EU Regulations on AI and Cybersecurity

Prof. Dr. Konstantinos Sergakis

SAI Reset IT 2025

EU Regulations on AI and Cybersecurity

Implications for IT Governance:

- Reshaping?
- Transforming?
- Impeding?
- Window dressing?

Digital Omnibus:

- Removing friction?
- Boosting innovation?
- Enabling abuses?

The New Landscape

EU AI Act • EU NIS2 • EU DORA • EU GDPR etc

Regulation as driver of **trust** and **accountability**

- Regulations are now a primary factor in architecture, procurement and vendor oversight.
- Treat regulation as a design constraint that can also unlock trust — and therefore business value.

The EU AI Act at a Glance

- The EU AI Act uses a risk-based approach: certain systems are prohibited, others are classified as high-risk and face strict requirements, while low-risk systems are largely unrestricted.

- Key obligations target transparency, human oversight and robust documentation — not just technical controls but records showing why a model is used and how it was validated.

- If you are deploying models in decision-making, compliance isn’t optional — it is core to product governance and procurement.

Cybersecurity Regulation Overview

EU NIS2: broader scope & reporting
EU DORA: operational resilience for finance

- EU NIS2 widens the scope of critical sectors and tightens incident reporting and governance duties.
- EU DORA focuses on operational resilience for financial entities, demanding rigorous ICT third-party risk management.
- Combined, they raise the bar for incident preparedness, supplier oversight and board reporting.
- IT must be ready not only to prevent incidents, but to demonstrate governance, detection and timely reporting when they occur.

Intersection of AI & Cybersecurity

AI as asset & threat • Shared controls required

AI is a dual-edged sword: it empowers detection and automation, but it also expands the attack surface — model poisoning, data exfiltration, and adversarial attacks become real threats.

Regulators expect coherent controls across data, model governance, and system resilience.

That means your cyber team and AI team must operate on the same risk language.

Cross-functional governance is essential: one risk register, shared KPIs and integrated incident playbooks.

Regulatory Heat Map

EU Timeline: 2025–2027

- Plan
- Prioritise
- Execute

Early investment in compliance buys you breathing space for integration and testing

The New Landscape

EU AI Act • EU NIS2 • EU DORA • EU GDPR

What about the **Digital Omnibus**?

- Simplification at the cost of fundamental rights
  (e.g. **redefining “personal data” and new conditions for processing “sensitive data”**)?

- Training AI models on personal data without explicit consent would be allowed under certain conditions (e.g. high-risk AI systems).

- Reducing, or even removing, some cookie banners. Certain trackers could be used without prior consent. In healthcare, how can true transparency be ensured?
  How can misuse be prevented?

But what about ***Digital Omnibus***?

Ambition: Streamline EU GDPR and EU AI Act

Reality: More chaos on our way?

How are companies expected to innovate when uncertainty reigns?

- EC will delay the EU AI Act’s high-risk requirements yet brings fresh layers of legal uncertainty

- Businesses will not know when the core of the EU AI Act will bite until the EU co-legislators strike a deal on the entire AI omnibus, and even then, the EC could decide that the clock starts ticking sooner than expected.

Governance Implications

At its core, governance questions who is accountable.

Is the AI risk owned by the Chief Technology Officer, the Chief Data Officer, or a cross-functional risk function?

Regulators increasingly expect executive and board-level oversight.

You should also be ready to show evidence: records of testing, regular impact and oversight system assessments and methods, and decisions taken by governance bodies.

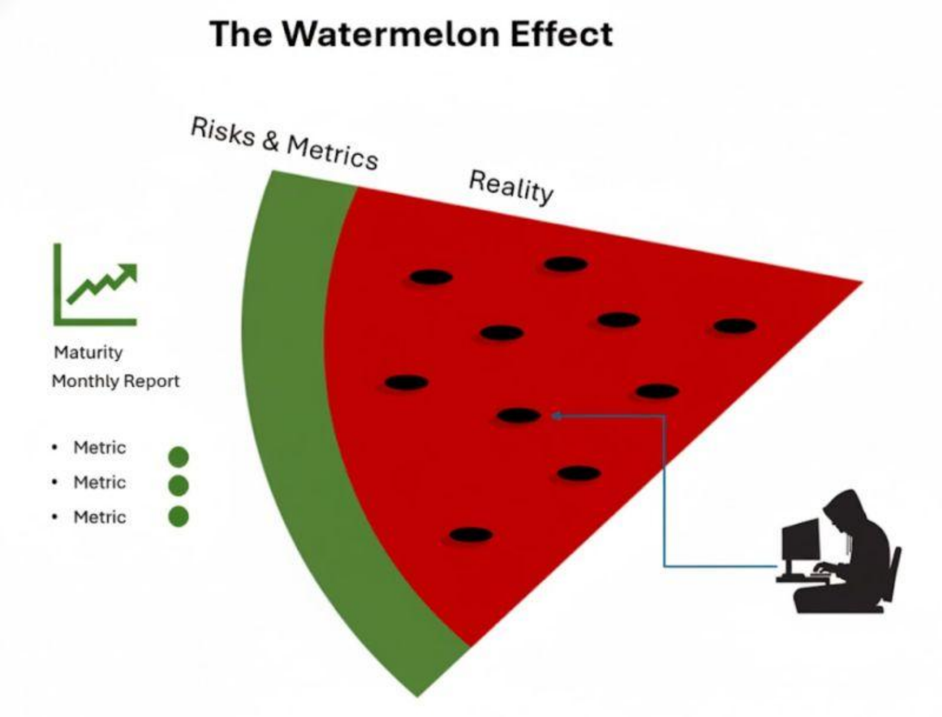
Governance Implications

The "Watermelon Effect" is a real issue

- strategic and technical knowledge can never be replaced by compliance optics only

- reliance on audit and compliance professionals, who may lack the technical understanding of cyber threat models and adversary techniques, leaves significant risks and vulnerabilities unaddressed

- If board and executive leadership better understands all cyber risks, they can make more informed decisions about how to allocate resources and prevent high-impact incidents.



Governance Implications

Accountability • Board oversight • Framework extension

- Demand for "compliance optics" is driving a dangerous trend: technical capabilities are being replaced by (non-technical) GRC practitioners, especially in leadership roles.

- We must improve the executive fluency of our deep technical specialists and train them in GRC, not the other way around.

- Boards may not need AI expert directors, but people who can understand the risks/opportunities and ask the right questions.

Governance Implications

Accountability • Board oversight • Framework extension
Recent studies show ***different trends:***

- companies are now providing significantly more **detail on their AI governance frameworks** **=>** the gap between high-level AI strategy disclosure and detailed governance reporting is beginning to narrow [**Decoding AI Disclosure 2025 report**]

- many C-suite leaders are not aware of appropriate controls for key AI risks [**EY Global Responsible AI Pulse 2025**]

- 79% of board directors have minimal AI knowledge [**Deloitte Governance of AI report 2025**]

Governance Implications

1/ map your landscape — catalogue AI systems, datasets and where personal or sensitive data flows.

2/ classify those systems against the EU AI Act risk categories and against criticality under EU NIS2/ EU DORA. That classification determines the controls and reporting cadence you will need.

3/ assign clear ownership — a named responsible party for each AI system and for third-party suppliers.

4/ conduct regular oversight reviews of systems and processes.

Governance Implications

5/ design a governance operating model: policies, approvals, an AI ethics or oversight board, and a set of technical controls mapped to legal obligations.

6/ invest in assurance: model validation, red-team exercises and continuous monitoring. These are not one-off checks; they're part of the lifecycle.

7/ run targeted training for executives and teams so compliance becomes part of decision-making, not an afterthought.

Governance Implications

How to liaise with boards? **UK NCSC guidance 2024**

- ***Understanding your audience***
  - Ensure the cyber security implications of strategic decisions are understood by decision makers.
  - Ensure that risks (boards get risks!) to delivering the organisation’s strategy are identified, evaluated, and mitigated in line with the business risk appetite.
  - Engage outside of Board meetings
  - Expect to be asked about the big picture

- ***Engaging strategically*** (Own the problem, **Provide a holistic view**, **Advise rather than educate)**

- ***Communicate clearly***
  - Pick a model and stick with it
  - Keep it simple
  - Less is more

Governance Implications

“What does *good* look like operationally?”
A regular governance forum (monthly), a risk register that includes AI & cyber, and dashboards for the board with clear KPIs:

incidents, time-to-remediate, model drift, and supplier risk scores.

Integrate these metrics into existing reporting channels; do not create parallel silos.

Automate evidence collection where possible — pipelines should log validation, testing and approvals.

The aim is a governance rhythm that makes compliance visible and manageable, not paperwork.

The Opportunity Mindset

Trust = market advantage • Link to ESG

Let’s reframe regulation as an opportunity.

Organisations that get this right earn trust — from customers, partners, and regulators.

That trust converts into market advantage, especially for B2B services and heavily regulated sectors. Compliance maturity can also be a differentiator in procurement and partnerships.

Position it as part of your ESG and risk narrative. Leaders who invest early can move from defensive compliance to proactive governance that accelerates innovation.

What’s Next

- "move fast and break things" to "move fast with guardrails" is not retreat, it is maturation.

- Operationally, prepare for audits, certification schemes and more granular guidance as regulators publish standards. Expect enforcement and scrutiny to increase over 2025–2027.

- Conduct a readiness assessment, build a 12–18 months remediation roadmap, and secure executive sponsorship for the necessary investments.

- Make the plan visible to the board and tie key milestones to funding decisions.

Call to Action

Governance is not bureaucracy — it’s how we lead digital transformation responsibly.

Your job is to translate rules into reliable, auditable practices that support the business.

Start with mapping, classify, and build the governance operating model.
Make it visible — to your board, to your customers, and to your partners.

If you take one thing away today: view regulatory readiness as strategic advantage and make it part of your narrative.

Call to Action

Companies should comprehensively review the Digital Omnibus Draft, monitor developments, and start to consider potential operational and strategic implications.

It is the organisational change and the use of data that compliance sets in motion:

- TRANSFORMATION PROCESSES that compliance can trigger - including building more robust governance structures, professionalising and systematising processes that would otherwise remain ad hoc, and fostering deeper internal collaboration and stakeholder engagement.

- TANGIBLE OUTCOMES enabled by these processes - such as stronger risk management, better customer and client acquisition, and increased employer attractiveness.