GRCForce

Guia prático de integração regulamentar europeia

24 de junho de 2026

grcforce.com/pt/#contact

Practical governance, risk and compliance guidance for European organisations.

Um único modelo operacional para NIS2, DORA, ISO 27001 e TISAX

Um enquadramento prático para organizações europeias que necessitam de uma única estrutura de governação em vez de quatro programas de conformidade separados.

Objetivo: Integrar a NIS2, o DORA, a ISO 27001 e o TISAX num único modelo operacional, reduzindo evidências duplicadas, reporte fragmentado e programas locais paralelos.

Destinatários: CISOs, responsáveis de GRC, diretores de risco e responsáveis de conformidade de organizações europeias de média e grande dimensão com operações em vários países.

Posicionamento: Definir uma filosofia comum de controlos e documentar adaptações locais apenas quando a lei ou as orientações do regulador forem verdadeiramente diferentes.

Matriz de integração regulamentar

Mapeie cada domínio de controlo uma única vez e, em seguida, defina a base comum e quaisquer adaptações justificadas.

Domínio	NIS2	DORA	ISO 27001	TISAX
Governação	Responsabilidade do conselho de administração, supervisão da gestão e clareza de funções	Responsabilidade do órgão de administração pelo risco de TIC e pela resiliência	Compromisso da liderança, âmbito do SGSI e responsabilidade pelos controlos	Governação da segurança da informação para a confiança no setor automóvel
Avaliação de riscos	Medidas de gestão de riscos para entidades essenciais e importantes	Quadro de gestão do risco de TIC e conhecimento de cenários	Metodologia de avaliação e tratamento de riscos	Classificação de riscos alinhada com as expectativas dos parceiros
Notificação de incidentes	Classificação de incidentes significativos e prazos de notificação	Classificação, escalamento e reporte de incidentes graves de TIC	Processo de incidentes, evidências e melhoria	Gestão de incidentes de segurança e lógica de notificação a clientes
Risco de terceiros	Supervisão do risco de segurança de fornecedores e prestadores de serviços	Ciclo de vida do risco de terceiros de TIC e disciplina do registo	Controlos das relações com fornecedores e evidências de garantia	Controlos de fornecedores incluídos no âmbito TISAX
Testes	Testes de segurança adequados ao risco e à criticidade	Testes de resiliência operacional digital e remediação	Auditoria interna, monitorização e testes de controlos	Evidências de avaliação e remediação orientada pela maturidade
Documentação e evidências	Políticas, medidas e evidências que demonstrem diligência devida	Registos, relatórios, resultados de testes e evidências para o conselho	Registos do SGSI, evidências de controlos e pistas de auditoria	Artefactos preparados para avaliação e pacotes de evidências
Adaptações locais	Transposição nacional e expectativas da autoridade competente	Expectativas setoriais e de supervisão quando aplicáveis	Âmbito local de certificação ou requisitos jurídicos adicionais	Requisitos do setor automóvel específicos do cliente ou do mercado

Como utilizar o guia

1. Selecione um domínio de controlo, por exemplo controlo de acessos, notificação de incidentes ou governação de fornecedores.
2. Recolha as obrigações atuais de cada regulamento ou referencial.
3. Defina uma política base única e um conjunto de controlos que satisfaça o requisito mais exigente.
4. Documente adaptações locais apenas quando a lei, as orientações do regulador ou as expectativas do cliente forem verdadeiramente diferentes.
5. Acorde a evidência uma única vez, mapeie-a para todos os referenciais e reutilize-a.

Anti-padrões comuns a evitar

- Quatro modelos separados de avaliação de riscos
- Definições de incidente diferentes consoante o regulamento
- Equipas locais que criam políticas paralelas em vez de adaptações
- Programas estáticos que nunca reveem os mapeamentos quando as orientações mudam

Próximo passo

Utilize esta matriz num breve workshop de integração regulamentar. Para testar o seu modelo atual, contacte a GRCForce para uma Revisão de Integração Regulamentar focada através de https://grcforce.com/pt/#contact.

GRCForce | Governação, risco e conformidade práticos para organizações europeias | grcforce.com