Joint Committee of Public Accounts and Audit

Answers to Questions on Notice

Department/Agency: Australian National Audit Office
Inquiry: Cyber Resilience: Inquiry into Auditor-General's Reports 1 and 13 (2019-20)
Committee Member: Ms Lucy Wicks MP
Type of question: Written
Date set by the committee for the return of answer: 4 August 2020

Questions regarding measuring a cyber-resilient culture

During the previous hearing, the Committee heard about the importance of a strong cybersecurity culture within Commonwealth entities and the community generally. In particular, the ANAO advised that they developed their own framework for measuring culture, as one did not previously exist (see Table 1 of Submission 6 – Supplementary Submission 1).

1. **Can you please explain how you developed this framework? Was there any consultation involved?**

Answer

JCPAA Report No. 467 (2017), *Cybersecurity Compliance*, recommended that in future audits on cybersecurity compliance, the ANAO outline the behaviours and practices it would expect in a cyber resilient entity, and assess against these.[1] Auditor-General Report No. 53 Cyber Resilience, included a list of 13 behaviours and practices (reproduced in Table 1 of Submission 6 – Supplementary Submission 1) that may assist agencies to build a strong cyber security compliance culture and meet mandatory requirements.

The 13 behaviours listed in Table 1 can be used to measure culture, but this does not necessarily mean that an organisation that exhibits these behaviours is cyber resilient. Having a good culture helps achieve compliance. The behaviours should be read in context with our assessment against the Protective Security Policy Framework (PSPF) Policy 10 requirements[2] and IT general controls (ITGC), which are the other factors that were considered by ANAO for assessing cyber resilience.

The ANAO analysed guidance and reports in relation to governance, risk management and cyber security across relevant Australian government frameworks, policies and standards, such as but not limited to the following:

- Protective Security Policy Framework;
- Information Security Manual;
- Commonwealth Risk Management Policy;

[1] JCPAA Report 467, *Cybersecurity Compliance*, Recommendation 6, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/CybersecurityCompliance/Report_467

[2] PSPF Policy 10, *Safeguarding information from cyber threats*, specifies the implementation of four ACSC mitigation strategies for mitigating common and emerging cyber threats, and the consideration of the other remaining ACSC mitigation strategies for mitigating cyber security incidents.

- Australian Cyber Security Centre (ACSC) Cyber Security Surveys and Essential Eight Maturity Model;
- National Institute of Standards and Technology Cybersecurity Framework; and
- Reports and guidance on risk culture from other regulatory bodies, such as Australian Prudential Regulation Authority and Australian Securities and Investments Commission.

The ANAO sought input from: the Attorney General's Department; Australian Signals Directorate; Digital Transformation Agency; senior executives of the non-corporate Commonwealth entities involved in the cyber security performance audits between 2013 and 2018; and cyber security specialists within firms, such as United States Government Accountability Office, KPMG and PwC.

2. How were the 13 behaviours and practices identified as key to a strong cyber-resilient culture?

Answer

The 13 behaviours and practices were identified through the review of relevant guidance, reports and consultation with policy and audited entities. Through that development process, the 13 behaviours were noted as being common against the audit entities.