Discussion paper - Strengthening operational risk management

NCC Group's response to the Australian Prudential Regulation Authority's (APRA) consultation, October 2022

NCC Group is pleased to offer its observations in response to APRA's consultation.

We support APRA's objectives to introduce a new standard for operational risk management to reflect the changing risk landscape. As the discussion paper highlights, the evolving risks facing financial services – in particular, the increasing reliance on IT systems and use of third parties – requires sound risk management and improved business continuity. To this end, **we believe that APRA could strengthen and future-proof its standard by adopting more explicitly a 'Resilience by Design' approach**, providing firms with additional guidance on the practical steps they can take to implement the required sound risk management of third-party technologies and services.

About NCC Group

With over **30 years' experience protecting business critical software, data and information through escrow, secure verification testing, and cloud hosted software continuity services**, NCC Group has followed regulatory developments regarding supply chain risks and third-party arrangements closely, not least to ensure that we, too, are able to meet our customers' evolving demands as regulatory requirements change. We work with customers operating across financial services who understand how cyber security and software resilience can add value and represent a competitive advantage both in their own business as well as across their portfolios. We hold a rare position where we see compliance from the end-user's perspective as well as from the viewpoint of the IT provider, and to assist both in achieving their aims.

NCC Group is a global cyber security business, headquartered in the UK, but with a growing presence in Asia Pacific. Indeed, our regional head office is in Sydney. Through the $220m acquisition of Iron Mountain's Intellectual Property Management division (IPM), NCC Group has **expanded its significant footprint in North America, alongside our existing presence in Europe, the Middle East and Asia Pacific**. This means we are able to take an international perspective to regulatory approaches to cyber security and third-party risk management. The IPM business has been operating in the North America operational resilience regulatory market for over 30 years. We believe strongly in the potential of appropriate regulatory measures to unleash the innovative ingenuity of adjacent services sectors to develop practical solutions that allow organisations to meet regulatory requirements in the most effective way.

Embedding a 'Resilience by Design' approach

We are passionate in our advocacy for a greater regulatory-driven focus on the adoption of cloud, software and technology escrow solutions as the baseline implementation of what we're calling 'Resilience by Design', to meet the financial sector's increased demand for third-party risk management, business continuity and operational resilience.

We note, and support, APRA's intention to require regulated entities to identify their material service providers and manage the associated risks. However, we would highlight that it is not always feasible to exhaustively identify supplier risk. A supplier's overall risk profile is generally the result of a combination of a multitude of factors (including, as APRA highlights, the supplier's own supply chain). Identifying all possible scenarios is likely disproportionate to its potential benefits, and risks increasing costs, creating barriers to innovation, and subsequently reducing access to financial services. For that reason, no less, we do believe that cloud, software and technology escrow solutions can offer legal, technical and proportional assurance to firms in dealing with their third-party suppliers, particularly where they embrace the concept of 'Resilience by Design'. This would assume supplier failure / compromise by default, regardless of their risk profile, and encourage or mandate using cloud, software and technology escrow agreements, as a proportionate and cost-effective solution for regulated entities to mitigate against this, by offering a minimum level of resilience through the legal and technical means to ensure continuity of services while a service is being restored and/or alternative options are being implemented. In this sense, escrow agreements and verification services act as a technical insurance policy and business continuity strategy, safeguarding the long-term availability of business-critical technologies and applications while protecting intellectual property.

Establishing cloud, software and technology escrow agreements with supporting verification services will create a baseline to:

- Grant organisations access to the source code and the right to access the cloud environment where it is hosted, where: an application is material to the organisation's operational continuity, if the service is deployed in the cloud; or if the application presents a concentration risk. For example, the role of escrow agreements is reflected in the US Cybersecurity and Infrastructure Security Agency's (CISA) guidance on ransomware[1] which states that, in being prepared for a ransomware incident, organisations should ensure the availability of source code through backups or escrow agreements. The details of any access rights and conditions will be set out in individual agreements, offering a legal basis with full transparency for all involved parties over when any such rights can be invoked.

- Specify how the agreement and access rights are to be used in the event of supplier compromise / failure. This goes beyond cyber risk, taking a broader view which includes non-technical risks such as bankruptcy / liquidation / insolvency, failure to maintain / inability to fix the service, transfer of ownership of intellectual property rights to the software, or the supplier company as a whole, unless the new owners agree to keep in place the agreement. Principally, financial entities rely on failed services continuing to operate while full recovery plans are being implemented. That means that continuity and exit planning needs to take account of implementation, testing and training times that impact on the ability to exchange or replace products and services expediently, safely and compliantly.

- Advance capabilities to automate risk tolerance at the application programable interface (API) gateways level to permit control to gracefully failsafe services or providers who may go out of compliance, removing exposure latency in a real-time digital economy.

[1] Ransomware Guide | CISA

Many financial services firms already use escrow solutions as part of their comprehensive business continuity planning when mitigating supplier risk, and some third-party service providers themselves have opted to build these solutions into their offer to support their customers' compliance with regulatory requirements.

By way of example, NCC Group has worked with banking technology provider Mambu on developing a cloud escrow solution. Built within Amazon Web Services (AWS) infrastructure, Mambu's cloud hosted digital banking software-as-a-service (SaaS) solutions supports more than 6,000 loan and deposit products serving over 14 million end customers worldwide. Working with NCC Group, Mambu adopted a cloud escrow solution to establish a robust approach to its customers' regulatory compliance, offering business continuity assurance by ensuring that financial institutions deploying Mambu's solution would have access to their application and specific cloud environment as well as support for the ongoing maintenance and management of their application.

However, we believe that there is still insufficiently widespread awareness of the benefits of software and technology escrow solutions, and the role they can play in addressing regulatory requirements on outsourcing and third-party risk management. To address this lack of awareness, we believe that **there is a role for regulators and policymakers, including APRA, to do more to promote and educate financial firms on the benefits of cloud, software and technology escrow solutions** as a practical means, and a baseline Resilience by Design solution, to meet outsourcing and risk management requirements - be that through explicitly encouraging the mandating of escrow solutions or by encouraging much greater inclusion of it in implementation guidance. This would align with approaches taken by other regulators, particularly those in the financial services sector including UK Prudential Regulatory Authority (PRA)[2], the Hong Kong Monetary Authority[3] (HKMA), the Reserve Bank of New Zealand[4], the Indonesian Financial Services Authority (Otoritas Jasa Keuangan)[5], the State Bank of Pakistan[6], the Securities and Exchange Board of India[7], and the Monetary Authority of Singapore[8] (MAS).

Additional Resilience by Design elements could include:

- **Ensuring the development and regular testing requirements of business continuity and exit plans forms part of licensing or contractual agreements** between regulated entities and their third-party suppliers, particularly through the release lifecycle of critical applications.

- Broadening business continuity and stressed exit plan requirements so that:

    - Cloud providers should advise their software vendors to initiate stressed exit plans where the latter provide services to critical financial service providers.
    - Software contained within other solutions, as well as the internal infrastructure of third parties supplying software and technology solutions, should also be subject to stressed exit plans.

[2] SS2/21 'Outsourcing and third party risk management' (bankofengland.co.uk)
[3] Microsoft Word - TM-G-1.doc (hkma.gov.hk)
[4] 2017 09 19 - Final BS11 redraft (rbnz.govt.nz)
[5] SAL SEOJK 21 - MRTI.pdf
[6] C6-Annex-II.pdf (sbp.org.pk)
[7] Chapter 2 - Trading Software and Technology p.pdf (sebi.gov.in)
[8] TRM-Guidelines-18-January-2021.pdf (mas.gov.sg)

In addition, **we advocate for greater information sharing to improve shared and contextualised understanding of concentration and cyber risk** through elements including:

- Anonymous outsourcing arrangement audits to gain early insights and intelligence on emerging dependencies and criticalities.

- Firms' assessments of non-material outsourcing arrangements from the outset so as to be able to track trends over time, for example, where non-material services are supplied by a single provider to a large number of financial organisations.

- Failed business continuity and stressed exit plans, particularly where these plans relate to larger suppliers.

Conclusion

NCC Group very much welcomes the opportunity to contribute. We have positively contributed to other regulatory authorities' consideration of cyber security, operational resilience and third-party risk management and would welcome the opportunity to engage in more proactive dialogue with you to support your objectives. NCC Group is able to offer interactive dialogue with its IT technical experts, solutions architects and qualified legal advisers each of which have years of experience in navigating the mitigation of risks for clients.