This proposed addition is related to the new 2023-2030 Australian Cyber Security Strategy, strategy Shield 6, and the addition of a new paragraph.

Shield 6: Resilient region and global leadership

Implementing cybersecurity standards according to best practices

The problem we face:

Information and cyber security play a vital role in all types of organizations. Every organization possesses data that requires protection from malicious actors and threats. Considering the rising number of attacks and data loss statistics, every organization must adhere to specific standards to enhance its information security.

Organizations must know where to begin and how much they should protect their data. In addition to existing requirements such as the Security of Critical Infrastructure Act 2018 and the 2023-2030 Australian Cyber Security Strategy concerning information security, there will be a need for a step-by-step guide to attain security standards equivalent to some international best practice standards. Organizations face challenges due to an insufficient workforce and lack of skills, particularly in cyber security.

How the Government will take action:

Organizations need to establish a dedicated cyber security department and appoint a senior cyber security officer equipped with the necessary skills in the field. They should also adhere to best practices such as Essential 8 compliance, ISO 27001 from the International Organization for Standardization, and the Payment Card Industry Data Security Standard (PCI DSS) for all entities handling customer and financial data.