GRCForce

WEEK 3 RESOURCE

European Regulatory Integration Playbook

One Operating Model for NIS2, DORA, ISO 27001 and TISAX

A practical canvas for European organisations that need one governance spine instead of four separate compliance programmes.

Purpose	Map NIS2, DORA, ISO 27001 and TISAX into one operating model, reducing duplicate evidence, fragmented reporting and parallel local programmes.
Who it is for	CISOs, Heads of GRC, Chief Risk Officers and Heads of Compliance in mid-to-large European organisations with multi-country operations.
Positioning	Define one baseline control philosophy, then document local overlays only where law or regulator guidance truly differs.

Regulatory Integration Canvas

Map each control domain once, then decide the shared baseline and any justified overlays.

Domain	NIS2	DORA	ISO 27001	TISAX
Governance	Board accountability, management oversight, role clarity.	Management body ownership of ICT risk and resilience.	Leadership commitment, ISMS scope, control ownership.	Information security governance for automotive trust.
Risk assessment	Essential/important entity risk management measures.	ICT risk management framework and scenario awareness.	Risk assessment and treatment methodology.	Risk classification aligned to partner expectations.
Incident reporting	Significant incident classification and reporting timelines.	Major ICT incident classification, escalation and reporting.	Incident process, evidence and improvement.	Security incident handling and customer notification logic.
Third-party risk	Supplier and service-provider security risk oversight.	ICT third-party risk lifecycle and register discipline.	Supplier relationship controls and assurance evidence.	Supplier controls in the TISAX scope.
Testing	Security testing appropriate to risk and criticality.	Digital operational resilience testing and remediation.	Internal audit, monitoring and control testing.	Assessment evidence and maturity-driven remediation.
Documentation and evidence	Policies, measures and evidence that show due care.	Registers, reports, testing records and board-level evidence.	ISMS records, control evidence and audit trails.	Assessment-ready artefacts and evidence packs.
Local overlays	National transposition and competent-authority expectations.	Sectoral and supervisory expectations where applicable.	Local certification scope or legal additions.	Customer or market-specific automotive requirements.

How to Use the Playbook

1	Pick one control domain, for example access control, incident reporting or supplier governance.
2	Capture current obligations under each regulation or framework.
3	Define the single baseline policy and control set that satisfies the strictest requirement.
4	Document local overlays only where law, regulator guidance or customer expectation truly differs.
5	Agree evidence once, map it to all frameworks, and reuse it.

Common Anti-Patterns to Avoid

Four separate risk assessment templates; different incident definitions by regulation; local teams creating parallel policies instead of overlays; static programmes that never revisit mappings when guidance changes.

Next step	Use this canvas in a short regulatory integration workshop. To test your current model, contact GRCForce for a focused Regulatory Integration Review via grcforce.com/en/#contact.

GRCForce | Practical governance, risk and compliance for European organisations | grcforce.com