The Institute of Internal Auditors Australia

Dear Q&A

Should organisations have a formal risk acceptance process where management temporarily accepts risks outside risk appetite and the closure process or where not all action has been completed and the residual risk may be outside risk appetite?

Answer

The fundamental point is that when an outstanding internal audit action is closed, then the risks as they exist at that point are being accepted. It is therefore sensible the closure process follows the risk acceptance path.

If the action is completed, there may be many good reasons for re-assessing the risk with the treatment in place to see whether it is acceptable. The situation should be placed before management of appropriate status to accept the risk. If the risk being addressed was outside the organisation risk appetite, then it may be unwise to assume the action has fully addressed the risk – ISO 31000:2018 'Risk management – Guidelines' Note 2 of 3.8 makes the comment that controls do not always have the effect intended. The organisation needs to be comfortable that it knows the risk that is left.

If the action is partially complete and more activity is scheduled, there may be justification in re-assessing the risk and deciding whether this risk should be temporarily accepted.

If the action is not completed, then management are accepting a risk as it was at the time the internal audit was completed.

The acceptance process should be the same in either case and should match the acceptance process in the rest of the risk management activity.

In summary:

- If the remaining risk is within risk appetite and no further action is proposed, then accept closure.
- If the remaining risk is not within risk appetite but more action is proposed, then do not close the action and refer the matter to the risk acceptance process – this may warrant a holiday in reporting but that will be driven by your process.
- If the remaining risk is not within risk appetite and no further action is proposed, then employ the organisation process for acceptance of such risks, which might mean reference to the board.

Regardless of the situation, these decisions should be reported to the audit committee. They may be happy with a bulk representation of lower rated risks, but higher rated risks would warrant a full description.