PFS CONSULTING

FORESIGHT INSIGHT OVERSIGHT

REGULATORY UPDATE AUGUST 2024

By Jane Byrne

The new financial year has seen a range of updates to financial services regulation and administration. Here we summarise the important ones so you don't have to, and share our views on them.

CONTACT

JANE BYRNE
janebyrne@pfsconsulting.com.au
Phone: (02) 9225 6100

MADELEINE MATTERA
madeleinemattera@pfsconsulting.com.au
Phone: (02) 9225 6100

APRA PRUDENTIAL HANDBOOK

APRA has finalised its new prudential framework (23 July 2024) which includes the digital prudential handbook https://handbook.apra.gov.au. It aims to provide easier navigation and search functionality when referencing the Prudential Standard and all other material issued by APRA including information sheets and letters to industry. In addition, within each of APRA's primary industry groupings (ADIs, Insurance and Super) information has been categorised into four groups:

- Governance,
- Risk Management,
- Recovery and Resolution, and
- Financial Resilience (Banking and Insurance) / Business Operations (Superannuation).

One of the main benefits of this new handbook is the improved search facility allowing searching within documents, by industry or by document type.You can filter by document type: discussion paper, FAQs, information paper, Letter, prudential practice guide and prudential standard; and by status: current, final not yet in force, and superseded.

PFS Insight: The ability to filter will be of great value to those providing governance, risk management and compliance services within their organisation as it will allow quick access to relevant materials. It also provides the ability for users to export materials, for example, obligations registers and year-end Risk Management Declaration Attestations.

SENATE COMMITTEE REPORT ON ASIC

The Senate's Economic References Committee recently published its report (https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/ASICinvestigation/Report) following its inquiry into the capacity and capability of the Australian Securities and Investment Commission to undertake proportionate investigation and enforcement action arising from reports of alleged misconduct.

In summarising its findings, the Committee said:

"To improve investigation and enforcement outcomes, a new framework is needed to recognise that it is impossible for ASIC to administer its exceedingly broad remit to the high standard expected by Australians."[1]

Summary of recommendations

- **Separate the functions** between a companies' regulator and a separate financial conduct authority
- **Investigate reports of alleged misconduct** at an appropriate rate and develop consistent standards to transparently report data to the public
- The Government's statement of expectations should include **expectations and priorities relating to transparency**
- ASIC to establish and maintain a high level of **transparency of investigation and enforcement outcomes** including establishing a searchable public register of civil or criminal outcomes arising from reports of alleged misconduct, and a consistent long-term public reporting framework.
- **Investigate amending the whistleblower protection provisions** in the Corporations Act to include pecuniary incentives and compensation for whistleblowers who make a substantiated disclosure.

[1] Executive Summary, ASIC Investigation and enforcement, Senate Standing Committee on Economics 3 July 2024

Summary of recommendations

- Adopt an enforcement approach which **prioritises the litigation of all serious instances of suspected breaches of corporations law**
- **Review the governance structure** to have a Chair or CEO as the sole statutory appointee and accountable authority
- **Include a legislated code of conduct** as part of the governing documents of ASIC
- Financial Regulator Assessment Authority (FRAA) **reviews be undertaken every two years**
- The Australian Government **re-assess the funding arrangements** for ASIC.

PFS Insight:

- Many of the recommendations would require significant legislative change. As this was an inquiry led by the Federal opposition there would need to be appetite from the Government to do this. A number of the governance requirements such as the annual statement of expectations including priorities relating to transparency and legislating a code of conduct, could be implemented relatively easily.
- the implications for AFSL holders is not clear but the dual regulator model appears to draw on the UK regulatory model. Therefore a single/dual regulated distinction could emerge. We can expect significant consultation on proposed changes before any new legislation is introduced to Parliament. Whether that is achievable before the next Federal election remains to be seen.
    - for companies that operate with an Australian Financial Services Licence this could mean that they would be required to report to an additional regulatory body
    - improved transparency may highlight the extent of alleged misconduct, although details would only be publicised should action taken by ASIC be successful.

PFS Insight:

- What's next? There was general agreement by both Opposition and Government members within the Committee that 'there remains opportunity for improvement in ASIC's operation'. There was also general agreement that significant improvements are required to communicate with those who report allegations of misconduct and the recommendations for ASIC to transparently report data on the handling of reports of alleged misconduct. However an alternative model for regulation was not proposed apart from suggesting two bodies rather than one.

Privacy Act changes

- The Attorney-General's Department conducted nearly three years of consultation and delivered a Report in 2023[2] that concluded that the Privacy laws need to be strengthened to ensure the collection, use and disclosure of people's personal information is adequately protected from unauthorised access and misuse. The Government agreed to 38 proposals and these are expected to be the subject of a Bill due in August 2024.

PFS Insight: the changes to the Privacy Act, which we are yet to see, may reinforce the requirements that Financial Institutions have with CPS230/234 with operational risk, cyber risk and the interplay with data governance where personal information and/or sensitive information is held. Increasing the consumer protection with legal recourse under a statutory tort for invasion of privacy means the cost of getting it wrong for financial institutions increases yet again.

Finally, we have noted an increase in the number of APRA and ASIC penalty actions. It may be that both APRA and ASIC are coming down hard on regulated entities for various issues including greenwashing, data reporting and meeting financial reporting obligations. Significantly whilst ASIC has often imposed financial penalties on corporations, the recent penalties imposed by APRA are unprecedented.

[2] https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report

INFORMATION SECURITY AND CYBER RISK

Information security and cyber risk remain front of mind for all financial institutions and APRA issues regular updates on the importance of these issues. Head of Information Security & Cyber Risk Richard King says:

*The heightened cyber security focus reinforced by APRA on the **15th of August** is an opportunity for risk and security practitioners to re-evaluate their businesses for cyber security risk. The move to cloud services has removed many of the segregation and control layers that have historically provided physical layers of protection.*

With commercial pressure on IT to make older systems more self-service and intuitive to the user, IT departments have lifted and shifted legacy systems into the cloud. Many of these older systems were designed for use in multi layered, secure environments (data centers). Truth be told, a few of these systems should have been retired a long time ago.

To make this older technology meet the changing needs of the business, many IT departments have migrated these legacy systems into the cloud. Unfortunately, the majority of the cloud migrations I have had the pleasure of security assessing have ended up with less effective security than the business expected. This unexpected vulnerability has been based on primarily a lack of cloud experience in the migration team, insufficient security representation in the project or, financial pressure to complete the migration.

Be aware that each time an IT person makes a configuration decision during the migration they are essentially accepting risk on behalf of the business. If the impact of the decision is not fully understood, then your business is exposed. Security must be baked in to the delivery of the migration for the project to be successful.

With these risks, as with all IT security risk management, it is important to remember that the intent of standards and regulations is that they are the minimum you need to meet to keep your system secure, the lowest target you need to hit to be compliant. If your cyber security goal is limited to "just get us over the compliance line" then, taking into account any additional technology risks being accepted by the IT department in the background, you are much more exposed than you realize.

Adopting the Essential 8 controls is a great place for you to start. Independent auditing and review using cloud security experts is a critical part of working with cloud services. Remember, if your security consultant does not know how to ask the right IT questions, you need another opinion.

TOP 10 TIPS

Here are our Top 10 things for Financial Institution Boards to consider

1. Monitor the progress of the Privacy Act changes for impact on their organisation and seek reports from management about how they will implement any new requirements.
2. Consider how you ensure you understand what personal and/or sensitive information is held, who holds it, where it lives and what you use it for.
3. Consider how you go about ensuring your organisation does not collect more personal or sensitive information than you need.
4. Ask about data destruction and/or de-identification – do you do it and how effective is it?
5. Ask your management team how they are using the new APRA regulatory digital handbook to drive efficiency and improved reporting to the Board.
6. Consider training for the Board to give them a greater understanding of the contents of the APRA Prudential handbook
7. Challenge management on the controls, checks and balances ensuring accuracy of APRA reporting.
8. Consider how you exercise governance over representations to consumers regarding sustainability in your investment products.
9. What training have directors received on hot topics like privacy and impending changes, CPS 234 tripartite review results, current regulator priorities and the regulatory change agenda?
10. Do your products “do what it says on the tin”? Consider what steps are being taken in product governance to ensure you meet your promises to consumers.

OUR TEAM

PFS Consulting is an actuarial and risk consultancy. It provides insight, foresight and oversight and always seeks to leave its clients better placed after engagement than they were before. One of the keys to PFS's success is that its approach embodies some of the core actuarial perspectives and attributes outlined above.

MADELEINE MATTERA
Head of Risk Advisory

Mobile: 0413 309 481

Email: madeleinemattera@pfsconsulting.com.au

JANE BYRNE
Director

Mobile: 0407 660 931

Email: janebyrne@pfsconsulting.com.au

DANIEL FRANK
Senior Consultant

Mobile: 0402 349 777

Email: danielfrank@pfsconsulting.com.au

SEAN WILLIAMSON
Principal

Mobile: 0408 133 123

Email: sean.williamson@pfsconsulting.com.au

PFS Consulting