



Follow Up on Audit Findings

Ensure risks are remediated

By Scott C. Gerard, CPA

An internal audit report is not worth the paper it's written on unless management implements the action plans to remediate the issues reported. Consequently, our professional standards require the chief audit executive (CAE) to establish a follow-up process. The objective is “to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action.”¹

With all the compliance, information technology, cyber, clinical and operational risks in the healthcare industry, internal auditors must conduct thorough follow-up to make sure management has addressed the risks and deficiencies noted within issued audit reports.

“Internal audit reports in and of themselves create value, but this value is diluted if audit findings are not remediated within expected time frames and follow-up procedures are not performed timely,” stated Peter G. Hanelt, chair of the CommonSpirit Health audit and compliance committee. Rick Corcoran, board chair of SSM Health, added, “A formal and thorough follow-up process enhances an organization’s level of accountability and sends a strong message to

management that they are responsible for the timely implementation of corrective action plans.”

Comply with professional standards

Although the Institute of Internal Auditors (IIA) requires the CAE to establish a process for conducting follow-up activity, flexibility is allowed in the nature, timing and extent of follow-up, considering several factors, including:

- Significance of the audit finding
- Effort and cost associated with remediation
- Complexity of the management action plan (MAP)
- Impact to the organization if corrective action is not taken or fails

¹ The Institute of Internal Auditors, Performance Standards, 2500.A1, <https://na.theiia.org/standards-guidance/performance-standards/Pages/Performance-Standards.aspx> (requires login)



Most healthcare professionals agree and count on their CAE's flexibility. As Corcoran stated, "I would expect our internal auditors to adjust the nature and extent of their follow-up procedures to align with the severity of the associated audit finding."

No matter how an internal audit function determines the nature and timing of follow-up, the auditor must perform evaluation and testing procedures using the professional standards of evidence. Follow-up evidence needs to be as good as evidence used during the audit. The evidence must prove that the issue is resolved, and the related risk is mitigated.

Depending on the nature of the action plan, follow-up testing procedures should include examining written documentation, observing the controls, and/or performing substantive testing. Inquiry alone is not enough evidence to determine whether the action plan has mitigated the risk. Action plans should go through a follow-up validation process.

Validate MAP status

Internal controls are strengthened when action plans for issues are implemented and validated. Internal auditors must discuss all issues with process owners during each audit project so that process owners agree on the issues and take responsibility for formulating corresponding action plans.

Although some internal audit departments require follow-up audit activity only for high risk or top priority issues, any rating system related to internal audit issues is subjective. Consequently, many CAEs suggest following up on 100 percent of reported issues as a professional leading practice.

Aside from eliminating the subjectivity involved, if an audit function conducts follow-up procedures on all issues, management pushback or negotiation related to audit issue ratings during the audit closing meeting can be reduced. Process owners and management can trust that all issues will be treated equally for follow-up purposes.

Regardless of the follow-up work performed, you should:

- Gather enough evidence to determine of whether management's action plan was completed.
- Include documentation for all action plans tested and marked as complete in the work paper system along with detailed explanations as appropriate.

For any project in which a specialist—IT auditor, clinical auditor, 340B specialist or other subject matter expert—was involved, the lead internal auditor should coordinate the appropriate follow-up testing with the specialist. If the action plan was not appropriately implemented, the specialist will work with the lead internal auditor to communicate what still is required.

Consider innovative techniques

The following techniques offer leading and alternative practices to enhance the internal audit follow-up process.

Expand coverage of identified risks – To effectively complete follow-up on audit reports and at the same time expand audit coverage, some progressive internal audit departments have implemented an innovative audit methodology. When the auditors conduct their follow-up testing at hospitals or locations where the original audits were conducted, they conduct abbreviated audits at a select number of other hospitals or locations.

The abbreviated audits are limited to the risk areas that resulted in the significant issues noted from the original audit projects. The expanded coverage of the most important risks and action plans across the entire health system provides more value from the original project.

Leverage technology – Some internal audit departments that have implemented automated workflow and work paper applications have also implemented automated email alerts to remind action plan owners and executive leadership of upcoming due and past-due action plans. The emails also instruct the action plan owner about emailing supporting documentation to the auditor to facilitate the follow-up validation process.

Other internal audit departments have developed or acquired technology that allows action plan owners to provide ongoing status updates to the internal auditor and to upload documentation that supports the follow-up validation process.

Develop status reports

Status reported either to management or to a governance committee should be based on the original implementation

Follow-up sends a strong message to management that they are responsible for corrective action.

date even if the action plan owner has provided the auditor with a revised date for remediation. Statuses reported should include the following categories:

Complete – All related action plans were implemented and have mitigated the risk.

Not due – The incomplete action plan's original implementation date is beyond the status reporting date.

Past due – The original implementation date has passed and management has not completed implementation of all related action plans.

Will not be implemented – Management has decided not to implement the action plan as the risk is no longer applicable or management is accepting the risk. In all situations in which management chooses to assume the risk associated with not implementing an action plan on reported issues, the following actions should be taken:

- The CAE should ask governance to formally approve or acknowledge this assumption of risk to release internal audit from further responsibility for performing follow-up testing.
- If the internal auditors believe that management has accepted a level of residual risk that might be unacceptable to the organization, the CAE should discuss the matter with management and governance. The discussion could be held in an executive session during a governance committee meeting.

When multiple action plans exist for an issue, the CAE should report at the issue level rather than action plan level for the purposes of implementation status and mitigation effectiveness. When reporting the number of open or past-due issues, the CAE should keep in mind that the risk that led to the issue reported is not mitigated until all associated action plans are completed. If an issue contains several action plans and one or more of these action plans is past due, the status of the issue will be considered past due.

An issue that has been communicated as complete should be removed from future follow-up presentations.

Communicate with process owners and executive management

You must maintain regular communication with process owners and executive management in order to discuss the

status of open action plans and to collaborate and schedule follow-up validation as action plans are implemented. To promote a no-surprises approach, share these updates with process owners and executive management in advance of any governance meetings at which the status of follow-up is presented. Corcoran said, "I appreciate when our internal auditors and management collaborate to address open corrective action plans."

Internal audit teams that use electronic work paper systems should produce periodic reports of all open action plans along with each action plan owner's name and due dates. Regular reporting, monthly or quarterly, of open MAPs will summarize any coming due and past due items with action plan owners, along with functional management and senior leadership.

Regular communication keeps action plan owners, process-level management and executive management aware of action plans that need attention. Regular communication also demonstrates that the internal auditors are working collaboratively to report the current status of past-due issues to governance.

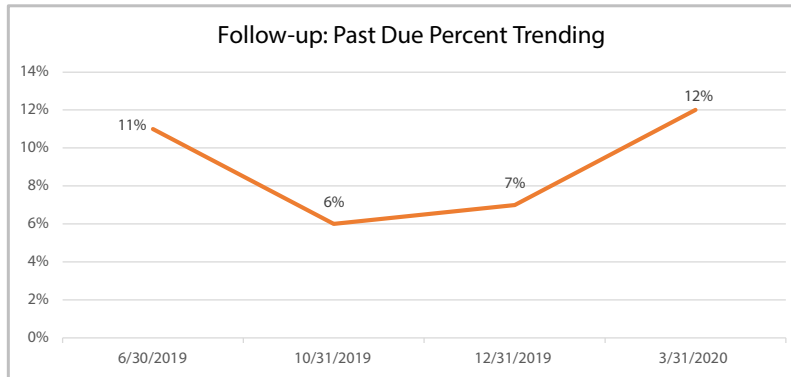
Validate the resolution of issues by testing the completion of action plans as they come due. The CAE should communicate to management the importance of maintaining controls necessary to sustain the mitigation of risk once internal audit has validated completion of the action plan.

Governance reporting

Internal audit is required to provide executive leadership and governance—typically the board audit and compliance committee—with independent and objective assurance that the organization's internal control, risk management, and governance processes are operating effectively. An issue reported by internal audit and its associated risks are not mitigated if not adequately and timely addressed by management.

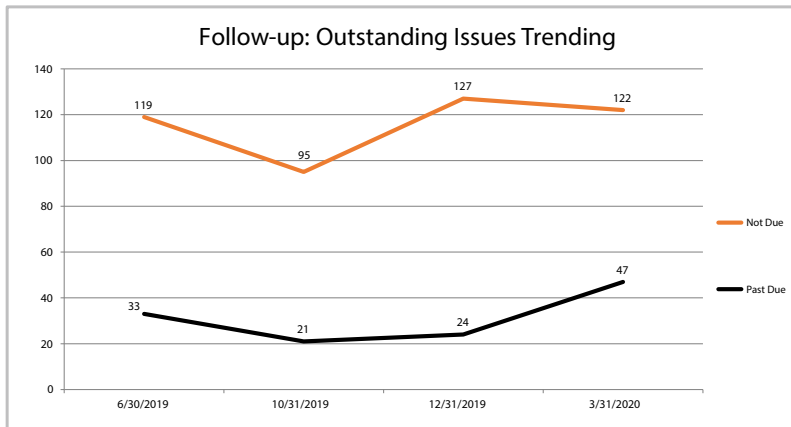
Publicize board committee reporting – Internal audit is responsible for tracking and reporting unresolved issues to the appropriate governance committee. Board audit and compliance committee members frequently use management's responsiveness to action plans as a barometer of the control environment across the organization.

Exhibit 1 – Percentage of open issues with past-due action plans



Source: Crowe, LLP

Exhibit 2 – Number of open MAPs not due and past due



Source: Crowe, LLP

A good practice for the CAE is to make sure all levels of management, including at the process level, the hospital level and the health system office, understand the scope of reporting. All stakeholders should be aware that the board audit and compliance committee receives periodic status reports related to past-due MAPs.

The CAE should request commentary from process-level management to discuss why an issue has not been resolved and why the action plans are past due. The practice provides the CAE with more detailed status and helps to increase the accountability of action plan owners as they become more aware that the audit and compliance committee is monitoring their efforts.

Establish an acceptable tolerance level for past-due MAPS – “An audit and compliance committee should not tolerate a high percentage of past-due MAPs; a high percentage correlates to a failure of management to support its investment in internal audit,” said Hanelt.

Some action plans are delayed for valid reasons—such as the time required to obtain funding, implement an automated solution, or obtain regulatory approvals. Consequently, some of the most engaged audit and compliance committees have set an acceptable tolerance level for past-due action plans.

To set a strong tone at the top, a committee might establish an informal not-to-exceed goal for past-due issues. For example, past-due issues may not exceed 10 to 15 percent of all open issues. The strong message to management regarding goals goes a long way to support the CAE in gaining cooperation from all levels of management in implementing open action plans.

Exhibits 1 and 2 are examples of ways to highlight the status of issues with past-due action plans for executive management and the board audit and compliance committee. The charts can inform and also generate discussions regarding trends identified, and can encourage management to focus attention when the number and percentage of past-due action plans begin to grow.

Conduct follow-up procedures once the action plan owner indicates that remediation is complete.

Consider your protocols

Communication and timing of follow-up activity – You should maintain regular communication with action plan owners and monitor action plan completion throughout the year. You should also conduct follow-up procedures as soon as practical once the action plan owner has communicated that remediation efforts have been completed.

Timing of follow-up could be affected by the auditor's location as compared to the location of the action plan owner and the auditor's ability to conduct validation testing remotely. For example, reviewing a data file, invoice or scanned document can be performed remotely. But observing controls within an operating room might not be able to occur remotely due to Health Insurance Portability and Accountability Act requirements or other challenges.

Supervision and review – Your internal audit department may be large enough to maintain a hierarchy including reviewers of work papers and reports. If so, then reviewers should be required to formally review and approve completed follow-up testing prior to reporting issues as complete to governance. The review should focus on whether the controls implemented, or activities completed by management, mitigate the original risk and whether the documentation within the audit work papers adequately supports the testing performed by the internal audit department.

The review should be formally documented in the audit work papers. A leading practice is for the auditor and reviewer to collaborate in advance of performing follow-up validation procedures, so they agree on the nature and extent of testing. Proactive collaboration also can reduce the likelihood of surprises after the follow-up testing has been performed and results have been communicated to the action plan owner.

Reporting of attorney-client privilege issues and follow-up status – Issues identified from internal audits under attorney-client privilege should be reported to governance committees separately in an executive session. The status of follow-up activity related to these audits also should be delivered in an executive session. The organization's attorney must be present to maintain the privilege.

Summary

While the concepts for following up on audit findings might be relevant to all industries, timely and thorough follow-up is especially critical to the healthcare industry due to financial and regulatory pressures. You should perform follow-up evaluation and testing procedures using the same high standards of evidence as used during the audit. Inquiry alone is not enough evidence.

Consider adopting leading practices that include:

- Regular reporting to action plan owners and executive management on past-due and coming-due MAPs.
- Follow up on 100 percent of reported issues to eliminate the subjectivity involved in determining which issues require follow-up and which ones are exempt from follow-up.
- Implement automated email alerts to remind action plan owners of coming-due and past-due action plans, and of documentation requirements.
- Set an acceptable tolerance for past-due action plans such as an informal not-to-exceed goal of 10 to 15 percent of all open issues.

A well-defined and structured process with clear expectations for you and your stakeholders will ensure that the risks identified in your audits are remediated. **DI**



Scott C. Gerard, CPA, is a partner at Crowe, LLP. He serves the healthcare industry with internal audit and business risk consulting services. Scott can be reached at (818) 325-8457 and Scott.Gerard@crowehrc.com.