NIS2 + CRA | EXECUTIVE VIEW

European cybersecurity no longer fits into isolated legal instruments

NIS2, the Cyber Resilience Act and European reform are converging into a model of distributed responsibility.

Executive reading

The mistake is treating NIS2 and CRA as separate topics

Regulatory pressure is pushing companies towards one logic: governance, product, supply chain and incident response. Compliance, security, procurement and product can no longer be four disconnected conversations.

NIS2

What NIS2 changes in practice

NIS2 increases board exposure, raises the importance of incident reporting, brings third-party risk into scope and requires documented decisions, responsibilities and evidence.

Cyber Resilience Act

What CRA changes for digital products

CRA shifts security into design, development, maintenance and post-market monitoring. Security by design, vulnerability management, updates, value chain duties and evidence become product responsibilities.

Where companies fail

Fragmentation remains the central problem

Security works alone, legal arrives too late, procurement buys blind, product moves without regulatory ownership, and incident playbooks lack consistent escalation and accountability.

Quick wins

Five actions with immediate value

Review scope, connect legal + security + product, map critical suppliers, create evidence and treat the topic as governance rather than a purely IT exercise.

Conclusion

The serious question is governance

How does the organisation govern security, product, third parties and regulatory responsibility as one system? If the discussion is still in silos, execution is already late.