5.5 Focus Topic: Operational Risk in a Digital World

In addition to direct losses, the failure to manage operational risks can lead to reputational harm and loss of confidence in an institution's wider risk management practices.[1] The growing digitalisation of financial services, including reliance on third-party vendors, increases the vulnerability to, and impact from, cyber-attacks and technology outages. These risks present new governance and risk management challenges for institutions as they are inherently difficult to identify and quantify; regulators face similar difficulties in monitoring institutions' response to these risks. Furthermore, the rapidly evolving nature of these risks highlights the need for institutions to regularly test and review their risk management frameworks in line with changes to the threat environment.

This Focus Topic considers the key operational risks faced by financial institutions today, with a focus on cyber risk.

Cyber risk has emerged as a key operational vulnerability for the financial system.

The scope for, and consequences of, cyber-attacks has risen with the increased use of technology for the provision of financial services. Cyber-attacks have a higher potential than other types of incidents to be systemic: a well-resourced and sophisticated adversary seeking to cause widespread distress will actively exploit cyber vulnerabilities to maximise the impact of their attack.[2]

The number and severity of cyber-attacks in Australia has increased. In its latest annual report, the Australian Cyber Security Centre noted a 13 per cent annual increase in cybercrime reports over the year to June 2022, and Australians lost a record $3.1 billion to scams over the 2022 calendar year. Recent prominent examples in Australia include cyber breaches at Optus, Medibank Private and Latitude Financial, where attackers gained access to millions of customer records, including sensitive information, thereby facilitating further scams. Globally, a ransomware attack on Ion Markets in January 2023 disrupted critical processes at some derivatives market participants for several weeks and affected some of the world's largest banks.

A recent cybersecurity stocktake by the Australian Prudential Regulation Authority (APRA) highlighted gaps in many financial institutions' management of cyber and information security risks.[3] Common issues include:

- the failure to identify critical and sensitive information assets
- inadequate testing of control programs
- outdated incident response plans
- limited assessment of third-party information security capability.

The ongoing resilience of the Australian financial system depends on financial institutions addressing these shortcomings and ensuring they have a robust framework to manage information security.

The vulnerability to, and impact of, broader technology outages is rising.

Customers are increasingly switching to digital financial services and financial institutions are making more use of third-party services. The partial outage of Commonwealth Bank's website and banking app in June 2023 left many customers across Australia unable to access banking services or make payments. Meanwhile, the outage of the Reserve Bank's Fast Settlement Service and Low Value Clearing and Settlement Services in October 2022 caused disruption across the payments system. As services become reliant on an increasing and interconnected range of parties – from banks and superannuation funds to payments providers, cloud service providers and telecommunication companies – there are more possible points of failure, and outages have the potential to quickly cascade through the system.

Clearing and settlement facilities are increasingly undertaking multi-year projects to migrate critical services onto public cloud platforms. These platforms offer the potential for greater resilience due to their geographically diverse locations, system availability and security. However, they also concentrate operational risk. Given the importance of clearing and settlement services to the financial sector, it is vital that governance arrangements related to third-party outsourcing are robust and migration risks are appropriately managed to ensure continuity of service throughout the transition.

Ensuring a strong operational risk management culture in Australian financial institutions is a regulatory priority.

Australian regulators are focusing on close supervision, updated regulatory standards and enforcement actions against entities that have fallen short.[4] A core underlying principle is resilience: activities such as risk identification and assessment, risk mitigation (including the implementation of controls) and the monitoring of risks and control effectiveness work together to minimise operational disruptions and their effects.

APRA has recently finalised a new operational risk standard, CPS230, which modernises and brings together previously separate standards with the aim of closing regulatory gaps. This new standard will come into effect on 1 July 2025, although APRA expects entities to begin working towards compliance immediately and will be assessing their preparedness to the new standard throughout 2024. Key aspects of the standard include:

- *Increasing requirements to maintain and test internal controls*, with a focus on good governance. Management boards are expected to treat information security as a critical business risk, not just a technology risk.
- *Improving business continuity planning.* Unforeseen events will happen, and institutions must be prepared to operate critical services through severe disruptions and quickly return to business as usual.
- *Enhancing institutions' oversight of external service providers.* Third-party risk is becoming more important as financial services are increasingly digitised and financial institutions move more of their business onto cloud services.

The Cyber Operational Resilience Intelligence-led Exercises (CORIE) Framework, developed by the Council of Financial Regulators and led by the Reserve Bank, is another aspect of Australia's operational risk defence. Systemically important entities, including critical third parties not directly regulated by the financial regulators, were invited to participate. CORIE tests institutions'

readiness for and resilience to cyber-attacks: 'red team' exercises mimic the tactics, techniques and procedures of real-life adversaries, using tools and techniques that may not have been anticipated and planned for. These exercises help financial institutions identify and remediate weaknesses in their defences against cyber-attacks. Furthermore, the Australian Government established the National Office of Cyber Security in May 2023 to coordinate and strengthen cybersecurity policy, preparedness and response across Australia.

Since 2013, the Australian Securities and Investments Commission (ASIC) has conducted regular self-assessment surveys to assess the cyber resilience of financial markets. ASIC extended the scope of this initiative this year to include a wider range of regulated entities across all financial services. The survey is designed to help organisations evaluate their cybersecurity posture, controls, governance arrangements and incident preparedness. Earlier this year, ASIC also introduced market integrity rules that set out minimum expectations and controls to mitigate technological risks.

Authorities have taken enforcement actions against institutions that have failed to meet expected standards of conduct. These actions emphasise the importance placed by Australian regulators on good operational risk management. Recent examples include:

- A court-enforceable undertaking from the Bank of Queensland, relating to several breaches of APRA's prudential standards in 2022 and 2023 and notable gaps in its risk management framework, particularly in regard to non-financial risk, anti-money laundering and counter-terrorism financing.
- A $250 million capital charge for Medibank, due to weaknesses identified in its information security environment following the 2022 breach of customer records.
- A $4.5 million fine and enforceable undertaking for Openmarkets Australia Limited, after multiple compliance failures related to an inadequate framework to deal with suspicious trading.
- A $247,500 fine for BNK Banking Corporation for failing to meet its legal obligations to report balance sheet data to APRA.
- In May 2022, the Federal Court found RI Advice, an Australian Financial Services licensee, had breached its license obligations to act efficiently and fairly when it failed to have adequate risk management systems to manage its cybersecurity risks.

Regulators' renewed focus on operational risk is designed to lift industry practices and build on existing progress. Swift implementation of updated regulatory standards is an important step towards improving the resilience of the Australian financial system in the face of rapidly evolving risks.

Endnotes

[1] The failure of Credit Suisse in March 2023 highlights the danger of poor risk management practices, including operational risk. Repeated incidents at Credit Suisse over a number of years contributed to reputational damage and 'an increasingly critical assessment of the bank by its clients, market participants and rating agencies', according to the Swiss National Bank. During the period of stress in parts of the global banking system following the failure of Silicon Valley Bank in March 2023, this lack of confidence led to large deposit outflows and a liquidity crunch, ultimately resulting in Credit Suisse's acquisition by UBS. This occurred despite Credit Suisse meeting regulatory capital and liquidity requirements.

[2] See RBA (2022), 'Box C: Building Resilience to Cyber Risks', *Financial Stability Review*, April.

[3] APRA (2023), 'Cyber Security Stocktake Exposes Gaps', June.

[4] McCarthy Hockey T (2023), 'From Fires to Firewalls: The Evolution of Operational Risk', Speech to the GRC2023 Conference, 23 August.