



Standard
Intelligence

White paper

Who Owns the Harm?

The Sectoral Scramble to Govern AI in Europe, and Where the Rulebooks Collide

AUTHOR

Michael Clark
Standard Intelligence

PUBLISHED

October 2026

EDITION

General Edition

WEB

standardintelligence.com

AUDIENCE

For senior management of regulated firms in Europe

CONTENTS

Summary	3
1. One credit decision answers to five rulebooks written for different purposes	4
1.1 The AI Act regulates across the economy, sectoral law industry by industry	5
1.2 The UK regulates AI through existing law and regulators	5
2. The AI Act plugs into sectoral law at defined points	5
2.1 The high-risk regime was deferred, and some product requirements may be limited	5
2.2 Eight provisions connect the Act to sectoral law	6
2.3 Machinery shows where product-embedded AI may be heading	7
3. Sectoral supervisors have filled the interval with readings of existing law	7
4. Mapping the overlap does not remove five fault lines	8
4.1 London and Dublin disagree about automated credit decisions	8
4.2 Insurance regulates the lower-risk model first	9
4.3 Incident reporting may not follow the supply chain	9
4.4 One software update can face two reassessment tests	10
4.5 Five requirements get no financial-sector relief	10
5. Three cases show the fault lines inside single firms	11
5.1 A cross-border lender can carry the heaviest burden in the entity with least relief	11
5.2 An insurer with two models runs two governance tracks for one set of executives	12
5.3 A grid operator and its vendor report on separate tracks	12
6. At EU level, personal accountability attaches to resilience and security	13
6.1 The AI Act penalises operators, not directors	13
6.2 DORA and NIS2 reach the management body	13
6.3 UK and Irish regimes can reach conduct outcomes	14
7. If accountability shapes priorities, fairness is left with the weakest owner	14
Where to start, and what it costs	14
Basis and Standing	15
Sources	17
About the author	18

Summary

A customer in Dublin applies online for a personal loan and is declined within seconds. In law that one decision answers to at least five rulebooks (data protection, consumer credit, prudential regulation, operational resilience and the AI Act), each written for a different purpose and none designed to fit the others. Until the AI Act's high-risk regime applies, much of the practical work of governing AI in banks, insurers, hospitals and utilities will run through older sectoral rulebooks and the supervisors who already know those firms.

The AI Act plugs into sectoral law at defined points. Eight provisions connect it to sectoral law, letting firms rely on sectoral arrangements, routing conformity assessment through sectoral procedures or leaving supervision to sectoral authorities. The Digital Omnibus, Regulation (EU) 2026/1744, in force since 27 July 2026, deferred the high-risk regime to 2 December 2027 for Annex III systems and 2 August 2028 for Annex I systems, moved machinery into Section B of Annex I and empowered the Commission to limit some requirements for other product-embedded AI.

Sectoral supervisors have filled the interval. The EBA has mapped the AI Act against banking law for credit scoring, EIOPA has set out how insurance law applies to AI systems that are not high-risk, and the Medical Device Coordination Group and the AI Board have issued joint guidance. In the UK, the Mills Review has found the overall regulatory framework sound.

Mapping the overlap does not remove five fault lines:

- the UK now generally permits solely automated credit decisions with safeguards, the EU prohibits them unless an exception applies, and from 20 November 2026 EU consumer credit rights reach decisions a human has reviewed;
- insurance regulates the model the AI Act treats as lower risk first, and the higher-risk model may answer to a different authority;
- the AI Act's limit on duplicate incident reporting turns on the provider's status, while DORA and NIS2 bind the regulated operator, usually the deployer, and resilience reporting does not automatically capture fundamental-rights harm;
- a software update to an AI medical device can face two reassessment tests that may give different answers;
- human oversight, data governance, accuracy, robustness and cybersecurity, transparency to deployers and AI literacy have no financial-sector relief, so each must be met on the AI Act's own terms.

The fault lines meet inside single firms. In a cross-border lending group, the entity that builds the model may carry the heaviest AI Act burden with the least EU relief. An insurer can run two governance tracks for shared code, and a grid operator and its vendor report one model failure separately while the people affected have no AI Act right to an explanation.

At EU level, the regimes that reach executives personally concern resilience and security. DORA and NIS2 attach responsibility to management bodies, and Germany makes NIS2 managers liable to their own entity, but the AI Act creates no comparable

regime of director or senior-manager liability. National regimes go further in some places. The UK's Senior Managers and Certification Regime, with the Consumer Duty, and Ireland's Senior Executive Accountability Regime can attach accountability for conduct outcomes to senior individuals.

The author's argument, an inference rather than a finding of law, is that this asymmetry may leave fairness with the weakest owner. Where no national regime attaches conduct accountability to individuals, firms may build AI governance around the resilience regimes that reach their executives and add AI Act obligations as documentation. Personal accountability is one plausible reason among several, alongside supervisory intensity, licensing consequences, litigation risk and group control design.

The first step is a register exercise, and the decisive one is naming an owner. Map each obligation once to the regime it satisfies, confirm which entity is the provider, settle incident duties with vendors and choose defaults for shared models on purpose. Then give a senior individual responsibility for unfair outcomes from each high-risk system, whether or not a statute yet requires it.

Basis and Standing, at the end, sets out which propositions are binding law, which are supervisory guidance or expectation, which are the author's interpretation, and which are recommended controls.

1. One credit decision answers to five rulebooks written for different purposes

The EU AI Act was meant to be the centre of gravity for AI regulation in Europe. For the next two years, much of the practical work of governing AI in banks, insurers, hospitals and utilities will run through older sectoral rulebooks, read by supervisors who already know those firms. The seams between those rulebooks are where AI governance will be tested.

A customer in Dublin applies online for a personal loan and is declined within seconds. The decision came from a credit-scoring model, perhaps with a human glancing at the output, perhaps not. It feels like one event, but in law it is at least five.

- **Data protection law** governs the automated decision.
- **Consumer credit law** governs the creditworthiness assessment behind it.
- **Prudential rules** govern the model as a source of risk to the bank.
- **Operational resilience law** governs the systems it runs on.
- **The AI Act** now governs it as an AI system.

Each of those laws was written for a different purpose. Data protection protects individuals' rights over their information, prudential regulation protects the stability of the bank, consumer credit law protects borrowers from unaffordable lending, and resilience law keeps services running. The AI Act adds a further aim, protecting health, safety and fundamental rights from the specific risks of AI.

The same model answers to all of them, and they were never designed to fit together.

1.1 The AI Act regulates across the economy, sectoral law industry by industry

The AI Act is a horizontal law. It entered into force on 1 August 2024, applies across the economy rather than to one industry, and grades AI by risk: a small set of practices is banned outright, some systems carry transparency duties, and the heaviest obligations fall on systems classed as high-risk.

High-risk systems come in two families. The first is AI built into products that EU safety law already regulates, such as medical devices, machinery and vehicles, listed in Annex I; the second is standalone AI used in sensitive settings listed in Annex III, including credit scoring, life and health insurance pricing, recruitment and safety components in the management and operation of critical infrastructure. Duties fall mainly on providers, who develop systems and place them on the market or put them into service under their own name, and on deployers, who use them.

Sectoral regulation grew up the other way, industry by industry:

- DORA, CRD and CRR for banks;
- Solvency II and the Insurance Distribution Directive for insurers;
- the MDR for medical devices;
- NIS2 for essential and important entities in designated sectors.

Each of these regimes has its own supervisors, who receive the firms' reports and hold enforcement powers, and in several regimes those powers reach individual executives. When a horizontal law lands on top of vertical ones, overlap is certain. The question is how the pieces fit, and what falls between them.

1.2 The UK regulates AI through existing law and regulators

The United Kingdom has no single AI statute. AI is regulated through data protection law and the existing sector regulators, each applying its current powers.

UK firms selling into the EU meet both models at once. The AI Act applies to providers placing systems on the EU market or putting them into service there, wherever those providers are established, and to providers and deployers in third countries where their system's output is used in the Union (Article 2(1)).

2. The AI Act plugs into sectoral law at defined points

The AI Act's drafters anticipated the overlap and built connections to sectoral law into the Act. The Digital Omnibus has since deferred the high-risk regime and added to those connections.

2.1 The high-risk regime was deferred, and some product requirements may be limited

The high-risk regime was due to apply on 2 August 2026 for Annex III systems and 2 August 2027 for Annex I systems. Under Article 113 as amended, it now applies from 2

December 2027 for systems classified as high-risk under Article 6(2) and Annex III, and from 2 August 2028 for systems classified under Article 6(1) and Annex I. The Digital Omnibus that made the change, Regulation (EU) 2026/1744, was published in the Official Journal on 24 July 2026 and entered into force on 27 July 2026, six days before the original Annex III deadline.

Under Article 111(2) as amended, a high-risk system already placed on the market or put into service before the relevant date is caught only if its design changes significantly from that date. Systems intended for use by public authorities must comply by 2 August 2030.

The delay drew the headlines, but a quieter change may prove more consequential. Under new Article 2(13), specific requirements in Articles 9 to 15 and 17 to 25 may be limited for high-risk systems under Article 6(1), but only where Annex I Section A legislation provides an equivalent or higher level of protection and the limitation does not reduce the overall level of protection. The Commission must adopt delegated acts by 2 August 2027 identifying the systems, requirements and conditions, and until those acts exist, nothing is limited.

2.2 Eight provisions connect the Act to sectoral law

Eight provisions make those connections, and the Omnibus amended two of them.

Table 1. How the AI Act connects to sectoral law

Provision	Mechanism	What it covers
Art. 17(4)	Deemed compliance	Most of the quality management system, for providers that are EU-regulated financial institutions
Art. 26(5) and (6)	Deemed compliance; integration	Deployer monitoring and log retention, for EU-regulated financial institutions
Art. 74(3) and (6)	Designated authority	Sectoral regulators act as AI Act market surveillance authorities
Art. 74(4)	Sectoral procedure	Sectoral procedures replace Arts 79 to 83 for Annex I Section A products where they ensure an equivalent level of protection
Art. 73(9) and (10)	Limited reporting	Reporting narrowed to fundamental-rights infringements where equivalent sectoral duties apply
Art. 43(3), as amended	Sectoral conformity route	AI Act requirements assessed within the sectoral procedure
Art. 86(3)	Residual right	Explanation right applies only where Union law provides none
Art. 2(2) and Annex I, as amended	Sectoral implementation	Machinery AI governed through the Machinery Regulation

None of these removes the AI Act's substance across the board. Each works in a defined way: a sectoral regime may be treated as satisfying an AI Act duty, AI Act requirements may be checked inside a sectoral process, or a sectoral authority may enforce them.

2.3 Machinery shows where product-embedded AI may be heading

The Omnibus moved the Machinery Regulation into Section B of Annex I. For AI systems classified as high-risk because they relate to machinery, Article 2(2) now applies only Article 6(1), Article 60a and Articles 102 to 112 of the AI Act. It does not list Articles 4, 5 or 50, so whether they reach such systems is not settled, though they apply in full to AI in machinery that is not high-risk.

The substance has not disappeared. The Commission must adopt delegated acts adding requirements for high-risk AI to the Machinery Regulation that reflect the AI Act's high-risk requirements and its Articles 17, 19, 72 and 73, and those acts shall apply by 2 August 2028 (Machinery Regulation, Article 8, as amended). The AI Act's requirements will reach machinery through machinery law rather than as a second layer, and for product-embedded AI that may be a preview of what comes next.

3. Sectoral supervisors have filled the interval with readings of existing law

The deferral left an interval, and banking, insurance, medical device and UK conduct supervisors have used it to publish opinions, mappings and reviews that apply existing rules to AI. This is the sectoral scramble. Supervisors are filling the gap because the firms they oversee are deploying AI now, and the supervisors already hold the data, the relationships and the enforcement tools.

Each item below is labelled by its form; Basis and Standing sets out the weight each kind of source carries.

Banking (supervisory mapping). The EBA mapped the AI Act's high-risk requirements against EU banking and payments law for credit scoring, in a letter from its Chair to the Commission of 21 November 2025. The letter, with the mapping table in its annex, sets out which requirements benefit from derogations or synergies. It also identifies requirements for which the Act envisages neither, such as human oversight, data governance and cybersecurity, although EU financial services law "already includes a wide range of requirements" in those areas.

Insurance (supervisory opinion). EIOPA's Opinion of 6 August 2025 sets out how the Insurance Distribution Directive and Solvency II apply to AI. It "does not set out new requirements", and it excludes prohibited practices and high-risk systems "to avoid regulatory complexities and overlaps".

UK financial services (review for the FCA Board). The Mills Review, conducted by Sheldon Mills at the FCA Board's request and published on 6 July 2026, finds the overall regulatory framework sound and says that neither the FCA nor anyone else should "rush to write rules". It recommends that the FCA monitor the transition to autonomous models and adapt regulatory frameworks.

Medical devices (joint guidance, partly legislated). Joint guidance from the Medical Device Coordination Group and the AI Board (June 2025) said that where a device is

high-risk under both Annex I and Annex III, Annex I “alone should prevail”. The Omnibus has since written that approach into Article 43(3): where a high-risk system is covered by Annex I Section A legislation and also falls within an Annex III category, the provider follows the conformity assessment procedure under that sectoral legislation.

Supervisors have mapped the overlap carefully, but mapping does not remove the tension. Some AI Act requirements are integrated or deemed satisfied, while others remain independently applicable, and several of the fault lines run along that divide.

4. Mapping the overlap does not remove five fault lines

At five points the rulebooks pull against each other, so that complying with one can make another harder, or leave a gap none fills.

4.1 London and Dublin disagree about automated credit decisions

On 5 February 2026 the UK changed its default. Under the former UK GDPR Article 22, solely automated decisions with significant effects were prohibited unless an exception applied; under Articles 22A to 22D, substituted by section 80 of the Data (Use and Access) Act 2025, they are permitted with the safeguards Article 22C requires, unless Article 22B restricts them (where the decision rests on special category data, or the processing relies on recognised legitimate interests). A decision counts as solely automated only where there is no meaningful human involvement in taking it (Article 22A).

The EU position differs. GDPR Article 22 remains a prohibition in principle, so a solely automated credit decision needs an Article 22(2) exception and its safeguards.

The second Consumer Credit Directive (CCD2) adds rights that reach further than the GDPR, through national measures that Member States must apply from 20 November 2026 (Article 48(1)). Whenever the creditworthiness assessment involves automated processing of personal data, the consumer can request human intervention, comprising an explanation, the chance to express their view and a review (Article 18(8)). A creditor with a human in the loop may therefore sit outside Article 22 GDPR and still be subject to CCD2.

The result is a divergence on two axes:

- **Permission.** The UK generally permits solely automated credit decisions with Article 22C safeguards (subject to Article 22B), whereas the EU prohibits them unless an exception applies.
- **Trigger.** The UK’s new framework applies only to solely automated decisions, whereas CCD2 rights apply to any creditworthiness assessment that involves automated processing.

Take a human-reviewed decline in each city. In London, other UK rules on fair treatment and complaints still apply, but the new automated-decision framework does not. In Dublin, CCD2 requires Ireland to attach specific intervention and review rights to the

same decline from 20 November 2026, although as at 11 October 2026 no dedicated Irish transposing measure appears in the EU's national-measures listing.

4.2 Insurance regulates the lower-risk model first

The AI Act treats one insurance use as high-risk, namely risk assessment and pricing for life and health insurance (Annex III point 5(c)). Other insurance uses of AI remain subject to existing sectoral legislation, and EIOPA's Opinion covers those other uses while excluding the high-risk ones.

That produces an unusual order. A motor pricing model sits outside the Act's Annex III categories but already falls within EIOPA's sectoral expectations. A life pricing model is expressly high-risk, yet its AI Act high-risk obligations do not apply until 2 December 2027 (and, if it is already in service, only on a significant design change under Article 111(2)); Solvency II, the IDD, data protection law and national insurance law continue to apply to it in the meantime.

The model the AI Act treats as higher risk may also answer to a different authority. Insurance Europe told EIOPA in May 2025 that some countries were likely to designate the data protection authority, or another authority, rather than the financial supervisor to oversee AI Act compliance. In its view, that could lead to dual supervision of high-risk and non-high-risk systems.

4.3 Incident reporting may not follow the supply chain

Article 73(9) is designed to prevent duplicate reporting. It limits AI Act reporting to fundamental-rights infringements for Annex III systems placed on the market or put into service by providers subject to equivalent reporting obligations under other Union law. The limit turns on the provider's status, whereas DORA and NIS2 bind the regulated operator, which is usually the deployer.

The limit may therefore not follow the supply chain. On the author's reading, a third-party provider may remain subject to Article 73 even where the deployer reports under a sectoral regime.

A second gap goes deeper. The EBA maps DORA's incident provisions as the banking counterpart to AI Act incident reporting, but DORA's regime is built around ICT-related incidents, and a discriminatory credit model can harm many applicants without ever registering as a major ICT-related incident. Operational resilience and fundamental-rights harm are different risk taxonomies, and one reporting regime does not automatically capture the other.

The reporting clocks also differ.

Table 2. Incident reporting clocks

Regime	Who reports	First deadline
DORA	Financial entity	4 hours from classification as major; no later than 24 hours from awareness
NIS2	Essential or important entity	24-hour early warning
AI Act, Art. 26(5)	Deployer	Immediately, first to the provider, then to the importer or distributor and the market surveillance authority
AI Act, Art. 73	Provider	Immediately on establishing a causal link (or its reasonable likelihood); outer limits from awareness of 15 days, 10 days if someone dies, 2 days for widespread infringement or serious and irreversible critical infrastructure disruption
GDPR, Art. 33	Controller	Without undue delay and, where feasible, within 72 hours of awareness of a personal data breach

The DORA timings come from the incident-reporting technical standards in Commission Delegated Regulation (EU) 2025/301: the initial notification is due within four hours of classifying an incident as major, and no later than 24 hours from awareness. The AI Act's duty to report immediately, and its outer limits, are set out in Article 73(2) to (4).

4.4 One software update can face two reassessment tests

The MDR requires notified body approval for changes to an approved device that could affect its safety and performance or the conditions prescribed for its use (Annex IX, section 4.10). The AI Act applies its own, separately defined concept of substantial modification (Article 3(23)). For a continuously learning device, the two tests can give different answers to the same question: does this update need reassessment?

The 2025 joint guidance did not settle every change-control question. It noted that guidance on predetermined change control plans for medical device AI was under development at the International Medical Device Regulators Forum, and would likely serve as a basis for future EU guidance. Manufacturers should check the current state of that work rather than assume the question is closed.

The calendar adds pressure, because the MDR applies now and the AI Act's Annex I obligations arrive on 2 August 2028. Notified bodies already notified under Annex I Section A legislation may assess AI Act requirements within the sectoral procedure if specified conditions are met, but they must apply for designation under the AI Act by 28 January 2028 (Article 43(3) as amended). Other conformity assessment bodies follow the AI Act's ordinary designation procedure.

Devices stay in Section A for now. The Commission's proposal of 16 December 2025 to revise the MDR and IVDR (COM(2025) 1023) would move both instruments to Section B of Annex I, as the Omnibus did for machinery. As at 11 October 2026 it was still at committee stage in the European Parliament.

4.5 Five requirements get no financial-sector relief

Human oversight, data governance, and accuracy, robustness and cybersecurity carry no financial-sector derogation or synergy in the AI Act, and nor do transparency to deployers and AI literacy. That is the EBA's point. EU financial services law already contains requirements in each of these areas, but the AI Act still requires each to be met on its own terms.

The purposes differ. Prudential rules on human judgement in credit risk models exist to keep risk estimates accurate, whereas the AI Act's oversight requirement aims to prevent or minimise risks to health, safety or fundamental rights (Article 14(2)). A bank can satisfy the first and fall short on the second.

5. Three cases show the fault lines inside single firms

5.1 A cross-border lender can carry the heaviest burden in the entity with least relief

A UK group builds a credit model in London and runs it for unsecured loans in the UK and Ireland. Declines are automated, and review is available on request.

In the UK this design can be lawful, provided Article 22B does not apply and the Article 22C safeguards are in place, alongside the usual creditworthiness and Consumer Duty requirements. If the UK entity is a bank with internal model approval, the PRA's model risk statement SS1/23 also applies. It expects responsibility for the model risk management framework to be allocated to the most appropriate Senior Management Function holder.

In Ireland, the same flow meets GDPR Article 22 now, so the lender needs an Article 22(2) exception and its safeguards, and from 20 November 2026 it meets the intervention and review rights CCD2 requires Ireland to implement. From 2 December 2027 the high-risk regime also applies to the model as an Annex III point 5(b) system, subject to Article 111(2) if it was already in service before then. If it is caught, the Irish deployer must carry out a fundamental rights impact assessment before deployment, as Article 27(1) requires of deployers of point 5(b) systems.

The harder question is which entity holds which role. If the Irish subsidiary is a financial institution subject to internal-governance requirements under Union financial services law, its deployer monitoring obligation is deemed fulfilled through those rules (Article 26(5)). If the UK parent places the model on the market or puts it into service under its own name, it is the provider, and the group should confirm this on the facts.

Article 17(4) extends quality management relief only to providers that are financial institutions subject to internal governance requirements under Union financial services law. On the author's reading, a UK-regulated parent does not obviously qualify. If so, the group entity with the least EU relief may carry the heaviest AI Act burden.

One likely response is to adopt the EU design in both markets. Whichever design it adopts, accountability sits with the relevant Senior Management Function holders under the UK Senior Managers and Certification Regime (SM&CR) in London and, if the subsidiary is within the Senior Executive Accountability Regime (SEAR), with its senior executives in Dublin. SEAR has applied to executive pre-approval controlled function holders since 1 July 2024.

5.2 An insurer with two models runs two governance tracks for one set of executives

An Irish insurer runs machine-learning pricing in its motor and life books, and the two models share features and an engineering team. The motor model is governed now through Solvency II and IDD product oversight, as EIOPA reads them. The life model falls outside the Opinion and becomes subject to AI Act high-risk obligations from 2 December 2027 (subject to Article 111(2)), possibly supervised by a different authority, with existing sectoral law applying meanwhile.

One thing holds constant. If the insurer is within SEAR's scope, the same senior executives carry a duty of responsibility for both books, whichever AI regime applies to which model. The firm runs two governance tracks for shared code, while its executives answer for both.

5.3 A grid operator and its vendor report on separate tracks

A German distribution system operator, an essential entity under NIS2, uses a vendor's AI system to balance load. Since the Omnibus, whether that system is high-risk needs careful analysis. Systems used solely for non-safety performance optimisation, service efficiency, automation or convenience are not safety components (Article 6(1a)), while systems whose failure or malfunctioning would endanger health and safety are (Article 6(1b)).

Classification turns on those facts. A system whose failure could endanger power supplies to hospitals is a plausible case for high-risk treatment under Annex III point 2, and the operator should document its analysis either way.

Assume the system qualifies, and a model failure causes a regional outage after December 2027. The operator's duties run on two tracks:

- it files a NIS2 early warning within 24 hours;
- as deployer, it must immediately inform first the vendor, as provider, and then any importer or distributor and the market surveillance authority (and Article 73 applies to it if the vendor cannot be reached).

If the outage amounts to a serious and irreversible disruption of critical infrastructure, the vendor must report under Article 73 immediately, and in any event within two days of becoming aware; otherwise the outer limit is 15 days. On the reading in section 4.3, it benefits from the Article 73(9) limit only if it is itself subject to an equivalent regime, for instance as a managed service provider under NIS2.

One AI Act protection is expressly unavailable to the people affected. The Article 86 right to an explanation of individual decisions excludes Annex III point 2 systems.

Management, meanwhile, faces German law's version of NIS2 accountability. Under § 38(1) BSIG, managers must implement the risk-management measures the entity takes under § 30 and monitor their implementation. Under § 38(2), managers who breach that duty are liable to their own entity for damage they culpably cause, through the corporate-law rules for its legal form (and under the BSIG itself only where those rules contain no liability rule).

A UK operator in the same position would face neither the AI Act nor, yet, a reformed NIS regime. The Cyber Security and Resilience (Network and Information Systems) Bill has

completed its Lords Committee stage, with the text as amended in Grand Committee published on 7 September 2026, and is awaiting Report stage.

6. At EU level, personal accountability attaches to resilience and security

6.1 The AI Act penalises operators, not directors

The AI Act’s penalties apply to infringements by operators, with fines of up to €15 million or 3% of total worldwide annual turnover, whichever is higher, for breaches of most operator obligations, including those on high-risk systems (Article 99(4)). Operators can include natural persons. What the Act does not do is create a general EU-level regime of director or senior-manager liability comparable to the sectoral regimes below.

Table 3. Personal accountability by regime

Regime	Personal accountability	Reaches unfair outcomes?
AI Act	No general director or senior-manager regime; penalties attach to operators under Art. 99 and national enforcement rules	Yes, at operator level
DORA	Management body bears ultimate responsibility for ICT risk; national law determines individual penalties	No; ICT risk
NIS2	Management-body responsibility; Member States must provide enforcement mechanisms, including possible temporary managerial prohibitions	No; cybersecurity risk
SM&CR (UK)	Senior-manager duty of responsibility under UK financial services law	Can, through the Consumer Duty
SEAR (Ireland)	Statutory duty of responsibility for Irish senior executives	Can, through the Conduct Standards

6.2 DORA and NIS2 reach the management body

The sectoral texts are explicit. Under DORA, the management body bears “the ultimate responsibility for managing the financial entity’s ICT risk” (Article 5(2)(a)). Member States must give competent authorities power to apply penalties to its members, subject to the conditions provided for in national law (Article 50(5)).

Under NIS2, management bodies approve the entity’s cybersecurity risk-management measures, oversee their implementation and “can be held liable” for the entity’s infringements of the risk-management article (Article 20(1)). Where an essential entity fails to remedy deficiencies by the deadline its authority sets, the authority can ask the relevant body or court to prohibit temporarily any person at chief executive or legal representative level from exercising managerial functions in that entity (Article 32(5)(b)).

6.3 UK and Irish regimes can reach conduct outcomes

The UK takes a different route. The Consumer Duty and SM&CR can attach accountability for outcomes to senior managers without a standalone AI statute, and the Mills Review agreed that the Senior Managers Regime “still applies”, while noting that firms and regulators will need to work through how it operates as AI systems become more autonomous. The Treasury Committee has asked the FCA to publish, by the end of 2026, guidance on accountability and “the level of assurance expected from senior managers” for harm caused through the use of AI.

Ireland’s route is national too. SEAR imposes a statutory duty of responsibility on persons in pre-approval controlled function roles in in-scope firms, alongside Conduct Standards that have applied to individuals in controlled functions in all regulated firms since 29 December 2023. Neither the UK nor the Irish regime is EU law, and neither reaches a firm outside its own scope.

7. If accountability shapes priorities, fairness is left with the weakest owner

What follows is the author’s argument, not a finding of law. At EU level, the regimes that attach responsibility to senior individuals are mainly concerned with resilience and security, and the AI Act’s distinctive concerns (bias, explanation and fundamental rights) carry no equivalent senior-manager regime. National regimes such as SM&CR and SEAR narrow that gap for firms within their scope, but they are not EU-wide.

Personal accountability is therefore one plausible reason firms may build resilience controls more thoroughly than AI-specific fairness controls. It will not be the only reason, since supervisory intensity, licensing consequences, litigation risk and group-wide control design all shape priorities too.

If the argument holds, AI governance in EU regulated firms outside such national regimes will tend to be built on DORA registers, NIS2 board approvals and management-body responsibility for ICT risk, with AI Act obligations added as documentation. That would serve resilience well. It would leave fairness, one of the fundamental-rights harms the AI Act addresses, with the weakest owner.

Where to start, and what it costs

The AI Act plugs into sectoral regimes at specific points, and by late 2027 supervisors are likely to have set expectations across much of the ground the high-risk regime covers. The control architecture inside a firm will be shaped by how horizontal obligations, sectoral rules, supervisory expectations and individual-accountability regimes interact,

not by the AI Act alone. The work comes in stages, and the first is a register exercise rather than a programme.

First: map each obligation once. For each high-risk system, record which regime each control satisfies and on what legal basis; for credit scoring, the annex to the EBA's letter is a ready template (section 3). In a cross-border group, confirm which entity is the provider, because the entity that builds the model may be the one with the least AI Act relief (section 5.1).

Next: settle incident duties and defaults with vendors and counsel. Agree with each provider how Article 73 reporting will run alongside the firm's own sectoral reporting, because Article 73(9) may not relieve the supplier even where the firm reports through a sectoral regime (section 4.3). Where UK and EU rules diverge, decide which standard a shared model follows rather than inheriting the jurisdiction it was built in (section 4.1).

Then: name an owner for fairness. Give a senior individual responsibility for unfair outcomes from each high-risk system, whether or not a statute yet requires it (section 7).

Ongoing: keep the map current. Delegated acts under Article 2(13) and the Machinery Regulation, national CCD2 measures and the device proposal could each change where obligations sit (sections 2 and 4).

On timing. The AI Act's high-risk obligations apply from 2 December 2027 for Annex III systems and from 2 August 2028 for Annex I systems, subject to Article 111(2), and as at 11 October 2026 no fine under the AI Act had been confirmed by any regulator or official source. Sectoral law, and the supervisors' readings of it, apply now.

The rulebooks will keep multiplying. A firm that has mapped each obligation once and named its owners can say, for every high-risk system, who owns the harm.

This paper reflects the author's reading of the primary texts as at 11 October 2026 and is regulatory analysis for general information, not legal advice; take advice on the position of your own firm. Four points are interpretation rather than settled law: the Article 17(4) point about UK-regulated providers, the Article 73(9) point about provider status, the high-risk classification in the grid example, and the argument about how personal accountability shapes firms' control priorities.

Basis and Standing

Binding law.

- The AI Act, Regulation (EU) 2024/1689, as amended by Regulation (EU) 2026/1744 (in force 27 July 2026): Articles 2(1), 2(2), 2(13), 3(23), 6(1a) and (1b), 14(2), 17(4), 26(5) and (6), 27(1), 43(3), 73, 74(3), (4) and (6), 86, 99(4), 111(2) and 113; Annex I and Annex III points 2, 5(b) and 5(c). High-risk obligations apply from 2 December 2027 (Annex III) and 2 August 2028 (Annex I).
- The Machinery Regulation (EU) 2023/1230, Article 8, as amended by Regulation (EU) 2026/1744.

- The GDPR, Articles 22 and 33. The UK GDPR, Articles 22A to 22D, substituted for Article 22 by section 80 of the Data (Use and Access) Act 2025, in force 5 February 2026.
- CCD2, Directive (EU) 2023/2225, Articles 18(8) and 48(1); national transposing measures apply from 20 November 2026.
- DORA, Regulation (EU) 2022/2554, Articles 5 and 50, and Commission Delegated Regulation (EU) 2025/301, Article 5.
- NIS2, Directive (EU) 2022/2555, Articles 20, 23 and 32, and in Germany § 38 BSIG.
- The MDR, Regulation (EU) 2017/745, Annex IX, section 4.10.
- The UK Senior Managers and Certification Regime and Consumer Duty, and Ireland's Senior Executive Accountability Regime under the Central Bank (Individual Accountability Framework) Act 2023, are named where used.

Supervisory guidance and expectation, not law.

- The EBA's letter of 21 November 2025 is a mapping offered to the Commission; it creates no obligations.
- EIOPA's Opinion, EIOPA-BoS-25-360, is addressed to national supervisors and sets out no new requirements.
- AIB 2025-1 / MDCG 2025-6 is joint guidance, not binding interpretation; the Omnibus has since legislated its Annex I and Annex III point.
- PRA SS1/23 is a supervisory statement for UK banks, building societies and PRA-designated investment firms with internal model approval.
- The Mills Review is a review conducted for the FCA Board, not FCA policy, and the Treasury Committee report is a parliamentary recommendation.

Legal force. The sources carry different weight: binding legislation (such as the AI Act, DORA or CCD2), delegated acts and technical standards made under it, supervisory opinions and guidance (such as EIOPA's Opinion), and supervisory expectations expressed in reviews and speeches. Section 3 labels each supervisory source by its form.

Proposals. The Commission's proposal to revise the MDR and IVDR, COM(2025) 1023, had not been adopted as at 11 October 2026, and the delegated acts under Article 2(13) of the AI Act and Article 8 of the Machinery Regulation had not been adopted either.

Interpretation, not settled law. Four points are the author's reading: that a UK-regulated provider does not obviously qualify for Article 17(4) relief (section 5.1); that the Article 73(9) limit turns on the provider's status and so may not follow the supply chain (section 4.3); that a grid-balancing system whose failure could endanger power supplies to hospitals is a plausible high-risk case (section 5.3); and the argument in section 7 about how personal accountability shapes firms' control priorities.

Recommended controls, not regulatory requirements. The obligation map, provider confirmation, vendor incident terms, deliberate choice of defaults and the named owner for fairness in the closing section are the author's recommendations. No regime requires a named senior owner for unfair outcomes from AI systems as such.

Research, and what it does and does not support. The paper cites no empirical study of how accountability regimes shape firms' control priorities. The argument in section 7 is an inference from the structure of the regimes, to be tested against a firm's own control design.

Enforcement position. As at 11 October 2026, no fine under the AI Act had been confirmed by any regulator or official source.

Sources

1. Regulation (EU) 2024/1689 (Artificial Intelligence Act), consolidated version of 27 July 2026 [eur-lex.europa.eu](#), as amended by Regulation (EU) 2026/1744 (Digital Omnibus on AI), OJ L 2026/1744, 24 July 2026. [eur-lex.europa.eu](#)
2. Regulation (EU) 2023/1230 (Machinery Regulation), Article 8, as amended by Regulation (EU) 2026/1744, Article 3. [eur-lex.europa.eu](#)
3. Directive (EU) 2023/2225 on credit agreements for consumers (CCD2), Articles 18(8) and 48(1) (national transposing measures apply from 20 November 2026) [eur-lex.europa.eu](#) national transposition measures listing. [eur-lex.europa.eu](#)
4. Regulation (EU) 2016/679 (GDPR), Articles 22 and 33. [eur-lex.europa.eu](#)
5. Data (Use and Access) Act 2025, section 80 [legislation.gov.uk](#), commenced on 5 February 2026 by SI 2026/82, regulation 2(j) and (z8) [legislation.gov.uk](#), inserting UK GDPR Articles 22A to 22D. [legislation.gov.uk](#)
6. Regulation (EU) 2022/2554 (DORA), Articles 5 and 50 [eur-lex.europa.eu](#) Commission Delegated Regulation (EU) 2025/301 on incident reporting, Article 5. [eur-lex.europa.eu](#)
7. Directive (EU) 2022/2555 (NIS2), Articles 20, 23 and 32. [eur-lex.europa.eu](#)
8. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), § 38. [gesetze-im-internet.de](#)
9. Regulation (EU) 2017/745 (MDR), Annex IX, section 4.10. [eur-lex.europa.eu](#)
10. European Commission, proposal to simplify the rules on medical devices and in vitro diagnostic medical devices, COM(2025) 1023, 16 December 2025, procedure 2025/0404(COD). [oeil.europarl.europa.eu](#)
11. Joint AI Board and MDCG, AIB 2025-1 / MDCG 2025-6, Interplay between the MDR, IVDR and AI Act (June 2025). [health.ec.europa.eu](#)
12. European Banking Authority, letter from the EBA Chair to the European Commission on the outcome of the EBA's AI Act mapping exercise (21 November 2025). [eba.europa.eu](#)
13. EIOPA, Opinion on artificial intelligence governance and risk management, EIOPA-BoS-25-360 (6 August 2025), paragraphs 2.6 and 2.8. [eiopa.europa.eu](#)
14. Insurance Europe, response to EIOPA consultation paper on its Opinion on AI governance and risk management, COB-TECH-25-064 (12 May 2025). [insuranceeurope.eu](#)
15. Prudential Regulation Authority, Supervisory Statement SS1/23, Model risk management principles for banks (May 2023; effective 17 May 2024; updated with effect from 23 April 2026). [bankofengland.co.uk](#)
16. Financial Conduct Authority, The Mills Review: AI and the future of retail financial services (6 July 2026) [fca.org.uk](#) review page. [fca.org.uk](#)
17. House of Commons Treasury Committee, Artificial intelligence in financial services, Fifteenth Report of Session 2024-26, HC 684 (20 January 2026), paragraph 22. [publications.parliament.uk](#)

18. Central Bank of Ireland, Individual Accountability Framework (SEAR and Conduct Standards). [centralbank.ie](https://www.centralbank.ie)
19. UK Parliament, Cyber Security and Resilience (Network and Information Systems) Bill, HL Bill 49 (as amended in Grand Committee, 7 September 2026). bills.parliament.uk

Provisions are cited by article, section or paragraph in the text above.

About the author

Michael Clark is CEO and co-founder of Standard Intelligence, which builds a system of record for AI governance. He is the author of five books on AI regulation.



Standard
Intelligence

GET IN TOUCH

Name an owner for every AI harm.

EMAIL

hello@standardintelligence.com

WEB

standardintelligence.com

LOCATION

Manchester, United Kingdom

AI Use: AI tools were used in research, editorial review and drafting support. All sources were retrieved and checked against the published record by the author, who holds editorial responsibility for the contents and for the conclusions drawn. This disclosure is made voluntarily. To the extent the Article 50(4) obligation in Regulation (EU) 2024/1689 applies to this paper as text published to inform the public on matters of public interest, the exception for content that has undergone human review and for which a person holds editorial responsibility applies.