GRCForce

Lista de verificação da estrutura de preparação para auditorias

1 de julho de 2026

grcforce.com/pt/#contact

Practical governance, risk and compliance guidance for European organisations.

Utilize esta matriz para testar se o âmbito, as evidências, a responsabilidade, a cadência e a cultura são suficientemente sólidos antes de surgir a pressão de uma auditoria.

Página 1 — Matriz da estrutura de preparação para auditorias

Camada	O que significa	Verificação ISO 27001	Verificação TISAX	Responsável pelas evidências	Estado
Âmbito	Os limites são claros e correspondem à realidade	A declaração de âmbito está atualizada e reflete serviços, localizações e sistemas	O âmbito da avaliação corresponde às necessidades de proteção de dados dos clientes	Responsável do SGSI / GRC	Verde / Âmbar / Vermelho
Evidências	A prova é criada pelas operações normais e não em situação de pânico	As revisões de acesso, decisões de risco e aprovações têm data e estão armazenadas	As evidências de cada objetivo de controlo estão atualizadas e são verificáveis	Responsáveis pelos controlos	Verde / Âmbar / Vermelho
Responsabilidade	Cada controlo tem uma pessoa responsável identificada	Existe uma lista atualizada de responsáveis pelos controlos	Cada controlo TISAX tem uma pessoa responsável	Responsável de GRC / Risco	Verde / Âmbar / Vermelho
Cadência	As revisões acontecem de forma previsível e não aleatória	As revisões de riscos, revisões pela gestão e auditorias internas estão programadas e são realizadas	A preparação TISAX é revista em intervalos definidos	Gestor do programa	Verde / Âmbar / Vermelho
Cultura	A organização escala os problemas em vez de os ocultar	As conclusões são comunicadas e corrigidas com transparência	As surpresas são reduzidas através de reporte aberto	Equipa de liderança	Verde / Âmbar / Vermelho

Página 2 — 10 verificações críticas de saúde

1. A avaliação de riscos está atualizada

A avaliação de riscos foi concluída nos últimos 12 meses ou após uma alteração significativa. As decisões de tratamento têm responsáveis e datas.

Estado: Preparado / Necessita de trabalho / Não preparado

2. A Declaração de Aplicabilidade reflete a realidade

A SoA é revista, justificada, aprovada e sustentada por evidências de implementação.

Estado: Preparado / Necessita de trabalho / Não preparado

3. O programa de auditoria interna está em funcionamento

Existe um calendário anual de auditoria interna, é cumprido e as conclusões anteriores são encerradas com evidências.

Estado: Preparado / Necessita de trabalho / Não preparado

4. A revisão pela gestão foi realizada

As atas formais, decisões e ações da revisão pela gestão estão documentadas e armazenadas.

Estado: Preparado / Necessita de trabalho / Não preparado

5. As políticas estão ligadas à prática
As políticas principais são revistas segundo o ciclo definido e correspondem à forma como o trabalho é realmente realizado atualmente.

Estado: Preparado / Necessita de trabalho / Não preparado

6. As revisões de acesso têm evidências
São realizadas revisões formais de acesso para sistemas críticos e as evidências são armazenadas na fonte.

Estado: Preparado / Necessita de trabalho / Não preparado

7. Os controlos de fornecedores são mantidos
Os fornecedores críticos são avaliados dentro do ciclo requerido e a exposição a subcontratantes posteriores é documentada.

Estado: Preparado / Necessita de trabalho / Não preparado

8. Os registos de incidentes são exatos e completos
O registo de incidentes está atualizado e revisto, e as vias de escalamento foram testadas.

Estado: Preparado / Necessita de trabalho / Não preparado

9. Os objetivos são acompanhados e relevantes
Os objetivos de segurança têm metas mensuráveis e são revistos pela gestão.

Estado: Preparado / Necessita de trabalho / Não preparado

10. As ações corretivas estão encerradas
Os elementos em aberto têm responsáveis identificados, causa raiz, datas-alvo e critérios de evidência para encerramento.

Estado: Preparado / Necessita de trabalho / Não preparado

Página 3 — Como utilizar esta lista

Avalie a sua situação atual
Analise honestamente a matriz e a lista de 10 pontos com a equipa responsável pelo âmbito do SGSI ou TISAX.

Dê prioridade aos pontos fracos
Concentre-se primeiro nas lacunas suscetíveis de provocar uma não conformidade grave, uma preocupação do cliente ou um rasto de evidências insuficiente.

Atribua responsáveis e prazos
Cada elemento em aberto necessita de uma pessoa responsável, uma data de encerramento realista e uma expectativa de evidência.

Realize uma revisão 30 dias antes da auditoria

Volte a avaliar a situação 30 dias antes da auditoria. Os elementos que continuem não preparados exigem uma decisão de escalamento.

Mantenha a lista ativa trimestralmente

Utilize-a entre auditorias para que a preparação continue a fazer parte do modelo operacional.

Pontos de falha comuns

Falha	Como se manifesta	Ação corretiva
Desvio das políticas	As políticas já não correspondem à forma de trabalhar	Atribuir responsáveis e rever trimestralmente
Evidências apenas para auditoria	São criadas capturas e pastas durante a preparação	Integrar a produção de evidências nos fluxos normais
Ações corretivas em aberto	As conclusões são reconhecidas mas não encerradas	Atribuir responsáveis, datas e critérios de evidência
Desalinhamento do âmbito	O âmbito do certificado já não corresponde às operações	Rever anualmente e após alterações importantes

Próximo passo com a GRCForce

Para avaliar o seu programa através desta lista, solicite uma Revisão de Preparação para Auditorias de 30 minutos em https://grcforce.com/pt/#contact.