Exposure Draft of the Critical Infrastructure Risk Management Program Rules

SAP Australia Response

Version: [<1.0>]
Date: 1 May 2026

Table of contents

Background **3**
Response **3**
Reiteration of SAP general feedback to December 2025 discussion paper 3
Applying the enhanced CIRMP to the data storage or processing asset class 3
Expanding the enhanced CIRMP to all CIRMP-applicable asset classes 4
Conclusion **5**

This document is SAP Australia's response as the Responsible Entity for a Critical Infrastructure Asset to the Exposure Draft of the Critical Infrastructure Risk Management Program Rules issued 30 March 2026.

Background

SAP is the responsible entity for a critical data storage or processing (DSoP) asset; thus, is not directly impacted by the amendments detailed in the exposure draft. However, SAP and the critical DSoP sector more generally is in the supply chain of the other critical sectors. Indeed, its asset registration is triggered by the storage or processing of business-critical data of other critical infrastructure asset owners (SOCI Act s12F(2) refers). Reflecting on SOCI Act implementation experience to date, there is significant potential the amendments introduce indirect regulatory impact, often based on varied interpretation of the Act and its subordinate Rules. SAP has experienced varied interpretation from several customers on the same regulatory security baseline as SAP, and there is already disparity between security baselines where a DSoP asset enables, or is otherwise in the supply chain, of systems of national significance.

SAP responded to the December 2025 consultation paper that discussed the amendments and made comment on the potential for indirect regulatory impact to lead to unnecessary regulatory impost on entities already subject to the Act and how this may be avoided.

Response

SAP acknowledges the feedback provided at Annex B of the exposure draft. General feedback row 3 states "Submissions commonly suggested the inclusion of additional asset classes and sectors to the enhanced CIRMP Rules.". In addressing the feedback, the Department noted the asset classes were identified due to their risk profile, and the expansion of the enhanced Rules would not extend beyond them. It noted the enhancements are considered best practice and encourages voluntary compliance for all assets.

SAP is in a good position to voluntarily follow the enhanced CIRMP Rules and will do so as far as is reasonably practicable. This may mitigate the challenges identified in its response to the December 2025 consultation paper. SAP's rationale detailed in the earlier response for applying the enhanced CIRMP to the data storage or processing asset class or to all asset classes is repeated herein for the purpose of context.

Reiteration of SAP general feedback to December 2025 discussion paper

Applying the enhanced CIRMP to the data storage or processing asset class

In CSIRO's engagements as part of its Critical Infrastructure Protection and Resilience mission with the Trusted Information Sharing Network, particularly the Resilience Expert Advisory Group, observations were made that critical infrastructure assets rely on electricity, telecommunications,

DSoP, and space technology assets for enablement of their own essential service delivery. Noting space technology does not yet have a defined asset class, focus herein is placed on the other three asset classes as cross-sector enabling assets.

SAP suggests that any disparity between CIRMP obligations between the owners of these cross-sector enabling assets and critical infrastructure assets singled out for the proposed enhanced CIRMP will likely create increased contractual demands and potential commercial tension between parties. It may also increase operational overheads to the cost of delivery, which could drive up service costs to customers.

It is safe to assume that all assets that are subject to the enhanced CIRMP are dependent on the cross-sector enabling assets. Taking one as an example, a broadcasting asset owner, subject to its interpretation of the SOCI Act and the CIRMP Rules, may seek to place contractual demands on its suppliers to mitigate risk to its essential service delivery. Currently, the broadcasting asset owner may rely in large part for its supply chain risk mitigation that its providers of electricity, telecommunications and DSoP services are regulated to the same security baseline as itself. In the case of its electricity reliance, the broadcaster and the electricity provider will remain on the same baseline as their CIRMPs are enhanced. In the case of telecommunications reliance, the broadcaster and their telecommunications provider will share the same security baseline assuming the enhanced CIRMP reflects the enhancements to the TSRMP. In the case of DSoP reliance, the broadcaster and their DSoP provider will not share the same security baseline and there may be increased contractual demands. Particularly so, considering the DSoP sector's trigger for asset registration is based on being in the supply chain of other critical infrastructure asset owners, i.e., storing or processing their business-critical data (SOCI Act s12F(2) refers). Extrapolating this potential contractual demand across the nine asset classes subject to the enhanced CIRMP, the DSoP sector may become subject to a greater regulatory impost than if it had been subject to the enhanced CIRMP requirements.

Therefore, SAP suggests including the DSoP asset class for the enhanced CIRMP. This would apply to those assets, principally software-as-a-service, that are not covered by the strategic hosting certification exemption from having a CIRMP at s30AB(4) of the SOCI Act, effectively imposing the enhanced CIRMP on critical infrastructure assets that are software-as-a-service. Arguably, this would pose less of a regulatory impost than multiple customers with multiple contractual demands to enable their enhanced CIRMP obligations.

Expanding the enhanced CIRMP to all CIRMP-applicable asset classes

Noting the statement of issue that there is an increasingly dynamic, diverse and changing security environment requiring a flexible approach to risk identification and mitigation, SAP suggests the environment could rapidly adapt to capture any of the critical sectors or asset classes as warranting an enhanced CIRMP. SAP considers that creating two differing regulatory baselines may erode confidence across the critical infrastructure community in the collective attainment of a common foundation for defence against cyber and other threats.

Therefore, SAP suggests expanding the enhanced CIRMP requirement to all asset classes that currently have a CIRMP obligation. There could be a process of prioritisation for those asset classes identified by the intelligence community as currently more prone to targeting by hostile foreign state actors and their proxies. For example, a less cyber security mature asset class that is not currently identified as higher risk could be given an extended timeframe for implementation.

Conclusion

SAP is not currently subject to the proposed enhanced CIRMP. SAP is concerned that operating two sets of CIRMP requirements would create two security baselines and diminish confidence in security practices between entities within the critical infrastructure community. This may create challenges and increased regulatory impost for the DSoP sector, which has cross-sector enabling assets, based on contractual demands from customers designed to enable their compliance while addressing any disparity between the current and enhanced CIRMPs.

Therefore, SAP reiterates its rationale to apply the enhanced CIRMP to all asset classes or to the DSoP sector specifically. However, SAP will seek to voluntarily implement the enhanced CIRMP requirements as far as reasonably practicable to mitigate the potential for conflict between customers' and SAP's security baselines regulated under the SOCI Act.

www.sap.com.