

Dear Q&A

Who should track, validate and close findings from external IT penetration tests?

Answer

In 2021, IIA-Australia issued a Factsheet 'Getting Audit Actions Implemented', which can be found at: https://iia.org.au/sf_docs/default-source/technical-resources/2018-fact-sheets/factsheet-getting-audit-actions-implemented.pdf?sfvrsn=2

Every time an audit, review or evaluation is commissioned in an organisation, there are typically improvement actions to be implemented by management.

An internal audit role is often to monitor and track these to ensure they are properly implemented in a timely way. While internal audit should track audit actions from its reports, it doesn't matter who tracks audit actions from other audits, reviews and evaluations so long as there is effective tracking and follow-up.

Without effective tracking and follow-up, the cost and effort involved in audits, reviews and evaluations is potentially wasted if things do not change for the better. All remedial and improvement actions should be tracked, with progress reported to senior management and the audit committee from reports containing recommendations from:

- › Internal audit.
- › External audit.
- › Reviews by scrutineers and subject matter experts.
- › IT reviews.
- › Evaluations.
- › Significant enquiries.
- › Royal commissions.

There should also be a formal close-out process for each recommendation when action has been fully implemented – close-out should not be left to the implementer to decide.