Public Consultation on ‘Strengthening operational risk management’ Prudential Standard CPS 230 Operational Risk Management

SUBMISSION

AUSTRALIAN INFORMATION SECURITY ASSOCIATION

COVERING LETTER

21.10.2022

The Australian Prudential Regulation Authority (APRA)
E-submission via PolicyDevelopment@apra.gov.au

Dear Policy General Manager,

Re: Public Consultation on 'Strengthening operational risks management – CPS 230 (Draft)

We have attached a submission on the Public Consultation on '**Strengthening operational risks management - Prudential Standard CPS 230 Operational Risk Management**,' from our perspective as the peak professional body for information security and cyber security in Australia.

Thank you for the opportunity to contribute our views and your consideration. Please do not hesitate to contact Eugenia Caralt, Michael Trovato, or myself if you would like clarification of any of the comments made in this submission.

Sincerely,

Damien Manuel
Chairperson, AISA

Email: damien.manuel@aisa.org.au
Mobile: +61 439 319 603

INTRODUCTION

The Australian Information Security Association (AISA) champions the development of a robust information security and privacy sector by building the capacity of professionals and advancing the cyber security and safety of the Australian public as well as businesses and governments in Australia. We welcome the request for submissions in response to Public Consultation on the draft 'Prudential Standard CPS 230 Operational Risk Management'.

Established in 1999 as an independent not-for-profit organisation and charity, AISA has become the recognised authority and industry body for information security, cyber security and security-related privacy matters in Australia. AISA caters to all domains of the information security industry with a particular focus on sharing expertise from the field at meetings, focus groups, and networking opportunities around Australia.

AISA's vision is for a world where all people, businesses and governments are educated about the risks and dangers of invasion of privacy, cyber-attack and data theft, and to enable them to take all reasonable precautions to protect themselves. AISA was created to provide leadership for the development, promotion and improvement of our profession. AISA's strategic plan calls for continued work in the areas of advocacy, diversity, education and organisational excellence.

This submission represents the collective views of over 9,500 cyber security, information technology and privacy professionals, allied professionals in industries such as the legal, regulatory, financial, and prudential sector, as well as cyber and IT enthusiasts and students around Australia. AISA members are tasked with protecting and securing public and private sector organisations including national, state and local governments, ASX listed companies, large enterprises, NGO's as well as SME/SMBs across all industries, verticals and sectors.

AISA proactively works to achieve its mission along with its strategic partners. These include the Australian Institute of Company Directors (AICD); the Australian Security Industry Association Limited (ASIAL); Australian Women in Security Network (AWSN); Cyrise; grok academy; International Association of Privacy Professionals (IAPP); the Risk Management Institute of Australia (RMIA); the Oceania Cyber Security Centre (OCSC); untapped; as well as international partner associations such as ISACA; (ISC)^2; and the Association of Information Security Professionals (AISP). AISA also works closely with both federal and state / territory governments to ensure a robust and safe sector.

It is AISA's hope that our views will be considered. In this submission, we have covered matters of particular interest to AISA at this stage of the consultation.

EXECUTIVE SUMMARY

AISA welcomes the opportunity to provide feedback on the draft 'Prudential Standard CPS 230 Operational Risk Management'. We offer our perspective as a members-based association, and as advocates for enhancing responsible information security standards and initiatives that in turn will address systemic challenges, improve digital trust and enhance resilience in a cyber world.

Draft CPS 230 forms part of the broader APRA project to review and update APRA's prudential framework in respect of qualitative management of operational risk across all APRA- regulated industries. To do so, APRA has leverage from international peers' approach and guidance such as the Prudential Regulation Authority (PRA) in the UK. AISA understand that once in force, CPS 230 and CPS 234 Information Security (unchanged) will form the new operation risks management framework.

AISA acknowledges the essential role of APRA in developing and enforcing robust prudential frameworks to provide financial safety and system stability. In the current landscape, where organisations across Australia are still dealing with the consequences of a global pandemic, more frequent natural disasters, complexities in the supply chain due to international war conflicts and recent nation-wide data breaches, calls for refocusing the importance of cyber security and organisational resilience across the financial services industry is paramount.

APRA's new draft CPS 230 standards looks to not only improve operational risks practices, but bring together related concepts in relation to effective internal controls monitoring, readiness to deliver critical operations during periods of disruption, and management of risks associated with services providers.

APRA does not see operational resilience as something novel or separate from operational risk management. It is the outcome of prudent operational risk management, and it is an extension of business continuity management that is reinforced by sound crisis management and communication strategies. What is expected from organisations is not all novel. Having said that, the devil is in the detail, as the new draft represents a game changer on how APRA governed entities may have developed business continuity plans to date. These changes will impact technology procurement and will no doubt multiply in numbers the list of service providers and report requirements. As such, we envisage that the amount of work required to be compliant with the proposed requirements as of January 2024 will be substantial due to the challenge of meeting the proposed timelines and the significant investment required.

APRA initiated consultation on updating its requirements for operational resilience in 2018, with the release of a discussion paper and draft prudential standard on information security management. The discussion paper in 2018 outlined three policy options for developing and updating prudential standards and guidance on operational resilience[1]**. As APRA noted at that time, its preferred approach was a - stepped approach – and to prioritise information security given the heightened risk in that area.** Under this option, APRA would continue to prioritise information security management and introduce prudential requirements[2] on information security, and then develop standards and guidance for operational risk management more broadly. **AISA supports APRA's approach to date and recommends[3] to continue completing CPS 234 independent assessment and secure cyber resilience foremost. Further, AISA agrees with APRA and advocates that boards have a key role to play.**

However, AISA would like to comment that draft of CPS 230, is one of several frameworks either under review or already in force that cannot be considered in isolation, such Privacy Act 1988 (Cth), Corporations Act 2001 (Cth), Australian Consumer Law and of course the amendments to the Security of Critical Infrastructure (SOCI) Act 2018 (Cth), which in turn will assist APRA regulated entities to strengthening operational resilience. AISA previously offered a submission to the Department of Home and Affairs in relation to strengthening Australia's cyber security

[1] https://www.apra.gov.au/information-security-requirements-for-all-apra-regulated-entities
[2] https://www.apra.gov.au/sites/default/files/cpg_234_information_security_june_2019_1.pdf
[3] https://www.apra.gov.au/news-and-publications/improving-cyber-resilience-role-boards-have-to-play

regulations and incentives. Although, Government response to the submission has yet to be released, our view is that if timings align with the final issue of CPS 230, APRA should consider its outcomes.

Observations of particular interest from AISA are listed below:

Business Continuity Plans re-write

Operational resilience requires an end-to-end business process view, centred on critical operations that cuts across various lines of business, including technology and data. AISA recognises that the draft standard, represents an opportunity for breaking internal silos that may have been in place ensuring technology and information security professionals have a seat at the table while developing and testing business continuity plans.

Having said that, the draft may represent significant challenges as it provides a list of critical operations to ensure consistency across the industry. The consequence AISA observes is that the new proposed definition, may require organisations to revisit how business continuity plans have been completed to date (i.e., by division or teams – (vertical) versus end-to-end service (horizontal)). As such significant re-drafting may be needed before plans are ready for testing. If this is the case, timelines proposed by APRA may not be archivable as organisations will need to revisit their stakeholder engagement approach as part of the business continuity lifecycle used to date and possibly also the tools.

In the situation where APRA may set the tolerance level for a regulated entity (or class of entities), AISA appreciates that a common baseline and expectation for consumers would be prudent (especially in an environment of open banking), but those tolerance levels need to be advised early in the adoption of CPS230 to avoid confusion and potential delays in implementation.

The cyber security skilled gap and lack of standardised accreditation

AISA champions the development of a robust information security sector by building the capacity of professionals in Australia and advancing the cyber security and safety of Australian public as well as businesses and government in Australia. This month, as part of the Australian Cyber Conference 2022, also known as CyberCon, in her opening speech, The Hon Clare O'Neil MP said:

"*The new Government in Australia has made the decision to have a cyber security minister because we want to elevate this issue to the level of importance that it so clearly is for Australia business, for Australia citizens and very much for our nation. Cyber is everything and it is everywhere. A resilient cyber ecosystem is going to be fundamental to our country's future. Cyber security underpins economic growth both here in Australia and across our region more broadly. It provides confidence in the services and infrastructure that enable business activity. It supports our economy and it enables our way of life.”*

AISA applauds the announcement but is also raises the following statistics of concern that APRA entities will have to confront:

The severe shortage or accessibility of job-ready cyber security and technology focused risk professionals will remain a key challenge. It is estimated that Australia may need around 30,000 additional cyber security workers for technical as well as non-technical positions by 2026. Growth is not sufficient to meet demand.[4] While there are challenges to solve at both the supply (education) and demand (hiring / employer) sides it is evident that remediation will take many years while the cost of obtaining and retaining cyber security, cloud and technology risk staff will continue to increase.

[4] Data raised by The Upskilling and Expanding the Australian Cyber Security Workforce research report from CyberCX September 2022.

Support for industry accreditation is mixed and not sufficiently supported by industry leaders. Recent AISA Research into Cyber Security Accreditation in Australia [5] indicates that: (i) support for industry accreditation is mixed. Only 53.1 % of respondents support accreditation of the sector to ensure a base level of qualification and standard; and (ii) Industry leaders from Executive Advisory Board for Cyber (EABC) see accreditation of the cyber sector as unnecessary and complex to be inclusive. In addition, hiring managers consider a candidate's aptitude, attitude and work experience to be the most important when making hiring decisions. Industry certifications and educational background are deemed much less important when recruiting cyber security staff.

AISA acknowledges that a holistic approach for skilled cyber security work force is required to address market complexities and existing challenges across the industry. AISA urges that APRA will consider the need for **detailed succession plans** for key security roles and the transition of "institutional knowledge" in order to support resilience and compliance of the proposed new framework by January 2024 and beyond.

Operational risks management - The shared risks landscape

We are witnessing how data breaches directed outside an APRA regulated entities, have a direct impact to the financial sector and how the financial sector can be called upon to combat cybercrime[6]. Interconnectivity and dependencies on material service providers will not go away. As such, draft CPS 230 is increasing risk management requirements and APRA regulated obligations in relation to supply chain. However, it is important to acknowledge that the definition of materiality in relation to service providers will vary greatly from entity to entity and AISA recommends APRA works closer with organisations to define suppliers who actually are critical, highly linked or have access to large customer data sets, are appropriately classified as material.

AISA recommends APRA to consult the Commonwealth Risks Management Policy [7] and consider the definition of shared risk and consider the benefit of its inclusion as an element of the entities risks management framework and service providers policy.

According to the Department of Finance, shared risks are those risks extending beyond a single entity which emerges from a single source and impacts interrelated objectives of entities. A collaborative approach to managing shared risk is required to: identify accountability, nominate transparent roles and responsibilities, define risk appetite boundaries, and seek agreement between all parties. This may require extended application of CSP 234 to supply chain entities of all industry types across several verticals outside of financial services. Additional delays managing the risks of fourth parties may be encountered due to contractual uplift requirements with service providers.

Further, the potential toxic combination of big data, cloud, Application Program Interfaces (APIs) and third-party apps via Open Banking or other data sharing regimes should be called out in the draft.

[5] https://www.aisa.org.au/common/Uploaded%20files/PDF/Surveys/2022/AISA%20Accreditation%20Survey%20Report.pdf
[6] Optus data breach: an update for APRA regulated entities | APRA
[7] https://www.finance.gov.au/government/comcover/commonwealth-risk-managment-policy

About the Lead Authors

Michael Trovato – AISA Board Member, MAISA, GAICD, CISA, CISM, CDSPE

Mike Trovato joined IIS in 2018 with over 40 years' experience in consulting and financial services in Australia, Asia Pacific, and the USA. He is a cyber security, privacy and technology risk advisor to boards, board risk committees, and executive management.

Mike focuses on assisting key stakeholders with understanding the obligations and outcomes of effective privacy and cyber security. This includes solving an organisation's issues with respect to regulatory, industry, and company policy compliance and to protect what matters most in terms of availability, loss of value, regulatory sanctions, or brand and reputation impacts balanced with investment.

At IIS, Mike has led over 100 privacy and security governance, risk, and compliance client engagements across government, health care, education, retail, financial services, and technology sectors. He has also advised clients about the direct impact of cyber security on privacy and data protection and how to provide greater resilience to assure better organisational outcomes.

Mike also serves as ICG's Global Cyber Practice Leader and IIS is an ICG Affiliate. Prior to joining IIS, he was the Founder and Managing Partner of Cyber Risk Advisors. Before then, he was Asia Pacific, Oceania and FSO Lead Partner EY Cyber Security; GM Technology Risk and Security for NAB Group; a Partner within Information Risk Management at KPMG in New York; and has held financial services industry roles at Salomon Brothers and Mastercard International. At EY, Mike was responsible for creating the largest, sustained "Big-4" cyber security practice, deploying Privacy and Data Protection solutions, and building the Melbourne Advanced Security Centre (ASC), specialised in attack and penetration testing.

As the NAB's first Group Technology Risk and Security GM, Mike was responsible for risk assessment, strategy, and the security program with a budget of AU$6 million, 11 direct reports and 40+ team members. He focused on enhancing technology risk and security governance, functional security analysis capabilities, and establishing key regulatory and compliance activities.

Mike is a Graduate of the Australian Institute of Company Directors (GAICD), Member Australian Information Security Association (MAISA), an AISA Board Member, ISACA Melbourne Chapter Board Member, Member of National Standing Committee on Digital Trade.

Mike's professional credentials include being a Certified Information Systems Manager (CISM); Certified Data Privacy Solutions Engineer (CDPSE); and Certified Information Systems Auditor (CISA). He is also a member of the International Association of Privacy Professionals (IAPP) and is an ICG Accredited Professional. He has an MBA, Accounting and Finance and BS, Management Science, Computer Science, and Psychology.

Mike is the co-author of The New Governance of Data and Privacy: Moving from compliance to performance, Australian Institute of Company Directors, November 2018.

Eugenia Caralt – MAISA, AFBCI, CISA, CDPSE

Eugenia Caralt joined IIS in 2018 and has over 20 years' experience in organisational resilience, crisis management, information security, and privacy. She is interested in helping clients develop mid-to-long-term performance strategies achieve their desired organisational outcomes while enhancing its operational resilience. She has extensive experience and skill in helping organisations prepare for and respond to significant business disruption and to thrive as a result.

Eugenia has been leading privacy and security engagements across the education, health, critical infrastructure, non-for profit and government sectors. Recent client engagements include:

- Supporting a NT Government agency to response to a data breach impacting personal information of vulnerable groups.
- Providing addition support to an acting CISO for a critical infrastructure provider and responding to the Ukrainian – Russian war threat and supporting the uplift efforts to enhance cybersecurity resilience.
- Uplifting the level of maturity of privacy programs in particular for humanitarian non-for profit, retail and education sectors.
- An independent review of an organisation in response to an enforceable undertaking from the Office of the Australian Information Commissioner.
- Supporting a long-term data breach response and recovery as part of a multi-disciplinary team for the NSW Government for a major cyber incident, and PIA to support for Service NSW (SNSW) application for a Direction under s 41 of the Privacy and Personal Information Protection Act 1998 (NSW) (PPIP Act).
- Assisting clients with strategic privacy and security advice and thought leadership.

Prior to join IIS, Eugenia worked in France, Spain and the UK on complex IT and telecommunications projects. Eugenia worked for EY IT Risk and Security Advisory for more than 10 years and then joined Colt Technology Services in Europe where she was the Group Head of Business Continuity over a decade. Returning to Australia in 2017, she worked in the NBN Co Risk & Resilience team.

Eugenia holds a Law Degree from the University of Barcelona, a Master in Law from ISDE Business School and a Post Master in Technology Law from ESADE Business School.

Contributors

Joshua Craig, AISA Board Member, MAISA, MIT, CISM, CISSP, GIA(Cert)

Joshua Craig has worked in Information Security, Risk and Compliance for over 18 years in the Australian banking industry with expertise in both commercial and technical sectors.
Joshua has been leading cloud, technology and security risk teams across diverse services in the banking sector with particular focus on:

- Control environments for heightened and extreme inherent risk workloads
- Cloud regulatory requirements for 28 International Banking jurisdictions
- Cloud risk management processes and assurance
- Board engagement and uplift on cloud and security
- Security, cloud and technology risk management skills training programs

Joshua holds a Master in IT as well as industry qualifications such as CISM and CISSP, and currently volunteers as a Director for the Australian Information Security Association.

Damien Manuel – Chairperson, AISA and Adjunct Professor

As an experienced, results-driven ICT business professional, Damien Manuel has more than 25 years of experience specialising in cyber security, business governance, compliance and risk management.

Damien is the Chairperson of the Australian Information Security Association (AISA), a not-for profit organisation which aims to improve Cyber Security in Australia at a Government, Industry and Community level. Damien also provides advice to several boards both in Australia and internationally. He is a well-known leader in the Australian cyber security sector and works closely with both federal and state / territory governments.

In his former role as the Chief Information Security Officer (CISO) for Symantec Australia and New Zealand, Damien worked with senior executives in the region to align security architectures to industry best practices. He also worked as a senior information security governance manager and later as an enterprise IT and security risk manager at National Australia Bank (NAB), where he was responsible for managing the bank's information security standard globally. He also held senior roles at RSA, Telstra and Melbourne IT and is currently on CompTIA's Executive Advisory Committee.

Damien has supported CompTIA for over 14 years through the development of CompTIA Server+, CompTIA Network+, CompTIA Security+ and more recently the CompTIA Advanced Security Practitioner certification.

Damien's passion for making a difference motivated him to establish Information Technology community resource centres to improve literacy and skills in impoverished and disadvantaged communities in Kenya, Laos, Uganda and Cambodia.

Underpinning his experience is a diverse educational grounding ranging from the highest security, audit and governance certifications complemented by an Executive MBA with an international business focus.