Como apoia a Cyber Crucible a resposta às expectativas da FFIEC e de gestão do risco de terceiros?

Resposta curta: A Cyber Crucible foi concebida para ser examinável em relação às expectativas de segurança, operações e continuidade de negócio que os examinadores aplicam à tecnologia bancária, e o seu pacote preparado para fornecedores está organizado para servir como evidência de due diligence de que uma instituição financeira necessita ao abrigo da orientação interagências de 2023 sobre relações com terceiros.

Saiba mais: proteção contra ransomware e infostealers para o setor financeiro

No que o programa de um banco se pode basear

- Detalhe de controlos mapeado para os domínios encontrados em questionários padrão (SIG, CAIQ) e para os Trust-Service Criteria do SOC 2 e o NIST CSF.
- Validação independente de drivers (WHCP) como atestação externa de qualidade.
- Uma postura de continuidade de negócio documentada e testada, com a propriedade importante de que a proteção de endpoint continua mesmo durante uma indisponibilidade do backend de gestão.
- Evidência de seguros, informação financeira e uma lista de subprocessadores disponibilizadas aos revisores mediante pedido.

Por que a arquitetura reduz o risco de terceiros

O facto mais útil para um analista de risco de fornecedores de um banco é que a Cyber Crucible nunca recolhe ficheiros, credenciais ou chaves de clientes. Os dados que preocupam um revisor quanto a um manuseamento indevido por parte de um fornecedor não estão sob a custódia da Cyber Crucible para serem mal geridos. Trata-se de uma redução estrutural do risco, não de uma

promessa de o gerir bem.

Revision #3
Created 2026-07-24 06:01:11 UTC by Dennis Underwood
Updated 2026-11-24 15:49:13 UTC by Dennis Underwood