

EU AI Act + “Safe AI”

A Practical Guide



Understanding the EU AI Act

Entered into force: 1 Aug 2024. Applies in phases (high-risk dates now Dec 2027 / Aug 2028 after the 2026 Omnibus)

What It Is

The EU AI Act is the world's first comprehensive legal framework regulating artificial intelligence systems. It establishes harmonised rules for the development, placement on the market, and use of AI systems across the European Union.

The EU AI Act is ethics turned into law: transparency, fairness, human oversight.

Why It Matters to You

Even if your firm doesn't develop AI tools, you're likely procuring them. The Act makes you responsible for choosing and using systems properly—particularly where AI affects workers' employment, safety components of products, or critical infrastructure.

The Ethical Foundations of the EU AI Act

Transparency

know when AI is being used

Accountability

humans remain responsible

Human Oversight

AI cannot operate without supervision

Fairness

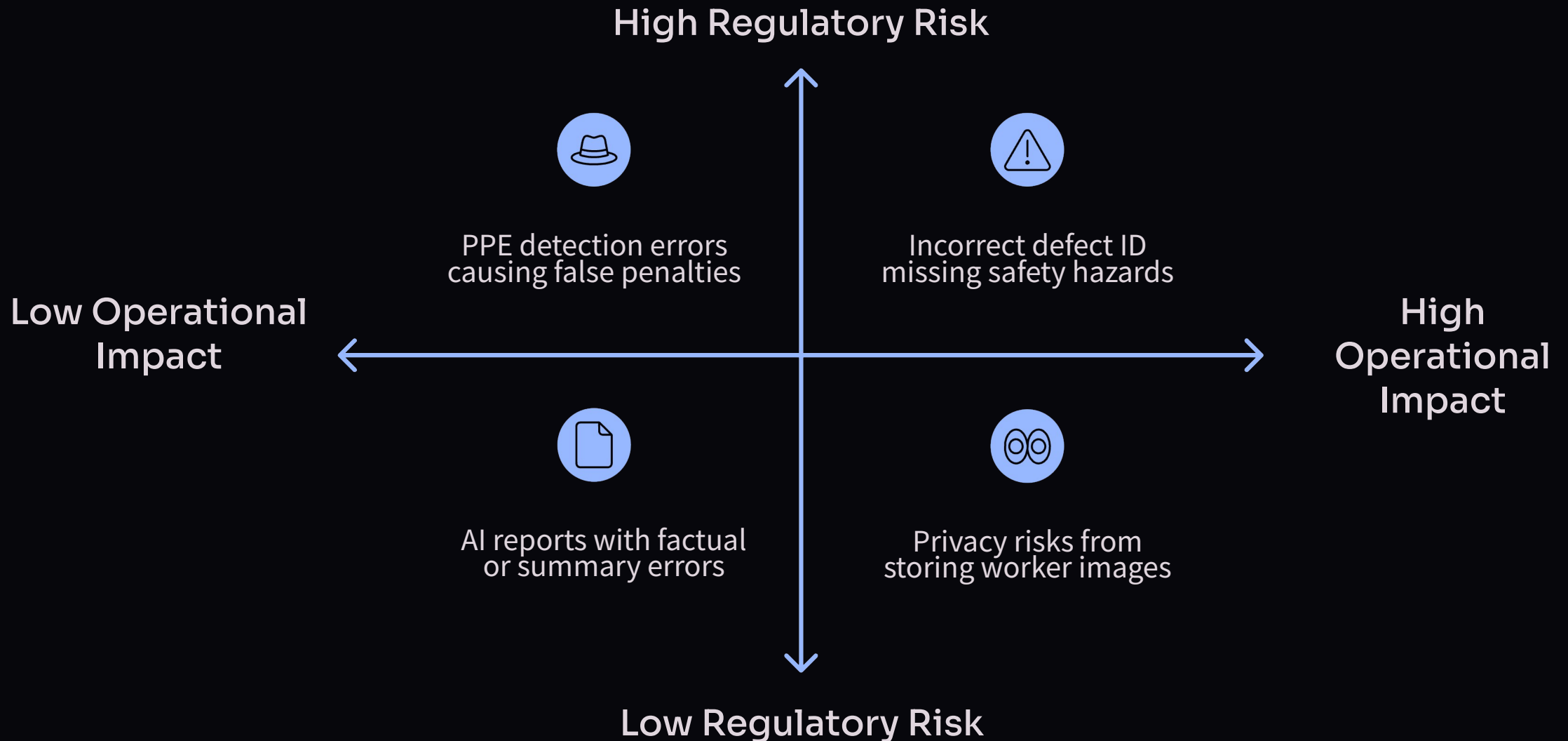
avoid bias in safety, HR, or inspections

Privacy

protect worker and site data

These principles become legal requirements under the EU AI Act.

Ethical Risks Construction Firms Must Understand



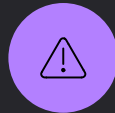


Why Construction Executives Must Pay Attention



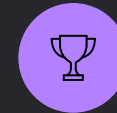
AI Proliferation

Construction increasingly relies on AI for project planning, quantity surveying, safety monitoring, inspections, and scheduling optimisation.



Regulatory Risk

Choosing non-compliant AI tools exposes your organisation to legal penalties, project delays, and reputational damage under the new regulatory framework.



Competitive Edge

Early adoption of well-documented, trustworthy AI systems positions your firm as a responsible leader, improving client confidence and tender success rates.

The EU AI Act in 60 Seconds

01

Risk-Based Approach

AI systems are classified by risk level—minimal, limited, high, and unacceptable—with requirements scaling accordingly.

02

Phased Implementation

The Act rolls out between 2024 and 2028: prohibitions first, then general-purpose AI rules, then high-risk requirements — pushed back by the 2026 Digital Omnibus.

03

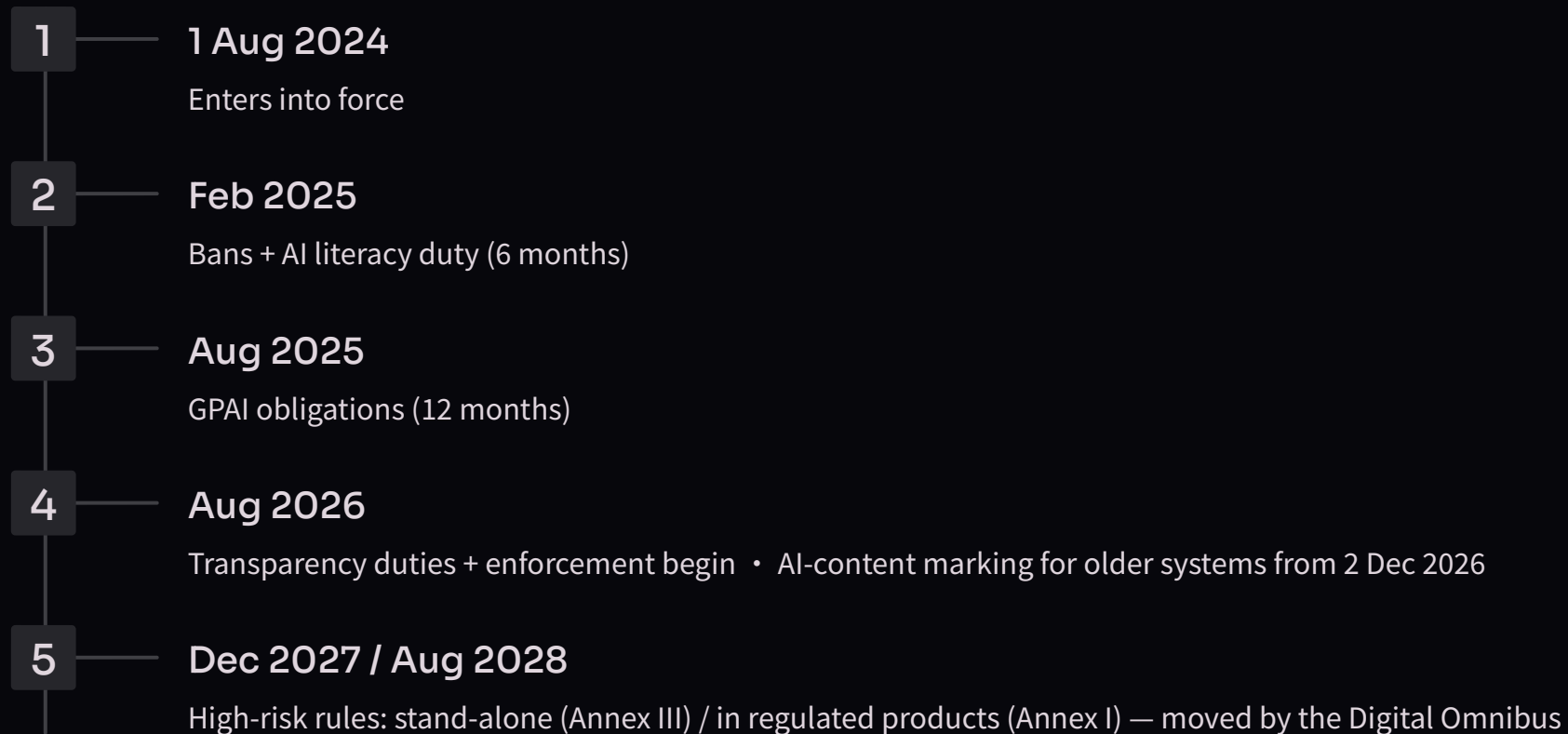
Core Principles

Three pillars underpin the framework: safety (protecting people), transparency (explainable decisions), and accountability (clear responsibility chains).



The Act applies to any AI system used within the EU, regardless of where the provider is based.

AI Act timeline: what applies when (updated October 2026)



What execs should do now:

- Start an AI inventory (tools+use cases)
- Decide who owns AI procurement/governance
- Build a simple risk triage (low/limited/high)

Ireland: Who Regulates AI Here

01

The Law

The Regulation of Artificial Intelligence Act 2026 was signed into law on 21 July 2026. It gives effect to the EU AI Act in Ireland.

02

The Regulator

The AI Office of Ireland, announced on 30 July 2026, coordinates enforcement and is the single point of contact. Other regulators share the work.

03

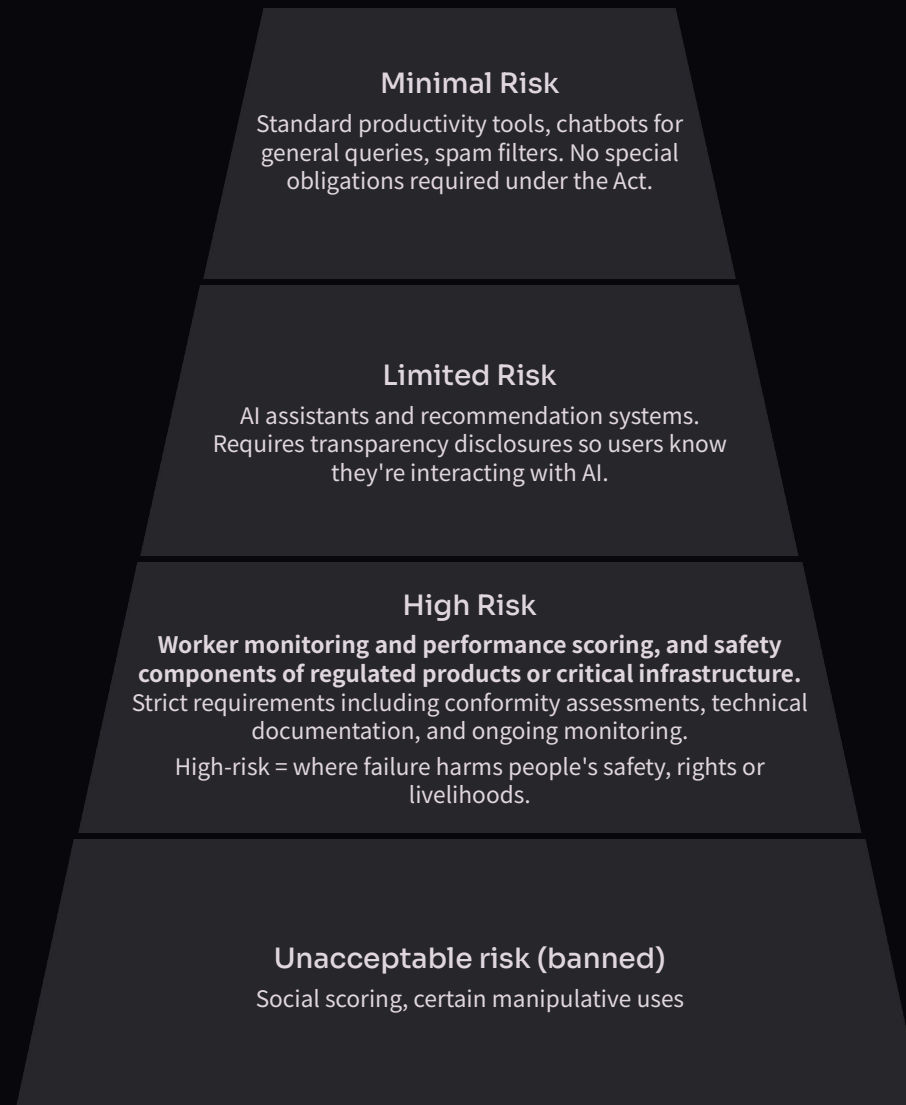
What's Next

A second bill to bring in the Omnibus changes is expected this autumn. Expect guidance, regulatory sandboxes, and AI questions in client PQQs.



For most contractors, the first contact will be client questionnaires and vendor due diligence, not a regulator.

Understanding AI Risk Levels



Where Construction AI Can Be High-Risk

Where construction AI can land in high-risk territory — always check the vendor's classification:

Site Safety Monitoring

AI that tracks or scores individual workers, or acts as a safety component of regulated machinery or equipment.

Structural Integrity Assessment

Check whether the AI is a safety component of a regulated product. Most analysis and design tools are not high-risk.

Compliance Inspections

Automated compliance or certification checks. Usually not high-risk on their own — but check the vendor's classification.

Workforce Monitoring

Biometric systems, behavioural tracking, or performance evaluation tools that impact workers' employment or working conditions.

Critical point: High-risk tools must follow strict EU rules including conformity assessments, CE marking, and comprehensive documentation.

AI scoring operatives for 'productivity risk' → HR/high-risk territory

Use cases to check carefully — ask the vendor for its classification



Safety Monitoring AI

Smartvid.io uses AI to analyse site photos and videos for safety risks. Whether it is high-risk depends on how it is used — for example, if it feeds decisions about individual workers. Ask for the vendor's classification.



Structural Integrity Assessment AI

Converge uses AI to monitor concrete curing and strength. Treat its outputs as engineering inputs a person verifies, and ask whether the vendor classifies it as high-risk.



Compliance and Inspection AI

Buildots analyses 360-degree site footage to track progress. Progress tracking alone is not on the high-risk list, but footage of workers raises privacy questions.



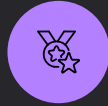
Workforce monitoring / Performance scoring (next slide)

Prohibited Uses: Don't-Touch List (Construction Lens)

Red-flag AI uses: "Stop / escalate" If any of these show up, treat it as a legal + leadership decision, not an IT experiment:



Manipulative AI that materially distorts behaviour / decisions



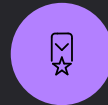
Sensitive biometric categorisation or risky biometric uses



Employee scoring / automated disciplinary decisions without strong safeguards



Covert monitoring that creates HR/legal exposure



Anything that looks like social scoring or unfair ranking of people



Practical rule: If AI is judging people, employment, or rights → escalate.

What High-Risk AI Tools Must Comply With

- 1 Human oversight required**
No fully autonomous decisions.
- 2 Logging & traceability**
Activity logs for audits.
- 3 Data governance standards**
High-quality, well-documented datasets.
- 4 Accuracy & performance testing**
Must meet defined thresholds.
- 5 Risk management system**
Ongoing monitoring of failures.
- 6 Technical documentation**
Must be provided by vendor.
- 7 Conformity assessment / CE marking**
For high-risk AI tools.

Executives must ensure vendors meet these obligations before adoption.



Examples of Lower-Risk AI (Usually 'Limited' or 'Minimal' in practice)



AI-Powered Virtual Assistants for Project Planning

Tools like Alice Technologies offer AI-driven scheduling assistants that help optimise construction timelines. These are usually minimal or limited risk: they influence planning but don't decide safety or anyone's employment. Keep a human in charge of the programme.



AI for Equipment Maintenance Predictions

Platforms like Hilti's ON!Track use AI to predict when construction equipment might need maintenance. This is usually minimal risk: important for efficiency and cost control, but not a safety-critical decision on its own.

GPAI (ChatGPT/Claude/etc.): What Execs Must Know

📄 GPAI reality check (ChatGPT / Claude / Gemini / Copilot)

GPAI = general-purpose AI used across many tasks. Risk comes from how you use it, not the tool name.

3 rules for safe, scalable use

01

Control data

no client-confidential details in public chats; use business controls where possible

02

Control outputs

treat AI as a junior analyst → verify before relying

03

Control adoption

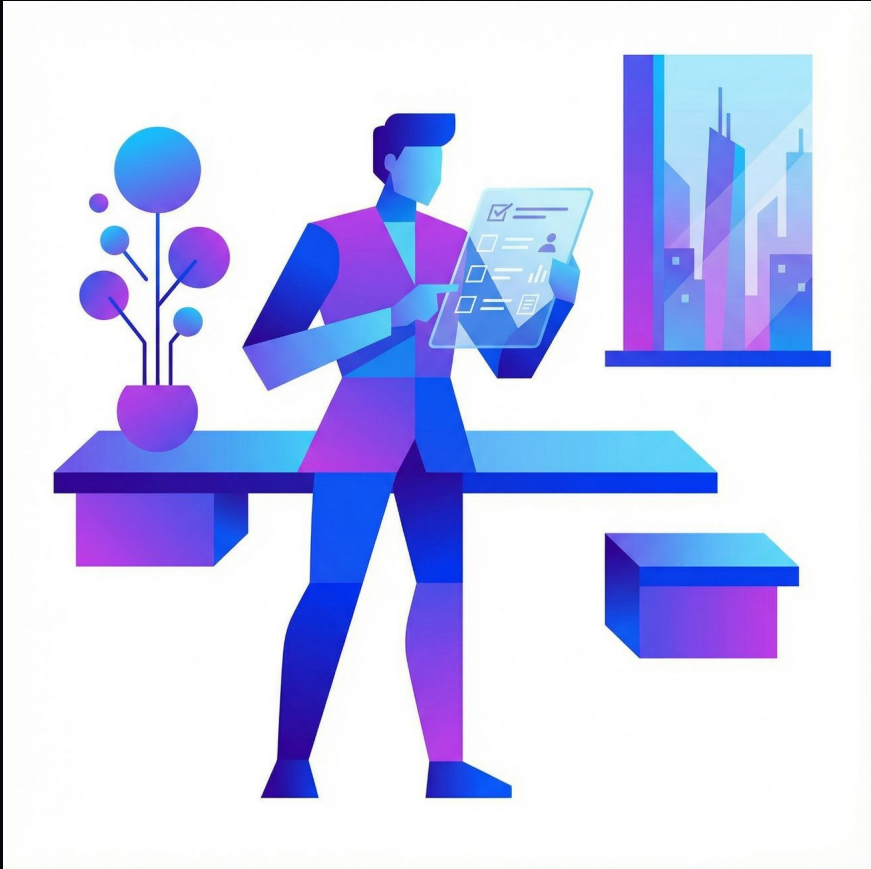
define allowed use cases + build an AI register

Procurement question set (ask vendors)

- Where is data processed/stored? Who can access it?
- Is our data used for training by default? (opt-out/opt-in)
- What logging/audit controls exist?
- Can we restrict file uploads / connectors?

Safe zone: progress reports, tender clarifications, programme narratives (sanitised + verified)

Your Responsibilities as an AI User



Essential Actions for Procurement

- Request formal compliance documentation from all AI vendors before purchase
- Verify proper risk classification of tools according to EU AI Act standards
- From Dec 2027: confirm conformity assessment and CE marking for high-risk systems
- Reject "black box" AI tools that lack transparency in decision-making processes
- Establish contractual obligations for vendors to maintain compliance

Remember: As the deploying organisation, you share responsibility for ensuring AI systems meet regulatory requirements.

If you substantially modify an AI system or repurpose it into a high-risk use case, you may take on 'provider' obligations.

Vendor Compliance Checklist

1

Risk Classification

Is this tool classified as high-risk under the EU AI Act? Does the vendor provide written risk assessment documentation?

2

Technical Documentation

Does the system come with comprehensive technical documentation, including training data, algorithms, and validation results?

3

Conformity Assessment

For high-risk uses: what is the vendor's plan for conformity assessment and CE marking before the December 2027 deadline?

4

Human Oversight

Is there meaningful human oversight built into the workflow? Can operators intervene, override, or stop the AI system?

5

Data Governance

How is data collected, stored, and processed? Are privacy protections and data quality measures in place?

6

Incident Response

What processes exist for reporting malfunctions or serious incidents? Does the vendor provide ongoing monitoring and updates?

Building Internal AI Governance



Adopt Procurement Policy

Develop a simple, clear AI procurement policy that embeds compliance checks into your standard vendor assessment process.



Train Your Team

Provide AI literacy training for procurement staff, project managers, and site supervisors who evaluate or deploy AI tools.

Meet **AI literacy** expectations (training + guidance for users and managers).



Maintain AI Register

Keep an internal inventory of all AI systems in use, including risk classifications, vendors, and compliance status.



Weekly Review Slot

Half an hour a week on what the AI got wrong and which rule would have caught it. Vendor and regulatory checks quarterly.



RICS: Mandatory AI Rules for Surveyors

01

Register + Risk Check

Firms keep a written register of AI systems and record a risk assessment before using AI that materially affects a surveying service.

02

Named Surveyor Signs Off

For each material AI output, a named, qualified surveyor records whether it is reliable enough to use, and takes responsibility for it.

03

Tell Clients in Writing

Clients must be told in advance, in writing, when and how AI will be used, with terms covering redress and opting out.



In force since 9 March 2026 for RICS members and regulated firms — closer to home for Qs than the EU AI Act.

The Business Case for Compliance

Reduced Legal Risk

Avoid substantial fines and legal challenges by ensuring all AI systems meet regulatory standards from day one.

Improved Site Safety

Compliant AI systems undergo rigorous testing, delivering more reliable safety monitoring and incident prevention.

Trusted Data Workflows

Transparent, auditable AI builds confidence in decision-making across project teams and stakeholders.

Smoother Approvals

Clients and regulators increasingly require evidence of responsible AI use, simplifying tender and permitting processes.

Competitive Positioning

Demonstrate leadership in responsible technology adoption, differentiating your firm in a crowded marketplace.

Non-compliance can trigger major fines and procurement exclusion risk.

Penalties & Business Impact (Why This Matters)

Fines can be severe (top tier up to €35m or 7% global turnover)

Enforcement aside, clients will increasingly require:

- Proof of governance (AI policy, training, risk approach)
- Vendor due diligence and documentation
- Clear accountability for AI-assisted decisions

□ Compliance is becoming procurement hygiene, not "nice to have."





SAFETY MONITORING

Case Study (Illustrative): Two Safety Tools

Vendor A: Can't Show Its Working

- Proprietary algorithm with no documentation
- No written risk classification
- Limited human oversight capabilities
- Vague incident reporting process

Result: after a safety incident, nobody can show what the tool did or why. Delays, legal costs and a difficult client meeting.

Vendor B: Ready for 2027

- Complete technical documentation provided
- Written classification and a plan for Dec 2027
- Robust human oversight framework
- Clear incident protocols and updates

Result: the incident is traced from the logs in a day, and the client's audit questions are answered from the file.

Key Takeaways

Responsibility Extends Beyond Builders

You don't need to develop AI to be accountable for it. Procurement decisions carry regulatory obligations.

Vendor Selection Is Everything

Compliance starts with choosing the right partners. Demand documentation, transparency, and proof of conformity assessments.

The Act Supports Better Construction

Ultimately, these regulations drive safer sites, higher-quality delivery, and more trustworthy technology throughout the industry.

"The EU AI Act isn't a burden—it's a framework for building confidence in the technologies transforming our industry."

Menti poll



Interactive presentation software

Interact with your audience using real-time voting. No installations or downloads required – and it's free!

