This proposed addition is related to the new 2023-2030 Australian Cyber Security Strategy, which is about the new Shield strategy.

Shield 7: Enforcing information security audits facilitates continuous improvement.
Australian businesses must prioritize periodic information security audits to validate recommended controls for securing organizational data.

What success looks like
By 2030, the Australian government will emphasize the implementation of cybersecurity controls across all organizations, focusing on validating these controls through periodic audits to ensure continuous improvement and validation of cybersecurity measures.

How we'll get there

To achieve our 2030 vision, the Australian Government will:

- Assist businesses in conducting periodic individual and third-party cybersecurity audits.
- The Australian government will ensure that all businesses undergo audits to validate the implementation of cybersecurity strategies across all organizational functions.

The problem we face
Implementing cybersecurity controls is crucial for safeguarding organizational assets, but many organizations need help validating whether these controls are implemented effectively. In today's rapidly evolving cyber landscape, there's a pressing need to continuously optimize and adapt cyber controls to address emerging threats and attacks. However, organizations often need to catch up and achieve continuous improvement, leading to uncertainty about the adequacy and currency of their cybersecurity measures.
Organizations often need help validating cybersecurity controls regularly due to constraints such as limited resources and budgets. There needs to be a strategy or administrative framework to ensure the continuous improvement of cybersecurity controls.

How the Government will take action

The Australian government mandates and supports businesses to conduct periodic audits, either internally or through third parties, to validate cybersecurity controls. Audit reports must adhere to Australian cybersecurity standards and recommendations.

1. **Conduct cyber security Periodic audits.**

   Organizations must strategize, oversee, and track the rapid evolution of technologies to facilitate introducing and maintaining new products, services, and delivery channels. Given these changes and the growing dependence on technology, comprehensive cybersecurity audit coverage becomes indispensable for an effective overall audit program. This audit program should encompass technology risks across the organization, including cyber security management, strategic planning, cyber security operations, physical and information security, electronic products and services, systems development and acquisition, and business continuity planning, among other areas.

   The cyber security audit function within organizations should ensure that an approved audit program, overseen by senior management, encompasses the following key components:

   Annual Audit Plan: This plan should outline the budgeting and planning processes for cyber security audits, including goals, schedules, staffing requirements, and reporting protocols.

   Risk Assessment Process: Establish a process for describing and analyzing the risks inherent in each line of business to determine the scope and frequency of audits.

   Audit Cycle: Develop a cyber security audit cycle that determines the frequency of audits based on a robust risk assessment process.

   Audit Report Format: Define the format for audit reports to ensure consistency and clarity in communicating findings.

   Document Maintenance and Retention Policy: Implement a policy for maintaining and retaining documents related to cyber security findings to facilitate accountability and progress tracking over time.

   Follow-Up Processes: Establish procedures for addressing significant cyber security audit findings, including timely follow-up actions to remediate identified issues.

   By adhering to these components, organizations can ensure a structured and practical approach to cyber security auditing, enhancing their overall security posture and resilience to cyber threats.