ProcessUnity

5 Global Regulations Reshaping Cybersecurity in Financial Services

What Risk Leaders Need to Know (Before Fines Hit)

The question is no longer if financial services organizations will act in accordance with adapting regulations, but instead how quickly they can adapt and manage third-party cybersecurity risk management.

What's Turning the Heat Up?

Skyrocketing breach costs	Highly regulated industry	Global impact	Complex, fragmented mandates
$6.08M — average cost of FinServ data breach (2024)	Financial institutions face **constant, intense** scrutiny	Regional requirements **cascade across** global operations	No **unified regulatory** framework for oversight

Keeping the Pressure in Check

Here are five critical regulations reshaping third-party cybersecurity risk management:

	Focus	Key requirements	Who's affected
DORA Digital Operational Resilience Act (EU)	▸ Strengthen financial services organizations against ICT-related risks and protect the EU consumer base.	▸ Mandatory risk assessments of ICT service providers, incident reporting, and simulation testing for operational resilience.	▸ EU-based financial entities and financial firms with EU partners or customers.
APRA CPS 230 Operational Risk Management (Australia)	▸ Setting the global standard for operational risk regulation.	▸ Managing operational risks, maintaining business continuity plans, and arranging third party contracts.	▸ Australian financial entities and financial firms with APRA-regulated partners.
CSDDD Corporate Sustainability Due Diligence Directive (EU)	▸ Enforces ethical and sustainable business practices across supply chains.	▸ Mitigating ethical and environmental risks and enforcing due diligence across supply chains.	▸ Large EU companies, non-EU companies in the EU, and financial firms contracted by CSDDD-covered entities.
LkSG Supply Chain Due Diligence Act (Germany)	▸ Requires companies to maintain human rights and reduce environmental risks across their global supply chains.	▸ Conducting risk analyses on suppliers, taking preventive and corrective ESG measures, and establishing complaint processes.	▸ Companies operating in Germany and financial firms that service German companies.
ABAC Anti-Bribery and Anti-Corruption Laws (Global)	▸ Global network of anti-corruption frameworks, e.g. FCPA (U.S.), Bribery Act (UK) that prevent bribery and corruption in business transactions.	▸ Setting policies and controls to prevent bribery and corruption, due diligence efforts, documentation, and incident reporting on third parties.	▸ All financial institutions operating internationally.

Stay Ahead of the Regulatory Pressure

Forward-thinking organizations are turning these challenges into competitive advantages when they evolve their programs using TPRM solutions. Is your business taking the right approach?

See how top financial institutions **transform TPRM challenges into opportunities** with an integrated technology-based strategy.

Download the full guide

About ProcessUnity

ProcessUnity is The Third-Party Risk Management (TPRM) Company. Our software platforms and data services protect customers from cybersecurity threats, breaches, and outages that originate from their ever-growing ecosystem of business partners. By combining the world's largest third-party risk data exchange, the leading TPRM workflow platform, and powerful artificial intelligence, ProcessUnity extends third-party risk, procurement, and cybersecurity teams so they can cover their entire vendor portfolio. With ProcessUnity, organizations of all sizes reduce assessment work while improving quality, securing intellectual property and customer data so business operations continue to operate uninterrupted.

To learn more or request a demo, visit www.processunity.com.