Cyber Security Update

June 2021

Tim Daly & Jason Smith

The threats are real and increasing…

What we know about the 'sophisticated, state-based' cyber attack on Australia

By Dannielle Maguire

Posted Fri 19 Jun 2020 at 11:35am, updated Fri 19 Jun 2020 at 5:48pm

Every level of Australian government is currently under attack by hackers.

This is what the PM has told us about it so far.

Who is being attacked?

Mr Morrison **wasn't specific** about the hackers' individual targets, but all levels of government, critical infrastructure and essential services have been affected.

"This activity is targeting Australian organisations across a range of sectors, including all levels of government, industry, political organisations, education, health, essential service providers and operators of other critical infrastructure," Mr Morrison said.

Source: https://www.abc.net.au/news/2020-06-19/cyber-attack-no-australian-government-organisations-explained/12373190

Bloomberg

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra

June 5, 2021, 5:58 AM GMT+10

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

LISTEN TO ARTICLE

▶ 4:58

The hack that took down the largest fuel pipeline in the U.S. and led to shortages across the East Coast was the result of a single compromised password, according to a cybersecurity consultant who responded to the

LIVE ON BLOOMBERG

Watch Live TV

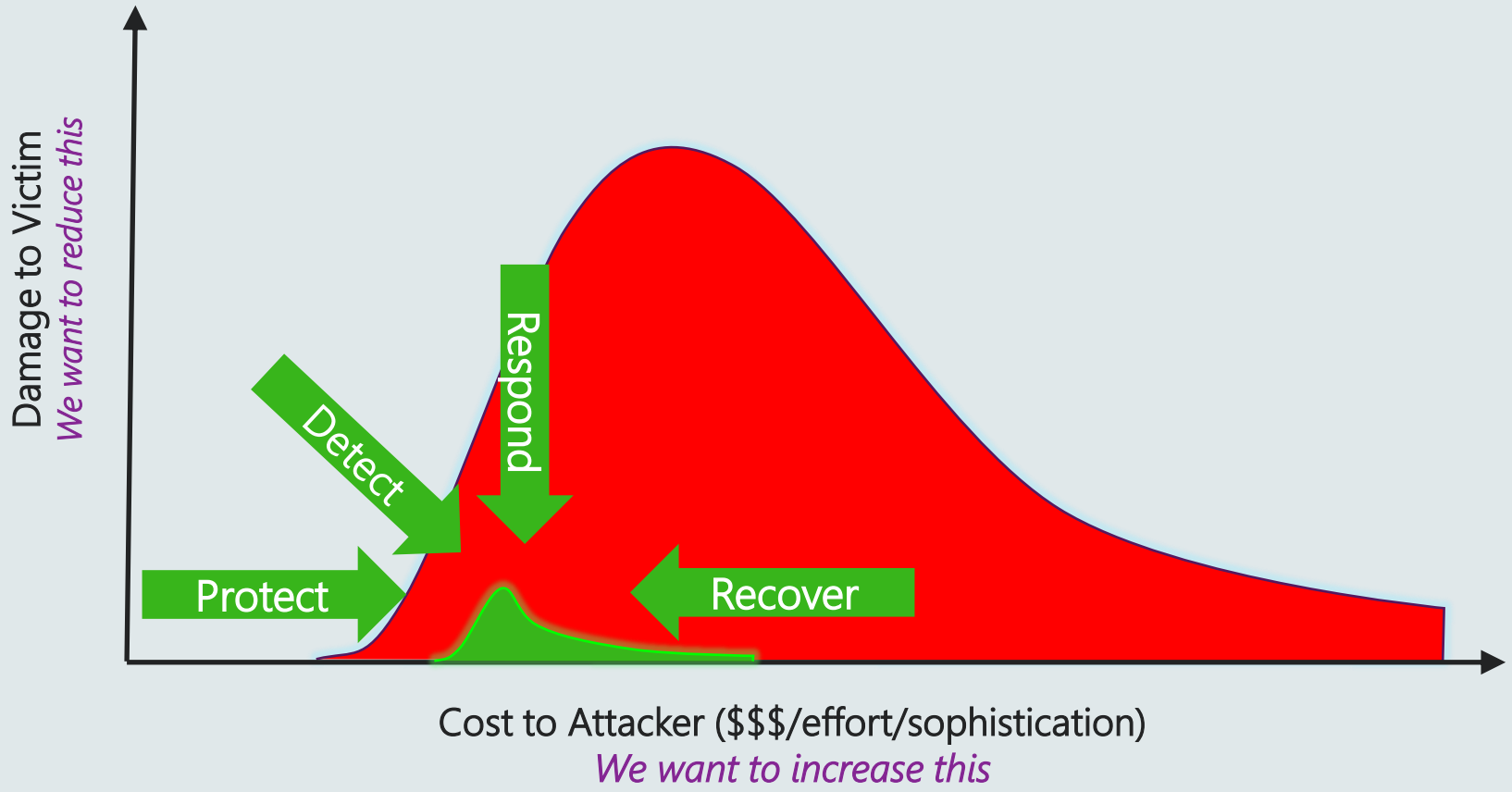
Listen to Live Radio

Source: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

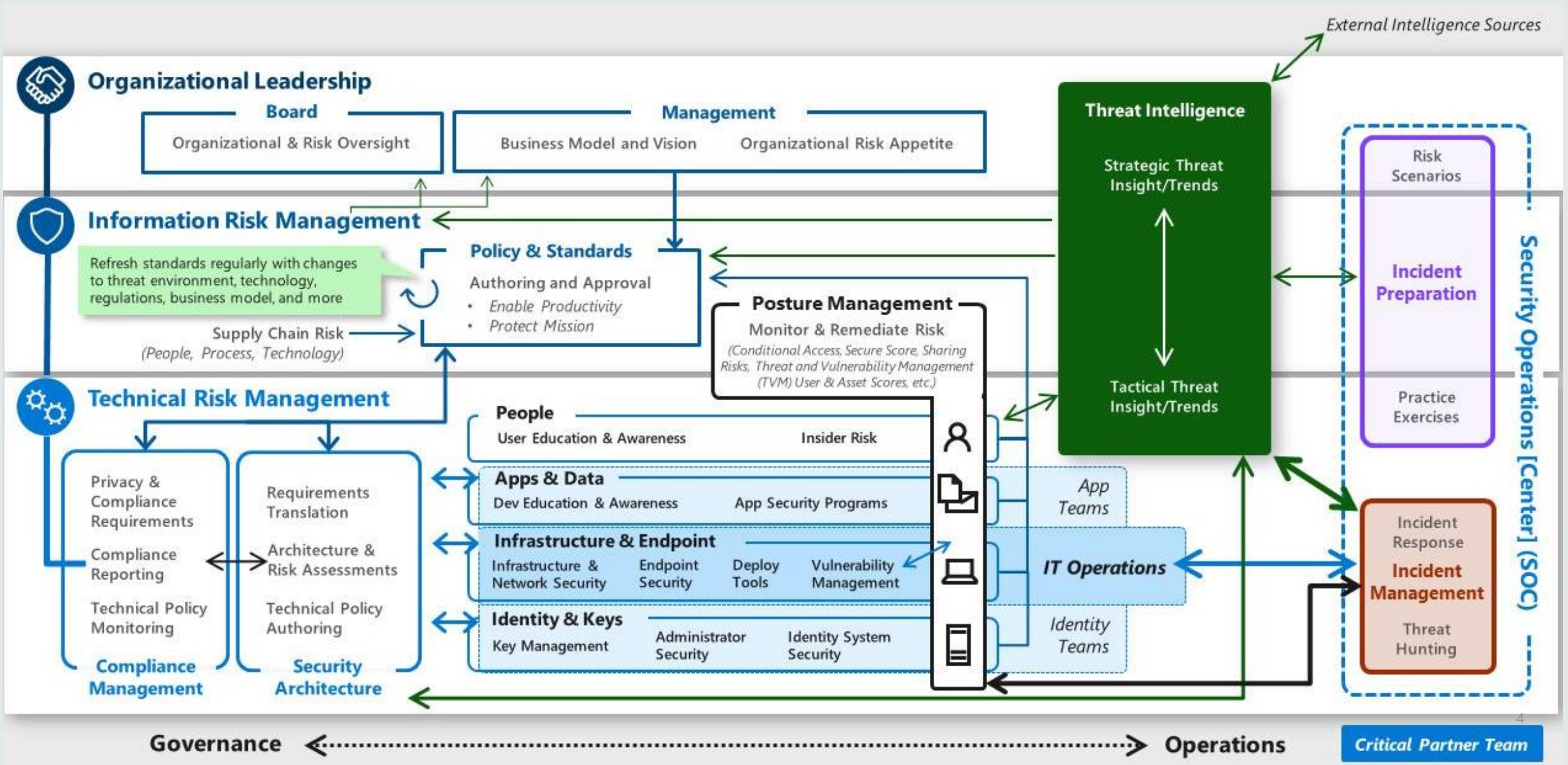
Cyber – what does good look like?

- Attacks are going to happen
- Huge amount of change and complexity
- There is no such thing as perfect security
- Need to have baseline protective controls
- Understand and have visibility of the environment
- Rapidly detect and respond to attacks early



AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

Managing Cyber Resilience @ AEMO – on a Page



SOCI Act Reforms

Protecting Critical Infrastructure and Systems of National Significance (CI SONS)

Risk Management Plan

AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE CENTRE

Protecting Critical Infrastructure and Systems of National Significance

Governance Rules - Risk Management Program

1 June 2021

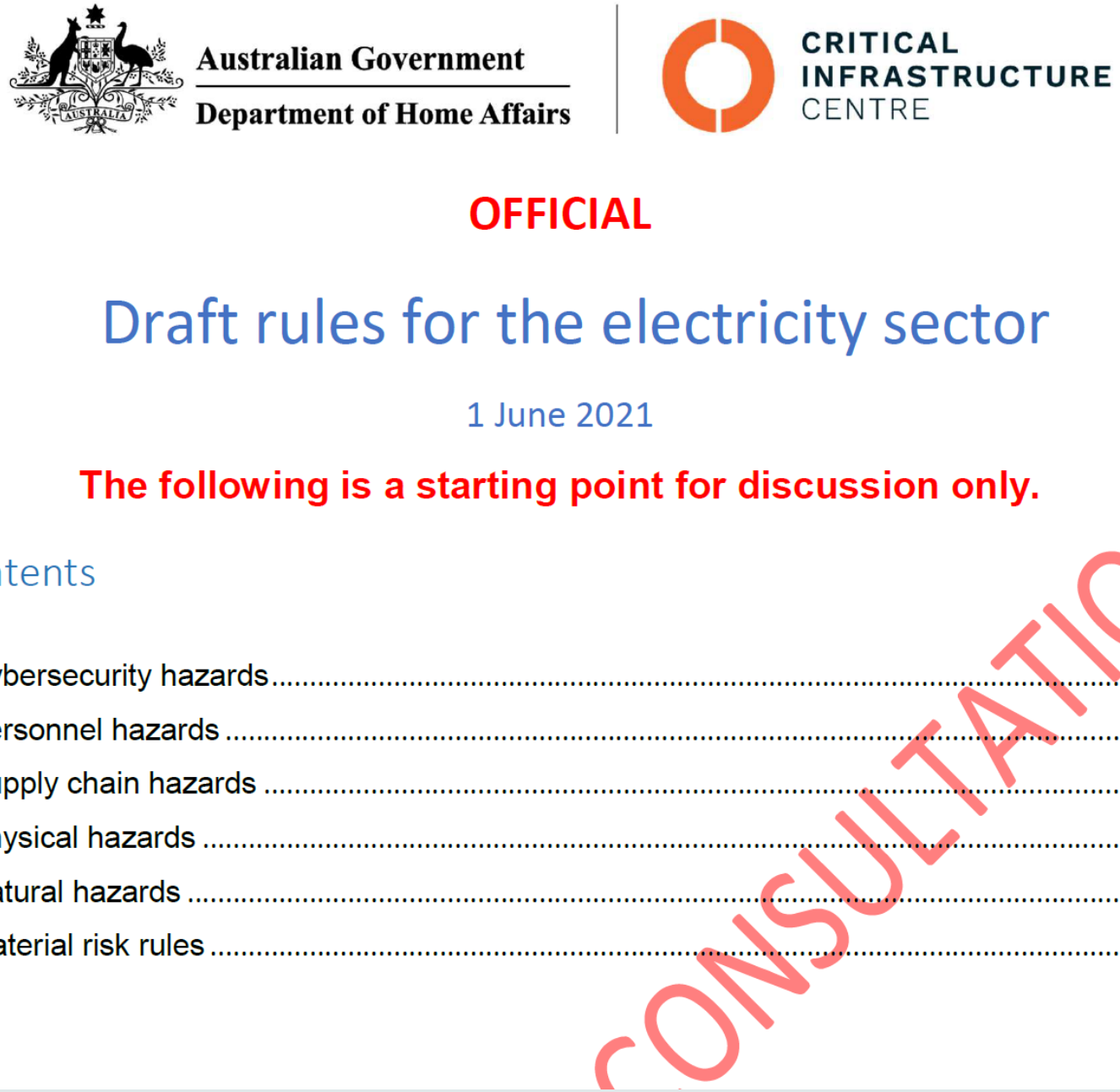
1. Responsible entities must, within six months of the commencement of this rule, document in their risk management program:
    a. the process by which the responsible entity identifies it's context for risk management purposes; and
    b. the outcomes of the entity's risk context identification process.
2. Responsible entities must, within six months of the commencement of this rule, ensure that their risk management program includes details of the individuals responsible for the development and implementation of the risk management program as a whole, as well as the activities detailed within.
3. Responsible entities must, within six months of the commencement of this rule, document in their risk management program how they will take a holistic approach to risk management, outlining how the entity will consider the relevant impact of different material risks on their assets and the mitigation or minimisation of those threats or hazards across their organisation.

SOCI Act Reforms

Protecting Critical Infrastructure and Systems of National Significance (CI SONS)

Electricity Sector Rules

AEMO
AUSTRALIAN ENERGY MARKET OPERATOR



Australian Government
Department of Home Affairs

CRITICAL INFRASTRUCTURE CENTRE

OFFICIAL

Draft rules for the electricity sector

1 June 2021

The following is a starting point for discussion only.

Contents

CONSULTATION

SOCI Act Reforms

Protecting Critical Infrastructure and Systems of National Significance (CI SONS)

Cyber -> AESCSF

AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

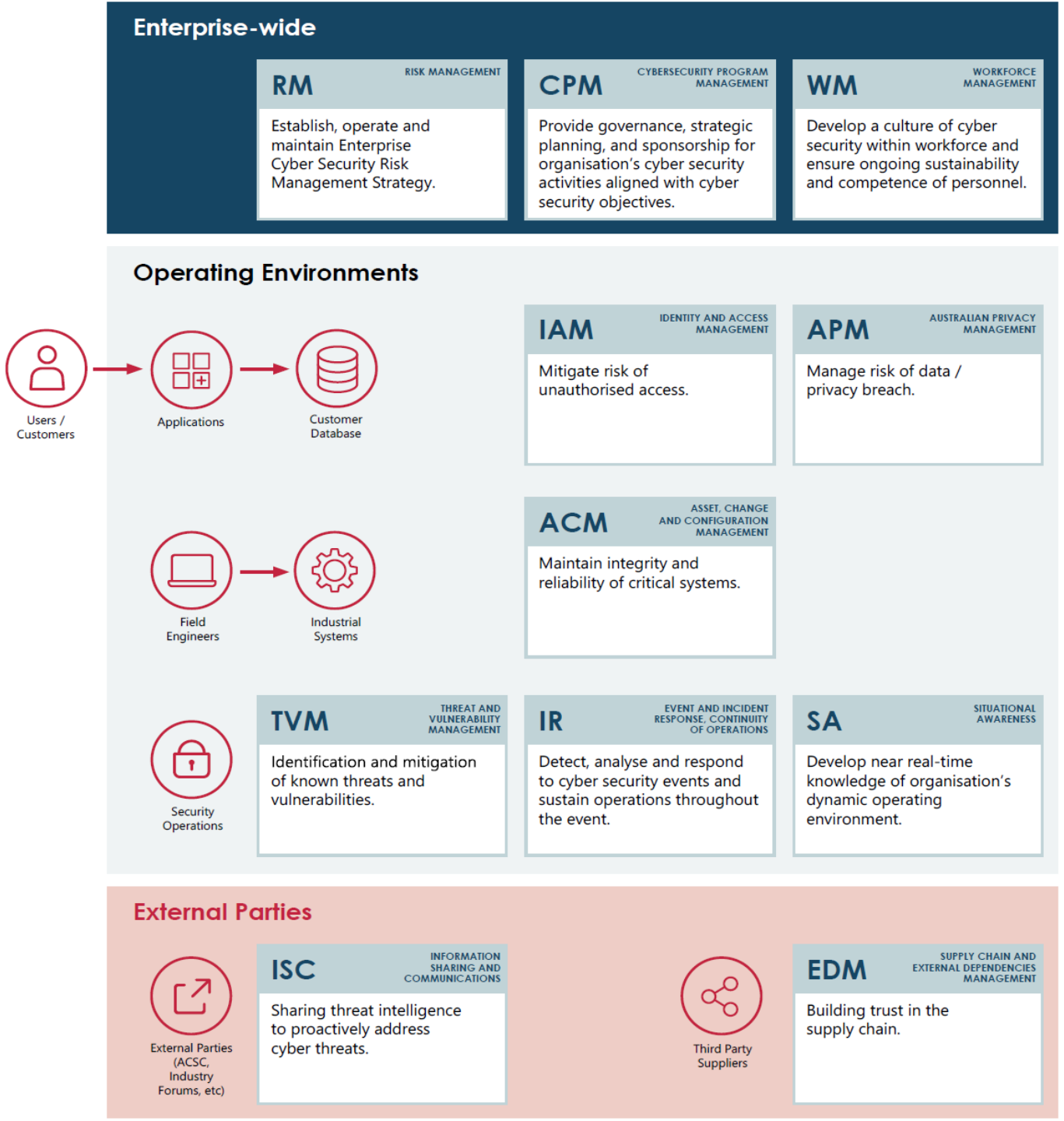
Cybersecurity hazards

The Department intends that the rules promote a general uplift of cybersecurity across the sector. The Australian Energy Sector Cyber Security Framework has been identified as an appropriate and common standard used across the electricity sector that aligns with Government policy. The framework, based on United States Department of Energy States Cybersecurity Capability Maturity Model (C2M2) and further refined by the Australian Energy Market Operator and Australian Cyber Security Centre (ACSC), in consultation with industry, is a suitable measure of target state maturity for the energy sector. Security Profiles (SP), based on Maturity Indicator Levels (MIL) and refined by the ACSC, have been identified as the appropriate requirement for responsible entities for critical electricity assets to achieve because practices, patterns and anti-patterns apply collectively across all domains, and not independently to each domain like MIL.

1. Responsible entities for critical electricity assets must, within 12 months of the commencement of this rule, ensure that their risk management program includes mitigations that comply with the requirements to meet SP-1 of the Australian Energy Sector Cyber Security Framework within 12 months of the commencement of this rule.
2. Responsible entities for critical electricity assets that are:
    a. electricity generation assets with an installed capacity of greater than or equal to 250MW;
    b. transmission network assets;
    c. distribution network assets; or
    d. interconnector assets

    must, within 24 months of the commencement of this rule, ensure that their risk management program includes mitigations for technology networks connected to these assets that comply with the requirements to meet SP-2 of the Australian Energy Sector Cyber Security Framework.

Australian Energy Sector Cyber Security Framework (AESCSF)



AEMO
AUSTRALIAN ENERGY MARKET OPERATOR


AEMO
AUSTRALIAN ENERGY MARKET OPERATOR