

## Dear Q&A

### Is it appropriate for an audit committee to direct the chief audit executive to change the internal audit report observation rating process?

#### Answer

The manner in which internal audit observations are ranked is a matter for an individual organisation. Best practice is that internal audit observations align with the corporate risk appetite and risk rating process in use across the organisation. The reason for aligning in this way is to ensure internal audit observations receive no more or no less attention than they would deserve had they been raised in another way.

In a well-governed organisation, the risk appetite and rating process will have been approved by the board (or its equivalent). This is an important step as these items help managers in the organisation make rational decisions about priorities and resource allocation. It helps ensure decisions are aligned with the wishes of the board.

Internal Audit Standard 2500 'Monitoring Progress' requires the chief audit executive to "establish and maintain a system to monitor the disposition of results communicated to management". While this will take into account relative risk and will not be unnecessarily onerous for low level risks, the Internal Audit Standard does not say "subject to board approval". Internal Audit Standard 2600 does require the chief audit executive to escalate any situation where a manager accepts "a level of risk that may be unacceptable to the organisation". This would include not acting on a matter identified by internal audit. Most internal audit functions routinely report all outstanding recommendations, remediation progress, and whether progress is acceptable given the risk.

In 2004 an independent report into a significant failure at a major Australian bank concluded the underling fault was not addressed partly because the fault had been given a rating that was below the threshold for consideration by the audit committee. The matter had been raised by internal audit but not accurately rated, and therefore not brought to the attention of the audit committee.

In 2016 a large local government council lost more than \$450,000 to fraudsters because management had failed to act on observations made by internal audit.

In indicating they do not wish to track a matter, the audit committee are relying on the internal audit function entirely in assessing its importance. But they are also encouraging matters that might become more serious over time to not be addressed. They are relying on the chief audit executive to get the initial rating correct and are assuming that the underlying circumstances (and therefore the risk) will not change.

While the audit committee are at liberty to make such a decision, they are exposing themselves and the organisation to potential harm.