



01 February 2023

# Following up recommendations/management actions

## Chartered Institute of Internal Auditors

At the conclusion of an audit, findings and proposed recommendations are discussed with management and subsequently management action plans are developed to explain how the agreed recommendations will be implemented.

Competing priorities, budget limitations and other factors may prevent managers from implementing agreed actions in the agreed timeline or as previously designed to mitigate the risk. The purpose of follow up is to ensure that management has implemented the action, and that it has addressed the issue. In practice, this is often easier said than done!

The purpose of follow up  
Responsibility for follow up  
The follow up process  
Bespoke systems  
Policies and procedures  
Targeting high priority risks  
Follow up engagements

---

### The purpose of follow up

Managers who do not implement agreed actions arising from internal audit findings expose the organisation to risk. Following up on your actions helps to prevent this becoming an issue.

Arrangements need to be clear on:

- how outstanding recommendations/management actions will be tracked
- how resolution will be reported and validated
- what follow up action might be needed (this may also link to the nature of the risks/findings identified by internal audit – with high risk areas having more internal audit resource or input as part of the follow up)
- how this will be carried out in order to provide assurance that identified risks are being appropriately addressed.

The degree of follow-up activity may be influenced by the size and nature of the risk identified.

---

### Responsibility for follow up

Responsibility to resolve issues and manage agreed actions lies with management. Internal audit may help the organisation to track the implementation of actions and periodically follow up to see

that risks are being adequately managed.

The International Standards require internal audit activities to monitor what is happening to the results of audit engagements. This does not mean that internal auditors have to undertake the follow up but they do have to ensure that actions have been implemented effectively or that management has accepted the risk of not taking action. This applies to agreed actions from both consulting and assurance engagements.

---

## **The follow up process**

The International Standards recognise the importance of follow up to ensure management actions effectively mitigate the risk identified but are not prescriptive as to how it should be done as each organisation is different.

Where risk management is fully embedded, the monitoring of action plans arising from assurance activities may be integrated into wider performance reporting. In this situation management take full responsibility for all the related reporting, up to and including reporting to the audit committee.

For example, management at one bank compile a quarterly report for their audit committee that includes the status of all assurance recommendations/management actions and observations, including those from internal audit.

The report highlights whether recommendations/management actions are pending, in progress or complete in the form of a dashboard for senior management and committee use.

Similarly, an NHS trust forward copies of all assurance reports, including those from internal audit to a member of the organisation's risk management team who is responsible for logging all agreed actions on an internal tracking system.

In accordance with implementation deadlines an email is sent to the responsible manager to request confirmation that the action has or has not been implemented. The tracking log is then presented by the risk manager to the audit committee. Internal audit choose to independently verify implementation of some recommendations.

---

## **Bespoke systems**

Bespoke systems designed by the organisation or purchased from software suppliers can make follow-up more efficient and effective. This approach enables the ownership of actions to be assigned to managers and enables tracking of action through to completion.

Automated emails often notify and remind managers of tasks allowing them to add completed actions and up to date reporting. Such systems can either be set up by management or jointly with assistance from internal audit with input and viewing facilities assigned where appropriate. Software tools such as these are particularly helpful in large organisations where managers operate in different parts of the country or operate in different countries.

A UK FTSE100 organisation tracks internal audit recommendations/management actions using an 'audit work system' that establishes a review date and target implementation date. When actions

are approaching their review date a reminder is sent to the internal auditor.

This prompts the internal auditor to contact the operational owner and client audit liaison within 20 working days of the original target implementation date for a progress report. The progress update may be received directly from the client by email or from the audit liaison through the submission of a progress review on the 'audit work system'. The client audit liaisons can view the actions assigned to them and raise progress reviews from a partitioned web view of the 'audit work system'.

If the client has stated that the action has been completed and it was rated as critical or significant in the final report re-testing must be completed by internal audit within 20 working days of receiving the progress update from the client.

If the action is rated as 'requires attention' internal audit accept management's representation and do not do any further testing. In addition all closed critical and significant actions are subject to review by audit management and are re-opened if there is insufficient evidence to support their closure. Re-testing is completed on an action by action basis.

It is the internal auditor's responsibility on a quarterly basis to flag up the time they will need to re-test actions, so that it can be built into their quarterly schedule.

---

## Policies and procedures

In other organisations the internal audit activity itself asks managers to report back that management actions have been implemented and then report this feedback to senior management and the audit committee.

For example, a large government internal audit activity builds follow-up into the audit plan so that each assurance review has scheduled follow up within three months of the completion of the original audit.

The scope of the follow up work varies but for most actions it is obtaining an update from management on what they have done to complete the agreed actions. If particularly high priority actions were agreed, then the audit department undertakes some work to verify the effectiveness of that action such as testing operating effectiveness.

Where follow-up is conducted in this way, the chief audit executive needs to develop a policy and supporting procedures that are communicated to the organisation's managers and internal auditors for clarity. For example the policy needs to explain:

- The objectives of follow-up exercises.
- How they are to be conducted.
- The frequency of follow up.
- How follow up is scheduled and prioritised within the organisation's timetable and the internal audit plan.

The FTSE100 company referred to earlier includes the following detail in its internal audit quality management system. Action tracking is important because:

- It is an IIA International Standard to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action

- It provides an assessment of the commitment and effectiveness of management in implementing actions
  - It is a measure of our effectiveness. The implementation rate provides a further useful measure of our performance and is a control over the quality of our recommendations
  - It assures management of our commitment and may stimulate implementation when actions are about to be reviewed.
- 

## Targeting high priority risks

A truly risk focused follow-up plan is targeted at the higher priority risks irrespective of the organisational context or internal audit review within which the recommendation was raised.

To meet its objective the follow-up process in a risk-based audit approach should report how effective managers are at implementing risk responses. This might be action to avoid or transfer the risk as well as those actions that reduce the risk. However, in practical terms it might prove more sensible to follow-up both issue and root cause based upon the original audit report, or by other key criteria.

Follow up should consider whether actions have been implemented and whether the identified risks have been adequately managed with anticipated benefits, and if not, whether the residual exposure is within the identified risk appetite.

In general, the follow-up process helps to determine the effectiveness of management's response to risk. In other words, it should be used to provide objective data about how well management understand the scale and priority of their inherent risks, and how effectively they are able to develop control arrangements to mitigate those risks to acceptable (residual) levels.

When the chief audit executive believes that senior management has accepted a level of residual risk that may be unacceptable to the organisation, the chief audit executive must discuss the matter with senior management. If the decision regarding residual risk is not resolved, the chief audit executive must report the matter to the audit committee for resolution.

---

## Follow up engagements

It is essential for organisations to have a good understanding of their risks and how well they are managed. Discrepancy between reported risk responses and the actual status could mislead those who rely on the information.

Internal audit should perform sufficient work in order to provide objective assurance to senior management and the audit committee that management's response to risk is satisfactory. Essentially, this means following up audit work in areas that have recently been audited to ensure that there is adequate remediation. This work should be effectively targeted to provide independent confirmation that action is being taken and that risks are being managed effectively, for example the higher the risk rating/level of risk, the greater the level and depth of validation and verification.

Working collaboratively with managers so that they actively report and evidence where recommendations have been addressed will help reduce the amount of objective follow up work necessary.

Managers need to be aware that internal auditors are likely to check on the adequacy of some mitigation and that outstanding actions may be escalated to the audit committee and this will encourage them to take timely action. Where time is of the essence, the internal auditor could focus on areas where the risks have the greatest potential impact and high likelihood of occurring.

Depending on the culture within the organisation the internal auditor may need to inform senior managers and operational managers when and where follow up engagements will take place. In less formal situations it may simply be a case of scheduling a short visit or meeting. Either way the internal auditor needs to observe and/or gather evidence to determine that actions have been implemented.

Where opinions have been expressed, the auditor may need to consider whether any subsequent improvement in control might warrant the opinion assessment to be revisited.

This should be handled cautiously as other aspects may have changed since the area was originally audited and the follow-up activity may not be sufficiently detailed to revise the opinion.

---

## **Practice advisories**

2500-1 Monitoring progress

2500. A1-1 Follow up process