audeamusrisk

24 October 2022

Australian Prudential Regulation Authority
Policy and Advice Division
Sydney NSW 2000

Via email

Dear Colleagues,

RE: Consultation regarding new Prudential Standards for Operational Risks Resilience

Please find below our response to questions and concerns raised in your Consultation Paper.

1. **Is a single cross-industry standard for operational risk management supported?**

While many would disagree with a single, cross-industry standard, we believe the core principles for Operational Risk are agnostic and can be applied in any industry, maturity of organisation and in any geography. Several important new ISO standards were introduced in 2015 and 2016, so there is no reason why these would not be finally implemented or embedded in CPS/SPS230. The most important are ISO22317 and ISO22318; unfortunately, these have been largely unnoticed by the industry.

Based on our experience, majority of institutions we have worked with had their Risk and BCM teams operating in a silo. Bringing the two together and building cohesiveness through a single standard will most certainly improve overall resilience.

2. **Are there specific topics or areas on which guidance would be particularly useful to assist in implementation?**

If the regulation is about moving from traditional (and very static) Business Continuity Management (BCM) towards robust Resilience, say dynamic monitoring and prevention; the most important element would be insisting on a high-quality Business Impact Analysis (BIA) and understanding all co-dependancies. The latest ISO standards provides a very clear and meaningful guidelines that can greatly assist not only BCM teams, but also senior management to understand their actual and potential operational risk exposures. Management boards are typically unaware or misinformed about these matters given that that no reliable “discovery tool” existed until recently. Prudential regulators like APRA, would greatly improve supervision quality, while management boards would be able to obtain unsurpassed transparency (granular data) that would reduce their professional and personal liabilities.

[redacted]

3. **How could proportionality be enhanced in the standard, and is there any merit in different requirements for SFIs and non-SFIs?**

It would be very difficult to apply different principles and potentially discriminate; therefore, a uniformed approach should apply across all organisations that have fiduciary duty or belong to a critical infrastructure domain.

4. **What are the estimated compliance costs and impacts to meet the new and enhanced requirements?**

Whatever the costs, these are fully justified, especially in light of recent cyber compromises in the corporate sector. Many of these institutions are deemed as critical infrastructure and systemically important. If these new principles are not fully implemented, organisations will face ongoing risk with a very long tail.

Based on our experience, implementation costs would be minimal, because most of these organisations already possess advanced software and systems. Many of these organisations have actually purchased a very sophisticated technology, but currently using only three or four out of say ten available modules. It is more about the activation of passive modules and employing the right staff to manage these systems.

Turnaround time in large organisations that possess the data, but which requires curation or further cleansing is about four to six weeks. This cannot be described demanding or expensive by any shape or form either.

5. **How could APRA improve the definitions of critical operations, tolerance levels and material service providers?**

Please refer to earlier comments regarding the BIA standards: ISO22317 and ISO22318. These are very specific but should be observed as sub-domain of Societal Security Standard ISO22301. Jointly implemented these provide a very reliable way to determine critical operations, tolerances and vital co-dependencies. This obviously does not imply a "compulsory certification;" it would just allow your supervised subjects to establish a baseline principle and mutual understanding. Once implemented these organisations can be further benchmarked and potentially incentivised.

While stochastic-modelling and Monte Carlo Simulations can be used to assess potential risk in both banking and insurance industries, current technology allows monitoring of risk at its source. Once again, these figures are available, but will never be visible unless asked to be presented. Actuaries could also greatly benefit from this information given that it would provide a missing data element.

6. **What additions or amendments should be made to the lists of specified critical operations and material service providers?**

Critical operation definition should be expanded to include relevant systems and organisations managing intangible assets too. Digital Assets (not crypto) that are currently being created by technological change represents enormous opportunity for Australia's banking and finance sector.

[redacted]

audeamusrisk

7. **Are the notification requirements and the time periods reasonable?**

Current velocity of the business requires rapid notifications and should be in real time, or close to real time. For instance, incident should be reported immediately, or as soon as it is discovered; details can be provided thereafter or once these can be verified.

According to Bank for International Settlements (BIS), current gap in recognizing Operational Risk losses is incredible 435 days. This is based on a sample of seventy-four large banks and seven hundred thousand incidents that include cyber, fraud, various types of non-compliance and natural hazards. As we have witnessed here in Australia, certain institutions had a silent business interruption unidentified more that five years. It is for that reason regulation should be tightened and reporting automated in order to avoid a red tape and unnecessary burden to organisations. These changes can be swiftly implemented and are achievable for most organisations.

8. **What form of transition arrangements and timeframe would be needed to renegotiate contracts with existing service providers (if required)?**

These would vary significantly, depending on the size and complexity of organisation. Strengthening resilience requires prompt action, especially after the most recent publicly announced incidents involving millions of Australians. Reasonable timeframe is anywhere between two and twelve months for most complex and demanding operations.

Should you require further clarification please feel free to contact me.

Once again, thank you very much for an opportunity to contribute to APRA's consultation.

Kind regards,

Aleksandar Kovacevic
Mob: [redacted]

[redacted]