Assessment of the Operational Resilience Capability Framework's Suitability

Summary This framework is well-designed for reviewing and assessing an entity's Business Continuity Management (BCM) and Operational Resilience (OR) capability. It is professional-grade, aligned with regulatory expectations (e.g., UK FCA/PRA, APRA CPS 230, DORA), and suitable for internal audits, gap assessments, or external reviews.

Key Strengths

Aspect	Why It Works
Maturity-based model	Three levels (Established → Effective → Embedded) allow you to assess not just *existence* of controls but their *quality and integration*.
Comprehensive scope	Covers all critical BCM/OR domains: governance, BIA/risk assessment, strategies, crisis/incident response, testing, culture, and continuous improvement.
Evidence-driven	Each criterion specifies concrete, auditable evidence — no vague or subjective measures.
Beyond traditional BCM	Integrates third-party resilience, cyber/IT DR, impact tolerances (not just RTOs), and scenario testing — essential for modern operational resilience.
Decision-useful outputs	Explicitly checks that outputs (BIAs, risk assessments, strategies) are *used* for investment, strategy, and risk decisions — not just filed.
Culture & capability focus	Recognises that resilience is also behavioural — includes training, leadership engagement, and day-to-day embedding.

Comparison to Common Standards

Standard / Regime	Alignment with this Framework
ISO 22301 (BCM)	Strong — adds impact tolerances and scenario testing beyond ISO.
FCA/PRA (UK)	Very strong — directly reflects their operational resilience expectations (critical services, impact tolerances, scenario testing).
APRA CPS 230	Strong — aligns with service provider resilience, governance, and tolerance requirements.
DORA (EU)	Moderate — covers ICT incident response and testing, but less focus on business-side BIA and manual workarounds.
Traditional BCM-only frameworks	This framework is *superior* as it bridges BCM, crisis management, operational risk, and third-party resilience.

Recommended Use Cases

Use Case	Suitability
Internal maturity assessment	✅ Excellent — provides clear progression path from E1 to E3.
Regulatory gap analysis	✅ Excellent — aligns with major operational resilience regimes.
Post-incident review	✅ Good — but you would need to adapt evidence to focus on incident learnings.
Third-party / supplier resilience assessment	⚠️ Partial — use sections 2, 3, 5, but add vendor-specific criteria.
Very small entity (e.g., <50 staff)	⚠️ Use proportionately — expect fewer formal committees, but core criteria still valid.

Recommendation

Use this framework as your primary assessment tool for reviewing BCM and operational resilience capability in medium to large regulated entities (financial services, critical infrastructure, healthcare, utilities).

For smaller entities, use it as a benchmark with proportionality adjustments.