Measure Resilience, Not Participation

The Cyber Wardens post-mortem shows that government can report strong participation while remaining unable to determine whether small-business cyber risk fell.

Prepared by Benjamin Mossé | 29 July 2026

Government can fund cyber activity at scale without knowing whether risk fell

1. Cyber Wardens was funded to improve small-business cyber resilience at scale.

2. Its disclosed evaluation tracked enrolments, graduations, engagement and participant intentions.

3. These measures demonstrated reach and participation, but not whether businesses implemented stronger controls or experienced less loss.

4. **Without verified outcomes, government cannot determine which interventions worked, whether public money reduced risk or what it should fund next.**

Cyber Wardens could report progress without verifying protection

1. The disclosed evaluation did not include before-and-after verification of stronger controls.
2. Evaluation focused on participation, satisfaction and intentions.
3. A platform test obtained a certificate without viewing all content.
4. The program demonstrated delivery—not reduced risk.

Survey respondents of Course Level 1 reported high levels of likelihood to undertake actions in relation to common threats and basic technical cyber security after completing their Cyber-Wardens course. On a scale of 1-5,

- 86% (62/72) were likely or highly likely to ensure automatic updates were turned off , upgrade passwords, and apply multi-factor authentication (rating 4/5 or 5/5)
- 76% (53/72) were likely or highly likely to appoint a team member as a Cyber Warden

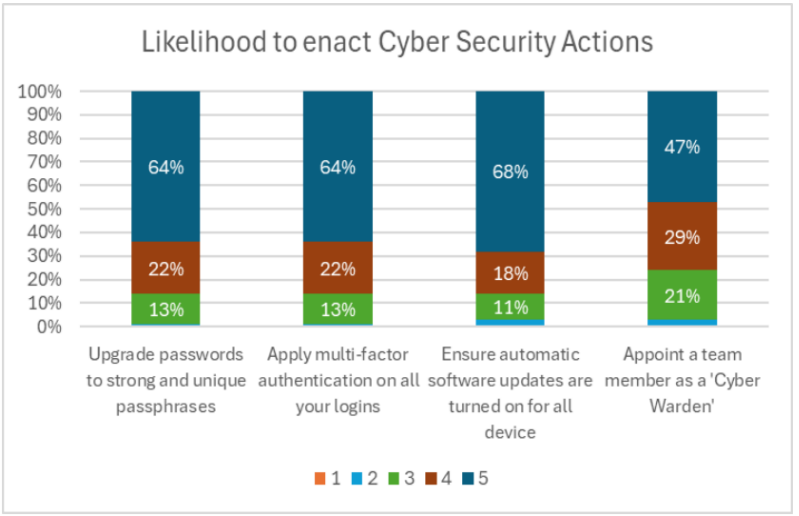
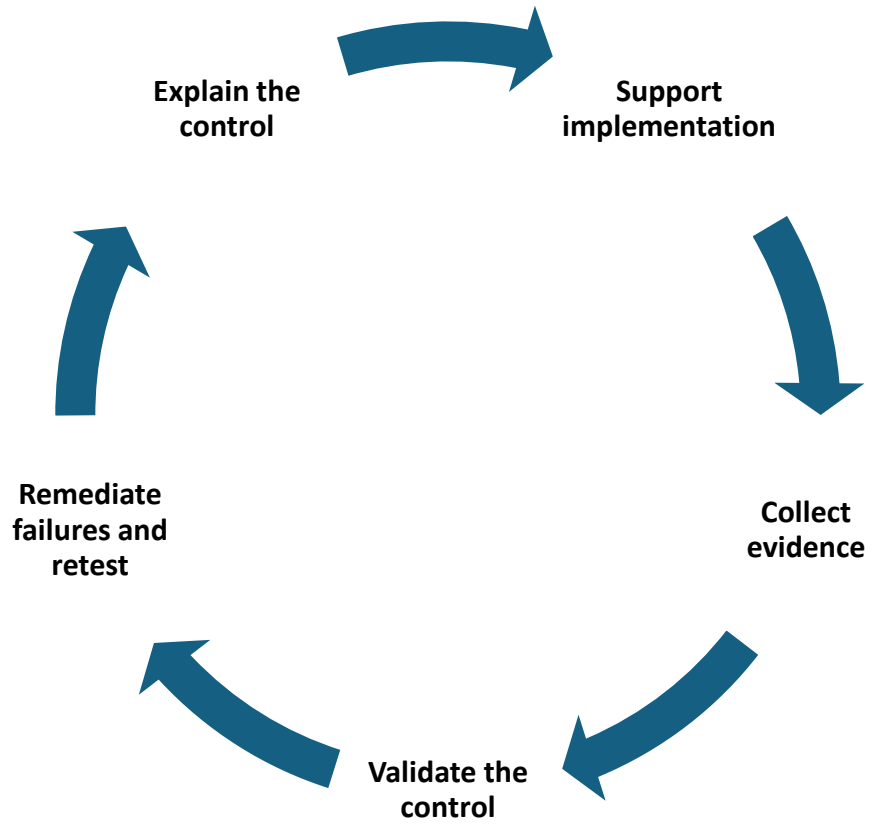


Figure 1: Graduation Survey, Course Level 1 responses to the question 'After Cyber Wardens Level 1 training, how likely are you to do the following?' with a rating of 1-5 (n=72).

Sources: Treasury FOI 4282; independent platform test conducted by Benjamin Mossé.

A closed assurance loop can verify implementation—and test what reduces loss

- Translate each recommended control into practical implementation steps and acceptable evidence.
- Combine automated checks, proportionate evidence review and expert support to verify implementation and remediate failures.
- Track verified controls separately from incidents and claims to test which interventions are associated with lower losses.



Conceptual closed-loop evaluation

Analysis of a GrantConnect export suggests the closed-assurance-loop insight may apply to $27.5–32.5 million in small-business grant funding.

Grant opportunity	Total funding	Funding in scope
GO1841 - Cyber Security Small Business Program	$10.0m	$10.0m
GO4346 - Business Connect and Protect	$6.9m	$6.9m
GO6705 - Small Business Cyber Resilience Service	$8.1m	$8.1m
GO7796 - ASBAS Digital Solutions Round 3	$25.1m	$2.5–7.5m
	Total:	**$27.5–32.5m**

Estimated cyber-relevant funding: Dedicated small-business cyber grants total $25.0m. The ASBAS estimate assumes cybersecurity represents 10–30% of its $25.1m funding because it is one of five program capabilities.

Data Export date: 29th of July 2026.

Apply the Cyber Wardens lesson to one grant already protecting small businesses

Decision requested: Approve the application of a closed assurance loop to one current small-business protection grant.

Use an existing grant. Do not commission another pilot.

1. Select one active grant and assign an accountable senior owner

2. Add implementation guidance, acceptable evidence, proportionate validation, remediation and retesting

3. Report participation, verified controls, incidents and losses separately—and use the findings to improve the grant while it is still running

Appendix A: Cyber Wardens was funded to improve resilience, but its headline targets measured scale

Grant summary table:

Grant element	Detail
Funding	Up to $22.995 million
Period	2023–24 to 2025–26
Recipient	COSBOA
Delivery partner	89 Degrees East
Objective	Help small businesses protect themselves from cyber threats

Headline program targets:

Target	Number
Enrolments	60,000
Graduates	50,000
Recertifications	24,000
Small businesses reached	15,000

Source: Department of the Treasury, FOI 4282. Targets are not mutually exclusive.

The grant defined ambitious targets for participation and reach but no equivalent target for verified control implementation or reduced loss.

Appendix B: The evaluation established reach and engagement—not implementation or reduced risk

Evaluation table:

Measure	What it established	What it did not establish
Marketing reach	Exposure to the program	Business action
Enrolments and graduations	Course participation	Control implementation
Engagement and retention	Use of the content	Improved security
Satisfaction and NPS	Participant experience	Reduced risk
Knowledge and intention surveys	Self-reported learning and plans	Completed action

Evidence ladder:

Evidence level	Status
Reduced incidents and losses	Not established
Verified control implementation	Not established
Knowledge and intended action	Measured
Reach and participation	Measured

Source: Department of the Treasury, FOI 4282. Assessment is limited to the records disclosed under the FOI release.

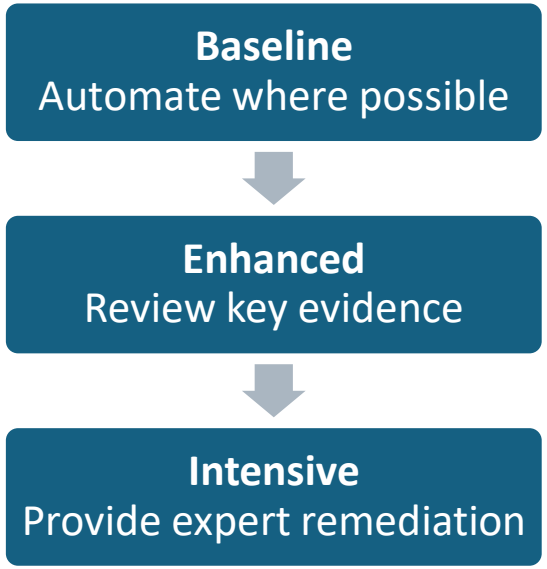
The disclosed evaluation could show who participated and what they reported not whether businesses became safer

Appendix C: Assurance should increase with business risk and complexity

Proportionate assurance table:

Level	Business profile	Validation approach	Support
Baseline	Micro business using standard cloud services	Automated checks and guided evidence	Self-service guidance
Enhanced	Small business with multiple systems or moderate exposure	Automated checks plus targeted manual review	Reviewer assistance
Intensive	Complex environment, high exposure or repeated control failure	Detailed evidence review, remediation and retesting	One-on-one expert support

Conceptual model. Eligibility, evidence and review thresholds would require policy, privacy and technical design.



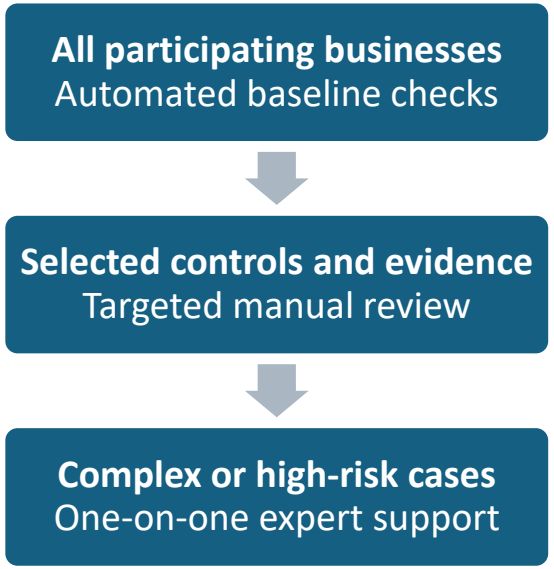
Every level follows the same loop: guide → evidence → validate → fix → retest.

Appendix D: Automation provides scale; human review provides assurance

Validation method table:

Control or evidence	Method	Examples
Externally observable controls	Automated testing	Exposed services, email-domain protection, web security
Internal configuration evidence	Manual review	Screenshots, redacted logs, backup tests, security settings
Complex or failed controls	Expert support	Legacy systems, recovery failures, unusual environments

Illustrative operating model. Automated testing should be limited to authorised and legally permitted checks.



Use the lowest-cost method that can credibly verify the control

Consent • Data minimisation • Redaction • Retention limits • Quality assurance

Appendix E: Control selection should combine technical evidence with observed loss data

Evidence-source table:

Evidence source	What it contributes	Limitation
Security agencies	Threat intelligence and technical experience	Does not quantify loss reduction for this business segment
Frameworks and standards	Structured control guidance	Controls may lack public actuarial validation
Insurers and incident responders	Claims, incident frequency and loss severity	Selection bias, policy limits and under-reporting
Program assurance data	Implementation rates and practical feasibility	Requires longitudinal incident and loss tracking

Public actuarial validation showing which Essential Eight or SMB1001 controls reduce losses for Australian micro and small businesses could not be identified.

Control-prioritisation matrix:

	Low feasibility	**High feasibility**
Strong loss evidence	Support deployment	Prioritise
Limited loss evidence	Deprioritise	Test before scaling

Control selection should combine technical advice with de-identified claims and incident data from insurers, actuaries, brokers and incident-response providers.

Technical soundness, practical implementation and demonstrated loss reduction are different questions and government should measure all three