CYBER ASSURANCE

Lista de verificação pré-auditoria

Dez controlos que separam as equipas que entram numa auditoria com confiança daquelas que improvisam.

01 Completude do inventário de ativos [ ]
Consegue enumerar cada dispositivo ativo, aplicação e conta de utilizador no perímetro? Uma avaliação regulatória começa aqui.

02 Prontidão da recolha de evidências [ ]
As evidências técnicas são recolhidas automaticamente ou dependem de esforço manual? A recolha manual custa 3–8 semanas; o EviGen custa horas.

03 Mapeamento da linha de base de controlos [ ]
Todos os controlos no perímetro estão mapeados para um referencial publicado: SWIFT CSCF, ISO 27001, DORA, NIS 2 ou LPM?

04 Registo de lacunas aberto [ ]
Cada lacuna está documentada com um responsável, um prazo de remediação e uma justificação de negócio escrita?

05 Quantificação do risco [ ]
Consegue exprimir o risco residual em termos financeiros, em euros ou dólares, e não apenas como vermelho, âmbar ou verde?

06 Exposição a terceiros [ ]
Os fornecedores são avaliados anualmente e a sua contribuição para o risco está incluída na sua exposição financeira total?

07 Ensaio do plano de resposta a incidentes [ ]
O plano de resposta a incidentes foi testado em condições de carga realistas nos últimos doze meses?

08 Reporte ao nível da administração [ ]
A sua administração recebe um relatório de risco em valores monetários, e não em semáforos?

09 Referência cruzada regulatória [ ]
Todos os controlos obrigatórios estão cruzados com cada regulamento aplicável, para que as lacunas não se escondam entre referenciais?

10 Completude da trilha de auditoria [ ]
Cada constatação do último ciclo de auditoria está formalmente encerrada ou aceite como risco, com as evidências conservadas?

Pontuação

9 – 10	Pronta para auditoria
6 – 8	Lacunas menores, resolúveis em semanas com esforço focado
3 – 5	Preparação significativa necessária, contacte a CCI agora
0 – 2	Urgente, três meses podem não bastar sem ajuda

Pronto para passar de uma lista de verificação a um quadro de risco calculado? Contacte-nos em **contact@cambridgecyberinternational.com ou visite cambridgecyberinternational.com/pt/contact/**