Classification:

- **Green – wider than the EU.** A jurisdiction's approach to operational resilience is defined as wider than the EU if it expands beyond the focus or scope of DORA. For example, it covers non-ICT related risks.
- **Dark blue – similar to the EU.** A jurisdiction's approach to operational resilience is defined as similar to the EU if the requirements mirror DORA's scope or prescriptive requirements. For example, it mandates specific ICT-focused risk management equivalent to the EU's technical requirements.
- **Light blue – narrower than the EU.** A jurisdiction's approach to operational resilience is defined as narrower to the EU if the requirements are more selective. For example, it applies only to a specific subset of institutions (such as major banks) or excludes direct regulatory oversight of third-party service providers.

VIXIO	Entity applicability	Scope	Third party risk management	Reporting
UK	Banks, building societies, designated investment firms, insurers, payment/ e-money institutions and recognised investment exchanges.	Focuses on identifying important business services and setting impact tolerances for disruptions. Requires testing against severe but plausible scenarios.	Operates a parallel Critical Third Party (CTP) regime (fully in effect from January 2025) which, like DORA, allows regulators to directly oversee certain firms. Requires firms to map service delivery and ensure third parties can meet the firm's impact tolerances.	Requires internal and external communication strategies to reduce harm. There are also updated operational incident reporting requirements and notifications for material third-party arrangements.
Australia	APRA-regulated entities: banks (ADIs), general and life insurers, private health insurers, and superannuation licensees.	Holistic management of operational risks (legal, regulatory, technology, data) and maintaining critical operations within tolerance levels.	Requires a comprehensive service provider management policy. Entities must identify material service providers and manage associated risks. Entities must also maintain a register of material service providers.	Requires appropriate monitoring, analysis and reporting of operational risks and escalation processes.
Singapore	All financial institutions.	Rests on four pillars: governance, external dependencies, managing cyber/system threats, and business continuity management.	Oversight extends to external dependencies. Current proposals suggest a lifecycle approach (due diligence, onboarding and monitoring) for all third-party arrangements.	Prescriptive incident timelines, plus proposed transparency disclosures for systemic banks.
Hong Kong	All authorised institutions (AIs). This includes licensed banks, restricted licence banks and deposit-taking companies.	Development of an operational resilience framework to identify risks, deliver critical operations during disruptions, and resume normal operations.	Requires mapping exercises to understand interconnections and interdependencies underlying critical operations.	Requires an incident management programme to effectively respond to and manage disruptions to critical operations. Firms must also develop communication plans for reporting incidents to all relevant stakeholders.
Malaysia	Licensed persons (FSA/IFSA), prescribed institutions (DFIA), e-money issuers, and payment system operators.	Entity-wide business continuity management (BCM). A 2025 discussion paper proposes a resilience-first approach assuming disruptions are inevitable.	Focuses on identification and assessment of internal/external interdependencies as part of a BCM framework.	Financial institutions must submit notifications to Bank Negara Malaysia (BNM) for incident occurrences.