



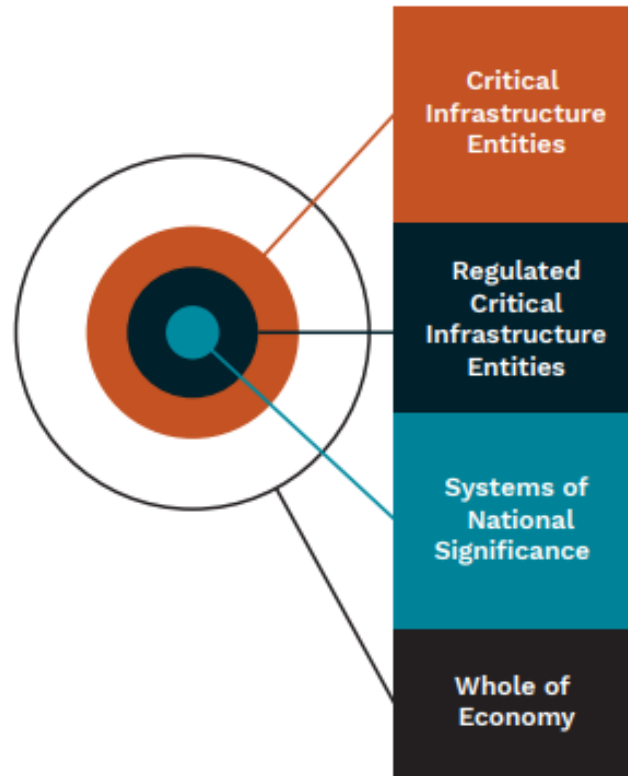
Australian Government

Department of the Prime Minister and Cabinet

Regulatory Impact Analysis

Applying RIA to Critical Infrastructure Investments

Cyber Security – challenges and context



Connectivity is integral during COVID-19

- Secure connectivity and secure digital platforms equally critical as we emerge from this pandemic

Critical infrastructure may not be front of mind, but you use it

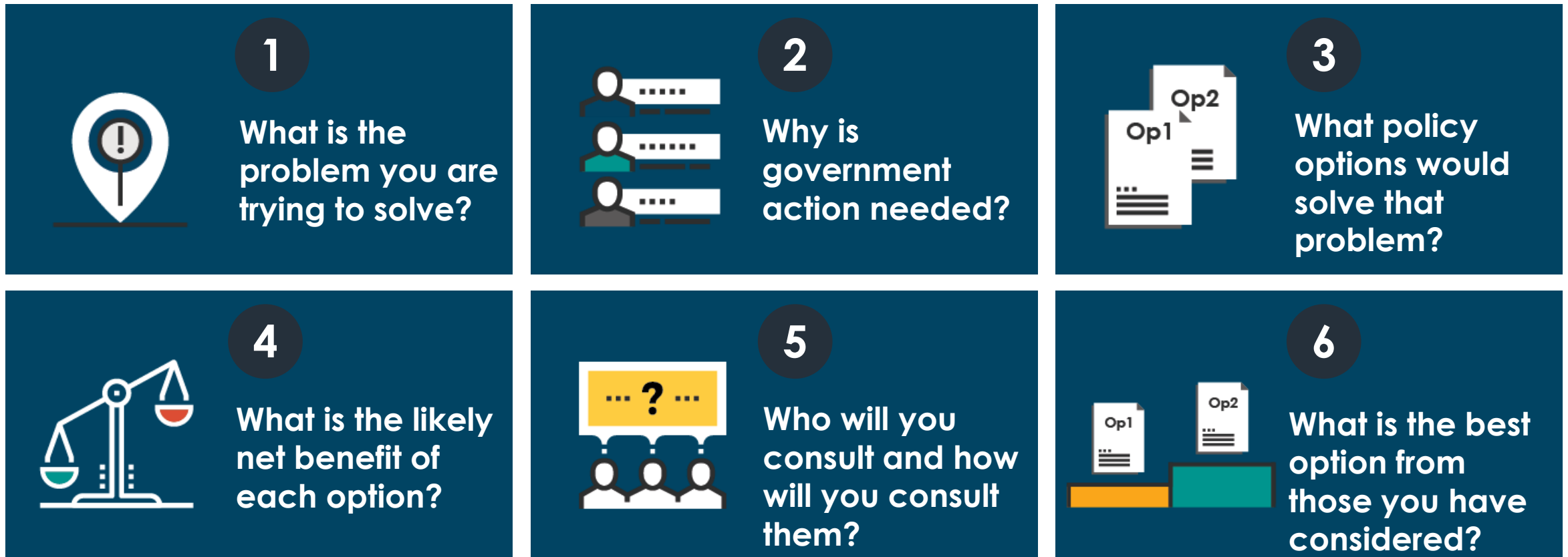
- Essential services are critical to us all, such as electricity, communications, transport and banking

Increasingly interconnected and interdependent services

- If one essential function is compromised, what might the domino effects be?

The Australian Government RIA framework

RIA is a methodology that explores the costs and benefits of items coming forward for Government decision with potential significant impacts. These are the key overarching questions answered when doing impact analysis



Applying RIA to cyber security issues

Trying to completely mitigate cyber security risks effectively could well come with costs

There are benefits as well, but how do we quantify these?

- It is almost impossible to estimate the risk, extent or frequency of certain events occurring

The nature of this risk is always changing

- Reducing some risks through better precautionary measures doesn't mean there won't be newer and more novel cyber security threats

Applied example – incident reporting

- Notifying cyber incidents to the Cyber Security Centre
- Even minor changes in the design of this component could mean large variances in impacts on businesses



Office of Best Practice Regulation - Resources



For more information on the Australian Government's Regulatory Impact Analysis framework and settings, visit us at: www.pmc.gov.au/regulation

In Australia, RISs are released at: <https://ris.pmc.gov.au>

Follow the OBPR @pmc_gov_au on Twitter and LinkedIn and the hashtag #OBPRgov