All Actuaries Summit
New age, new actuary

11-13 June 2025, Sydney

CPS230 Operational Risk Management Industry Survey 2025

Prepared by Madeleine Mattera

Presented to the Actuaries Institute

2025 All-Actuaries Summit

11-13 June 2025

Table of Contents

Abstract

On 1 July 2025, financial services enter a new age with the commencement of CPS 230:*Operational Risk Management*. The requirements of this prudential standard reflect a paradigm shift in how operational risk and related issues are to be managed. The core requirement of resilience reflects the need to maintain critical services through disruption.

The success test of operational risk management is now the extent to which consumer expectations continue to be met under disruption scenarios.

A population of approximately 300 financial institutions are working to implement CPS230 by 1 July 2025 to comply with the requirements imposed by the regulator, APRA.

PFS Consulting has conducted an industry wide survey of APRA regulated financial institutions to take the pulse of the industry on issues around readiness, operational complexity, governance and risk management.

We hope to transform our work into an annual survey to provide objective data for the industry and help in building capacity – ultimately to help support the industry in protecting the interests of policyholders, depositors and members and in supporting the resilience of the Australian Financial Services Industry.

This paper supplements a paper on Operational Risk presented by my colleague Jules Gribble to the same audience[1].

Keywords: APRA, CPS230, CPG230, Critical operations, Culture, Disruption, Governance, Operational risk, Operational resilience, Risk culture, Risk management, Risk maturity, Service Providers, Business Continuity

1 Context

1.1 Environment

On 1 July 2025, Australian APRA regulated financial institutions all enter a new era with the commencement of Cross-Industry Prudential Standard 230: Operational Risk Management (CPS230), see CPS230. CPS230 is supported by CPG230, the accompanying Cross-industry Prudential Practice Guide, see CPG230. Note that CPS230 applies across all regulated financial services without distinction.

[1] Actuarial Outreach: Taming the Operational Resilience Hydra

All Australian Significant Financial Institutions (SFI's) are expected to fully comply with CPS230. On 30 June 2024, APRA's list of SFI's included 14 Approved Deposit Institutions, 4 General Insurers, 4 Life Insurers, and 24 Superannuation entities.

Non SFI designated financial institutions have some time relief on some topics until 1 July 2026 when they are then all also expected to fully comply with CPS230.

The introduction of CPS230 is not occurring in isolation. A global trend was initiated by the Bank of International Settlements (BIS) in its 2021 document Principles of Operational Resilience. See BIS 2021. Global take-up of the concept has been broad. See IIF 2024. In the EU, the Digital Operational Resilience Act (DORA) officially started in January 2023 with full compliance expected by January 2025. In the UK the FCA set out final rules for Operational Resilience in March 2021 (PS21-3) with full compliance expected by the end of March 2025. In Canada, OSFI publishes its operational resilience requirements (Guideline E-21) in August 2024 with full compliance expected by September 2026. Experience shows that implementing operational resilience requirements can be time consuming, resource intensive, and have far reaching implications. Australia's timetable may lag some others, but we can gain the benefit of reviewing other experiences.

1.2 APRA expectations

APRA places a high priority on CPS230. This is shown by statements in various speeches and APRA's current 2024-25 Corporate plan regarding importance of increasing the minimum standards for operational resilience through the implementation of CPS230 and the raising of industry standards on cyber risk management. Cyber risk is an operational risk, even if it has been singled out for special treatment.

APRA and other regulators routinely conduct industry wide "stress tests" designed to measure operational resilience in defined disruption scenarios.

Note the word 'minimum' in APRA's stated focus. In a regulatory environment where there is an 'at all times' expectation by supervisors it is perhaps foolhardy to only seek to meet only minimum requirements. Unavoidable and random business and environmental fluctuations will likely mean that at some time(s) minimum requirements will be breached. It is therefore prudent and expected by both supervisors and the wider community that minimum requirements are exceeded, perhaps significantly. To illustrate this, we observe that the capital ratios for both life insurers and general insurers, overall, are approximately 2. That is, these industries, on average, hold about twice as much capital as the minimum prescribed requirements.

Holding Capital is part of the answer.

Other questions financial institutions are being asked to consider include whether the capital held in respect of operational risk is sufficient, and importantly whether the organisation is resilient enough to continue to protect the interests of policyholders, depositors and members in disruption scenarios (Business Not As Usual or BnAU) as well as Business As Usual.

CPS230 introduces new concepts to the Australian Financial Services Industry:

- Material Service provider
- Fourth Party Service Provider

These concepts are aimed at promoting entity understanding of and accountability for the various entities who play a role in the value chain or supply chain, involved in delivering services to the policyholders, depositors and members.

The requirements of CPS230 are also aimed at "raising the bar" and uplifting the expectations of financial institutions in an environment marked by:

- Increased economic volatility
- Increased geopolitical instability
- Supply chain fragility – sometimes as a result of the above factors
- Disruption and innovation including emergence of generative AI and ESG concerns
- Heightened cyber security risks

1.3 Introducing the CPS230 Operational Risk Survey[2]

With the deadline for CPS230 to become effective rapidly approaching, PFS Consulting developed and undertook a survey to assess key aspects of readiness for CPS230 and gain insights into how financial institutions are approaching CPS230.

The survey in early 2025 was the first such survey and the PFS team look forward to conducting the survey annually, and evolving the question set to align with industry practice and APRA's supervision approach.

We used the well known Survey Monkey survey platform.

The survey consisted of 41 questions across the four domains of CPS230, being:

- Governance,
- Operational Risk,
- Critical Operations and
- Service Providers

The nature of questions included quantitative and qualitative response sets, with free text responses to enable additional information and subjective information such as attitudes, to be captured.

The survey audience consisted of:

- General Insurers
- Life Insurers
- Friendly Societies
- Superannuation Funds (APRA regulated)

Due to resource constraints we did not include in our survey:

- ADIs ie Banks & Credit Unions
- Private Health Insurers

We intend to expand the survey in future years to the entire population of APRA regulated financial institutions.

PFS Consulting takes this opportunity to extend our thanks to the entities who participated in the survey and we look forward to welcoming you back to the Survey in 2026!

2 Survey Results

Overview of survey response by sector:

SECTOR	NO OF RESPONSES
Life insurance	12
General insurance *Including Friendly Societies*	16
Superannuation	Less than 5[3]

The entities who submitted a response collectively accounted for a significant proportion of the known assets of the General Insurance and Life Insurance sectors respectively.

A total of 61 surveys were issued to entities who has consented to receive it, mainly to insurers and super funds with whom PFS had an existing relationship.

The survey was generally enthusiastically received.

A number of entities who were approached about the survey opted not to receive it, citing workload issues or in some cases availability of operational risk event data. The majority of those entities expressed an interest in accessing the results of the survey.

Out of entities who consented to receive the survey but did not complete it, the majority cited workload pressures.

We have sought to avoid presenting response data in a manner that could identify any particular financial institution or person.

For entities who provided a response to the survey, PFS has committed to providing each entity with a separate confidential report showing their entity's responses compared to the industry as a whole. We intend to commence preparing each entity specific report in June/July.

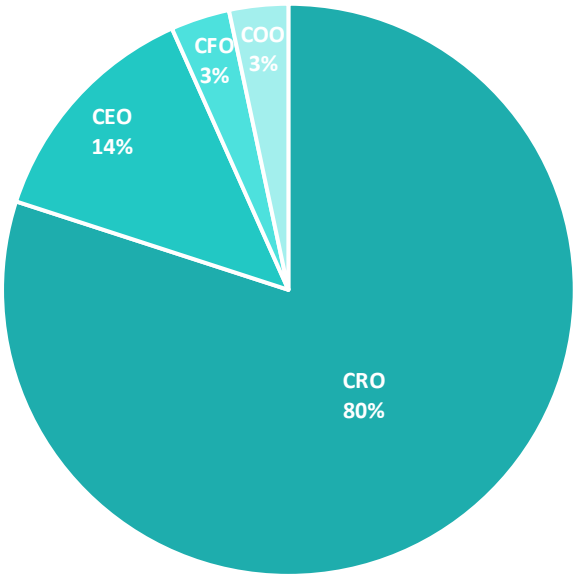
The raw survey data is reproduced at Appendix 1 for reference.

[3] The response rate for superannuation funds was low.
Anecdotal feedback attributes the response rate to the survey period coinciding with an unusually challenging period for super funds with a high profile cyber attack across numerous funds and consequential pressure on executive time and resources.
We have excluded super fund responses from the results where it is reasonably expected that the identity of a respondent organisation may be able to be inferred.

Questions 1-3 contain identifying data and contact information which has not been reproduced for confidentiality reasons.

Question 4:

Which role in your organisation (under FAR[4]) is responsible for the implementation of CPS230?



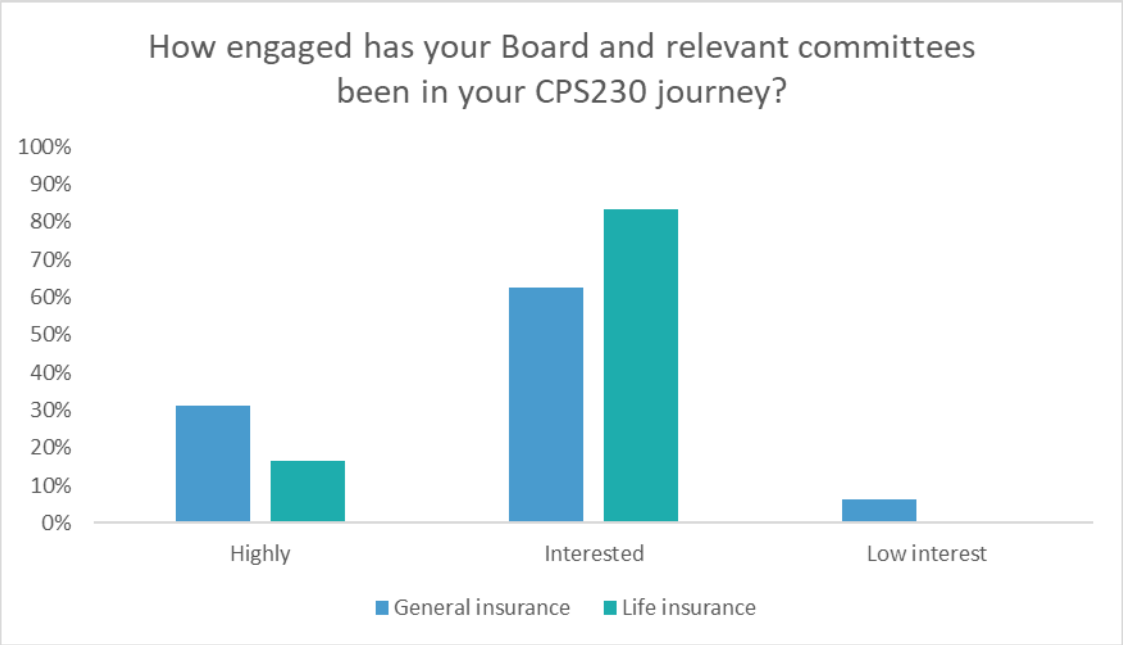
It is not surprising that the CRO has responsibility for the CPS230 implementation.

A total of 14% of entities have CPS230 under the leadership of the CEO -potentially indicating its enterprise wide importance.

[4] Financial Accountability Regime Act 2023, as amended from time to time, Minister Rules and Regulator Rules

2.1 Governance and Risk Culture[5]

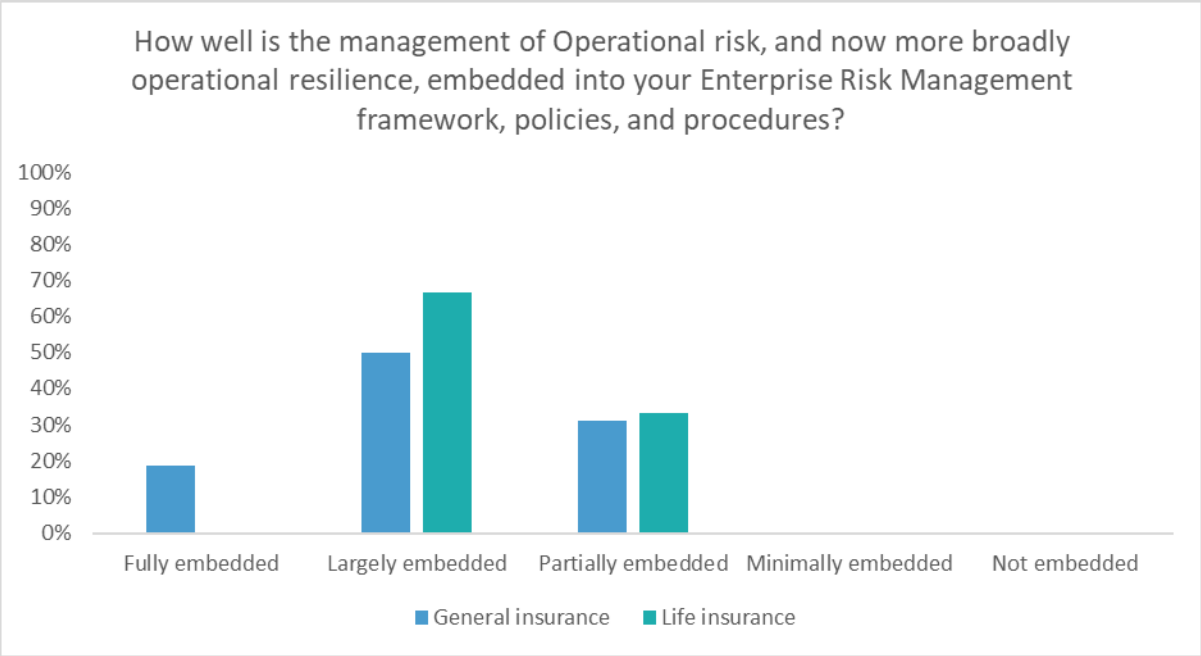
Question 5



It is pleasing to see the level of engagement by Board in the CPS230 journey. A small number of general insurer boards have a low interest in CPS230, potentially seeing it as a compliance exercise.

[5] These questions consider aspects of CPS230 paragraphs 20 - 23 inclusive, dealing with roles & responsibilities.

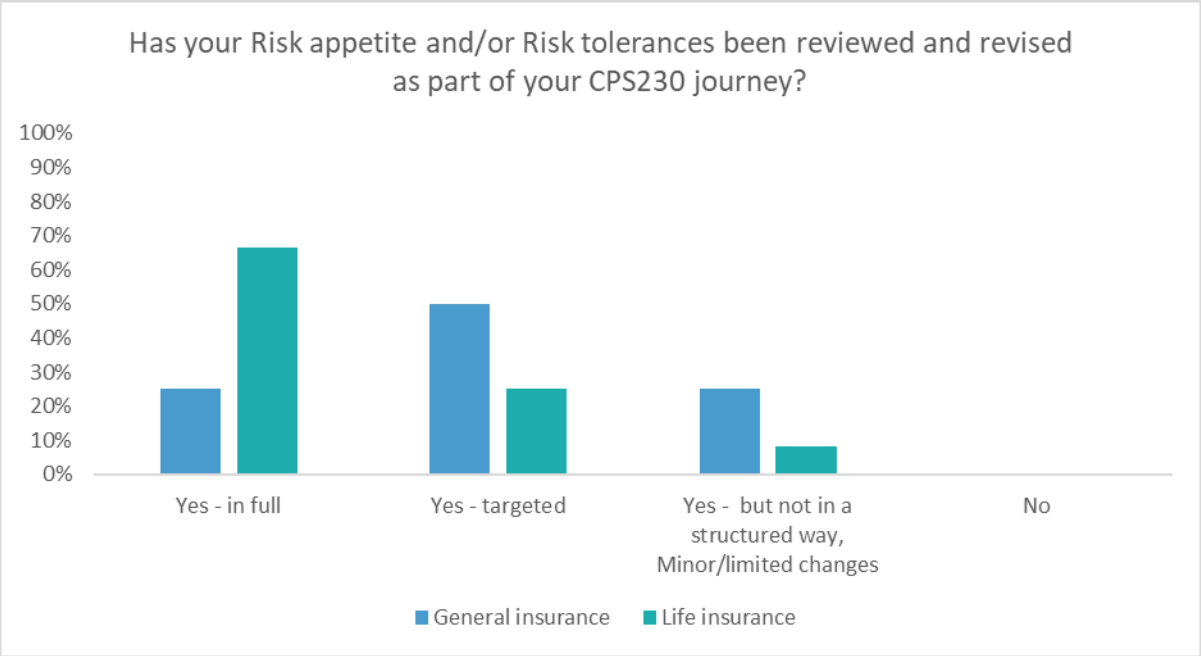
Question 6



The extent to which operational risk is embedded in the enterprise risk management framework may be subjective and also may be dependent on the entity's CPS230 journey.

Responses to a similar question in 2026 and future years may indicate progress to embedment.

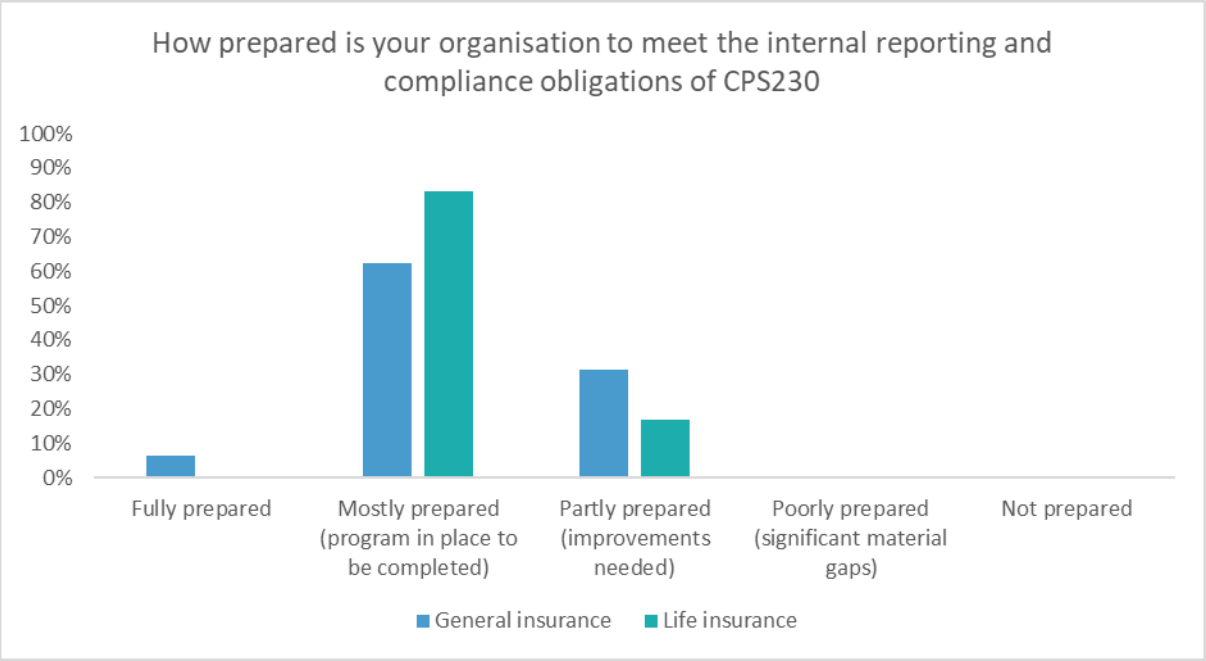
Question 7



Similar to the preceding question, the responses may be subjective and also may be dependent on the entity's CPS230 journey.

Responses to a similar question in 2026 and future years may indicate progress in refining risk appetite and tolerances.

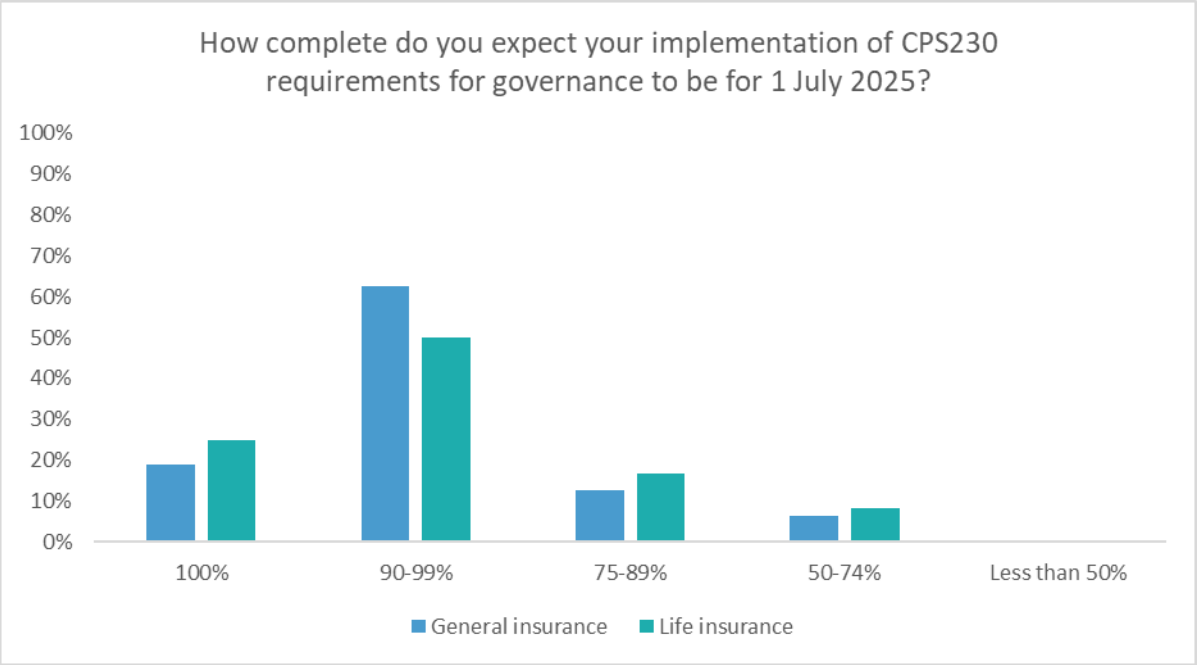
Question 8



This is a question about internal reporting and compliance obligations rather than CPS230 as a whole.

The responses indicate respondents see that there is considerable work still to be undertaken across GI & Life in the lead up to 1 July 2025.

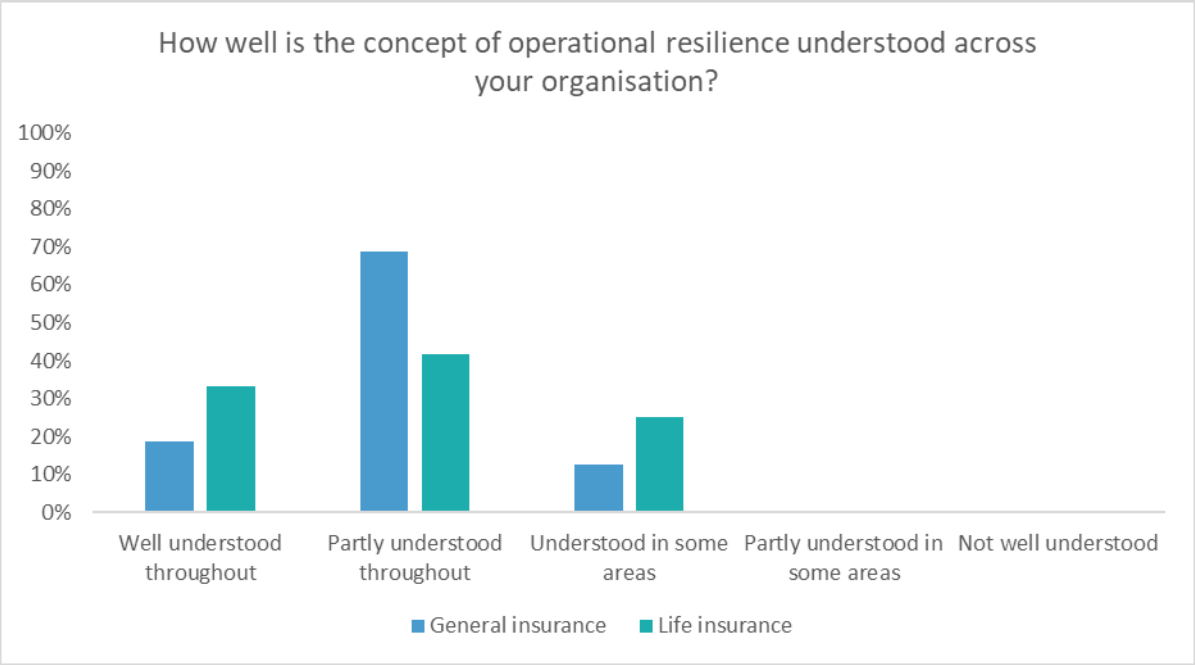
Question 9



In line with responses to the previous question, respondents see some work still to be done on the CPS230 Governance requirements.

Pleasingly, there are a significant proportion of entities who believe their governance is ready for 1 July 2025.

Question 10



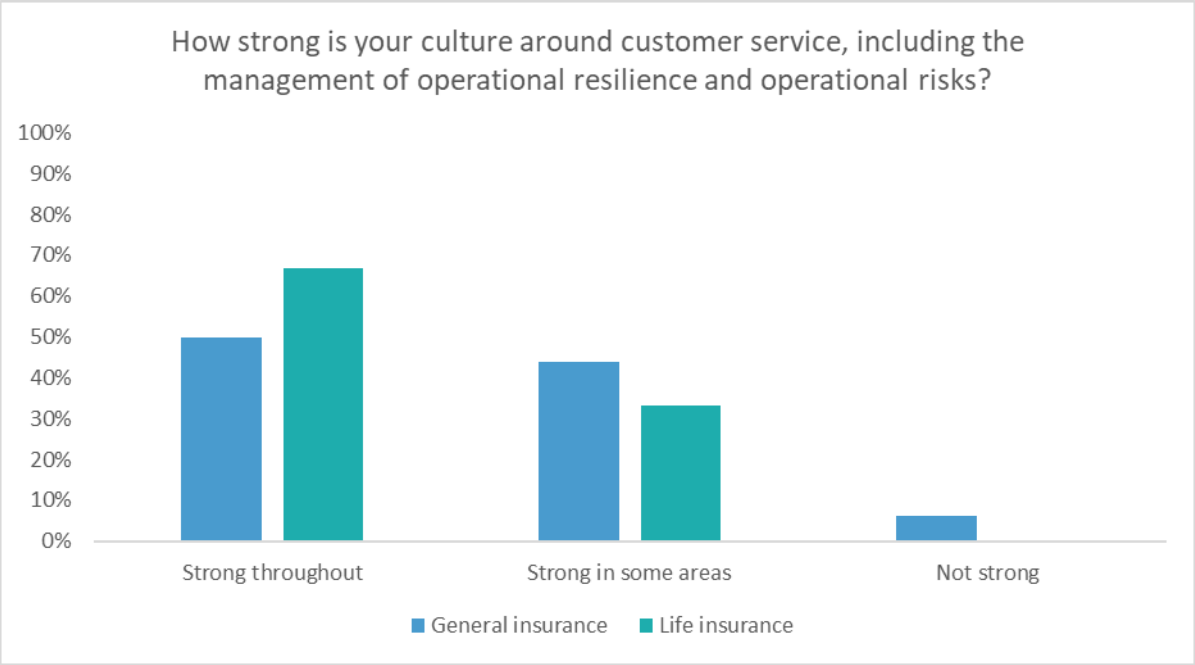
The concept of operational risk is not new however the need for CPS230 indicates APRA sees a need to raise the bar to ensure entities manage operational risk appropriately. The concept of operational resilience[6] is new in comparison – with the two terms often used interchangeably.

The level of understanding reported by respondents indicates the concept of operational resilience is not yet well understood industry wide.

Responses to a comparable question in 2026 may indicate progress in the level of understanding reported by the industry around operational resilience.

[6] Refer to Section 1.1 of this paper

Question 11

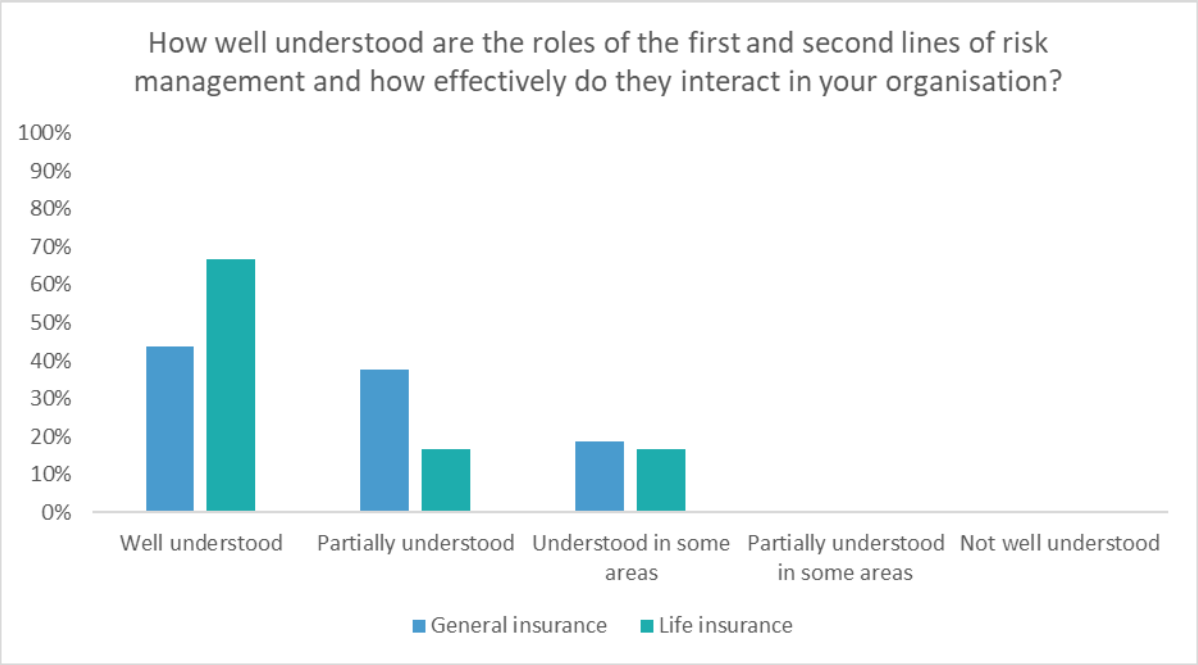


The results above are pleasing, demonstrating that financial institutions believe their customer focus is strong across all or part of their business.

PFS believes testing of operational resilience at an entity level can assist in validating the views reported by respondents.

APRA has not conducted an industry wide stress test involving insurers however such a test could provide useful data at the industry level and entity level.

Question 12



The Three lines of Defence (or Three Lines of Accountability) are far from new. It is surprising that over 50% of General Insurers and 30% of Life Insurers report "Partially Understood" or Understood in Some Areas".

Life Insurers report a better understanding of the Three Lines model General Insurers.

Question 13

Do you have further comments to add regarding Governance? (free text)

Selection of responses:

"Ongoing embedment and maturity is being actively pursued. We expect to continue to uplift with a sharp focus on risk maturity."

"We have a program of work in place to assist us be compliant by 1/7/25. We are on track to deliver this by the due date. Whilst it makes us compliant, we have additional work planned to enhance this compliance post 1/7/25."

"Increased Board oversight is a positive response generated by a small organisational structure"

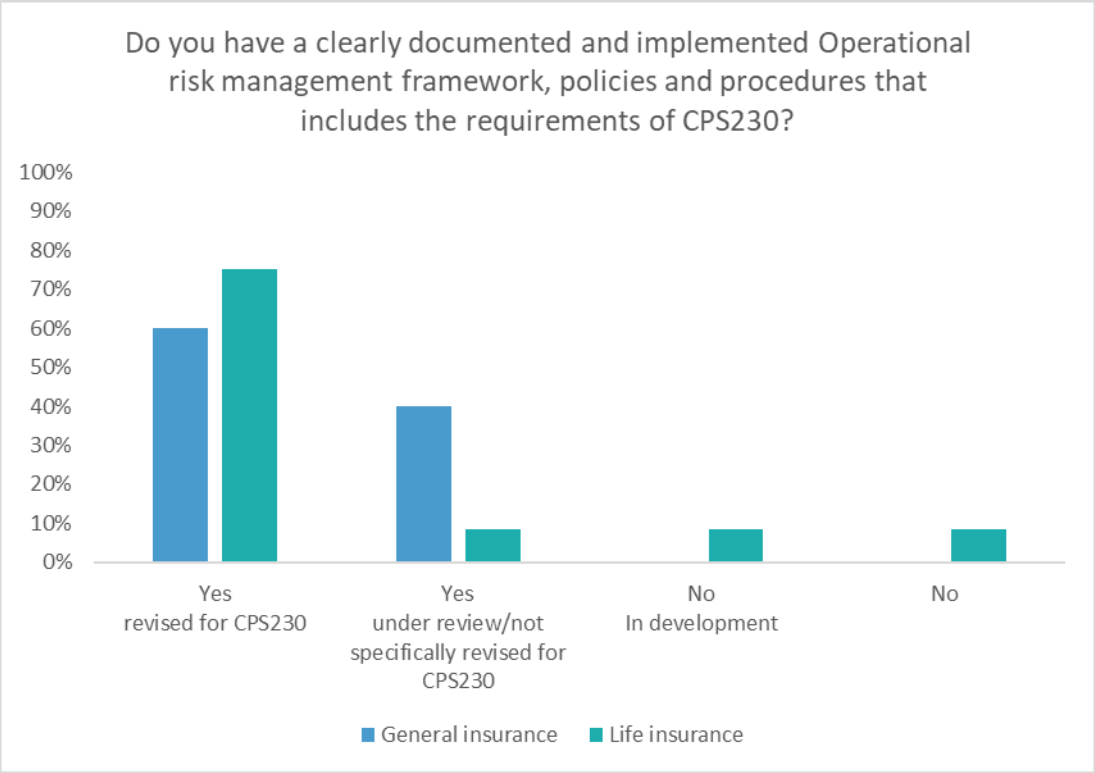
"Uplift in governance remains ongoing with key updates expected between now and 30 June including approvals of policy and framework updates and embedding training."

"The implementation of CPS 230 and FAR at the same time has led to a restructuring and repurposing of governance bodies"

"The challenge in a small organisation is to deliver the outcomes and comply with the provisions without creating a monstrous load of work."

2.2 Operational Risk[7]

Question 14



Entities are reporting significant progress with revised existing framework documents to make them CPS230-ready, although a significant proportion of insurers have substantial work to do pre 1 July 2025.

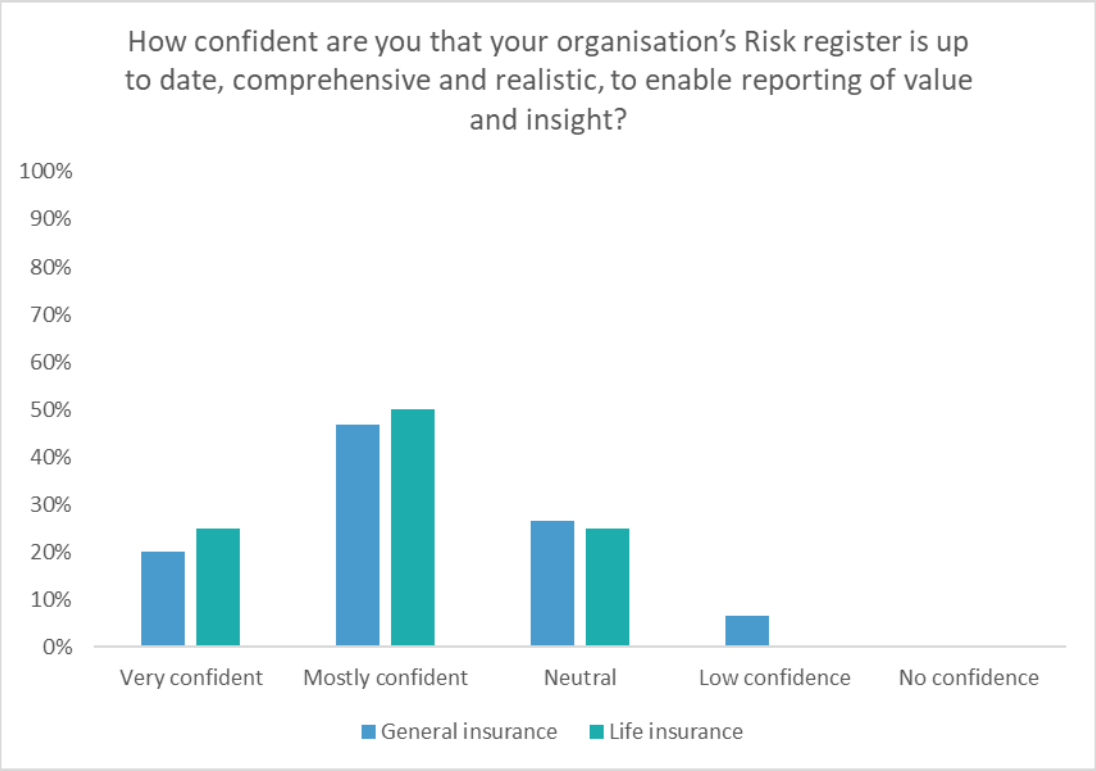
It is interesting to see a small proportion of Life Insurers reporting less progress than General Insurers.

[7] These questions consider aspects of CPS230 paragraphs 24 - 33 inclusive, dealing with operational risk profile, assessment, controls, and incidents.

Question 15

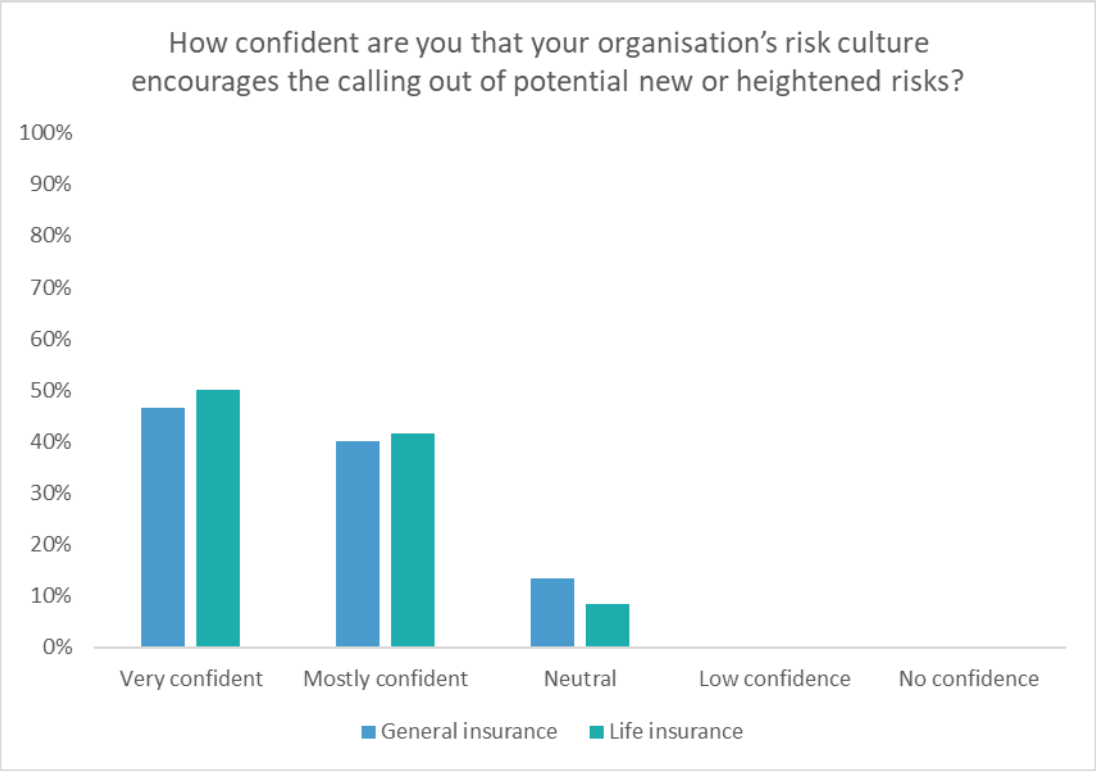
The level of confidence reported by respondents is pleasing.

Question 16



When comparing responses to Question 16 and 15, respondents are less confident in comprehensive documentation than in their ability to identify and manage operational risk.

Question 17

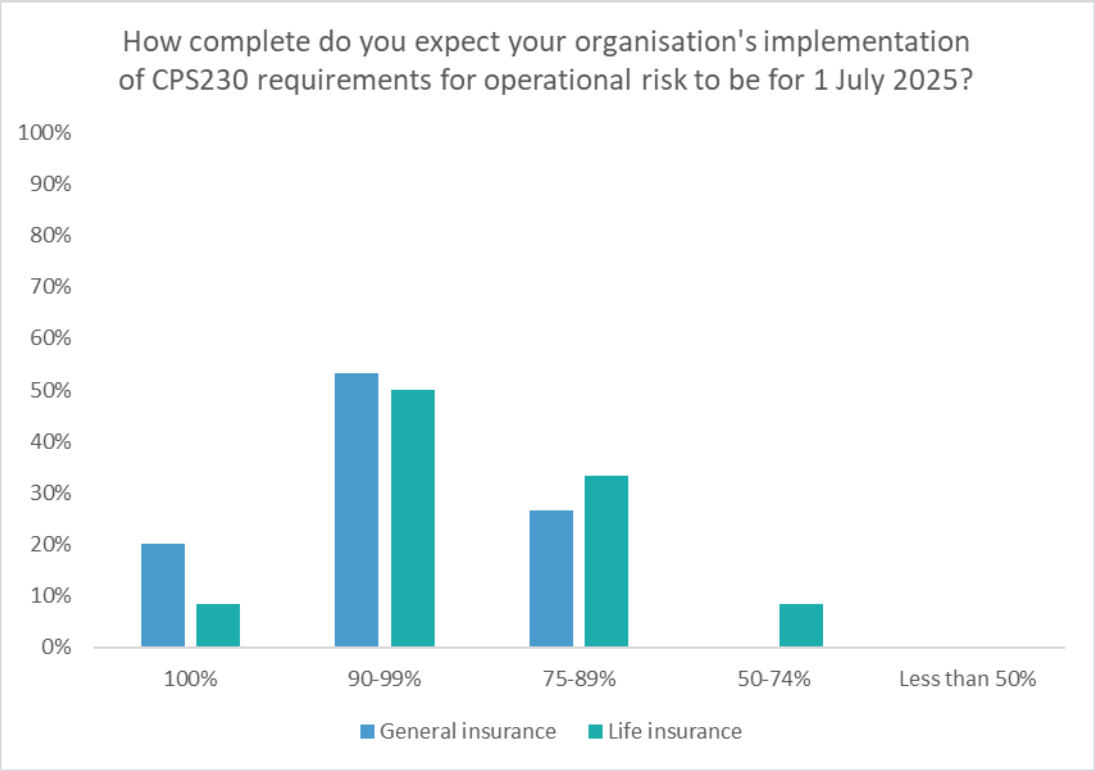


The level of confidence reported by respondents is very pleasing. PFS recommends respondents compare the responses to this question with their risk culture surveys and/or staff engagement surveys.

Question 18

The level of confidence reported in the responses to this question is pleasing, indicating that the overwhelming majority of financial institutions are focused on protecting the interests of customers such as policyholders.

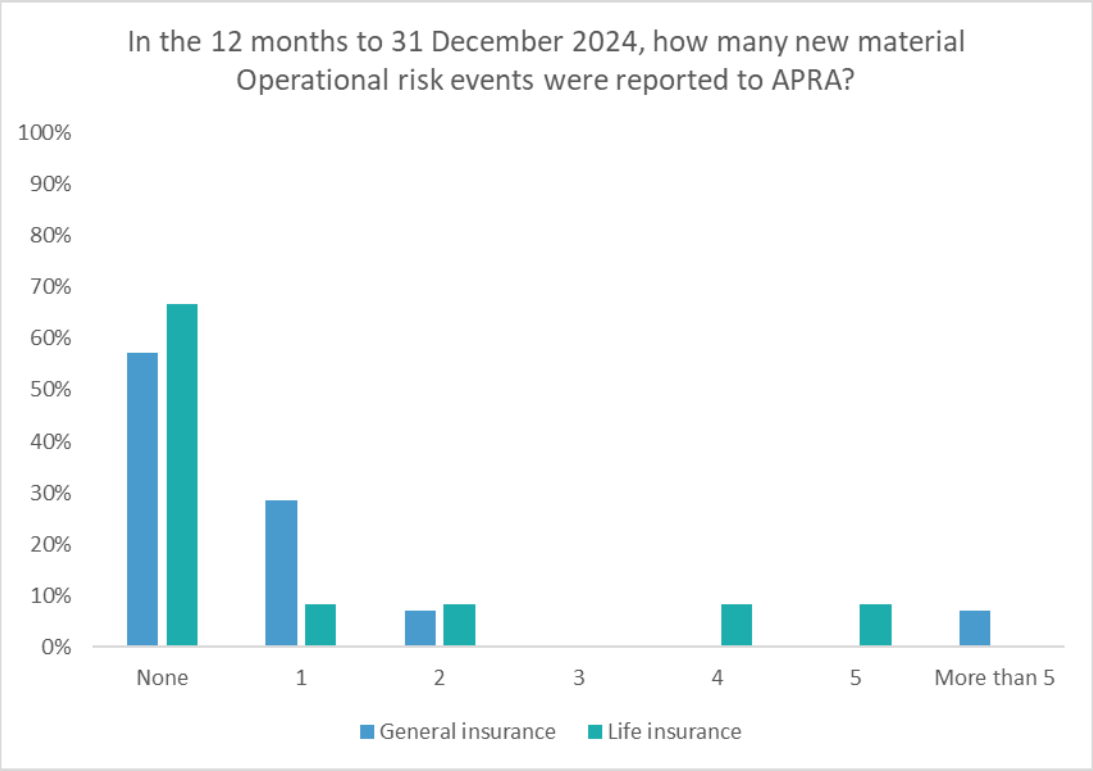
Question 19



The responses show an overwhelming majority of entities expect to be substantially compliant with operational risk requirements of CPS230.

Life Insurers responses indicate a lower level of confidence than General Insurers.

Question 20

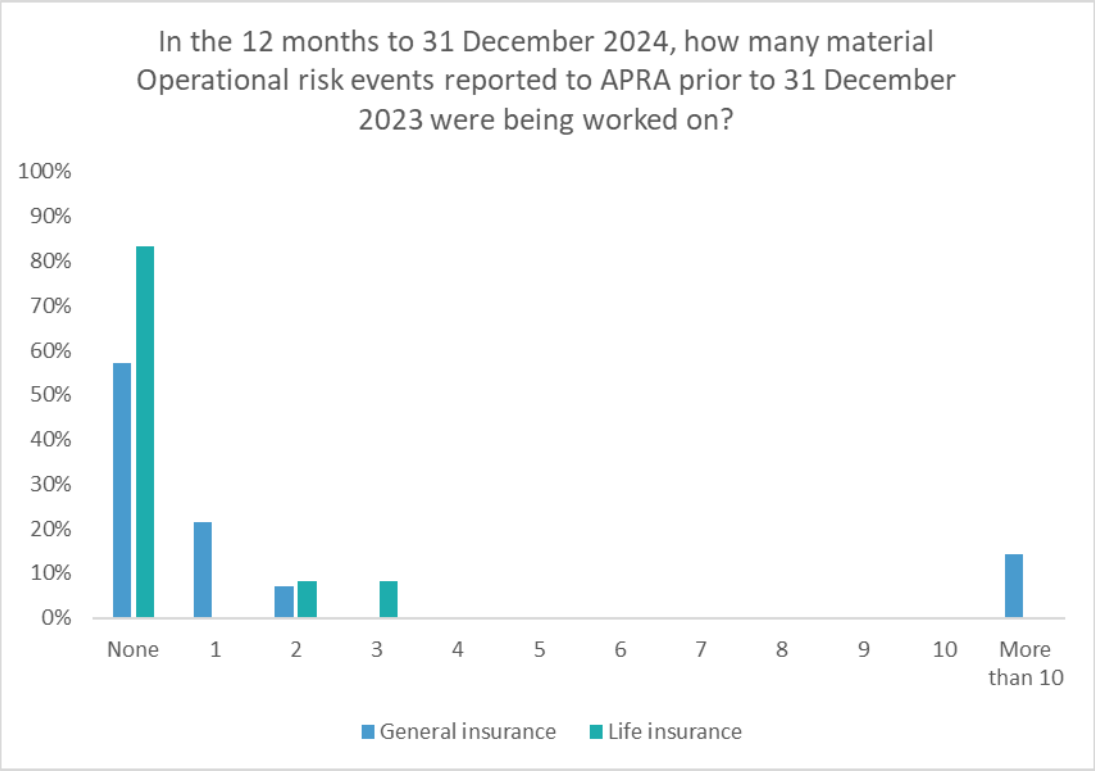


The majority of respondents report no new operational risk events.

However PFS recommend interpreting the results with caution as some respondents reported data issues and a history of not reporting operational risk events to APRA.

Post 1 July 2025, operational risk events are required to be reported to APRA within 72 hours of becoming aware of a material event. It may prove useful to compare responses to a comparable question in 2026 against the 2025 responses to this question.

Question 21

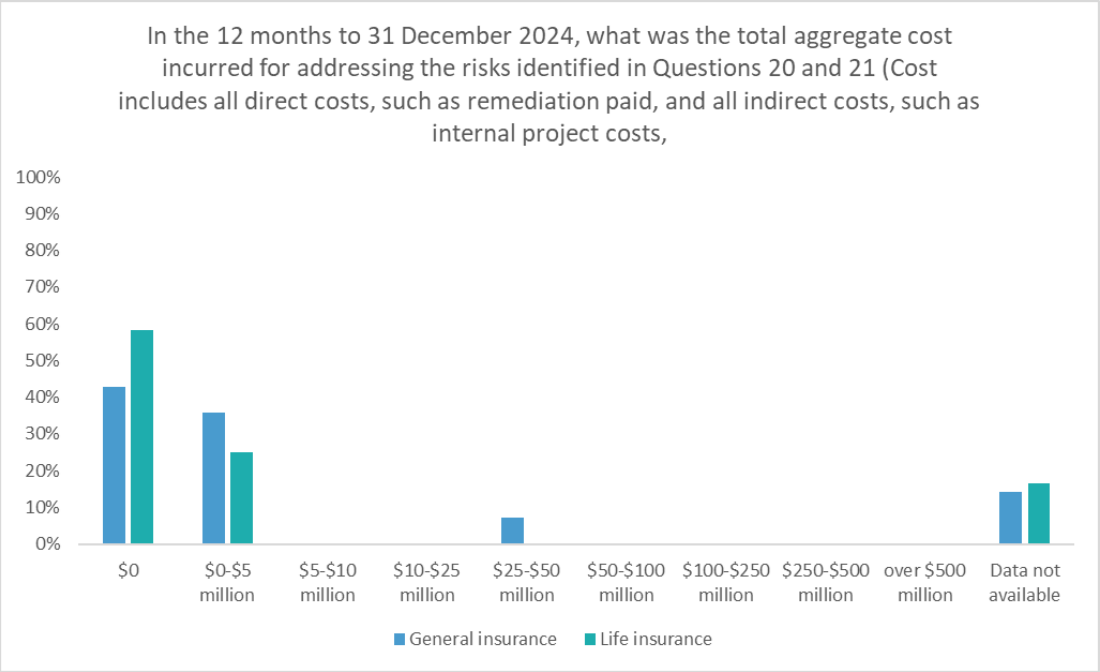


The majority of respondents report no operational risk events carried over from 2023 calendar year.

However PFS recommend interpreting the results with caution as some respondents reported data issues and a history of not reporting operational risk events to APRA.

Post 1 July 2025, operational risk events are required to be reported to APRA within 72 hours of becoming aware of a material event. It may prove useful to compare responses to a comparable question in 2026 against the 2025 responses to this question.

Question 22



The majority of operational risk events cost under $5million to remediate – including direct compensation to customers as well as legal, internal remediation programme costs and fines (if any).

PFS recommends interpreting the responses to this question with caution as several respondents reported data quality and availability issues.

It will be interesting to compare responses to a comparable question in a survey in 2026 as advances may have occurred in operational risk incident management and data governance.

Question 23

Do you have further comments to add regarding Operational Risk? (free text question)

Selection of responses:

"Heightened experience - focus on better capturing data and quantification of costs of op risk events. Changes to use of [op risk capital] noted and work in maturing this is on foot."

"As part of the implementation of CPS230, we revised our entire risk register. Updated material risks have been implemented / subject to final approval by the Board in May 2025, and are continuing to update operational risks through May to June 2025."

"We undertake a quarterly review of the risk profile and an annual deep dive, although additional work has been undertaken for implementation."

"Where operational risk is well understood, opportunity exist to refine the control environment, integrated business continuity plan and risk and control assurance."

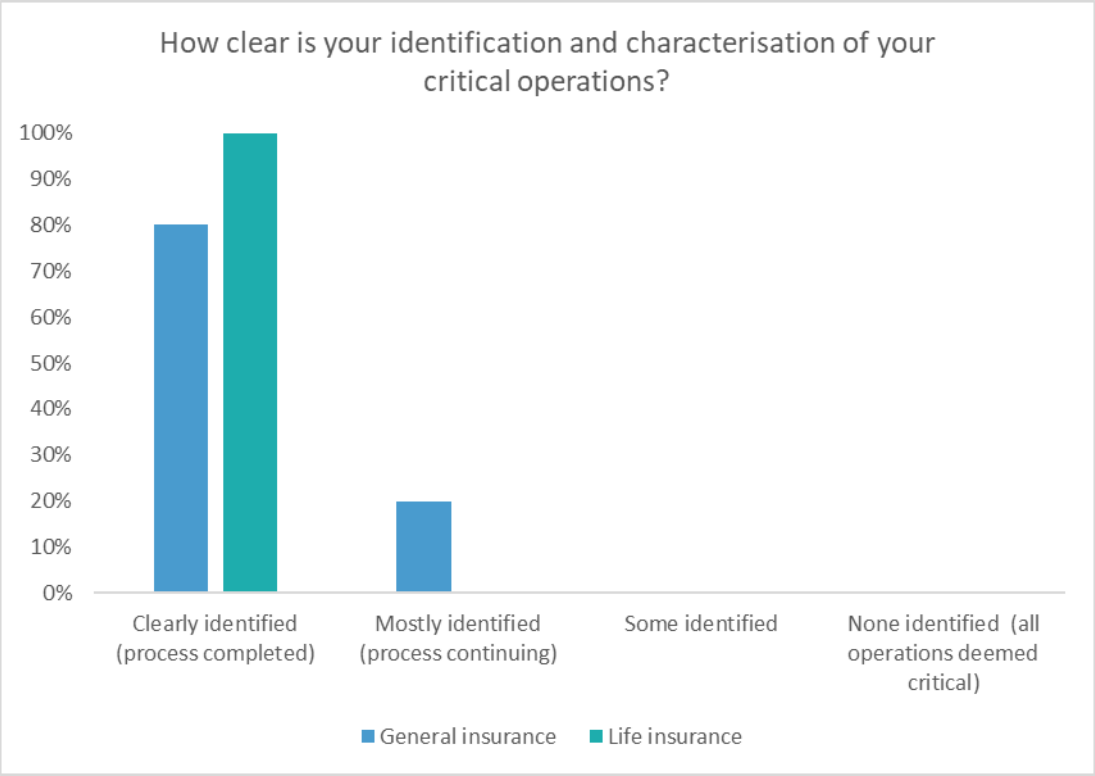
"Our company is small (47 employees) and simple. No operational risk incidents that occurred in this period had a material impact to financials or critical operations. "

"The elements of operational risk addressed by CPS230 have been embedded in the RMF for many years.

For questions 20 and 21 the reported risk events were not formal notifications."

2.3 Critical Operations[8]

Question 24



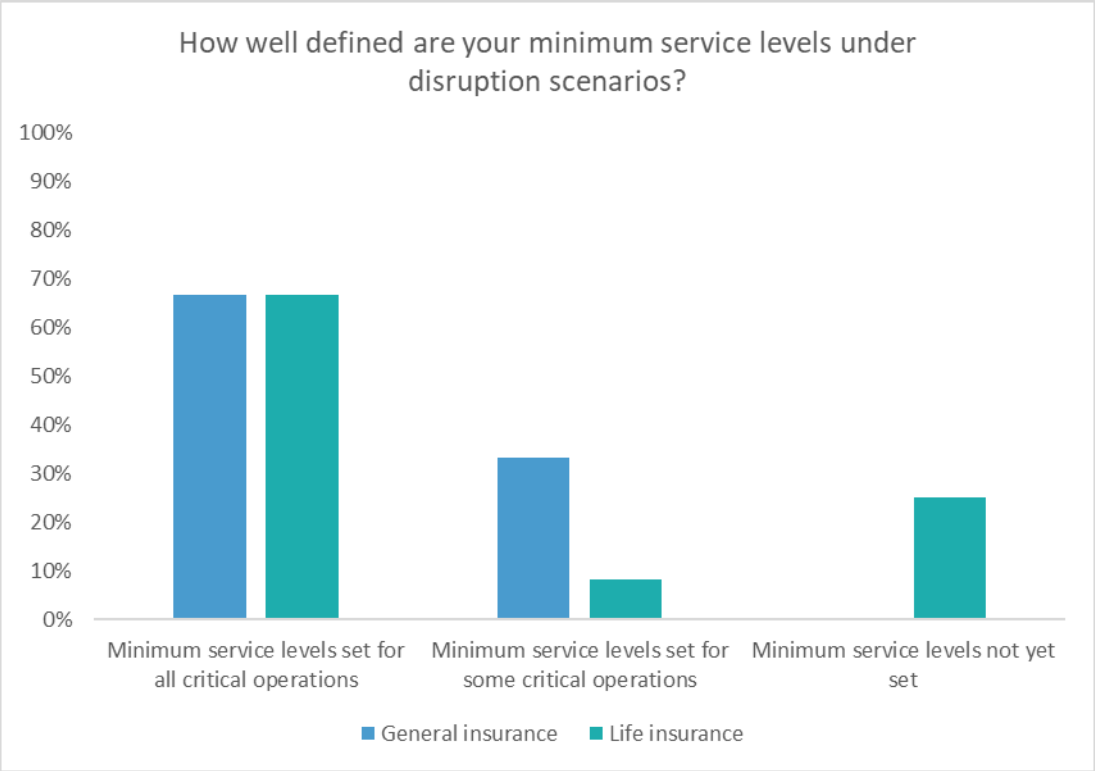
It is pleasing – although not surprising to see respondents report an advanced stage of identification and characterisation of critical operations.

In PFS' experience this is one of the very early stages of CPS230 compliance, providing a sound basis to progress the remaining requirements of the Standard.

Critical operations will evolve as an entity's business evolves and changes.

[8] These questions consider aspects of CPS230 paragraphs 34 - 46 inclusive, dealing with business continuity planning, disruptions and critical operations.

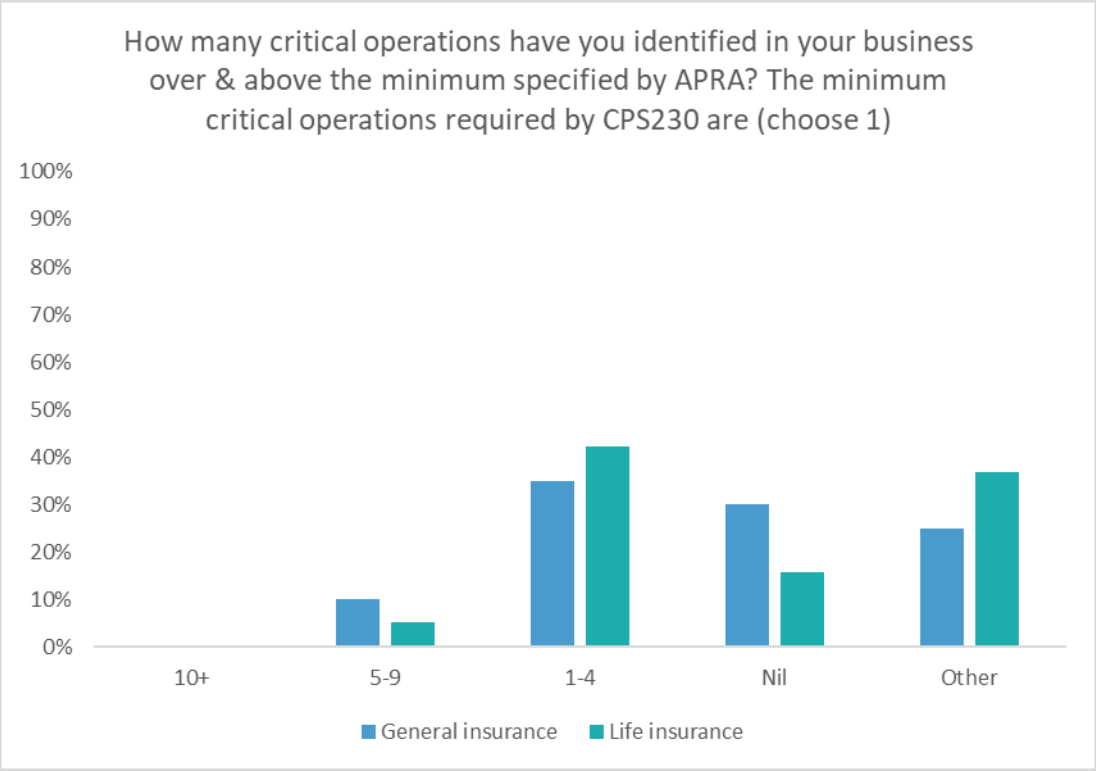
Question 25



Following on from the previous question, minimum service levels under disruption scenarios are naturally align with and are interdependent with the definition of critical operations.

A significant minority of Life Insurers report minimum service levels not yet set which in PFS' view may impede effective business continuity planning and testing, an important contributor to resilience.

Question 26



This question seeks responses for the number of critical operations **over and above**[9] the APRA specified minimums[10].

Some respondents may have misinterpreted the question, as they cite the APRA required claims processing as over and above the minimum.

Certain respondents indicated APRA had approved exemptions for certain processes being treated as critical operations.

PFS is aware of certain entities classifying critical operations into sub-operations, with varying tolerance levels, however we did not attempt to capture the extent of such classifications in the survey.

---

[9] Emphasis added

[10] CPS230.36 specifies minimum processes to be assessed as critical operations. For insurers, claims processing, and for all entities – customer enquiries and the systems and infrastructure needed to support critical operations.

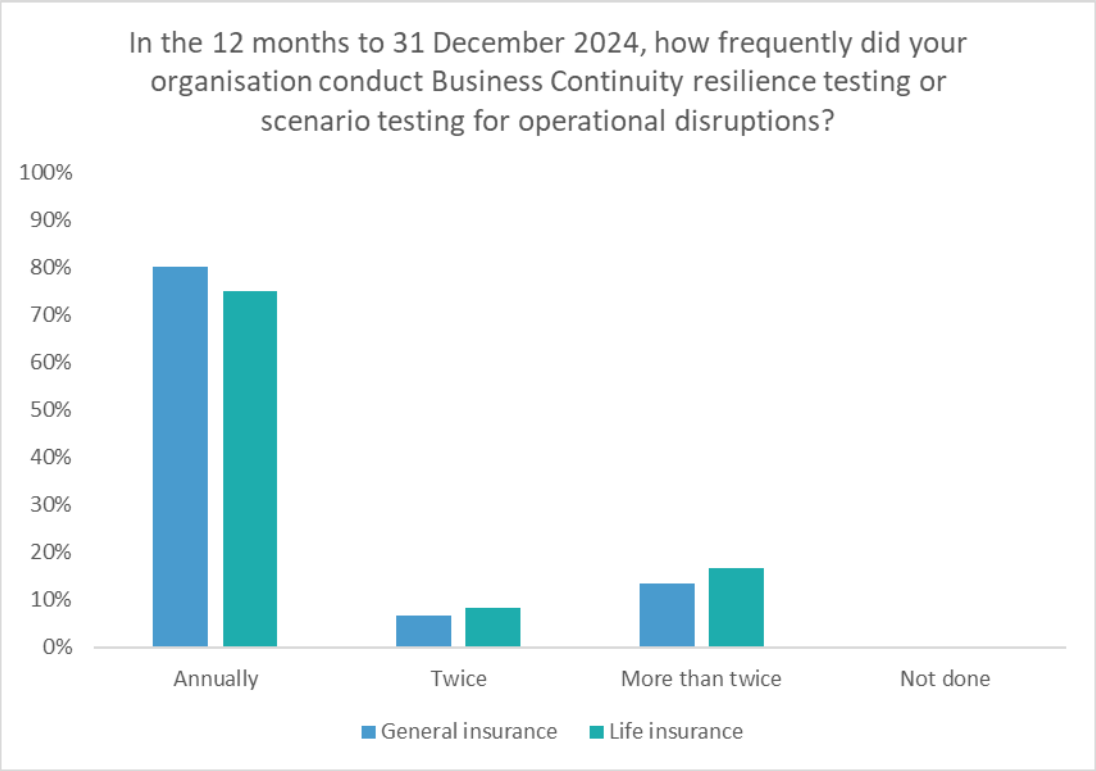
Question 26 (Continued)

The survey also asked respondents to enter free text responses for the nature of those critical operations, over and above APRA minimum requirements.

Selection of responses

- Please disregard, above, i don't know the answer to this question
- Dispute Resolution, Investments (Annuity payments)
- Contract issuing post U/W acceptance, Lapsed policy management, Premium collection and allocation.
- Registry processing, investment operations
- Policy administration
- Pricing of certain business; underwriting
- Processing of financial transactions (i.e. payments and receipts), policy processing, customer enquiries split into claims, policy and complaints
- Financial Reporting Closing Process, Actuarial, Regulatory reporting, Reinsurance, ITGC incl Information Security controls, Taxation, and Outsourcing / MSP.
- Claims payments (noting some may include that under Claims processing)
- Investment management

Question 27



No respondents reported conducting BCP testing less than annually, indicating at a minimum, the industry is compliant with this aspect of CPS232 *Business Continuity Management*[11].

PFS intend to include comparable questions in future surveys as we believe there is a trend towards more frequent testing accompanied by more robust testing.

[11] CPS232 will be withdrawn after CPS230 becomes effective however certain requirements will remain consistent

Question 28

Respondents report a high level of confidence that their organisation will be ready for the critical operations requirements on 1 July 2025.

Question 29

Do you have further comments to add regarding Critical Operations? (free text)

Selection of responses:

"Desktop testing primarily in lead up to 1 July Testing plan build and will be multiyear"

"Due to the wholesale nature of the products offered, none of the business operations qualify as Critical Operations. "

"Test program of BCP will not be completed for all critical operations"

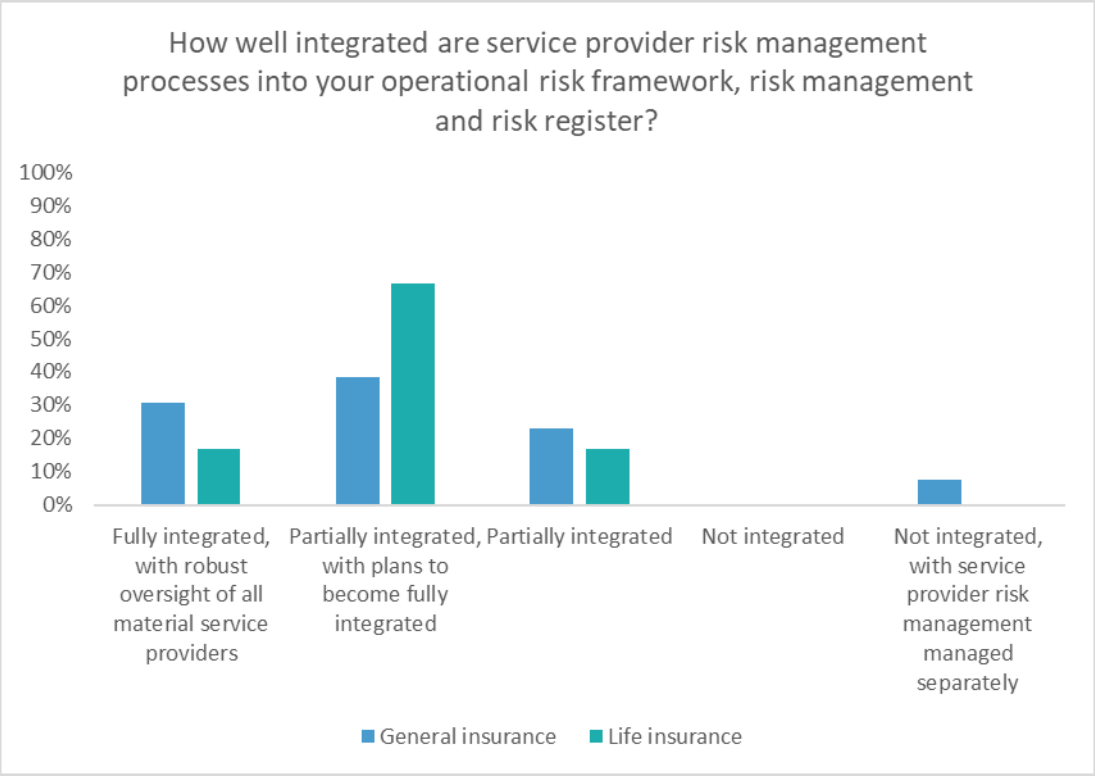
"Business continuity resilience testing covers a range of elements that are not necessarily done at the same time, particularly things like system testing or just simple call tree testing."

"Procedures/ process mapping of critical operations are available but need improvements."

"Only that the answer to question 28 is 90-99% because we expect to be "compliant" with CPS 230 but see there is continuing need for embedment and maturity (same for all aspects of CPS 230)."

2.4 Service Providers[12]

Question 30



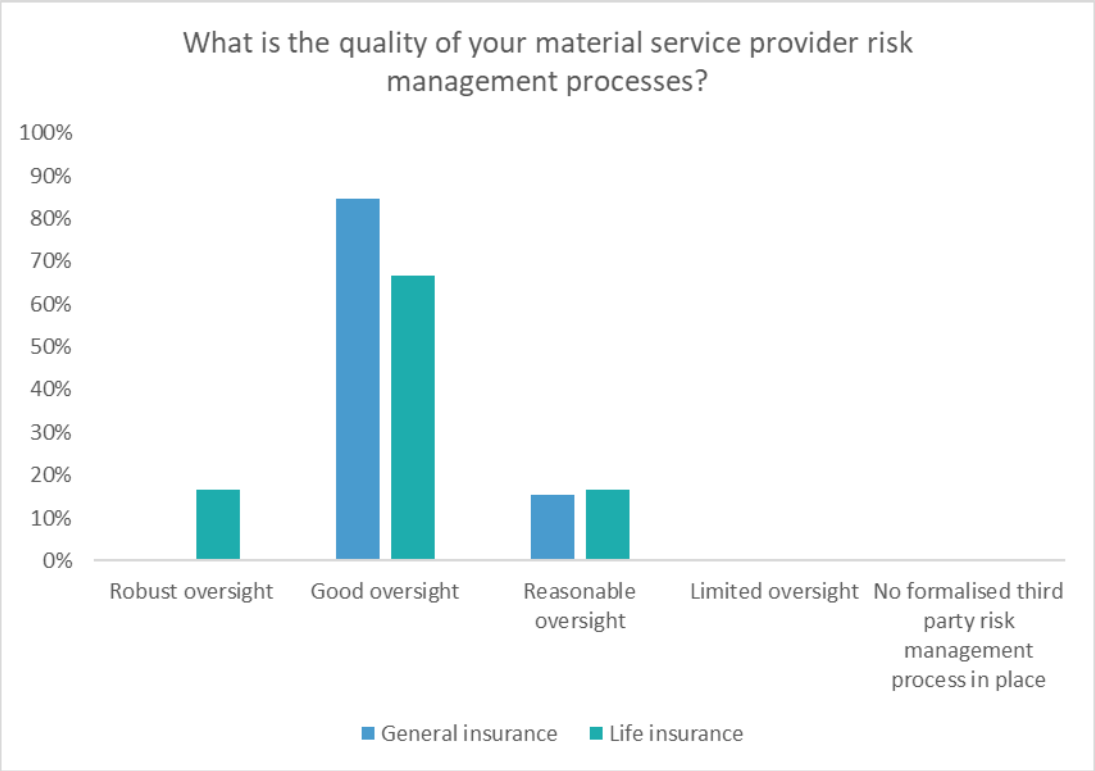
The concepts of service provider, material service provider and fourth party are - in varying degrees - new in the APRA Prudential Standard environment. The legacy concept of "*Material outsourced service provider*"[13] has been superseded.

PFS believes the pattern of responses indicates that respondents are on a journey to mature their service provider management frameworks and practices. Therefore it may be useful to compare the responses to a comparable question in a 2026 survey.

[12] These questions consider aspects of CPS230 paragraphs 47 - 60 inclusive, dealing with arrangements with service providers, the management of material service providers and their fourth parties.

[13] As per CPS231 Outsourcing

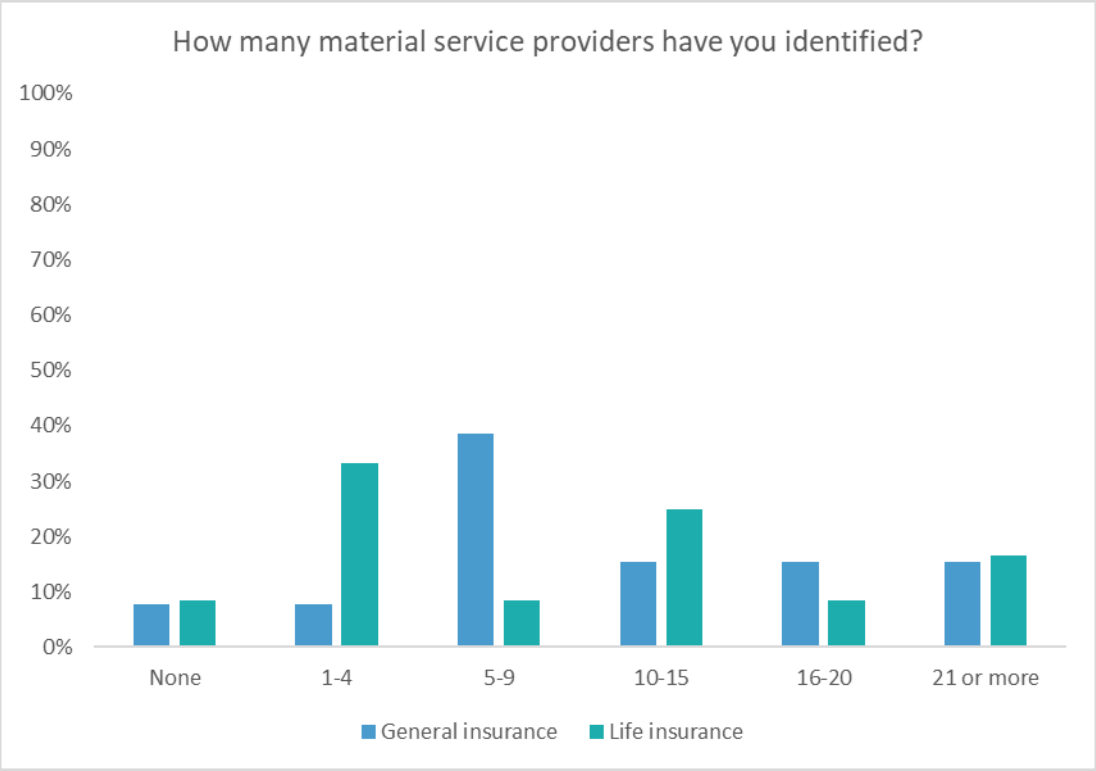
Question 31



Similar to the previous question, PFS believes the pattern of responses indicates that respondents are on a journey to mature their service provider management frameworks and practices. Therefore it may be useful to compare the responses to a comparable question in a 2026 survey.

The responses indicate Life Insurers rate their service provider management risk management processes as somewhat better than general insurers rate theirs.

Question 32



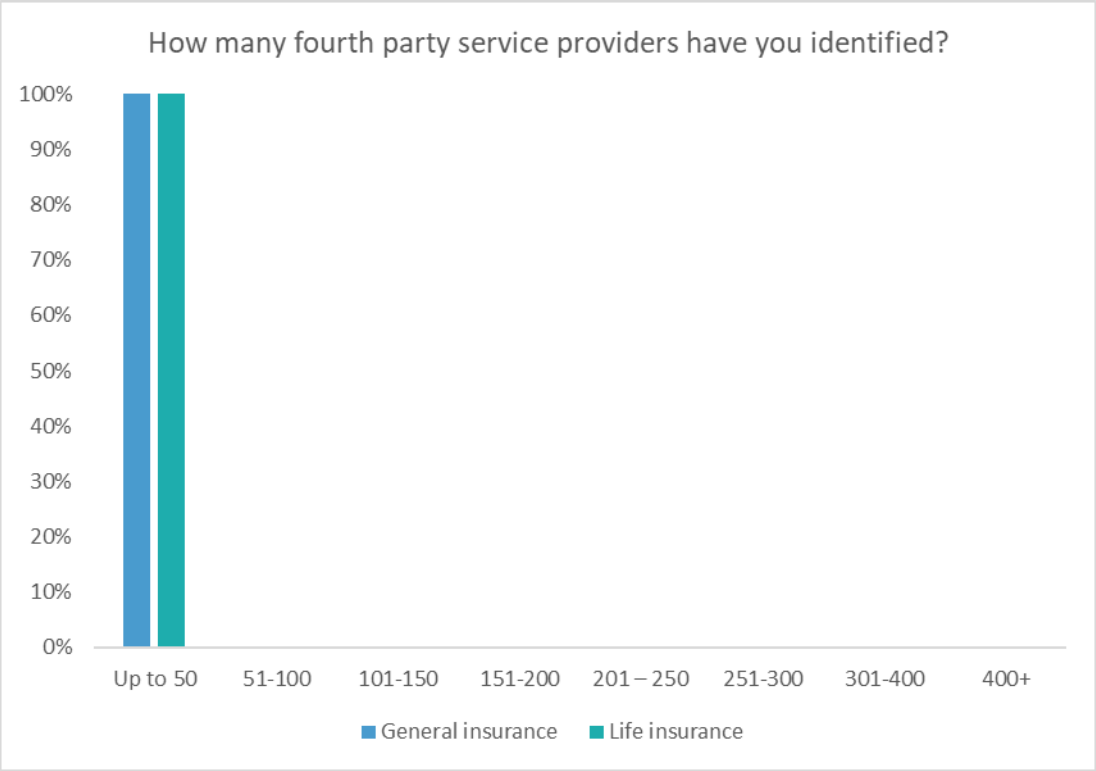
The responses indicate varying outcomes for entities and it is difficult to draw conclusions from the responses apart from that very variation.

Where a higher number of material service providers are identified, the entity may believe it is reasonable to conclude its third party operational risk is higher. The reverse may also apply.

However PFS believes that some entities with large numbers of material service providers may be over-identifying, or adopt a heavily outsourced operatingmodel. Entities with nil or a small number of material service providers may be under identifying or alternatively operate on an in-house model.

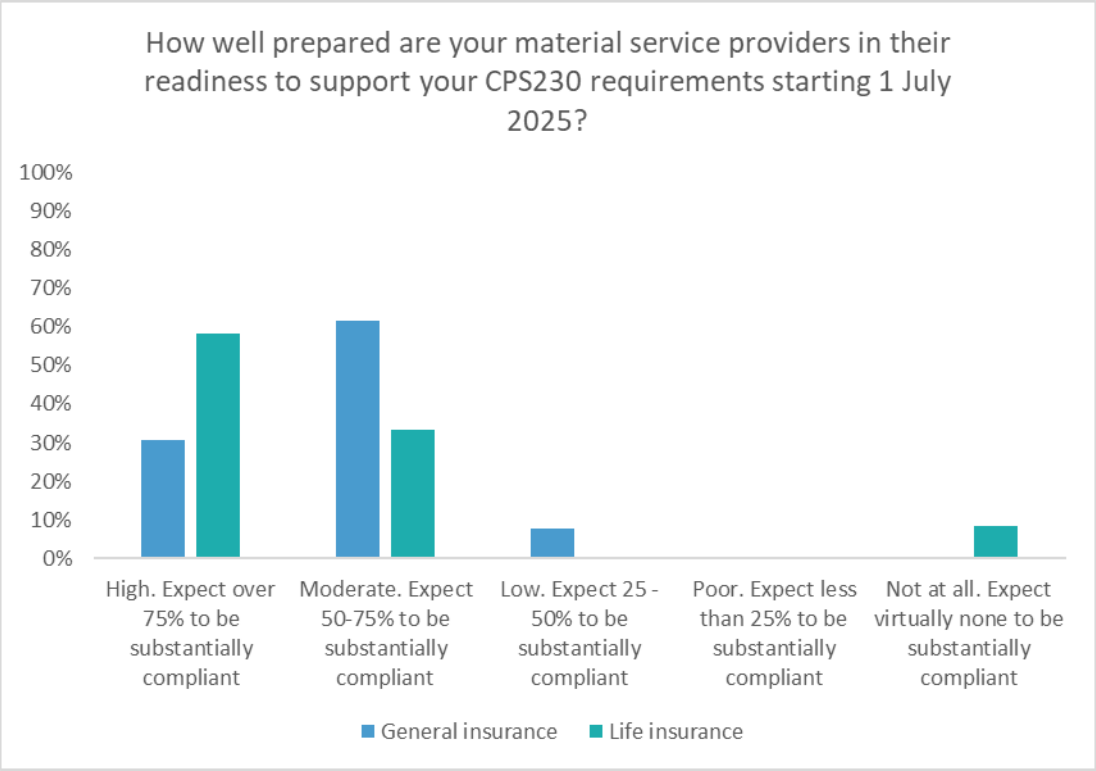
Future surveys may seek to address additional insights, such as any correlation between number of material service providers, robustness of oversight and operational risk events.

Question 33



UP to 50 fourth party service providers appears to be a manageable number. PFS believes the number of fourth parties may be underestimated. Future surveys will seek to compare numbers of fourth parties over time and develop insights such as correlations with number of material service providers and operational risk events.

Question 34

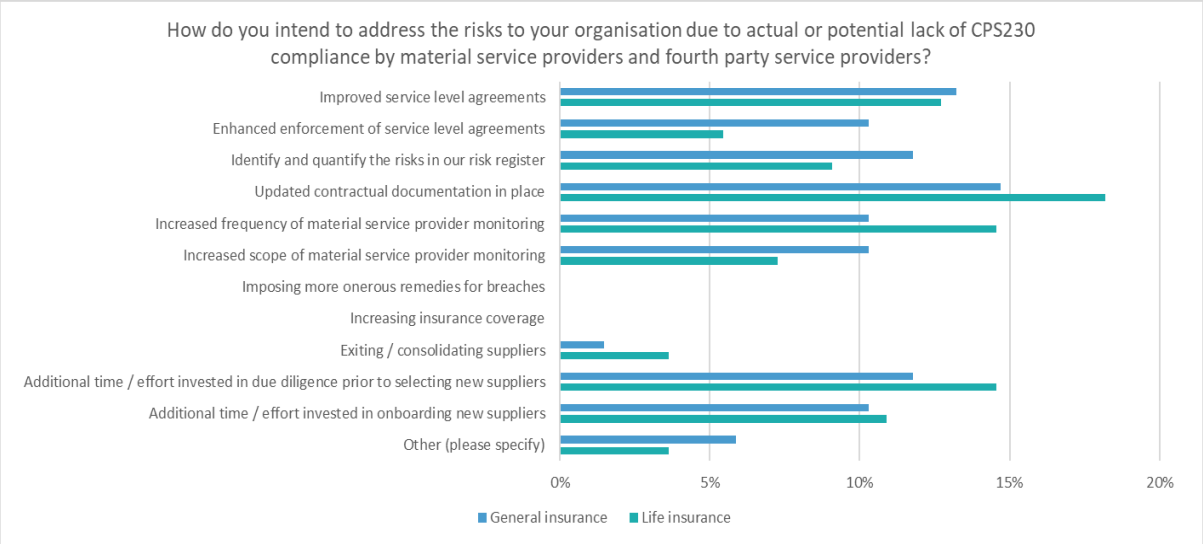


The responses indicate that material service provider readiness lags that of the APRA regulated entity.

Respondents cite issues with overseas entities' willingness to comply, and with local suppliers who are unfamiliar with APRA requirements.

Entities may wish to consider whether their own compliance level may require reassessment in the event of service provider compliance levels.

Question 35



Respondents report a range of mechanisms being implemented to address and uplift service provider compliance. PFS believes this indicates entities are availing themselves of numerous mechanisms.

Interestingly – and ironically - entities are not increasing their insurance coverage.

Nor are they seeking to impose more onerous remedies for breaches.

Future surveys will see this question being cast differently in light of ongoing CPS230 compliance, potentially focusing on which mechanisms entities find most effective in service provider management.

Question 36

The responses to Question 36 appear to be inconsistent with the responses to Question 34. Entities report more optimism regarding their own implementation of service provider requirements than they do for the service providers' readiness for CPS230.

Responses to a comparable question in 2026 and future years may reveal the extent and speed of the service providers' journey towards embracing CPS230 related expectations placed on them by APRA regulated entities.

Question 37

Do you have further comments to add regarding Service Providers? (free text)

Selection of responses:

"We already had strong contractual obligations for our service providers. These have been reviewed in line with requirements and our updated Procurement & Contracting Policy. In addition, we have strengthened the link to our CPS234 IT risk assessment process."

"We have amended our Vendor Management policy, procedure and framework, as well as our outsourcing procedures."

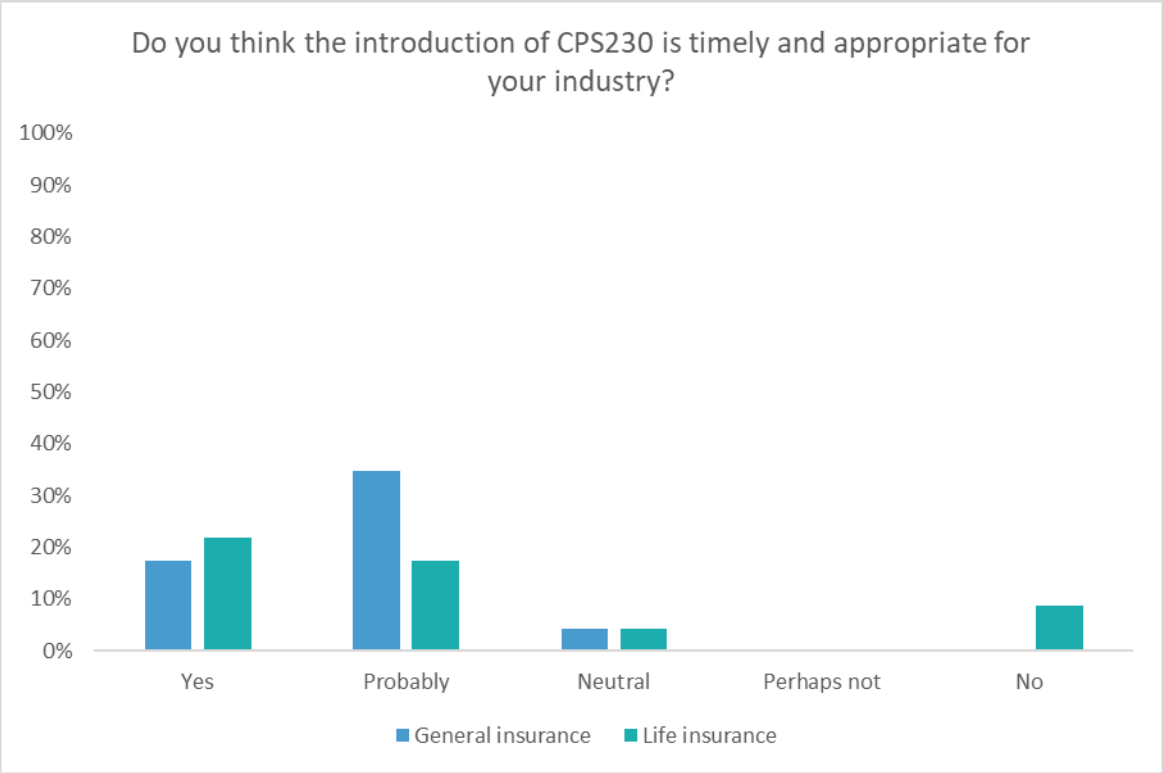
"Majority of MSPs are reasonably mature with comprehensive reporting already in place - key uplifts are updates to contracts/agreements, listing of key controls, results of controls testing and transparency of 4th parties."

"SLA enhancements and CPS 230 addendums to the agreement to be implemented post 1 July 2025"

"Some updating of contracts will only occur during '25 and '26"

2.5 CPS230 – the Report Card

Question 38



Respondents are generally supportive of CPS 230 with a small proportion of life insurers reporting a negative perception of the standard.

Question 38 (continued)

Please give the Rationale for your response: (free text)

"I can see some merit however it increases already high compliance costs on the industry"

"Focus on resilience is critical for promotion of trust and delivering on member outcomes. Explicitly aligning the concept of resilience with risks in a service focussed industry is inherent to risk maturity."

"It has been good for us off the back of CPS234 Tripartite findings and remediation work. As a small organisation however it is quite demanding of time and resources. Overall, worth the effort and time to review existing practices. It has also elevated the important of effective management of risks."

"There is no doubting it is the correct direction to go, but there is significant regulator change being imposed on the business such as CPS230, FAR, AML / CTF Regulation. The change imposes time and cost constraints on us."

"Governance, management and oversight practices have not kept pace with proliferation of 3rd party utilisation. These introduce significant operational risks to organisations (certainly a key focus for us for past few years) so the uplift to oversight, management, and due diligence is absolutely necessary."

"While the Service Provider ecosystem is becoming increasingly complex, Regulated Entities may not have full visibility, capacity and capability to assess the fourth party impact"

"Providing greater focus on Customer adverse impact driving changes to prioritisation of disruption point recoveries and detailed alternative BCP actions during disruption (before recovery RTO's)"

"A significant cost imposition on a small sector of the economy that competes with non APRA regulated managed investments. "

"Sharpens focus on some of the key risk areas that got less visibility under prior standards, such as end-to-end resilience and critical operations. "

"Consolidation of obligations"

"I would have thought that compliance with existing prudential requirements was sufficient"

"Uplift for operational risk was required, however, the impost and prescriptive requirements for non-SFIs are onerous."

"It has really driven a focus on resilience and understanding of our end to end operations including reliance on suppliers. Given then some of the recent challenges within the industry this has demonstrated the importance of this regulation."

"We have found that the implementation of CPS230 has generated quality risk focussed discussions across the Group and improved both our operational risk management framework and the detailed understanding of those processes at all levels."

"It is a lot of work but getting the pain over quickly is more effective and efficient"

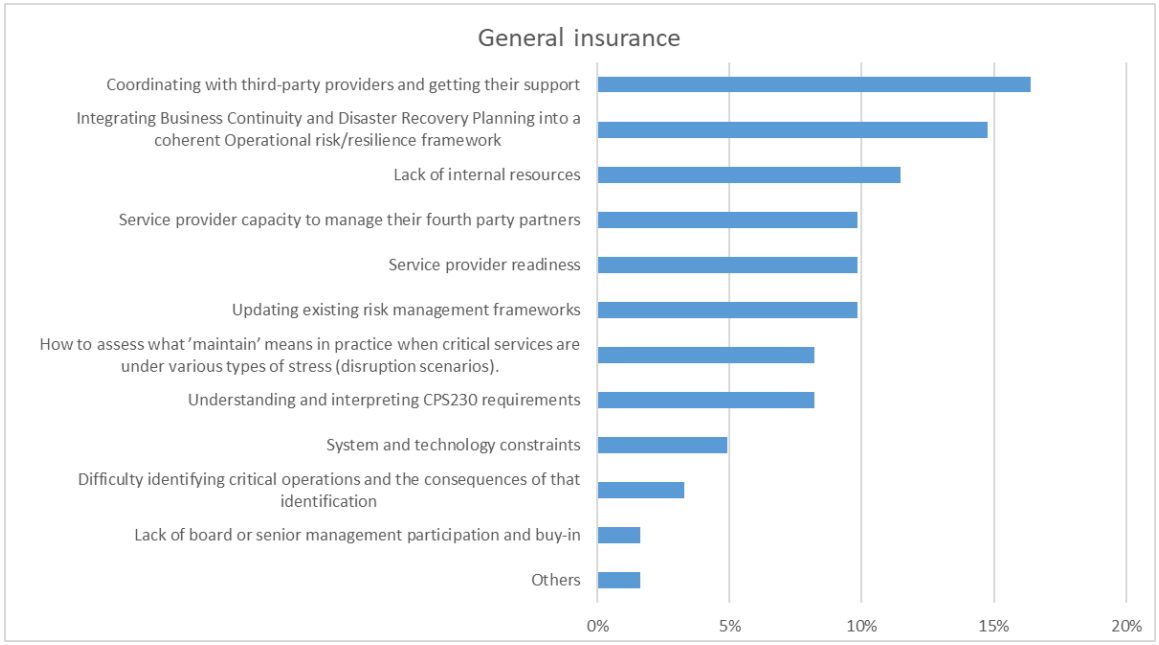
"Third party risks have been under appreciated/managed, this helps to focus on that."

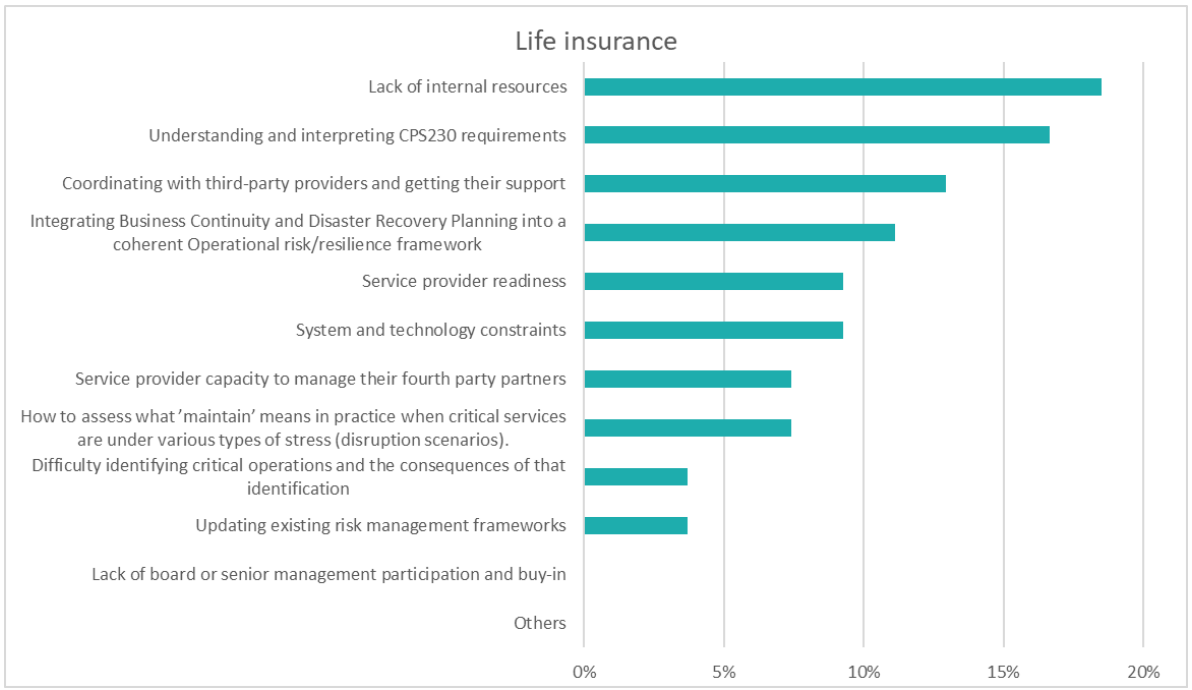
"Operational risk was not given the importance by management and board; this introduction should provide that thrust and weight."

"I think the concepts of CPS 230 make good business sense but for small organisations such as ours, redefining our existing documents and approaches to meeting the technical requirements is resource intensive (larger organisations have teams working on CPS 230 implementation but we do not have that luxury).

Question 39

What does your organisation see as the main challenges in complying with CPS230?



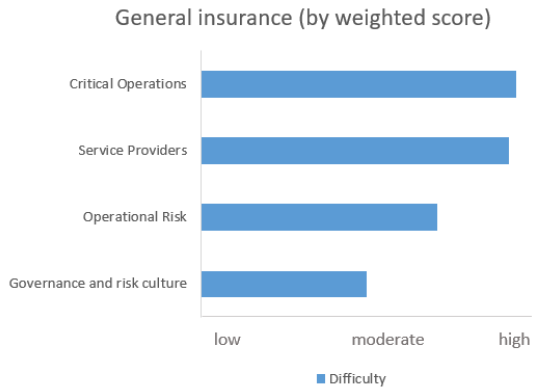


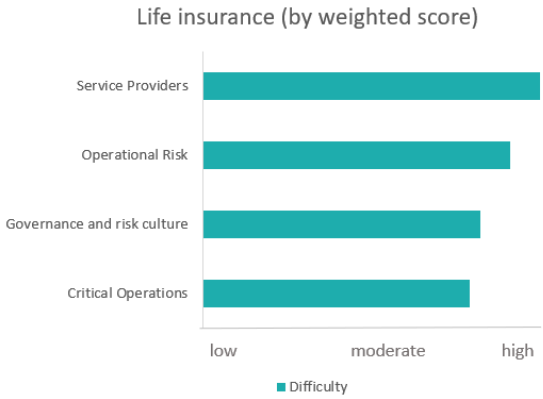
General insurers and life insurers report differing main challenges, with General insurers citing service providers as a more significant challenge.

Entities may wish to reflect on their own challenges in the CPS230 journey.

Question 40

Which areas of CPS230 does your organisation have the most difficulty with?





The responses above appear inconsistent with the responses to Question 39. However the above responses rank each key domain of CPS230 not root causes.

Entities may wish to reflect on the areas where they have found the most difficulty at varying stages over the CPS230 journey.

Question 41

Do you have any further comments to add (free text response).

Selection of responses:

"Ongoing embedment and maturity will be a focus and determining sufficiency of 'material compliance' and 'done' important to take an appropriately prioritised continuation of work forward will be important. Ongoing operational risk maturity will be pursued with broader risk uplift activity."

"It has been challenging but also valuable. The buy-in from a Board level has been extremely worthwhile. We have uplifted and strengthened the risk team, which was starting to lag significantly. Also elevated awareness of risk across the organisation, including responsibilities of Executives and Seniors."

"A key element will be the testing of Business Continuity Plans and alternative emergency operations in the event of a disruption of a critical process, especially when IT related ("proof of the pudding is in the eating")"

"We are targeting Day 1 compliance but are open about that being followed by a period of embedment following which the operational risk management framework will be stronger than it was on Day 1 compliance"

3 Conclusion

The CPS230 journey has played over more than 2 years, some entities commencing early, with others seeking to join the marathon at the 40 kilometre mark in early 2025.

Meeting the requirements of CPS230 begins the journey for developing operational resilience and some building blocks should already be in place. These requirements provide a minimal set of objectives to be met. Complying with CPS230 is a necessary foundation step, but it is not sufficient for success. Good practice will develop over time and can be expected to set higher standards of practice. As this journey progresses, risk culture and risk maturity can be expected to improve, contributing to improving ERM. The sufficient conditions for success focus on leadership, culture and risk maturity. Leadership will come from boards and senior management as they own, set, and implement clear policies and oversee process improvements.

The intent is to conduct this survey annually.

Point in time assessments are useful, but progress can be better assessed by reviewing trends.

Annual surveys also permit new topics to be included.

1 July 2025 is not the end game – it is the beginning of a new order with increased expectations of financial institutions.

What will the financial services sector look like in 1 year – 5 years – 10 years?

Acknowledgements

Feedback and review from colleagues, including Jules Gribble, Jessie Yu, Phil Stott, John Newman and Sean Williamson has been welcomed and helped improve this paper. Any errors in this paper remain my responsibility.

Author details

Madeleine Mattera, BEc, FCA, PMIIA, CIA, GAICD, is a Director at PFS Consulting and PFS' Head of Risk Advisory. She is based in Sydney NSW.

Madeleine can be contacted by:

✉: madeleinemattera@PFSConsulting.com.au

✆: +61 413 308 481

🌐: www.PFSConsulting.com.au

4 Sources

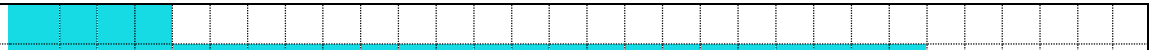
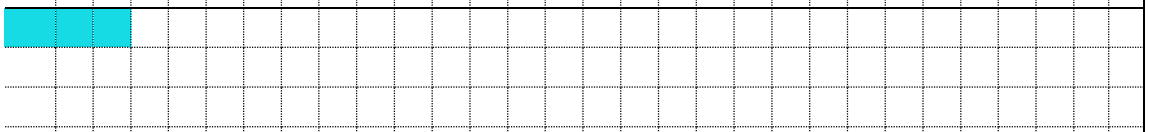
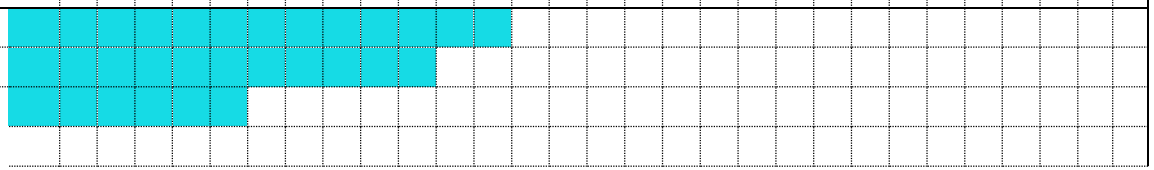
PFS 2024. *'CPS 230 Check in: How does your progress stack up?'*, PFS, August 2024. See https://pfsconsulting.com.au/wp-content/uploads/2024/08/CPS-230-Check-in-How-does-your-progress-stack-up.pdf

PFS 2023a. *'Operational Resilience: A bigger game and a broader perspective. How will you exploit this opportunity?'*, PFS, December 2023. See https://pfsconsulting.com.au/2023/12/11/operational-resilience-a-bigger-game-and-a-broader-perspective/

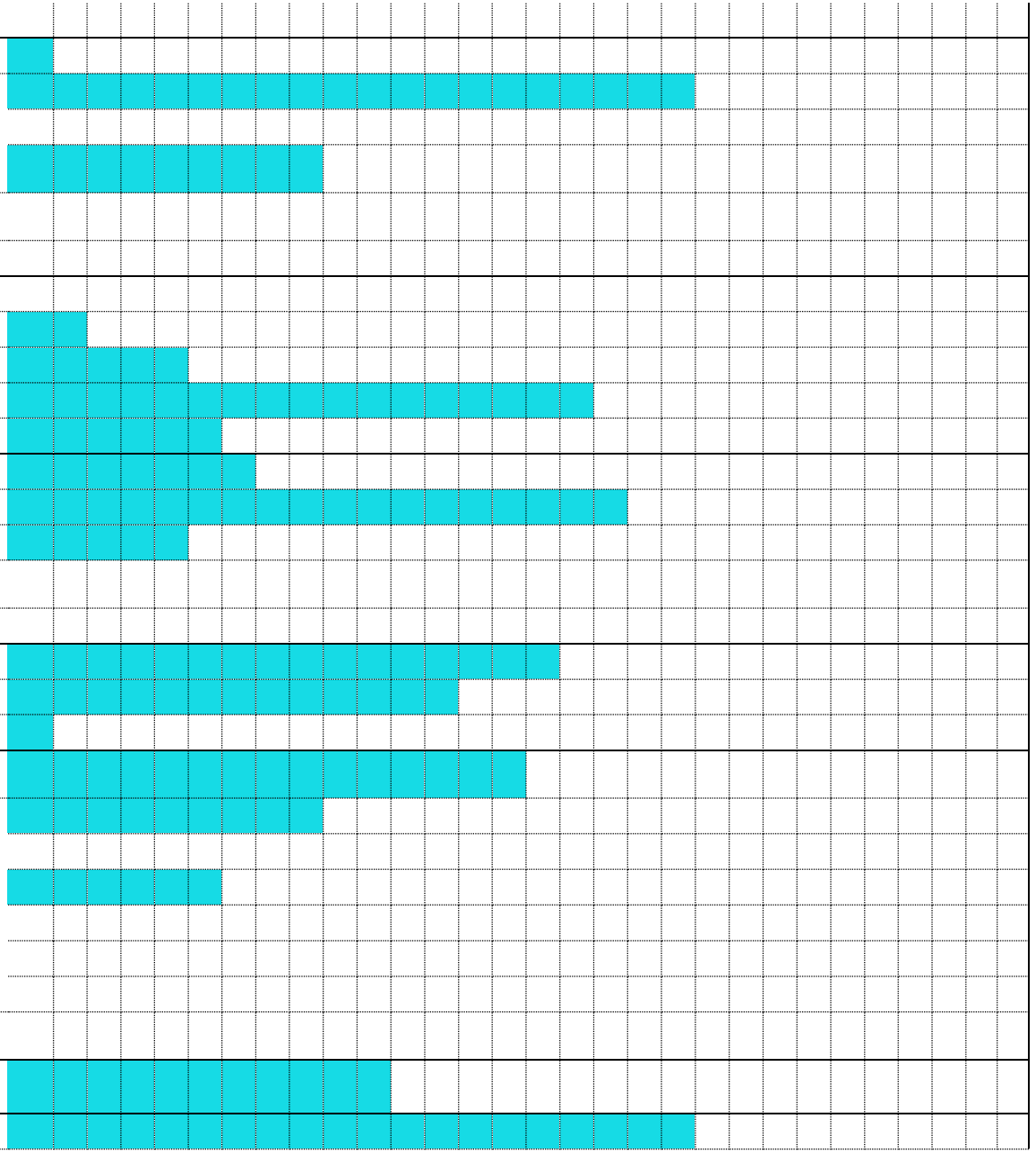
PFS 2023b. *'Operational Risk Management Top Tips on CPS230'*, PFS, August 2023. See https://pfsconsulting.com.au/2023/10/10/operational-risk-management-top-tips-on-cps230/

PFS 2022. *'CPS230 The Journey Toward Resilience and Adding Value. APRA's New Standard on Operational Risk Management'*, PFS, October 2022. See https://pfsconsulting.com.au/2022/10/06/cps-230-the-journey-towards-resilience/

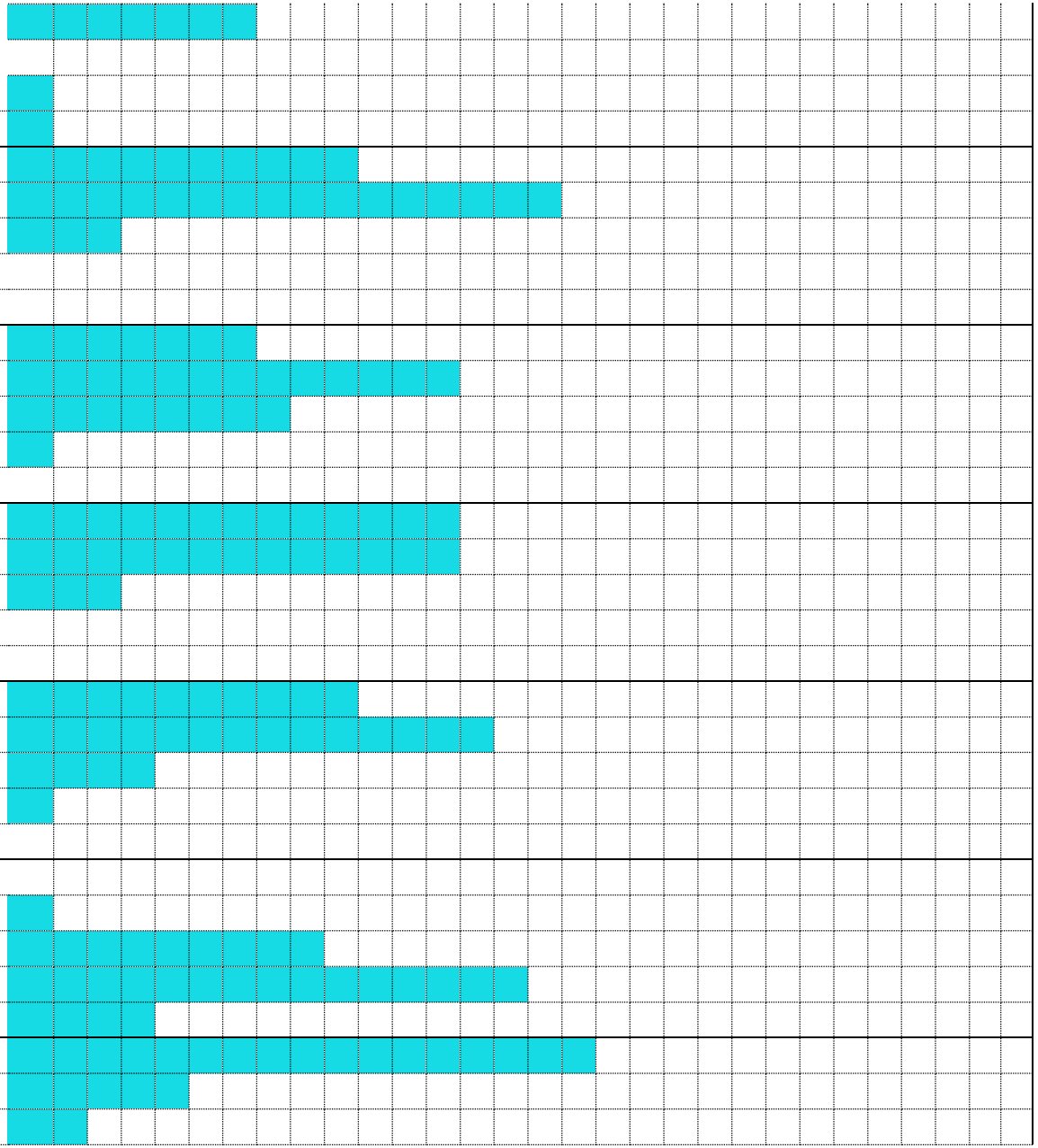
5 **Appendix 1:** All Responses

Q4: Which role in your organisation (under FAR) is responsible for the implementation of CPS230?	CEO	
	CRO	
	COO	
	CFO	
	Other	
	Other (please specify)	
Q5: How engaged has your Board and relevant committees been in your CPS230 journey?	Highly. eg scheduling special board meetings and/or involved in workshops	
	Interested. Receive regular reports and challenge management	
	Low interest. Passive and only receive reports, with little comment etc.	
Q6: How well is the management of Operational risk, and now more broadly operational resilience, embedded into your Enterprise Risk Management framework, policies, and procedures?	Fully embedded – Operational risk and resilience are seamlessly integrated into the Enterprise Risk Management framework, policies and procedures.	
	Largely embedded – Well integrated, with some areas of improvement.	
	Partially embedded – Some elements are in place, but gaps remain.	
	Minimally embedded – Limited integration, with significant gaps	
	Not embedded – No formal integration within the Enterprise Risk Management framework.	
Q7: Has your Risk appetite and/or Risk tolerances been reviewed and revised as part of your CPS230 journey?	Yes - in full	
	Yes - targeted	
	Yes - but not in a structured way, Minor/limited changes	

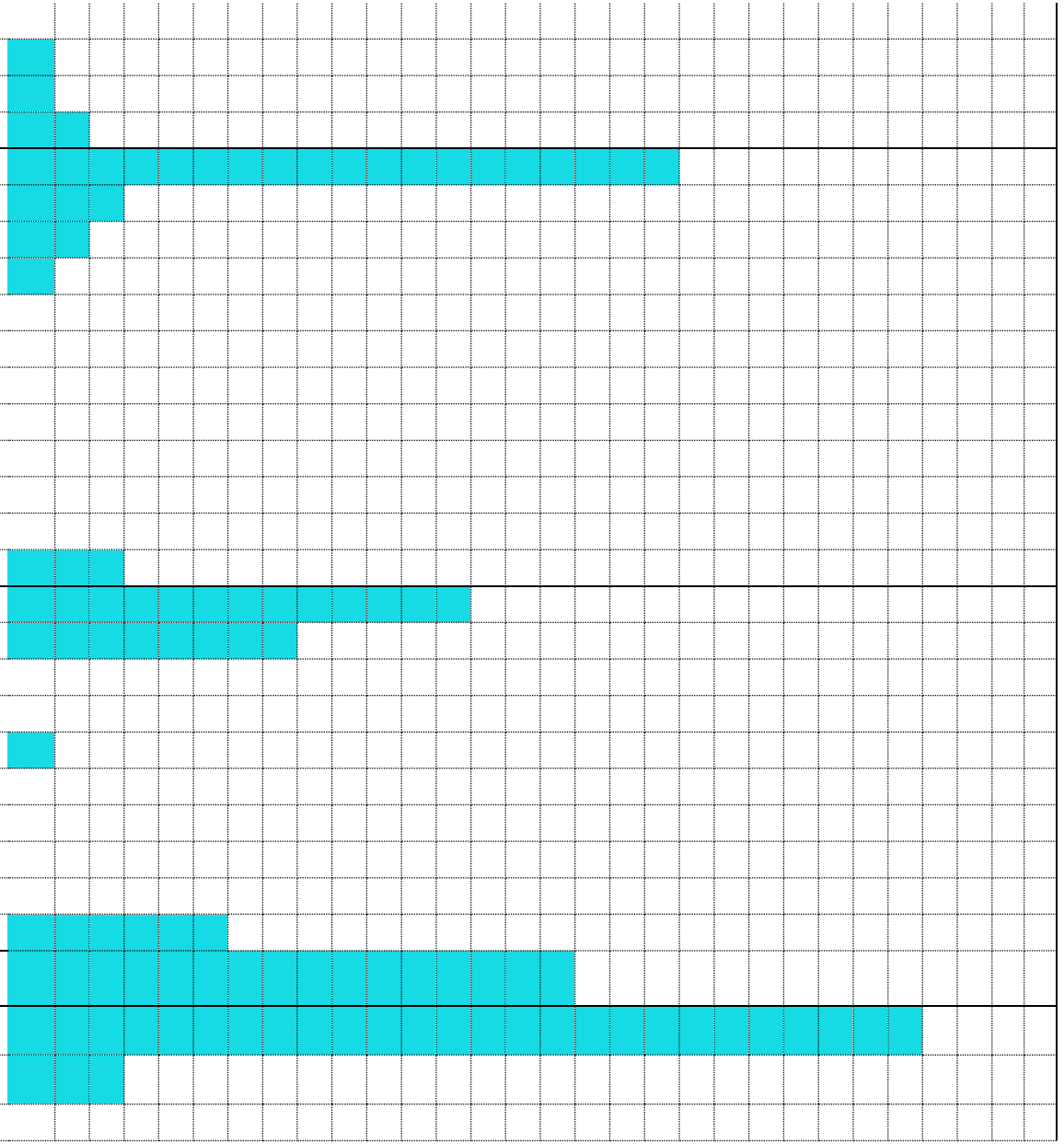
Q8: How prepared is your organisation to meet the internal reporting and compliance obligations of CPS230	No
	Fully prepared
	Mostly prepared (program in place to be completed)
	Partly prepared (improvements needed)
	Poorly prepared (significant material gaps)
	Not prepared
Q9: How complete do you expect your implementation of CPS230 requirements for governance to be for 1 July 2025?	Less than 50%
	50-74%
	75-89%
	90-99%
	100%
Q10:How well is the concept of operational resilience understood across your organisation?	Well understood throughout
	Partly understood throughout
	Understood in some areas
	Partly understood in some areas
	Not well understood
Q11:How strong is your culture around customer service, including the management of operational resilience and operational risks?	Strong throughout
	Strong in some areas
	Not strong
Q12: How well understood are the roles of the first and second lines of risk management and how effectively do they interact in your organisation?	Well understood, interact effectively
	Partially understood, interaction would benefit from improvement
	Understood in some areas, interactions would benefit from improvement
	Partially understood in some areas, interaction would benefit from improvement
	Not well understood, do not interact effectively
Q13: Do you have further comments to add regarding Governance?	Open-Ended Response
	Yes – revised for CPS230



Q14: Do you have a clearly documented and implemented Operational risk management framework, policies and procedures that includes the requirements of CPS230?	Yes - under review, Yes – not specifically revised for CPS230
	No - In development
	No
Q15: How confident is your organisation in identifying, assessing, and mitigating material operational risks?	Very confident
	Mostly confident
	Neutral
	Low confidence
	No confidence
Q16: How confident are you that your organisation's Risk register is up to date, comprehensive and realistic, to enable reporting of value and insight?	Very confident
	Mostly confident
	Neutral
	Low confidence
	No confidence
Q17: How confident are you that your organisation's risk culture encourages the calling out of potential new or heightened risks?	Very confident
	Mostly confident
	Neutral
	Low confidence
	No confidence
Q18:How confident are you that your organisation's focus is on customer service and satisfaction (even if sometimes this may not be the most 'cost saving' approach)?	Very confident
	Mostly confident
	Neutral
	Low confidence
	No confidence
Q19: How complete do you expect your organisation's implementation of CPS230 requirements for operational risk to be for 1 July 2025?	Less than 50%
	50-74%
	75-89%
	90-99%
	100%
Q20: In the 12 months to 31 December 2024, how many new material Operational risk events were reported to APRA?	None
	1
	2

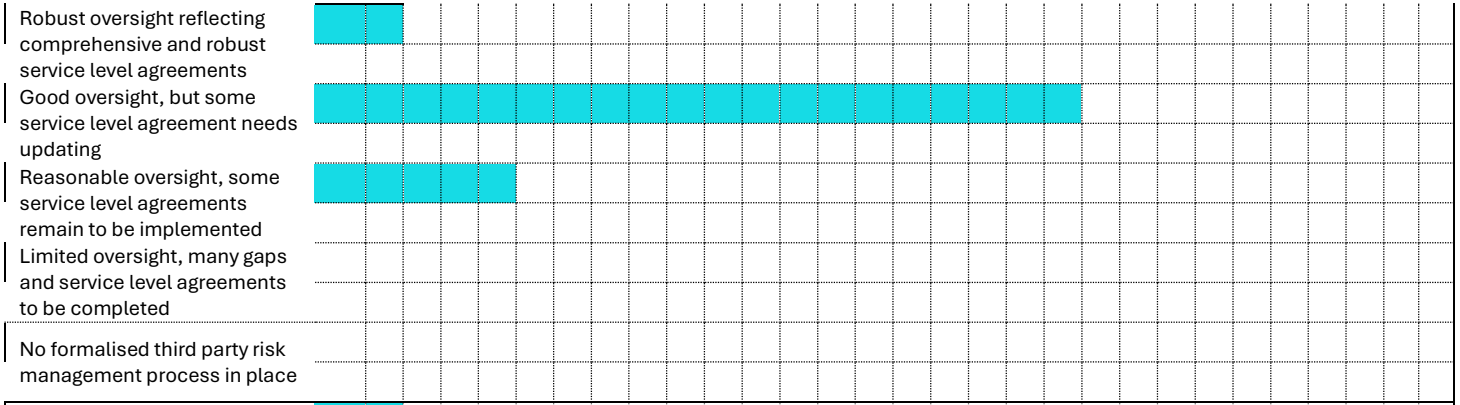


Q21: In the 12 months to 31 December 2024, how many material Operational risk events reported to APRA prior to 31 December 2023 were being worked on?	3
	4
	5
	More than 5
	None
	1
	2
	3
	4
	5
	6
	7
	8
	9
	10
	More than 10
Q22: In the 12 months to 31 December 2024, what was the total aggregate cost incurred for addressing the risks identified in Questions 20 and 21 (Cost includes all direct costs, such as remediation paid, and all indirect costs, such as internal project costs, consultants, fines etc)?	$0
	$0-$5 million
	$5-$10 million
	$10-$25 million
	$25-$50 million
	$50-$100 million
	$100-$250 million
	$250-$500 million
	over $500 million
	Data not available
Q23:Do you have further comments to add regarding Operational risk?	Open-Ended Response
Q24:How clear is your identification and characterisation of your critical operations?	Clearly identified (process completed)
	Mostly identified (process continuing)
	Some identified



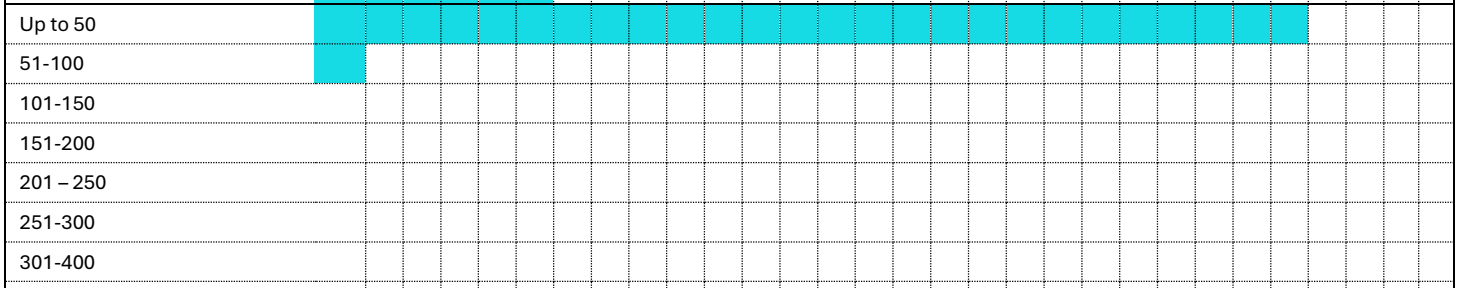
Q25: How well defined are your minimum service levels under disruption scenarios?	None identified (all operations deemed critical)
	Minimum service levels set for all critical operations
	Minimum service levels set for some critical operations
	Minimum service levels not yet set
Q26: How many critical operations have you identified in your business over & above the minimum specified by APRA?	10+
	5-9
	1-4
	Nil
	If response is other than 'Nil' above, please list the additional critical operations you have identified:
Q27: In the 12 months to 31 December 2024, how frequently did your organisation conduct Business Continuity resilience testing or scenario testing for operational disruptions?	Annually
	Twice
	More than twice
	Not done
Q28: How complete do you expect your organisation's implementation of CPS230 requirements for critical operations to be for 1 July 2025?	Less than 50%
	50-74%
	75-89%
	90-99%
	100%
Q29: Do you have further comments to add regarding Critical Operations?	Open-Ended Response
Q30: How well integrated are service provider risk management processes into your operational risk framework, risk management and risk register?	Fully integrated, with robust oversight of all material service providers
	Partially integrated, with plans to become fully integrated
	Partially integrated
	Not integrated
	Not integrated, with service provider risk management managed separately

Q31: What is the quality of your material service provider risk management processes?

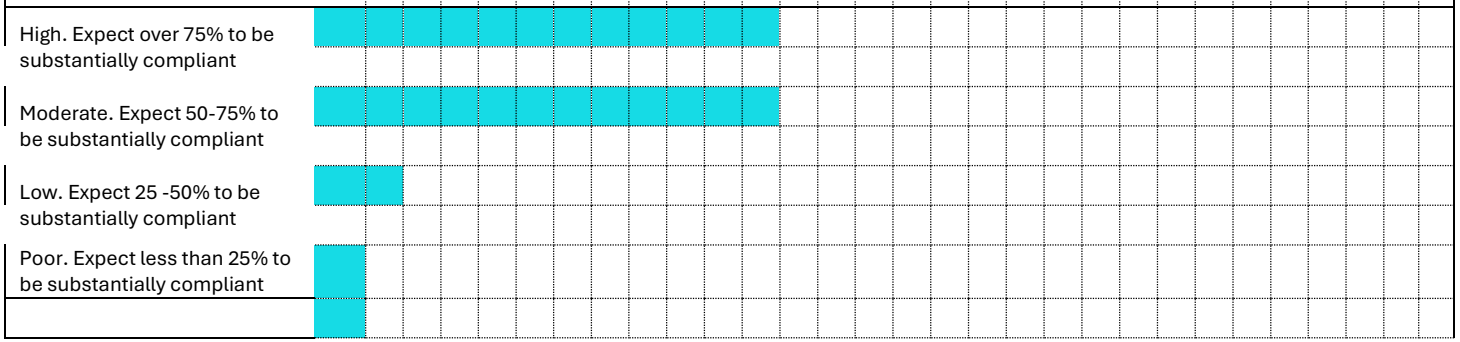


Q32: How many material service providers have you identified?

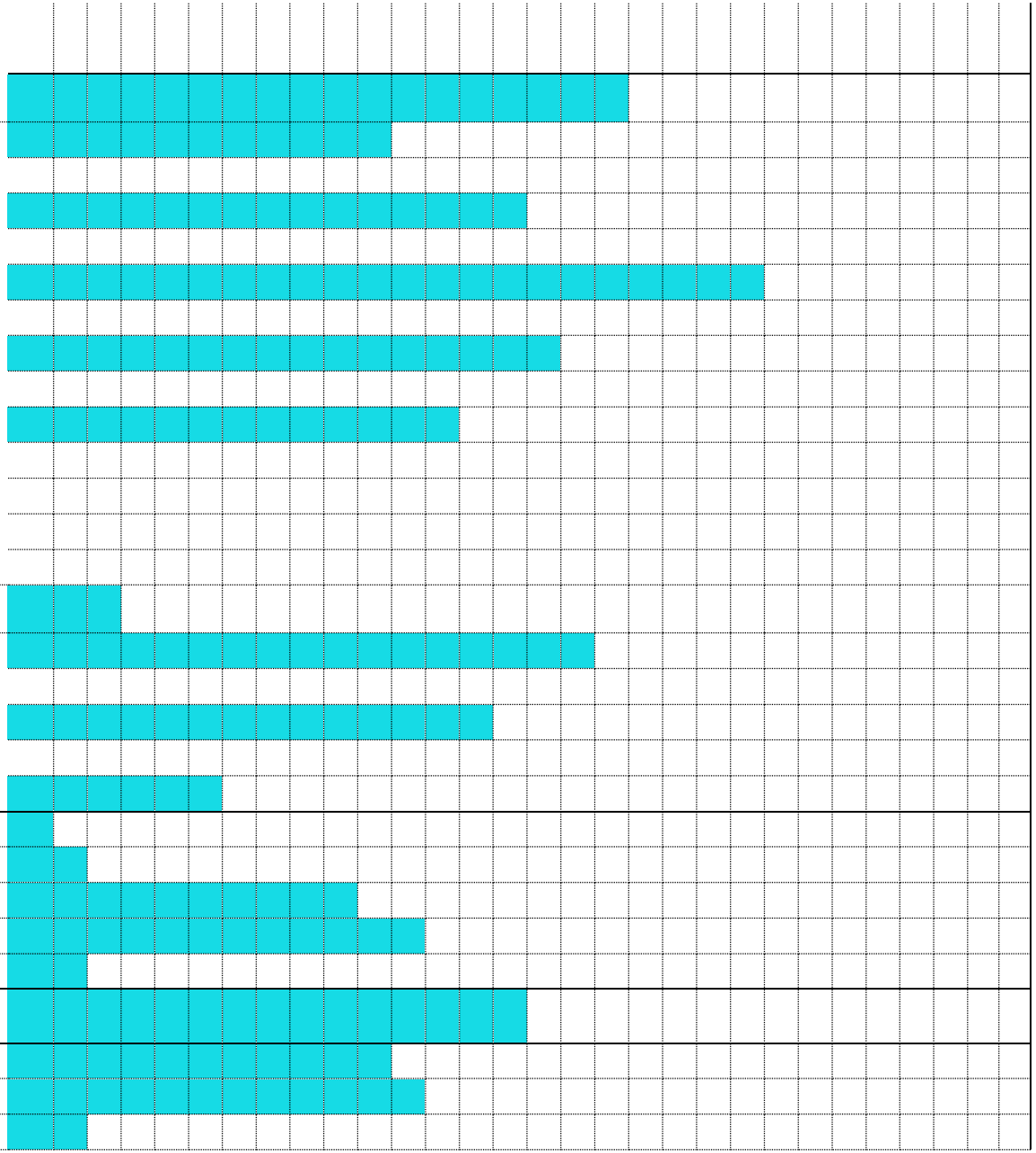
Q33: How many fourth party service providers have you identified?



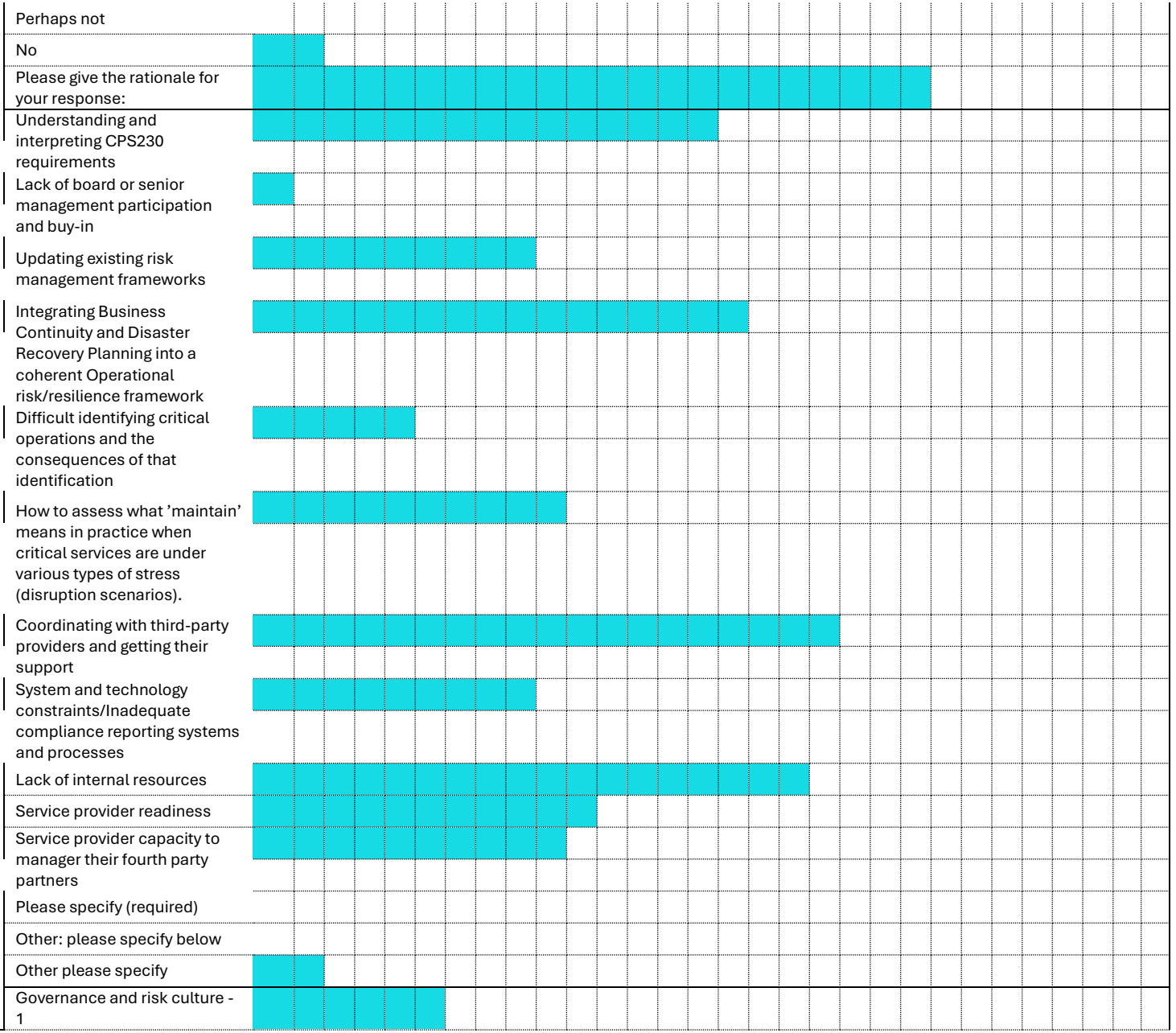
Q34: How well prepared are your material service providers in their readiness to support your CPS230 requirements starting 1 July 2025?



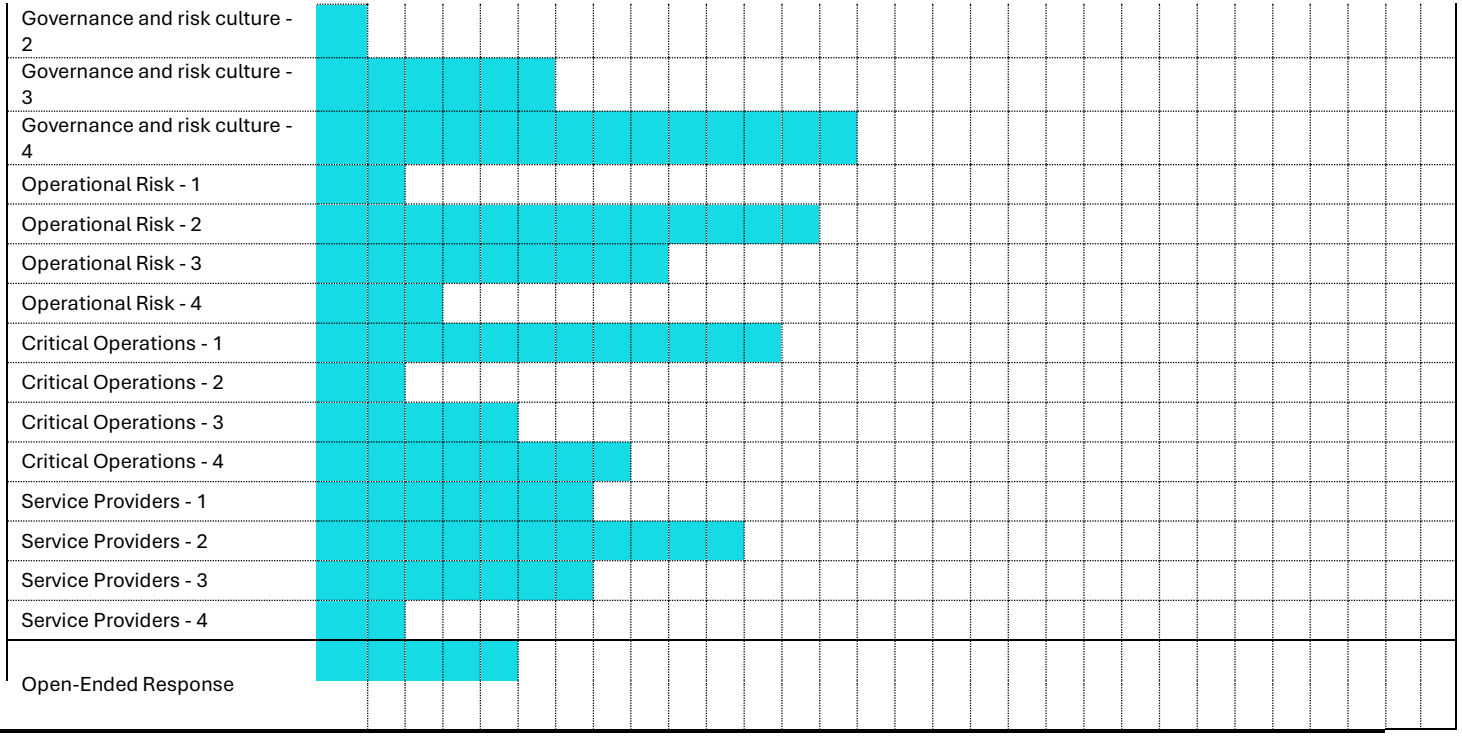
Q35: How do you intend to address the risks to your organisation due to actual or potential lack of CPS230 compliance by material service providers and fourth party service providers?	Not at all. Expect virtually none to be substantially compliant
	Improved service level agreements
	Enhanced enforcement of service level agreements
	Identify and quantify the risks in our risk register
	Updated contractual documentation in place
	Increased frequency of material service provider monitoring
	Increased scope of material service provider monitoring (eg move from 30 KPI's to 50)
	Imposing more onerous remedies for breaches
	Increasing insurance coverage
	Exiting / consolidating suppliers
	Additional time / effort invested in due diligence prior to selecting new suppliers
	Additional time / effort invested in onboarding new suppliers
	Other (please specify)
Q36: How complete do you expect your organisation's implementation of CPS230 requirements for service providers to be for 1 July 2025?	Less than 50%
	50-74%
	75-89%
	90-99%
	100%
Q37: Do you have further comments to add regarding service providers?	Open-Ended Response
Q38: Do you think the introduction of CPS230 is timely and appropriate for your industry?	Yes
	Probably
	Neutral



Q39: What does your organisation see as the main challenges in implementing CPS230? Choose all that are relevant:



Q40: Please rank, with 1 being the highest and 4 the lowest, your view of the components of CPS230 you think that regulated entities experience most difficulty with and so potentially need additional resources and support.



Q41: Do you have any comments you would like to add on your organisation's CPS230 journey and preparedness for the 1 July 2025 deadline.

Open-Ended Response