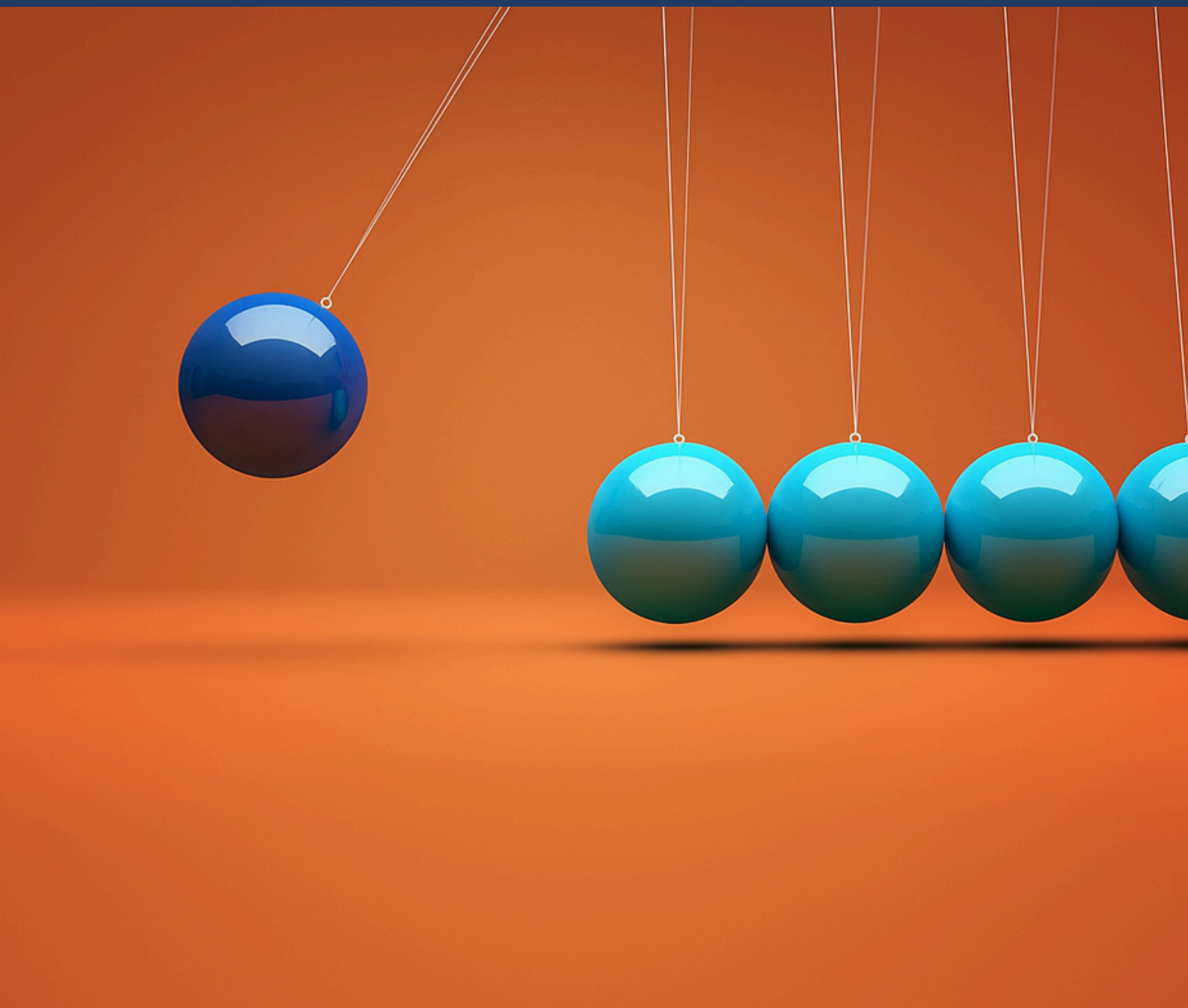
Amstelveen

Building Confidence in Vendor Business Continuity



Building Confidence in Vendor Business Continuity

As organisations become more reliant on third-party providers, the risk to operational continuity grows. Validating vendor Business Continuity Management (BCM) capabilities should be standard practice, not just for regulatory compliance, but to protect operations, ensure resilience across the value chain, and maintain stakeholder trust.

APRA's CPS 230 Prudential Standard on Operational Risk Management sets a new benchmark for operational resilience. Under this standard, financial services entities must assess the impact of Material Service Providers (MSPs), and their downstream third parties, on critical operations. This includes maintaining visibility across the full value chain to identify potential failure points and ensure continuity.

To do this successfully, it is important to understand that validating business continuity capabilities of vendors should not be treated as a compliance or tick box exercise. A disruption of processes on the vendor's side can quickly escalate to a serious issue for your organisation. Validating your vendors' BCM capabilities on a regular basis provides confidence that critical services can be restored efficiently and with minimal disruption when needed.

In practice, however, validating BCM capabilities across large, multi-client vendors is often challenging. Many critical service providers restrict access to their business continuity frameworks and testing outcomes due to the sensitivity of the information.

Effective validation goes beyond reviewing policy documents. It requires structured assessment across multiple domains of your vendor's BCM capabilities.

Consequently, organisations often need to place reliance on third-party attestations such as SOC 2 Type II reports, ISO 22301 certifications or other independent audit statements. While these reports are insightful, they are not without limitations. Their assurance is often limited in scope and may not reflect the resilience posture of the specific services your organisation depends on. These reports typically cover general controls or high-level systems, which may differ from the specific services your organisation uses. When leveraging such certifications, it is critical to ensure that the scope of the attestation covers the specific services your organisation utilises, and that recovery objectives and the BCM scope are aligned with your critical operations requirements under internal policies and regulatory obligations.

Although APRA's CPS 230 targets regulated financial entities, its focus on operational resilience, tolerance thresholds, and third-party continuity is increasingly viewed as best practice across industries, especially by organisations with complex supply chains. Crucially, it also highlights the need to assess fourth-party dependencies, extending continuity considerations beyond immediate vendors.

Key Actions to Validate and Strengthen Vendor Business Continuity

- Identify dependencies on your third parties within your critical operations and clearly determine their criticality thresholds.
- Review available attestations, such as SOC2 / ISO 22301 reports that specifically cover the services your organisation utilises.
- Include adequate contractual clauses for business continuity management in commercial agreements (right to review business continuity documentation, test outcomes or audit findings).
- Include disruptions to services provided by vendors in your business continuity testing, including assessing the impact of vendor outages on your critical operations, and effectiveness of contingency plans.
- If available, perform further due diligence, such as walkthroughs with vendors to ask scenario-based questions. Confirm the frequency of testing cadence and any recent findings related to service disruptions.
- Monitor business continuity risks continuously by tracking vendor performance metrics and public vendor disruptions and requesting regular evidence of recovery capability.

Through our work with clients, Amstelveen has found that CPS 230 provides valuable guidance for organisations reliant on external vendors, helping to strengthen operational resilience. Organisations that proactively and continuously validate the business continuity capabilities of third parties and their critical supply chain partners will be better equipped to respond to disruptions across the value chain.

Contact us

Poppy Fassos
Partner

With almost 30 years' experience, Poppy is a C-level executive with success in delivering and supporting some of the largest enterprise transformations in corporate Australia, building fit-for-purpose risk and compliance capabilities at an enterprise level, for Financial Services and Critical Infrastructure. Poppy offers experience in taking organisations on the full lifecycle of building and delivering risk and compliance capability and transformation through process and cultural change to enable business objectives and the right risk outcomes.

Romana Bizjak
Partner

Romana is a risk and compliance professional with over 15 years of experience across Australia and Europe. She has worked in delivery and assurance roles across risk, compliance and internal audit, including regulatory remediation programs, governance reviews and business continuity programs. Her experience includes leading and managing a variety of risk, technology and business change initiatives. Romana is a Graduate of the Australian Institute of Company Directors (AICD) and is a certified ISO 22301 Business Continuity Lead Implementer.

View all services and case studies

Amstelveen

Email info@amstelveen.com

Website www.amstelveen.com

LinkedIn www.linkedin.com/company/amstelveen-pty-ltd