A Global View on Cyber Resilience

Global financial institutions are navigating a rush of new cybersecurity rules for software and digital services that support markets and the broader financial ecosystem.

- **California's Auditing and Incident Reporting Rules (January 2026):** California's Privacy Protection Agency (CPPA) require banks and other businesses to notify individual consumers of a breach of unencrypted personal information within 30 days. Recent amendments to the California Consumer Protection Act (CCPA) add requirements for audit and risk assessments for high-risk data processing. California's Department of Financial Protection & Innovation (DFPI) requires detailed reporting of known or suspected cybersecurity incidents and urges financial institutions to report within 48 hours of discovery.

- **New York's Cybersecurity Regulations (November 2025):** New York's Department of Financial Services (DFS) amended Section 500.12 of its cybersecurity regulations to require enhanced multi-factor authentication (MFA) for individuals accessing financial firms' information systems. The DFS also adopted new rules for governance and incident reporting timelines.

- **Europe's DORA (January 2025):** The Digital Operational Resilience Act (DORA) requires banks, insurers, investment firms, and crypto-asset providers to include key contractual provisions in their ICT service agreements. These rules operate in parallel with the European Banking Authority's broader Outsourcing Guidelines. DORA also authorizes direct penalties on critical vendors for non-compliance.

- **Singapore's MAS Outsourcing Guidelines (December 2024):** The Monetary Authority of Singapore's (MAS) Guidelines on Outsourcing require institutions to uphold specified standards in governance, oversight, and confidentiality protections (especially for customer data), while reporting detailed registrations and monitoring of outsourced services.

Why it Matters. Instead of permitting a risk-based approach to vendor management, emerging frameworks prescribe mandatory requirements for training, stress testing, due diligence, information security, and business continuity for third-party technology providers.

Jake Vollebregt
Partner