

Contents

CONSIDERATIONS FOR BUILDING A QUALITY ASSURANCE IMPROVEMENT PROGRAM (QAIP).....	2
Background	2
QAIP ROLES AND RESPONSIBILITIES	3
QAIP Mandates / Program Objectives.....	3
QAIP Organizational Structure / Reporting Lines	3
Staffing Considerations.....	4
Independence Considerations for QAIP Team Members	4
QAIP SCOPE CONSIDERATIONS	5
Scope Considerations.....	5
QAIP Assessments.....	6
Internal Assessments.....	7
External Assessments	8
QAIP Plan Presentation	9
REPORTING.....	10
Internal Assessments.....	10
External Assessments	11
Audit Committee Reporting.....	11
Audit Senior Management Reporting	12
Regulatory Reporting.....	12
ISSUE TRACKING AND REMEDIATION.....	13
Tracking of Findings/Issues	13
Validation and Closure of Findings/Issues	14
Reporting Findings/Issues	14



CONSIDERATIONS FOR BUILDING A QUALITY ASSURANCE IMPROVEMENT PROGRAM (QAIP)

Internal audit (IA) functions in the financial services industry continue to be challenged to see what's coming around the corner and focus on the right things. In order to meet this challenge, most financial institutions have established a dedicated Quality Assurance Improvement Program (QAIP). While there are a range of acceptable variations in practice, the following sets out considerations from several U.S. financial institutions that could be used. These considerations are based on The Institute of Internal Auditors' (IIA) *International Standards for the Professional Practice of Internal Auditing* (Standards) as well as guidance from various U.S. regulators.

Background

A QAIP is mandated by The IIA through its International Professional Practices Framework (IPPF) Standard 1300 series, which requires that the chief audit executive (CAE) develop and maintain a QAIP as part of the internal audit function.

While IIA Standards apply universally, regulatory bodies have set forth additional guidance and expectations of the QAIP for its respective members. Those include both the Federal Reserve Bank SR 03-05, Interagency Policy Statement on the Internal Audit Function and its Outsourcing; and SR 13-01, Supplemental Policy Statement on the Internal Audit Function and Its Outsourcing; as well as the Office of the Comptroller of the Currency's Heightened Standard 3f; and the Comptroller's Handbook (Internal and External Audits).

Most banks have established dedicated QAIP teams. However, practices vary across financial institutions. To facilitate the sharing of best practices and to foster communication, a group of U.S. financial institutions have come together to prepare this white paper. Its objective is to spur discussion and to put forth suggested best practices that may be relevant to other financial institutions, depending on their individual circumstances.



QAIP ROLES AND RESPONSIBILITIES

QAIP Mandates / Program Objectives

The QAIP function should ensure that there is approved documentation to support its methodology and procedures, which promotes its ability to evaluate all aspects of IA activity and enables a comprehensive assessment of the IA function. Essentially, the QAIP function should act as the auditor of IA, as the primary objective of an effective QAIP function is to evaluate IA's conformance with IIA Standards, applicable regulatory guidance, and its own established procedures and methodology.

A secondary objective of the QAIP is to act as a driver of change. The QAIP helps to identify opportunities for continuous improvement in the effectiveness and efficiency of the IA function. The QAIP function provides assurance to key stakeholders — including audit committees (ACs), regulators, and external auditors — on the quality and reliability of IA's work.

As a leading practice, some QAIP functions may evaluate adequacy of practice through industry peer benchmarking to identify opportunities for improvement not otherwise identified through assessments of conformance with established procedures and guidance.

QAIP Organizational Structure / Reporting Lines

The QAIP function plays an important and unique role within IA. The QAIP function's organizational structure must be appropriately positioned to allow it to effectively and independently execute its mission. This includes considerations to ensure that the QAIP function has full authority to execute its work and reporting lines do not present any perceived or actual conflicts of interest. The authority of the QAIP function should be supported by an internal audit charter and/or AC backing.

Typically, QAIP functions report to the head of audit professional practice, or its equivalent. The head of audit professional practice has responsibility for determining the scope and staffing of the QAIP function. The head of audit professional practice may report directly to the CAE or a deputy CAE, depending on the size of the organization. Reporting alignment must ensure that the group performing the QAIP is not responsible for the execution of other internal audit activities. As a note, audit professional practice processes may be subject to QAIP reviews. In these cases, the review may include additional review/oversight by an independent group/individual to avoid potential conflicts of interest.

Smaller organizations that are not able to support a dedicated QAIP function could consider using independent external reviews of internal audit activities by a third party with appropriate experience and subject matter expertise. Additionally, an internal peer review program might be considered (either in conjunction with, or as an alternative to, an external review); however, the peer review program must be established in a manner that ensures the evaluation of internal audit work is performed independently, and appropriate follow-up is performed on any findings / issues identified during the review. Note that individual findings are tracked and are generally reviewed to identify key themes (collectively referred to as 'issues'). This is further discussed in section V (page 13, below). Overall, individuals performing QAIP activities should be mindful of the need to be objective within the QAIP program and take the necessary actions to ensure continued independence.



Staffing Considerations

QAIP functions should be staffed with an appropriate number of team members with sufficient subject matter expertise and/or industry experience in order to execute the QAIP in an effective and timely manner. The size of the team and the extent of subject matter expertise could depend on the size and complexity of the organization and its scope of business line products and processes.

The head of the QAIP function may have significant IA, risk management, and/or other relevant industry experience to allow for critical challenge of the execution of various internal audit activities. Based on the size of the organization, the QAIP function might also include one or more senior leaders and other levels of experienced individuals to effectively execute the QAIP mandate. When organizations do not possess the requisite level of expertise to effectively complete the QAIP for areas requiring technical expertise (e.g., BSA/AML, technology, regulatory compliance), the organization could consider the use of independent third-party resources to conduct and/or assist with these reviews.

Some organizations may also consider the use of an IA and/or line of business rotational program to assist the QAIP function by supplementing subject matter expertise while maintaining independence. These programs often add value to the QAIP function by providing other expertise and cross-functional training on specific business processes. As noted in the subsequent section, independence over the execution of the QAIP must always be adhered to when engaging any temporary QAIP team members. For example, resources from one audit team, with proper independence and subject matter expertise, may be used to perform an internal peer review of another audit team's work. This allows the QAIP function to tap into subject matter expertise without having to go outside the division/organization.

QAIP functions might also consider enrolling staff in periodic training courses, focusing on the execution of quality assurance reviews. Training programs for QAIP team members should be commensurate with the scope of work being performed and include training to enhance their required subject matter expertise.

Independence Considerations for QAIP Team Members

QAIP team members, as well as any other resources utilized, are subject to the independence standards applicable to the IA function, as well as any additional standards that are applicable to the QAIP function (e.g., not responsible for any front-line internal audit activity) and the Institute of Internal Auditors' Code of Ethics. As such, QAIP functions must be able to perform their duties with an impartial, unbiased mindset and avoid any conflict of interest. QAIP functions should also be staffed with dedicated team members who are not responsible for other functions in order to maintain their independence in fact and appearance. However, the core QAIP team could be supplemented with temporary staff, as necessary.

In situations where the QAIP function utilizes a resource from within the organization, efforts should be made to ensure that this individual does not review an area where they were previously involved for at least 12 months (the 'cooling off period'). The new staff member must declare any potential conflicts of interest at the time of the transfer. The independence and objectivity of each QAIP member may be continuously evaluated as part of each QAIP engagement. Additionally, IA may require all auditors to disclose any perceived or actual conflicts of interest, via a written attestation.

External parties/vendors hired to conduct QAIP work must also disclose any potential independence concerns that may impair their ability to complete the assigned work objectively, as referred to in IIA Standard 1312 – External Assessments. As per Standard 1312, this could be accomplished via discussions between the CAE, senior management, and the board. If any independence concerns are identified, QAIP responsibilities must be reassigned accordingly to avoid any actual or perceived conflict of interest.



QAIP SCOPE CONSIDERATIONS

Scope Considerations

While not required by the Standards or current financial services regulatory guidance, many institutions find benefit in developing a formal QAIP plan to assist the CAE in their responsibility under Standard 1300 – Quality Assurance and Improvement Program to develop and maintain a QAIP. When the QAIP function acts as the auditor of IA, the QAIP plan should be designed to cover all aspects of managing and operating the internal audit activity, including, but not limited to, risk assessment and audit plan development, audit and consulting engagement execution, issue follow-up and validation, continuous monitoring routines, and AC reporting. When determining the QAIP plan, it should be based on an underlying universe and risk assessment process, similar to the concepts that IA utilizes when preparing its audit plan.

QAIP universe

When determining the scope of the QAIP plan, the QAIP function may first determine the composition of the QAIP universe. As the auditor of IA, the concepts that IA uses to develop a risk-based audit plan may be utilized by QAIP to develop the QAIP plan. A risk assessment of the areas within the QAIP universe may be performed in order to develop and prioritize the QAIP plan. For example, the QAIP universe could include the following:

- **Scheduled audits and other reviews on the audit plan.** The QAIP plan may consider all of internal audit's engagements.
- **Advisory activities.** The QAIP Plan may consider any advisory activities that Internal Audit performs for any area of the organization.
- **Other IA key processes.** The QAIP plan may consider Internal Audit's key processes, such as:
 - Risk assessment and audit plan development.
 - Continuous monitoring.
 - Findings / issues validation such as MRA remediation.
- **Strategic initiatives.** The QAIP Plan may consider Internal Audit's strategic initiatives.
- **Professional practice activities.** The QAIP Plan may consider professional practice's activities such as audit methodology and board and management reporting,
- **An assessment of Federal Reserve Bank 13-1 and Office of the Comptroller of the Currency Heightened Standards.**
- **An assessment of internal audit's Independence.** The QAIP function may perform periodic assessments of IA's independence. Assessments could include a review of IA's adherence to its overall policies and procedures.

Note that the QAIP Universe may be continuously monitored, as internal and external factors may cause changes in the IA division's plans.

Risk Assessment

Once the QAIP universe has been determined, the QAIP function may complete a risk assessment of the QAIP universe in order to develop the annual QAIP plan. QAIP risk assessments should follow the same principles that internal audit follows when risk assessing the audit universe.



Scheduled audits and other reviews

Most institutions establish a minimum coverage percentage of audits in the annual audit plan. In selecting the audit engagements for inclusion in the QAIP plan, institutions generally consider coverage of each audit team (e.g., coverage of each of the CAE's direct reports) on an annual basis. Other considerations may include the coverage of high-, medium-, and, low-risk audits and lines of business present within the audit plan; current or upcoming areas of focus or concern; audit size and scope; and newly promoted or hired auditors.

A QAIP of internal audit key activities, strategic initiatives, and professional practice activities may risk assess all internal audit processes and rotate reviews over a multi-year plan. Such reviews may include key areas of focus such as the audit plan, top and emerging risks.

Internal audit's independence

To enhance the robustness of internal audit's independence testing, a QAIP may consider assessing internal audit's independence on an annual basis.

Budgeting time

The time spent on internal assessments is determined by the size and scope of the audit file under review. When determining the QAIP plan, the capacity of resources (or time spent per assessment) should be considered along with other factors such as internal or external scrutiny related to the projects under review and the expertise and/or training required to appropriately assess the project. The factors considered in the budgeting process for internal audits should be the same as when budgeting for QAIP reviews.

QAIP Assessments

As part of the development of the QAIP plan, it is common practice for the plan to include a combination of audit engagements and horizontal assessments. Audit engagement assessments may involve reviewing the quality of a completed audit engagement's work papers (from end to end), whereas horizontal assessments could address a specific objective (or objectives) across multiple audit teams or engagements, such as risk assessments or findings/issues management. Horizontal assessments can also include IA process reviews.

While audit engagement assessments and horizontal assessments are traditionally conducted after the underlying work is completed, an emerging practice is to consider utilizing, as needed, "in-flight" assessments of active audit engagements within the QAIP plan. The benefit derived from in-flight assessments is the ability for audit teams to make necessary changes and adjustments to their audit approach or audit work papers prior to completing the engagement. Due professional care should be used by the individual(s) conducting the in-flight assessment to ensure they remain independent of the audit process. Independence of the reviewers would follow similar procedures when determining/confirming QAIP members' independence.

The types of assessments described below are all considered when developing the plan to ensure there is adequate and sufficient coverage. Some institutions are beginning to develop fully comprehensive audit quality programs that go beyond the required assessments and include additional activities designed to enhance audit quality, including training programs and investments in tools intended to enhance quality within the audit process (such as checklists or other standard templates).

Planned QAIP activities each year may include reviews of IA's complete universe of audit activities. The approach to reviewing IA's activities can be separated into two types of assessments: internal assessments and external assessments, which are discussed further below.

As the adoption and implementation of data analytics (DA) and robotic process automation (RPA) continue to increase at an accelerated pace in the industry, the identification of opportunities to use DA and RPA to create efficiencies and increase the scope of coverage within the QAIP program can be considered. For example, DA and RPA tools can be leveraged to



perform attribute testing across full populations of audit activities within the scope of the QAIP assessment, as well as automate testing that is traditionally manual in nature.

Internal Assessments

As defined in Standard 1311, internal assessments include ongoing monitoring of the internal audit activity and periodic self-assessments.

- Ongoing monitoring by IA teams could be achieved primarily through continuous activities such as engagement planning, supervision, standardized work practices, work paper reviews and signoffs, issue vetting, and report reviews during the execution of an audit. Adequate supervision is a critical element of ongoing monitoring, beginning with planning and continuing through the fieldwork and reporting phases of the engagement.
- Periodic self-assessments by the QAIP team may be conducted to evaluate conformance with the Code of Ethics and the Standards, as well as evaluation of conformance with regulatory requirements and institutional policies and/or procedures.

QAIP internal assessments may include the following types of reports:

- Quality assurance reviews (QARs).
- Peer reviews.
- Targeted/horizontal reviews.

QARs

These reviews are performed on audit engagements and internal audit reviews. These reviews are typically performed by the QAIP and are a review of the entire audit file.

The objective of a QAR is to assess the quality and consistency of audit files, with respect to adherence to audit methodology, practices and procedures. The review may involve reviewing the quality of a completed audit engagement's work papers (from end to end). As noted earlier, an emerging practice has been to consider adding 'in-flight' assessments, which are conducted while the audits are underway, versus performing assessments on completed audits. This allows for early feedback and any issues to be addressed real-time.

Peer reviews

These reviews are performed on audit engagements and are typically performed by a peer reviewer (i.e., an individual from the audit function) who has not participated in the audit engagement and has the relevant subject matter expertise.

The objective of a peer review is to focus on the assessment of the effectiveness of audit planning, including risk identification and assessment, consideration of available information, audit scoping, and judgements/conclusions.

Targeted/horizontal reviews

These reviews may focus on adherence to policy, procedures, and/or methodology, as well as the effectiveness and efficiency of the work under review. These reviews are typically performed by QAIP.

These reviews most commonly relate to IA key processes, professional practice activities, or other specific topics. Examples of this type of review may include continuous monitoring, annual planning, processes, board and audit committee reporting, entity-level risk assessments, and sampling methodology.

As previously described, internal assessments typically include a combination of audit engagement assessments and horizontal assessments. Horizontal assessments may focus on adherence to policy, procedures, internal methodology, and/or the effectiveness and efficiency of the work under review. Examples include the following:



- Review of a sample of completed issue validations across multiple audit teams for adherence to internal audit procedures.
- Review of a sample of auditable entity risk assessments across multiple audit teams for adherence to internal audit methodology.
- Review of a sample of continuous monitoring routines across multiple audit teams for adequacy and consistency.
- Review of a sample of data analytic (DA) routines across multiple audit engagements for appropriateness/effectiveness.

Internal audit's independence

The independence and objectivity of IA are required for the board, AC, and external parties to place reliance on the work performed by IA. For the IA function to fulfill its mission, the board and management must be confident that there is a pervasive and sustainable level of independence and objectivity within the team and across all IA activities. IA should establish policies and procedures such as ongoing monitoring and training, which promote and enforce independence and objectivity.

The QAIP plays a critical role in the monitoring and assessing of IA's independence. To provide additional assurance, QAIP may perform a periodic assessment of IA's independence. This assessment could include a review of IA's adherence to its overall policies and procedures, including:

- Back-testing of adherence to mitigating measures that were put into place for team member conflicts.
- Retrospective reviews of auditors who transfer to auditable entities they audited before the transfer.

The QAIP might also include testing the annual independence assessment process for control design and operating effectiveness. The results of the assessment may be reported to senior internal audit leadership, the CAE, the AC, and external auditors.

Findings/issues validation

These reviews are performed by QAIP resources with the objective of validating any findings/issues raised by QAIP and regulatory findings issued to IA. Validation of the findings/issues may include conducting one audit test or it may require a targeted/horizontal review, depending on the depth and breadth of the finding/issue.

Validation of findings/issues may also include ensuring the sustainability of the actions taken to resolve the finding/Issue.

External Assessments

External assessments are completed by an independent third party who acts as an extension of the QAIP team. The QAIP team might assign reviews to the third parties based on their subject matter expertise to assist in completing the QAIP plan. The QAIP team may then help facilitate the review by setting up and attending meetings between the third party and the IA team under review. All conclusions and reports are reviewed and approved by the QAIP team prior to official completion.

QAIP external assessments may include the following types of reports:

- Peer reviews. These reviews are performed by an external third party firm. The reviewer will typically have specific subject matter expertise as it relates to the selected audit engagement
- External Quality Assurance Reviews (EQARs). These reviews are typically performed by a third party, often an external firm. A full external assessment may be completed by the third party. Alternatively, a self-assessment may be performed, which would then require an independent external validation. This review is performed in accordance with IIA Standard 1312 – External Assessments and is performed at least once every five years. It validates whether the



internal audit activity conforms with Standards/regulatory guidance and whether internal auditors conform to the Code of Ethics.

QAIP Plan Presentation

Many institutions prepare an annual QAIP plan that is aligned with the annual audit plan; however, the adaptation of preparing multi-year QAIP plans (in alignment with their audit cycle) is an emerging trend.

Completion of the QAIP plan may be scheduled for one quarter after completion of the audit plan, which allows for coverage of audits completed later in the year.

Annual QAIP coverage and approach are generally reviewed with, and agreed to, by the CAE, and potentially the AC, at the beginning of each plan year. Of those that present their QAIP plan to the AC, most also present review results and plan changes to the AC throughout the year, as applicable.



REPORTING

Throughout the duration of an assessment, open and frequent communication can occur between the QAIP team and the IA team under review. Best practices, issues, and findings could be discussed as they arise to ensure that these items are fully understood and vetted prior to the completion of the assessment. These findings, related responses, and actions taken to remediate should be documented within the quality assurance work papers. However, formal reporting for all activities performed by the QAIP should occur, as discussed below.

All QAIP reports should be approved internally (note that external parties may participate in drafting reports; however, they are subject to QAIP review/approval) and reviewed by the respective head of professional practice/QAIP before being released. The results would be reported to the audit team impacted, including the executive leadership team of the group (usually one level below the CAE) and possibly the CAE.

While executing the QAIP plan, periodic updates can be provided to the CAE and AC. The updates could include information such as progress towards completion, changes to the plan, and results of the reviews. The tracking and monitoring of the QAIP plan should be executed with the same amount of rigor as that of the monitoring and tracking of the audit plan.

All other reviews performed (such as horizontal assessments, targeted reviews, and in-flight reviews), might also be rated and presented to the audit senior management team and the CAE.

The results of all assessments could be formalized into a final deliverable, such as a memo or report, and include any findings/issues, audit team responses, remediation/action plans, and corresponding commitment dates. In addition, a formal rating may be provided for each assessment.

At a frequency agreed upon with the CAE and the AC (at a minimum annually), results of the QAIP may be presented to IA management, the CAE, and the AC to ensure awareness of strengths, opportunities, findings, thematic concerns, and the overall progress against — and results of — the QAIP plan. Key performance indicators (KPIs) and metrics can be used, as appropriate, to illustrate QAIP results and can include items such as internal assessment ratings, audit plan coverage, and the timeliness of completion against the QAIP plan, as applicable.

Internal Assessments

QAIP reviews may be conducted after the completion of the audit and, generally, do not require correction of issues within the audit reviewed. However, in cases where work papers are corrected based on QAIP findings, such changes should be documented in detail to leave an adequate audit trail.

Individual QAIP reports generally include individual findings/issues which are then assessed across all of the QAIP team's work. Findings/issues identified may also be risk rated. Risk ratings for findings/issues could be 'high', 'medium', or 'low'.

QAIP reports can be risk rated and include an overall conclusion of the review, in addition to any findings/issues noted during the review. Risk ratings differ between organizations and address conformity or degree of effectiveness. For example, the below 'Conformity' ratings are utilized by The IIA, while the 'Effectiveness' ratings are used by some financial institutions.

"Conformity" focused ratings include:

- Generally Conforms.
- Partially Conforms.
- Does Not Conform.



"Effectiveness" focused ratings include:

- Satisfactory.
- Requires Improvement.
- Unsatisfactory.

Generally, a "Satisfactory" or "Generally Conforms" rating cannot have:

- Any findings/issues that would call the audit scope or the audit conclusion into question.
- Major deviations from policy or methodology.
- Material misstatements, errors, or omissions in the audit report.

For less-than-satisfactory or non-conformance-rated reviews or material deficiencies identified, the CAE or CAE subordinate may be required to submit an action plan to remediate the findings/issues or implement the QAIP's recommendations. An action plan may include additional training for auditors (by either the audit director, audit manager, or the QAIP), clarifying audit methodology, enhancing quality controls by reviewers, establishing a higher-level review and challenge process, enhancing documentation by auditors, or — for pervasive, significant findings/issues — re-performing an audit.

External Assessments

External peer reviews will follow the internal assessment process discussed above, leveraging expertise and judgements from the external resources. For EQARs, QAIP may help facilitate the collection of information and the interpretation of work performed. Final assessments and conclusions would be determined by the external firm and communicated to QAIP function, as well as to audit senior management, the CAE, and the AC.

Audit Committee Reporting

As previously mentioned, updates can be presented to the AC at least annually, typically at the beginning of the QAIP plan year, with more frequent updates for larger institutions.

Considerations for AC reporting include:

- Strategy/approach and key areas of focus.
- Plan components and plan status.
- Plan results, including year-over-year performance.
- Issues, including year-over-year remediation/validation.
- QAIP team resources.
- Any KPIs such as QAIP results per team and tracking against QAIP plan results.

The strategy presentation may include a high-level overview of the QAIP plan for the upcoming year. As part of the planning process, some organizations are proactively presenting the key areas of focus to the individual/impacted audit teams.

If multiple QAIP presentations are made throughout the year, the final QAIP update could be presented to the AC at the end of the plan year as part of an overall report of audit performance. This update might include cumulative information such as any findings/issues identified by QAIP throughout the year, their status, key themes, performance of teams, and year-over-year comparisons.



Audit Senior Management Reporting

Internally, QAIP updates may be provided to the IA Division (or individual audit teams, the CAE, or the head of professional practice) via forums such as senior management team meetings or other smaller meetings. Some organizations are also producing quality dashboards to share with audit teams, with a sample of results, to aid in issue remediation efforts.

Regulatory Reporting

Best practices may include the continuous sharing of QAIP progress and results, as well as regulatory findings, to the regulators on a recurring basis.



ISSUE TRACKING AND REMEDIATION

The issuance, tracking, and validation of QAIP findings/Issues usually aligns with IA's audit issue practices: QAIP findings are risk rated, remediation is required for higher risk-rated findings, action plans are developed/tracked, and validation of remediation is performed.

Findings can be defined as individual concerns identified in the respective internal assessments (findings identified via QARs and peer reviews), which would only impact the specific audit or horizontal review affecting processes within IA. To identify significant findings or themes, an approach should be established to identify issues, which are findings that are individually significant or those that are more pervasive throughout multiple QAIP reviews.

The QAIP's responsibilities related to issues tracking, remediation, and validation are generally limited to the QAIP's own findings/issues. In some organizations, the QAIP may be involved in validating matters requiring attention (MRAs) and matters requiring immediate attention (MRIAs) issued by regulators to IA itself, as the QAIP acts as the auditor of internal audit. However, if the MRA/MRIA finding is related to the QAIP, IA may outsource the validation to independent consultants.

In addition to conducting audits on the auditable entities within their portfolio, an audit team may also be responsible for tracking and validating other findings/issues, such as audit recommendations or MRAs/MRIAs (as issued to auditable entities within their portfolio). The QAIP may review audit teams' validations as part of either (a) full-scope reviews or (b) horizontal reviews of the recommendation follow-up process or the MRA/MRIA validation process.

Another situation when QAIP may be called upon to review issues is when regulators disagree with IA's conclusions (e.g., IA supported closure of an MRA/MRIA, but regulators failed IA validation). In this instance, a deficiency in IA's validation process may require the performance of a look-back analysis (or a retrospective review). As noted in FRB SR13-1 and the OCC Internal and External Audit Handbook, a lookback analysis (or retrospective review) is required when a breakdown in the IA division has been identified. A root cause analysis of the breakdown must be performed, and the IA division must develop an action plan to ensure that similar issues do not recur in the future. Best practices may entail (i) the QAIP performing the look-back analysis or reviewing the results of the look-back analysis, and (ii) tracking action plans and testing remediation.

Tracking of Findings/Issues

The issuance, tracking and validation of QAIP findings/Issues should be consistent with the standards and rigor of IA's practices.

Per the 2003 Interagency Policy Statement on the Internal Audit Function and its Outsourcing (OCC Bulletin 2003-12 et al.) and the 2013 Supplemental Policy Statement (SR 13-1), action plan progress should be monitored and subsequently closed after a period of sustainability. QAIP findings/Issues could be logged in either the organization's Governance Risk Control ("GRC") system as other audit issues, or in a spreadsheet that is centrally tracked. The findings/Issues tracker can facilitate theme or trend analysis, rating comparison, remediation and validation tracking. To make theme analysis easier, findings/Issues can be tracked based on risk or issue category. Action plans can be tracked in the same tool.

Generally, audit managers are responsible for remediating QAIP findings/Issues in their respective audits. QAIP tracks findings/Issues for remediation and validation purpose.



Validation and Closure of Findings/Issues

Action plans to address findings/issues are developed by audit teams and tracked centrally by the QAIP. Action plans should be reviewed and accepted by the QAIP to ensure underlying shortcomings will be addressed in a sustainable fashion.

Validation protocols should mirror those used by IA to assess proper design and operating effectiveness over a period of sustainability via sufficient sample sizes. Validation work should be properly documented utilizing the same concepts as those used by IA and be accomplished through work on a finding/issue or through scheduled reviews in the QAIP plan.

Once the audit manager informs the QAIP function that the issue has been remediated, the QAIP could validate the remediation within a reasonable timeframe (which could range from one to several quarters). The timeline should allow for sufficient time to demonstrate sustainability. A best practice may be for the QAIP team to proactively inquire about the QAIP finding/issue.

For full-scope reviews, validation typically involves reviewing areas where the high- or medium-risk QAIP findings/issues were identified in a new audit. Generally, low-risk findings do not require validation testing. The QAIP could document its validation (e.g., testing steps, samples selected, and conclusions) in a validation memo or a quality assurance memo similar to other full-scope reviews.

For horizontal reviews of specific processes, validation may involve reviewing new samples from those audit managers or audit teams with less-than-satisfactory results in the prior review or review of any process enhancements established by the CAE. Remediation involving methodology is done by the methodology team within the professional practice. The QAIP manager is responsible for approving closure of the related findings/issues as soon as QAIP is satisfied with the remediation.

Reporting Findings/Issues

According to SR 13-1, the CAE should communicate the results, planned actions, and status of remediation efforts to senior management and the AC at least annually. As noted in Section IV of the regulation, findings/issues can be reported via various avenues.

It is a best practice for the QAIP team to share common findings/issues or lessons learned with all audit teams, either in periodic QAIP trainings or IA meetings.



About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Disclaimer

The IIA publishes this document for informational and educational purposes. This material is not intended to provide definitive answers to specific individual circumstances and as such is only intended to be used as a guide. The IIA recommends seeking independent expert advice relating directly to any specific situation. The IIA accepts no responsibility for anyone placing sole reliance on this material.

Copyright

Copyright © 2022 The Institute of Internal Auditors, Inc. All rights reserved. For permission to reproduce, please contact copyright@theiia.org.

January 2022



The Institute of
Internal Auditors

Global Headquarters

The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101