CLYDE&CO

# Digital Security and Impacts of Regulation

## Underwriting Agencies Council

Alec Christie, Partner
Crystal Sanders, Special Counsel

20 September 2023

# Agenda

## What's out there, what's coming?

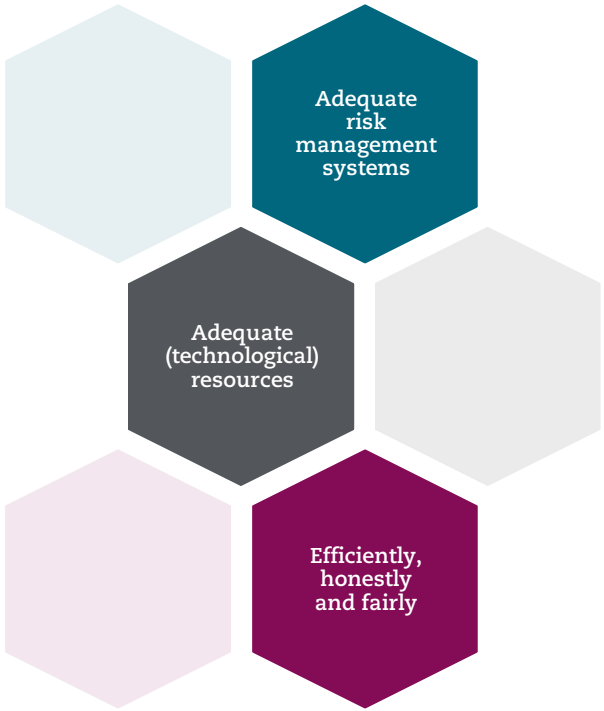
- Cyber security for AFSL holders
- SOCI Act considerations for service providers
- APRA CPS 234 and 230
- Changes to the Privacy Act and Regulator Attitudes
- Attorney-General's review of privacy and potential changes to cyber security
- Key takeaways
- Questions

# Cyber security for AFSL holders

## *ASIC v RI Advice Group Pty Ltd* [2022] FCA 496

- RI Advice was required to, but failed to:
  - identify the risks its AR's faced, including in relation to cybersecurity and cyber resilience
  - have adequate documentation, controls and systems in place that were adequate to manage those risks across its AR network

***"While it may be said that the public would expect the holder of an AFSL to have adequate cybersecurity measures … the reasonable standard of performance is to be assessed by … expert evidence before the Court, not the expectations of the general public."***



# SOCI Act considerations for service providers

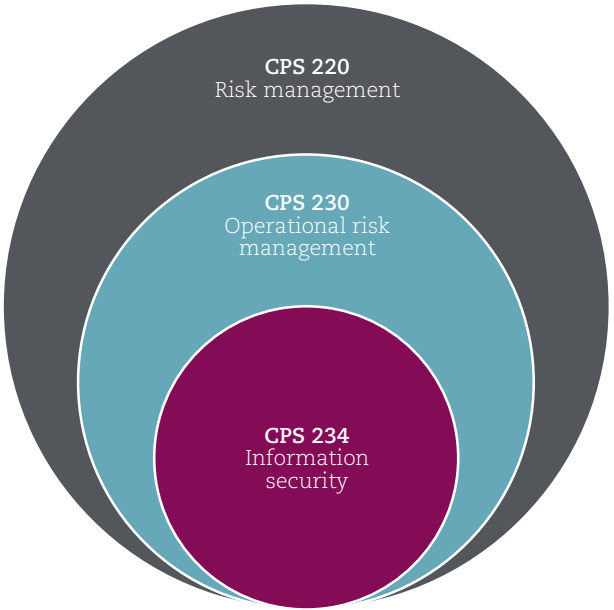
- What is the SOCI Act (and why should I worry about it)?
- Thresholds for Insurers
- Critical Infrastructure Assets for Insurers
- Key insurer Critical Infrastructure Asset obligations
- How can it affect me?
- What's next?

# APRA CPS 234 and 230

## Information security and operational risk management

*"Perhaps the most significant change introduced by [CPS 230] is the requirement for an end-to-end view of operational risk, with a focus on critical operations, including those performed by third and fourth parties. APRA-regulated entities will no longer need to simply be aware of their own internal operational vulnerabilities and have plans to mitigate them. From 1 July 2025, they must have the same level of understanding of their most critical third-party service providers – as well as their most critical fourth-party service providers. Those providers will need to be seen almost as a part of their own operation. An insurer may not be directly responsible for its website going offline when a network gateway fails, but it will be responsible for the outcome – which is the inability of customers to lodge claims or access other services."*

APRA Member Therese McCarthy Hockey speech at GRC2023 in Sydney (23 August 2023)



# Changes to the Privacy Act and Regulator Attitudes

- December 2022 changes to the Privacy Act passed in record time
- Increase of penalties for a serious “invasion” or repeated “invasions” of privacy from up to $2.2M to the greater of $50M and 30% of turnover for the greater of 12 months and length of the breach
- Change to the “Australian link” requirements (ie the extraterritorial application of the Privacy Act) - no longer requires any collection or storage of personal information in Australia
- Consequences of the recent high profile data breaches
- Convergence of application of various regulations and regulators’ thinking and approaches

# Attorney-General's review of privacy and potential changes

## They key proposals for privacy law changes

- The employee records' exemption:
  - starting with sensitive information
  - extending the APPs to private sector employees
- Vulnerable persons:
  - more consideration/acting in their interests
- 'Fair and reasonable' processing:
  - especially for sensitive information
- PIAs for 'high privacy risk' processing
- What is 'personal information' and 'sensitive information':
  - from 'about' to 'related to'
- De-identification and de-identified data:
  - higher bar as to what is de-identified
  - privacy protections extended to de-identified data
- Others
  - security
  - rights of the individual
  - the 'small business' exemptions

## What does it mean for you?

- All the new requirements and APPs will apply to you too
- Expect shorter timeframes to comply with changes
- Significantly more focus and obligations on sensitive information and vulnerable persons
- 'Improved' notifiable data breaches scheme
  - which will apply to employee data
  - a data breach involving sensitive or health information likely to be notifiable
- Security
  - increased information security obligations
  - especially for sensitive information
- Greater notification/consent obligations for collection, use and disclosure of sensitive and health information
- 'Improved' rights of the individual
  - 'right to be forgotten'
  - how to 'prepare' for this

# Key takeaways

- Adopt a systematic and proactive privacy approach across the entire data lifecycle
- Ensure collaboration between risk, IT, in-house legal and privacy teams with Executive/Board reporting
- Future proof your system by considering the key proposed changes and new developments (and how they might affect the project)
- Expect scrutiny from insurers and regulators
- Be prepared to demonstrate, and participate in testing to prove, your cyber security capabilities


Any questions?

# Key contacts

Alec Christie
Partner
t: +61 2 9210 4510
alec.christie@clydeco.com

Crystal Sanders
Special Counsel
t: +61 2 9658 2847
crystal.sanders@clydeco.com

# Thank you.



Clyde & Co LLP

www.clydeco.com