Submission to Australian Prudential Regulatory Authority – APRA on behalf of BHP Marine & General Insurances Proprietary Limited. October 2022.

To Whom It May Concern,

Thank you for the opportunity to provide a response during a formal consultation phase on Commonwealth Prudential Standard 230 – Operational Risk. Our comments below contain commentary on both the standard and its implications for our compliance regime as well as some broader observation on how this standard is emblematic of some recurrent thematic challenges we have observed in complying with all prudential requirements at BHP Marine & General Insurances Pty Ltd

CPS230 provides substantial detail regarding the requirements for the management of operational risk. Operational risk is a subset of risk that is managed by an overall framework – the requirements for which are articulated in CPS220. Taking risk management requirements out of a single standard increases the workload and complexity for compliance functions. Further, we note that within CPS220 there are eight types of risk articulated that must be managed, of which operational risk is one. It is unclear if APRA intends to have a standard for each one, or only operational risk. It is our view that all requirements should reside in the primary standard. Further, it is our concern that if a standard the size and complexity of CPS230 were established for each type of risk that APRA mandates are codified and managed, the compliance burden would become unmanageable. We propose that all risk management requirements be articulated in the one standard. We suggest that if this is not possible a clear rationale be articulated as to why CPS230 exists outside CPS220.

CPS230 contains requirements that business continuity be reviewed formally by internal audit. A similar requirement for risk management compliance to be audited is reflected in CPS220 and other standards. Audit activity is theoretically infinite, but in practice limited. The more audit activity APRA mandates, the more it erodes the function and mandate of risk and audit committees to direct assurance activities to areas of greatest risk or greatest benefit. In the context of our business model, where the processes are simple, easily able to be performed manually, or fully outsourced to another provider in the event our primary service provider is unable to deliver for any reason, business continuity presents as a less worthy subject for audit than many others. We propose that this requirement be attenuated to advice only, or on a frequency deemed appropriate by a risk and/or audit committee. We further suggest that this approach be adopted across all prudential standards where audit is currently mandated.

CPS230 contains requirements that the Board not only review and approve the business continuity plan, but also oblige the insurer to demonstrate that there has been appropriate Board challenge of the business continuity arrangements. This requirement is premised on the Board finding fault with, or questioning the veracity of the advice provided by management. In the event that internal and external audit reports find no control deficiencies and where there is no other source of information to contradict this, mandating Board challenge is a removal of the Boards discretion and the addition of a task that will be performed out of obligation rather than genuine need. We propose this requirement be changed to require demonstration of Board scrutiny, rather than challenge.

Submission to Australian Prudential Regulatory Authority – APRA on behalf of BHP Marine & General Insurances Proprietary Limited. October 2022.

CPS230 like many other Prudential Standards has a set of principles/objectives at the top of the standard that indicate the objectives of the underlying requirements. We understand that it is APRA's view that these objectives and principles should be what auditors or other assurance providers reference when determining whether the measures in place are sufficient and proportionate (as the standards apply to a range of institutions). We have observed over a number of years that internal and external auditors, instead of auditing against the principles and using the requirements as areas of focus, instead use the obligations as a de facto 'checklist' and require the auditee to demonstrate compliance with each line. We propose the strengthening of advice provided within the standard and externally that enables auditors to act with more discretion. We further suggest that this approach be adopted across all prudential standards.

Thank you for the opportunity to comment upon CPS230 and provide feedback. I would welcome the opportunity to discuss any of these matters further, should APRA require any further information.

Richard Hearn
Managing Director

BHP Marine & General Insurances