SAP NEW ZEALAND

SAP RESPONSE TO DISCUSSION DOCUMENT ‘STRENGTHENING THE RESILIENCE OF AOTEAROA NEW ZEALAND'S CRITICAL INFRASTRUCTURE SYSTEM

SAP New Zealand

8 August 2023

SAP RESPONSE TO STRENGTHENING THE RESILIENCE OF AOTEAROA NEW ZEALAND'S CRITICAL INFRASTRUCTURE

SAP New Zealand, a subsidiary of SAP SE (**referred to henceforth as 'SAP'**) a leading global software provider, would like to thank the Aotearoa New Zealand Government for the opportunity to contribute to the Strengthening the resilience of Aotearoa New Zealand's critical infrastructure (CI) Discussion Document (**the Document**).

SAP is a major provider of corporate software solutions to critical industries and government across the New Zealand economy. Globally, a large proportion of our customers are CI owners. For over 30 years we have continued to update our solutions to meet customer demand, evolving cybersecurity threats and legal requirements, including a significant move to offering our software through cloud-based solutions. Thus, we take particular interest in the inclusion of cloud services and data storage as two areas of potential CI identified in the Document.

SAP offers a response with respect to its experiences as a CI owner and participant in CI reform in Germany and Australia, which have both brought data storage and processing, i.e., cloud computing, into their CI mix. Therefore, our response is limited to considerations of cloud services and data storage, noting our role as a significant supplier of business software to companies that are likely to become CI providers in a resilient New Zealand CI system.

As a general comment, SAP suggests that availability of cloud services and data storage within New Zealand may be restricted by the small size of its population and business community. This may limit opportunities to apply regulation to cloud-based software with a limited amount being directly hosted within New Zealand. Noting that Australia is utilised by global cloud providers as a regional hub, and that CI regulation of cloud computing exists within Australia, we suggest it may be prudent to consider Australian registered CI as an option for the New Zealand Government and CI owners to use as part of a risk-based approach to cloud adoption. This would accelerate adoption of a NZ CI system by offering greater access to global software offerings, with assurance of Australian regulation.

Our response to the Document's questions is at Attachment A. We have responded in a manner relevant to our context and experience.

ATTACHMENT A

RESPONSES TO SPECIFIC QUESTIONS RAISED BY THE PAPER (USE THIS TO ANSWER SPECIFIC QUESTIONS)

Prelude: Objectives for and principles underpinning this work programme

Does more need to be done to improve the resilience of New Zealand's critical infrastructure system?
Yes, it is prudent to review what infrastructures support the delivery of essential services to New Zealanders, particularly in consideration of the changing technology landscape, which includes a shift to cloud computing to attain global economies of scale.

How would you expect a resilient critical infrastructure system to perform during adverse events?
It should perform with minimal loss of essential service delivery to an extent that economic disruption is minimised, and societal cohesion and national security are maintained. It should function as a complete system, recognising interdependencies across the infrastructures that support the delivery of essential services.

Would you be willing to pay higher prices for a more resilient and reliable critical infrastructure system?
SAP is subject to operating costs within each country it has a presence and offers no opinion in this regard.

The work programme's objective is to enhance the resilience of New Zealand's critical infrastructure system to all hazards and threats, with the intent of protecting New Zealand's wellbeing, and supporting sustainable and inclusive growth. Do you agree with these objectives? If not, what changes would you propose?
Yes.

Do you agree with the proposed criteria for assessing reform options? If not, what changes you would propose?
Yes.

Section 1: Background and context

Why a new regulatory approach may be required

The paper discussed four mega trends: i) climate change, ii) a more complex geopolitical and national security environment, iii) economic fragmentation, and iv) the advent and rapid uptake of new technologies. Do you think these pose significant threats to infrastructure resilience?
Yes, they do. However, we note that new technologies offer opportunities to increase resilience over time. It will be vital to have legislative and policy agility to both respond to threats and harness opportunities arising from rapid technological change.

Are there additional megatrends that are also important that we haven't mentioned? If so, please provide details.
No.

Do you think we have described the financial implications of enhancing resilience accurately? If not, what have we missed?
Yes.

Section 2: Potential barriers to infrastructure resilience

Building a shared understanding of issues fundamental to system resilience

How important do you think it is for the resilience of New Zealand's infrastructure system to have a greater shared understanding of hazards and threats?
It is very important. We suggest a review of the German UP KRITIS[1] and Australian Trusted Information Sharing Network (TISN)[2] as models for government-to-industry and industry-to-industry communities of practice that support shared understanding.

If you are a critical infrastructure owner or operator, what additional information do you think would best support you to improve your resilience?
Cyber threat intelligence and national security intelligence are useful for a CI owner's contextual awareness, particularly with respect to the four megatrends noted herein.

What do you think the government should do to enable greater information sharing with, and between, critical infrastructure owners and operators?
Establish an effective community of practice; note our previous response regarding UP KRITIS and TISN. Consider a collaboration and communication channel between a New Zealand community of practice and the Australian TISN, noting that for cloud computing, some providers are likely to feature in both nations' CI community.

Setting proportionate resilience requirements

Would you support the government having the ability to set, and enforce, minimum resilience standards across the entire infrastructure system? If so:

- **what type of standard would you support (e.g., requirement to adhere to a specific process or satisfy a set of principles)?**
- **do you have a view on how potential minimum resilience standards could best complement existing approaches to risk management?**

We support the government having the ability to do so. We note the two approaches we have exposure to:

- Germany, a systems certification and audit approach, featuring risk management.
- Australia, a risk management and attestation approach, featuring systems certification.

The two approaches are complementary, for example certifications generally involve risk management uplift, and well implemented certification criteria are compensating controls that contribute to mitigation of risk.

We note the importance of any certification requirements being built on a foundation of globally recognised frameworks/standards, or those that are demonstrably equivalent to them. This should reduce regulatory burden on companies that are operating globally or domestic companies that are aligning to global standards.

Regarding risk management, the Australian approach of risk management at the centre of CI resilience with an attestation from executive management as to its efficacy has the potential to be effective. It is in its infancy; however, it should enable innovation of approach and reduce the cost of compliance and potential regulatory duplication in comparison to a country CI-specific audit regime.

[1] See BSI - UP KRITIS (bund.de)
[2] See Trusted Information Sharing Network (cisc.gov.au)

In the Australian case audit activities relating to global certifications and standards can form part of the internal processes for delivery of an attestation.

Would you support the government investing in a model to assess the significance of a critical infrastructure asset, and using that as the basis for imposing more stringent resilience requirements? If so:

- **what options would you like the government to consider for delivering on this objective?**

Yes. The Australian Systems of National Significance model may be a good approach to monitor as it is rolled out. It has promise to be effective as it recognises the operating context of a particular CI and CI owner, allowing for negotiation of enhanced cyber security obligations that are both tailored to that operating context and the needs of the Government to have greater assurance for the resilience of the most critical of infrastructures.

What criteria would you use to determine a critical infrastructure asset's importance? investing in a model to assess a critical infrastructure asset's criticality, and using that as the basis for imposing resilience requirements that are more stringent on particularly sensitive assets? If so:

- **what options would you like the government to consider for delivering on this objective?**
- **What features do you think provide the best proxies for criticality in the New Zealand context?**

Criteria should be based on the extent of loss of:

- social cohesion
- economic disruption
- national security
- military capacity for the defence of New Zealand.

It is important that the risk of such loss is at the heart of any determination of importance. The Government should avoid imposing enhanced resilience requirements on CI owners that are not commensurate with the impact of the loss of the CI.

Managing significant national security risks to the critical infrastructure system

Do you think there is a need for the government to have greater powers to provide direction or intervene in the management of significant national security threats against a critical infrastructure? If so:

- **what type of powers should the government, consider?**
- **what protections would you like to see around the use of such powers to ensure that they were only used as a last resort, where necessary?**

We think there is a need and are supportive of those in the Australian legislation. We consider there should be sufficient legislated checks on power that consider the importance of open engagement with the CI owner to achieve a collaborative approach to threat and incident management, as is the case in the Australian legislation (at least conceptually).

Creating clear accountabilities and accountability mechanisms for critical infrastructure resilience

Do you think there is a need for a government agency or agencies to have clear responsibility for the resilience of New Zealand's critical infrastructure system? If so:

- **do you consider that new regulatory functions should be the responsibility of separate agencies, or a single agency?**
- **do you consider that an existing entity should assume these functions or that they should be vested in a new entity?**
- **how do you see the role of a potential system regulator relative to sectoral regulators?**

Ideally there would be one agency with overall regulatory authority for CI, working closely with regulators of established sectors/capabilities to ensure existing regulation is leveraged as part of resilience and regulatory duplication is avoided. The Government could consider the creation of an entity within an existing department of state, such as the Australian Cyber and Infrastructure Security Centre formed within the Department of Home Affairs. The German model of having an existing agency, the Federal Office of Information Security (BSI), take on the CI regulatory function is also workable.

Do you think there is a need for compliance and enforcement mechanisms (e.g., mandatory reporting, penalties, offences) to ensure that critical infrastructure operators are meeting potential minimum standards? If so:

- **do you consider that these should be applied to the entity, to the entity's directors/executive leadership, or a mix of the two, and why?**

Yes. Mechanisms are important to encourage proactive efforts to ensure resilience. Regarding mandatory reporting, we suggest the Australian model of an annual attestation report by the chief executive officer (however described) of a CI owner is a good approach to ensuring operators are meeting potential minimum standards. This is because the executive will necessarily take an active interest in compliance. We discussed the value of an attestation rather than an audit approach earlier in our response. We suggest audit powers should be exercised on an exception basis.

Regarding penalties or offences, in examining the Australian legislation as a contemporary example, it will be heavily dependent on the context of any specific noncompliance as to whether they would apply to the entity or the entity's directors/executive leadership.