Joint Committee of Public Accounts and Audit

Answer to Questions on Notice

Department/Agency: Australian National Audit Office
Inquiry: Commonwealth Financial Statements 2019–20
Date of inquiry: 15 September 2021
Committee Member: Mr Julian Hill MP, Deputy Chair
Type of question: Hansard, page 16-17
Date set by the committee for the return of answer: 01 October 2021

Number of pages: 2

Question

Mr HILL: So I suppose the question that I would put to you, and perhaps to Finance and ASD, to reflect on is: is there a systemic question, given cyber noncompliance IT issues in this case—sorry, the financial controls. It's a consistent topic. It's been running for years, and the self-assessments by agencies are shown to be consistently flawed every time the Auditor-General goes in, and it is of great concern and frustration to this committee and others in the parliament. Is there a need for an additional level of assurance sitting over cyber self-assessments, with some parallel, perhaps? We have a robust set of arrangements over financial auditing, and the Auditor-General frankly rarely finds serious errors or mistakes. We're introducing a system that the government has approved and that the committee has been working on for some years over assurance over the performance reporting framework and auditing of it. Is there an issue with cyber? I'd invite you to comment on that. Should we be looking at some kind of external assurance in the system so it doesn't just rely on the Auditor-General almost randomly wandering in, given the current system simply isn't working? Stunned silence.
CHAIR: I am not sure if there is a freeze on the technology.
Mr HILL: Maybe if I could put that to the Auditor-General, then Finance, then ASD, in that order.
Mr Hehir: Our performance audits would consistently raise concerns and make findings about the lack of assurance in that space.
Mr HILL: Before I pass to Finance, is there any comment you could make as to what a system of assurance could look like?
Mr Hehir: We've tended to keep away from what it would look like, for the standard audit excuse of not wanting to define what the framework is and then go and audit it. It would more raise concerns. I think the level of assurance that you put in place should be associated with the [inaudible] that you observe. Our commentary has generally been that the current level of assurance, which is basically largely attestation by entities, isn't consistent with the risk framework that we observed in implementation.
Mr HILL: In the interests of time I'll pass to the other agencies. I fully appreciate your reluctance to make a recommendation, if you like, or to have a stab at an answer. If it is possible for you to reflect on it and give us a short supplementary response to the question, it might help expand our thinking. Perhaps you could illustrate two or three different ways that an assurance framework around cyber could look. Is that a more doable thing?
Mr Hehir: We'll look at answering that.

Response

The ANAO does not provide detailed advice on management frameworks as this would impact independence when an audit is then undertaken on an activity subject to the framework.

Entities are required to report against the Protective Security Policy Framework (PSPF) on an annual basis. In Auditor-General Report No.32 of 2020–21 *Cyber Security Strategies of Non-Corporate Commonwealth Entities*, the ANAO recommended that the Attorney-General's Department implement arrangements to obtain an appropriate level of assurance on the accuracy of entities' PSPF Policy 10 self-assessment results.

In the ANAO's response to recommendation 4, *JCPAA Report 485: Cyber Resilience*, the ANAO noted that if there was an assurance process implemented by the Attorney-General's Department to assess the accuracy of entities' self-assessment, the ANAO could review such an assurance process.

An assurance framework should be designed to provide an appropriate level assurance. In determining the appropriate level of assurance required consideration should be given to the likelihood and impact if a risk were to eventuate, and the effectiveness of controls in place to mitigate the risk. Where risk is low, then a low level of assurance maybe be determined to be appropriate, and the nature and extent of procedures may be more limited. For example, the assurance may simply involve receiving attestations for very low risks or periodic sample based reviews of systems and processes (ie the appropriateness of policies and robustness of internal reviews). Where the risk is higher or there are issues with the effectiveness of controls, then the level of assurance and nature and extent of procedures should be more robust. For example, adding to a review of the control processes detailed substantive testing of the actual activity (ie whether the relevant PSPF policies are actually implemented).