Wie unterstützt Cyber Crucible die Cybersicherheitsanforderungen von New York DFS Part 500?

Kurzantwort: Für ein Finanzinstitut, das unter New York DFS Part 500 (23 NYCRR 500) fällt, unterstützt Cyber Crucible mehrere erforderliche Kontrollen – Multi-Faktor-Authentifizierung, Verschlüsselung, Zugriffskontrollen und Incident Response – und reduziert gleichzeitig das Drittanbieterrisiko, da es die durch die Vorschrift geschützten nichtöffentlichen Informationen niemals erhebt. Cyber Crucible ist im Sinne der Vorschrift ein Drittanbieter (Third-Party Service Provider), keine erfasste Einrichtung (Covered Entity) selbst.

Unterstützte Kontrollen

- **Zugriffskontrollen und MFA** für das Management-Dashboard, abgesichert durch starke Authentifizierung.
- **Verschlüsselung** von Daten während der Übertragung und im Ruhezustand.
- **Incident Response** im Rahmen eines dokumentierten Breach-Response-Prozesses, mit einer vertraglich zugesicherten Benachrichtigungsfrist – zur Unterstützung der 72-Stunden-Meldepflicht der erfassten Einrichtung gegenüber der DFS.
- **Reduzierung des Drittanbieterrisikos** durch Datenminimierung: Es werden keine nichtöffentlichen Informationen erhoben.

Die ehrliche Grenze

Die Verpflichtungen von Part 500 – Benennung eines CISO, Risikobewertung, die jährliche Zertifizierung – liegen bei der erfassten Einrichtung. Cyber Crucible liefert Kontrollnachweise für die Third-Party-Service-Provider-Richtlinie der Einrichtung (500.11). Cyber Crucible ist keine erfasste Einrichtung und besitzt keine „Zertifizierung“ nach Part 500. Nachweise werden im Rahmen einer NDA bereitgestellt.

Revision #1
Created 2026-07-24 04:55:00 UTC by Dennis Underwood
Updated 2026-07-24 04:55:00 UTC by Dennis Underwood