is terminal on that evidence, while Unresolved remains open.

At record level, the vocabulary changes deliberately. AUTHORISE permits only the exact action, class, object, scope, owners, limits and expiry that passed. DEFER leaves existing authority unchanged while a named item remains open. WITHHOLD grants no action authority because a required condition has failed. These decision values do not replace the question outcomes, and the question outcomes do not quietly authorise a plan measure.

What weakens a plan

- Comparing suppliers before the action, object, threshold, owner, rollback and recovery requirements are defined.
- Treating investigation, recommendation and a production change as one automation choice, although they carry different authority and consequences.
- Treating a reversible command as operationally recoverable without a tested route back to state parity inside the required recovery time.
- Treating Incumbent sufficient — No action, Unresolved or DEFER as drafting failures and replacing them with procurement activity that the evidence does not support.

An internal-audit or independent-assurance reader has a simple route through the finished artefact: start with the Field 9 decision, expiry and reopen conditions, then trace every condition back through Fields 1–8 to dated evidence and a named owner. Audit tests the route; it does not become the operational decision owner.

Status and limits

This editorial successor is dated 8 September 2026 and follows the separately maintained evidence record with a 4 September 2026 cutoff. It does not retroactively change the underlying report’s 31 August 2026 evidence date. Supervisory and national positions can move quickly; an expired source loses current-status use even where the dated historical fact remains sound.

This document is neither legal advice nor a compliance template, and it grants no authority. Applicability, legal deadlines and group-to-entity routing require current review for the named entity, service, duty, jurisdiction and date.

Companion to Autonomous Defensive Action: How Buyers Decide Action Authority and Accountability (Ascendo Analytics, 31 August 2026). The four decision questions appear in sections 4–7; the nine-field record is Annex D. ascendoanalytics.com

Evidence Record — Supervisory Addendum

Declared basket, source boundaries and current-use status

Cutoff: 4 September 2026

How to read this record

Each row states the most the cited source can carry for this addendum. A FACT records a source property or dated event. INTERPRETATION applies the report's method to named facts. NO_DATA records only a bounded absence inside the declared basket and date; it never means universal absence. "Current" means usable as at the cutoff, subject to the review trigger shown.

S1 — ESRB warning

Field	Value
Atomic statement	ESRB Warning ESRB/2026/3 was adopted on 25 June 2026 and announced on 7 July 2026; it classifies systemic cyber risk from frontier AI models as severe and asks European and national authorities to monitor and reassess the risk.
Claim type	FACT
Evidence class	E1 — official systemic-risk authority
Source and checked date	ESRB press release, 7 July 2026; checked 4 September 2026
Source interest	Public authority communicating its own warning; institutional supervisory-policy interest, no commercial interest
Freshness	Event-dated; review on correction, withdrawal or superseding ESRB assessment
Current-use status	CURRENT at cutoff
Maximum formulation and boundary	Supports the severe system-level risk classification and the monitoring request to authorities. Does not itself establish a firm-level action-plan submission duty or an automation rule.

S2 — ECB Banking Supervision letter

Field	Value
Atomic statement	The ECB's 7 July 2026 letter asks CEOs of significant institutions under direct ECB supervision to assess frontier-AI-enabled cybersecurity threats and submit a comprehensive action plan to the JST by 31 October 2026, with concrete measures, resources, roles, responsibilities and implementation timelines.
Claim type	FACT
Evidence class	E1 — official direct-supervisor communication
Source and checked date	ECB letter to CEOs of significant institutions, 7 July 2026; checked 4 September 2026
Source interest	Direct supervisor communicating its own expectation; institutional supervisory interest, no commercial interest
Freshness	Event and deadline dated; review on amendment, clarification or replacement and before relying on the deadline
Current-use status	CURRENT at cutoff
Maximum formulation and boundary	Supports the named addressees, required plan content, 31 October deadline and JST follow-up. Does not make that deadline universal or prove that it reaches a subsidiary without a separate group or local route.

S3 — European Commission action plan

Field	Value
Atomic statement	On 7 July 2026 the European Commission published an EU action plan for cybersecurity and AI, organised around prevention, preparedness, response and deterrence and described as building on the existing legal framework.
Claim type	FACT
Evidence class	E1 — official EU policy source
Source and checked date	European Commission, EU Action Plan on Cybersecurity and AI, 7 July 2026; checked 4 September 2026
Source interest	Policy maker describing its own programme; institutional policy interest, no commercial interest
Freshness	Programme-current; review within 180 days or on implementation update
Current-use status	CURRENT at cutoff
Maximum formulation and boundary	Supports the existence, date and stated programme direction. The reviewed publication does not itself establish a firm-specific submission duty or action-specific authority rule.

S4 — UKNF recommendations

Field	Value
Atomic statement	UKNF's 22 July 2026 recommendations ask relevant Polish financial-market entities to review frontier-AI cyber risk and prepare or adjust action plans with measures, resources, responsibilities and timelines; adequacy and effectiveness may be examined in ongoing supervision and inspections.
Claim type	FACT
Evidence class	E1 — official national-supervisor publication
Source and checked date	UKNF publication page and recommendations PDF, 22 July 2026; checked 4 September 2026
Source interest	National financial supervisor communicating its own recommendation; institutional supervisory interest, no commercial interest
Freshness	Supervisory-current; review within 90 days or on replacement or formal clarification
Current-use status	CURRENT at cutoff
Maximum formulation and boundary	Supports the plan-content expectation and supervisory follow-up. Does not support a fixed submission date, a universal legal obligation or blanket displacement of NIS2 by DORA.

S5 — Joint ESA statement

Field	Value
Atomic statement	On 31 July 2026 EBA, EIOPA and ESMA called for enhanced governance and a cross-sectoral, risk-based and consistent supervisory approach to frontier-AI-related ICT risk, linked to existing requirements and supervisory dialogue.
Claim type	FACT
Evidence class	E1 — official joint-supervisory publication
Source and checked date	EBA, EIOPA and ESMA joint statement, 31 July 2026; checked 4 September 2026
Source interest	European supervisory authorities stating their own approach; institutional supervisory interest, no commercial interest
Freshness	Supervisory-current; review within 90 days or on replacement or formal clarification
Current-use status	CURRENT at cutoff
Maximum formulation and boundary	Supports the governance, ICT-risk and supervisory-dialogue direction. Does not itself supply a universal action-plan deadline or action-specific automation boundary.

S6 — Defender-side controlled object

Field	Value
Atomic statement	None of sources S1–S5 expressly names the defender-side controlled object on which a privileged production action would operate.
Claim type	NO_DATA
Evidence class	E6 — bounded absence in a declared basket
Source and checked date	Sources S1–S5; basket reviewed 4 September 2026
Source interest	Mixed official authorities; no commercial source in the basket
Freshness	Recheck whenever an item in the basket is amended or a new directly relevant instrument is added
Current-use status	CURRENT only for the declared basket and cutoff
Maximum formulation and boundary	Supports the narrow decision gap stated in the addendum. Does not establish that no law, supervisor, contract or technical standard addresses controlled objects elsewhere.

S7 — Poland’s national implementation clock

Field	Value
Atomic statement	Poland’s 23 January 2026 amendment to the national cybersecurity act, published at Dz.U. 2026 poz. 252, entered into force one month after publication; for existing entities within the transitional rule, Chapter 3 obligations apply within twelve months and the first audit for key entities within twenty-four months, while registration timing follows the ministerial schedule.
Claim type	FACT
Evidence class	E1 — official enacted legislation
Source and checked date	Official act text, Dz.U. 2026 poz. 252, especially Articles 33, 34 and 49; checked 4 September 2026
Source interest	Legislature and official promulgation source; no commercial interest
Freshness	Legal-current; review on amendment, implementing schedule or authoritative interpretation
Current-use status	CURRENT at cutoff
Maximum formulation and boundary	Supports 3 April 2026 as the entry-into-force date and, where the transitional rule applies, twelve- and twenty-four-month implementation periods. Does not support one universal 3 October 2026 registration deadline; applicability and schedule remain entity-specific.

S8 — Czechia’s national implementation clock

Field	Value
Atomic statement	Czech Act 264/2025 Sb. entered into force on 1 November 2025; the reviewed official implementation materials use a sixty-day notification period for a regulated service and a one-year security-measure transition measured from delivery of the registration decision.
Claim type	FACT
Evidence class	E1 — official legislation and national-authority guidance
Source and checked date	Act 264/2025 Sb. and NÚKIB implementation FAQ; checked 4 September 2026
Source interest	Legislature and national cybersecurity authority; no commercial interest
Freshness	Legal-current; review on amendment or authoritative implementation update
Current-use status	CURRENT at cutoff
Maximum formulation and boundary	Supports the effective date and relative notification and implementation clocks. A calendar deadline requires the entity’s qualifying event and the date on which its registration decision was delivered.

Record boundary

This record supports only the companion addendum dated 4 September 2026. It does not alter the 31 August 2026 cutoff of the underlying report, determine legal applicability for an unnamed entity or authorise an action.