Risk and regulation

What risk is accepted and which rule applies to each system.

> *"A risk that nobody has accepted in writing is not under control. Every risk has an owner, it is assessed before investing, and whoever builds never accepts their own risk."*

WHAT IT IS

Inventory and classification

You cannot govern what you do not know. The inventory covers in-house AI, contracted AI, AI embedded in third-party products and unauthorised use. Each system is classified under the European AI Act, with legal judgement before the viability gate. When in doubt, the most demanding category applies.

Implication: Does your company know what AI arrives inside the software it already buys?

Risk: An unclassified system may be high-risk, or prohibited, without anyone knowing.

WHAT IT PROPOSES

Risk with an owner and acceptance

Each risk is assessed by likelihood and impact, using the worst of five impact axes, without averaging. The body that matches its level accepts it. A critical risk blocks viability unless the board accepts it within its appetite. A legal non-compliance is not accepted: it is corrected.

Implication: Who accepted in writing the high risks that are in production today?

Risk: Without a body to accept it, the builder takes on the risk and nobody is accountable.

HOW IT IS CHECKED

Tested controls and incidents

An untested control does not reduce risk: residual risk is verified before go-live. Only the AI auditor closes non-conformities. In an incident, contain first; notification deadlines run from when the company becomes aware. Omitting a notification is a critical non-conformity.

Implication: Has your company run a drill for a serious AI incident in the last year?

Risk: Without an incident protocol, deadlines for notifying the regulator are missed.

FOUR QUESTIONS FOR THE BOARD

1. **Have we inventoried all AI, including third-party AI?**
   A complete inventory, reconciled each quarter with purchasing and cloud billing. A system in production that has not passed the gates is a critical non-conformity.
2. **Which systems are high-risk under the AI Act?**
   Classification system by system, with legal judgement. The rule's application dates do not delay classification.
3. **Which high or critical risks have we accepted, and who did?**
   A risk register with owner, verified residual risk, accepting body and review date. A change to the system makes the acceptance expire.
4. **Are we ready for a serious incident?**
   A protocol with severities, notification deadlines per rule, a yearly drill and notice to the board within 24 hours of an incident of the highest severity.

WHAT FAILS IF IT IS NOT GOVERNED

WHAT FAILS	LEVEL	WHAT TO DO
Third-party AI in use that nobody has classified	HIGH	Reconcile the inventory with purchasing and cloud
Critical risks in production without acceptance	HIGH	Take each critical risk to the right body
Controls on paper that were never tested	HIGH	Verify residual risk before go-live
Late notification to the regulator	HIGH	Set the incident protocol and its deadlines
Risk concentrated in one supplier or one model	MEDIUM	Review risk concentration across the portfolio
Risk acceptances expired after a change	MEDIUM	Review acceptances after each relevant change

FURTHER READING

AI risk methodology
Document 33 · matrix, acceptance and standard risks

Risk matrix and register
Editable template

Inventory and regulatory classification
Document 32 · what AI exists and which rule applies

ISO/IEC 23894 · AI risk management
ISO/IEC JTC 1/SC 42 · 06-02-2023

Fernando García Varela · CC BY 4.0 · Version 0.x, under review

Generic help offered free of charge, with no legal review for any specific case: each organisation adapts it, identifies the regulation that applies to it and is responsible for its own compliance. It is neither advice nor certification. To the maximum extent permitted by law, the author accepts no liability for the effects of its application.