Additional IIA Resources

Urton L. Anderson, et al., *Internal Auditing: Assurance & Advisory Services,* Fourth Edition (Lake Mary, FL: Internal Audit Foundation, 2017). See in particular chapter 6, "Internal Control," chapter 9, "Managing the Internal Audit Function," chapter 10, "Audit Evidence and Working Papers," chapter 11, "Data Analytics and Audit Sampling," and chapter 13, "Conducting the Assurance Engagement."

IIA Practice Guide, Auditing the Control Environment (Lake Mary, FL: The Institute of Internal Auditors, 2011).

CHAPTER 13
Internal Audit Communication

Communication at every juncture of the audit process is critical. It is how internal auditors individually and the internal audit function as a whole build and maintain relationships that are crucial for delivering on the value proposition of internal auditing.

This chapter covers communication at all levels and throughout the entire audit process. It starts with development of the audit plan, discusses communication during engagements, including planning the engagement, development of engagement findings, the content and organization of engagement and summary reports, skills for writing high-quality communications, and the reporting process, follow-up and finding closure, and concludes with communicating with executive management and the audit committee.

Internal auditors and the internal audit function communicate with various stakeholders, including:

- Recipients of assurance and advisory services
- Business unit management
- Senior management within the organization
- The board (or its equivalent)
- Other assurance providers inside the organization, including second line of defense professionals
- Stakeholders outside the organization, such as external auditors and, for some organizations, regulators, legislators, the news media, and interest or advocacy groups
- Fellow internal auditors

Communication takes place continuously before and during the engagement, at the end of the engagement, and during follow-up on identified findings. As internal audit expands its roles in providing insights, having a seat at the table at committees, taskforces, and workgroups, and serving as trusted advisors, communications extend well beyond the engagement cycle. For senior management and the board, communication also takes place on a periodic basis, in particular to communicate the audit plan and status updates, summarize multi-engagement results, provide overall opinions, and report on internal audit activities.

Communication of the Annual Audit Plan

As discussed in chapter 1, "Developing an Internal Audit Strategy," and chapter 10, "Risk Assessment and Audit Planning," on an annual basis, internal audit management performs a risk assessment of

the processes, areas, and activities across the organization and develops an audit plan. Internal audit communicates and collaborates with business management across the organization and second line of defense professionals to appropriately prioritize organizational risks. To appropriately link the audit plan to strategic goals, the chief audit executive (CAE) discusses the proposed plan with other risk and assurance providers as well as senior management. Once finalized, the audit plan is communicated to business management and then submitted to the board for review and approval. The audit plan consists of a work schedule as well as budget and resource requirements for the next fiscal or calendar year, and the CAE communicates the impact of resource limitations and significant interim changes to senior management and the board. Any significant deviation from the approved audit plan is communicated to senior management and the board through periodic activity reports. As risk assessment is iterative, internal audit communicates with management regularly to make sure changes and emerging risks are considered.

Of Note to Internal Audit Staff

Audit communication transcends the individual engagements performed by the internal auditors. It happens continuously with various stakeholders:

- With other risk/assurance providers during the risk assessment process and as the audit plan is created
- With senior management to discuss the audit plan, report individual and aggregated engagement results, and provide statuses on finding remediation efforts
- With the board for approval of the audit plan, to report individual and/or aggregated engagement results, to provide statuses on remediation of findings, and to report on other audit activities and initiatives

Sometimes it is assumed that internal auditors are aware of all the communication that occurs outside the engagements they perform, when in reality they have not been kept abreast of this communication. Internal auditors should take the initiative to be aware of and understand what is being reported, when, and to whom. Having this information will enhance communication that does happen at the engagement level.

Communication During the Engagement

As the approved audit plan is executed, ongoing communication during the engagement helps the internal audit function achieve its objectives and accomplish its mission. Communication at the engagement level begins in the planning stage and stays constant through completion. It involves communicating status updates, developing findings, soliciting management action plans, and evaluating potential finding closure during the engagement. Internal auditors should institute regular communication points and employ various forms of communication as appropriate to build understanding during the engagement.

Communication During Planning

Communication at the engagement level begins in the planning stage. Internal auditors should involve business management for input on their specific objectives that support the strategic objectives of the organization and the corresponding risks that could jeopardize achievement of them. Any differences between what the internal auditors and the business perceive as important objectives and significant risks should be explored and resolved before beginning the engagement.

Internal auditors should also discuss any gaps the business area employees are aware of in their control environment and the remediation efforts that are underway to resolve them. In the United States, some regulators expect organizations (banks, in particular) to demonstrate awareness of their control environment through identification of these gaps, and the internal audit function can help document this by discussing them during planning, validating them through testing, assessing their significance, and including them as management-identified findings in final engagement communications, as applicable.

Upon achieving an understanding of the critical objectives and significant risks of the area or process subject to the engagement and gaining an understanding of any known control gaps, internal auditors finalize the scope of the engagement and communicate it to business management and begin requesting the information and documentation needed from the business to perform the engagement.

Developing a Communication Plan for the Engagement

During the planning stage, internal auditors should discuss with the business what they can expect in terms of communication. This includes requests for information, documentation, and other audit evidence that internal auditors will need to perform testing, as well as status updates to keep the business area informed of how the engagement is progressing. To the extent possible, internal auditors should tailor their requests and updates to the preferences of the business in terms of frequency and format.

Communication of Engagement Status

Status updates can consist of formal meetings or other communication venues, such as email, memoranda, and PowerPoint presentations, and are usually scheduled at the start of the engagement; however, the schedule may be altered during the engagement. These communications may be canceled or postponed when not needed or may be added when an important finding emerges, a significant change in the engagement objectives or schedule is anticipated, or an impediment arises.

Typical status updates occur weekly or biweekly throughout the engagement and include:

- How the engagement is tracking against the established timeline
- Outstanding requests that have not been received from the business
- Testing results, in particular those results that could become findings
- Next steps, including areas that will be tested next and the employees with whom internal auditors need to meet

Recipients of status update communications typically include the relevant employees of the audited business area and the internal auditors working on the engagement, but they may also include management representatives and internal audit management. Whether and when such additional recipients are included should be established at the start of the engagement. To be courteous to the employees with whom internal auditors are working, it is sometimes prudent to pre-communicate

sensitive information to staff-level employees to give them an opportunity to communicate the information to their superiors and provide any context before their superiors receive the communication from the internal auditors.

Communication of Findings

As discussed, internal auditors need not wait until the engagement is complete to communicate findings to the business. In fact, a best practice is to communicate them as they are identified during the engagement through status communications presenting the preliminary findings identified.

Communicating findings as they are identified during the engagement has several advantages:

- The engagement process overall is more efficient.
- Employees of the audited business often provide internal auditors with additional, pertinent information.
- Internal auditors' relationships with employees of the audited business area are enhanced.
- Business employees are better able to develop responsive action plans and do so in a timely manner.
- Business employees can begin remediation efforts immediately rather than waiting until the final communication is issued.

In communicating identified observations via status communications, internal auditors seek to solicit additional information and discuss the dimensions and ramifications of the finding. This communication helps internal auditors ensure that pertinent information has not been overlooked and findings have been thoroughly assessed. Furthermore, this communication provides business employees an opportunity to offer their perspectives. In particular, internal auditors may seek their perspectives on the cause(s) of the conditions found. This communication lays the groundwork for what will be included in the final engagement report. Finally, this communication has the potential to shorten the time to issue the final engagement report, as business employees (and, as appropriate, business management) are apprised of the findings in advance of the draft report.

Finding Closure During the Engagement

The findings are closed after the internal auditors validate that the corrective actions have been completed and they successfully remediate the risk to an acceptable level. Another advantage of communicating findings as they are identified is that the business can begin remediation efforts immediately. When business employees act to close the finding during the engagement, internal auditors should follow a process—understood by the internal auditors and the business—that clearly defines when such closure is acceptable and how it will be assessed.

To close findings during the engagement, internal auditors should assess whether the closure is valid and sustainable. Validity depends on addressing not only the condition but also the cause of the condition, and sustainability calls for evidence that the finding not only is closed but will remain closed. For example, if duplicate payments were found during an audit of accounts payable, the business would need to validate not only that the duplicate payments were recovered but also that the payables process—its design and execution—has been revised or improved to mitigate the risk of future duplicate payments. Furthermore, sufficient competent evidence would need to be available to provide the internal auditors with assurance that the revisions or improvements are sustainable—that they are in place and operating as intended.

This requirement for sustainability evidence makes it less likely that a finding can be closed during an engagement. For all but minor findings, the business likely cannot provide sufficient competent evidence to assure the internal auditors that the finding has been resolved in a sustainable way. In fact, to gain such assurance, the internal auditors usually need to reopen testing, and that may not be feasible within the timeframe of the engagement.

Communication During Exit Meetings

Exit meetings provide internal auditors with a final opportunity to ensure that engagement results are fully communicated to and understood by the business. In addition, exit meetings provide internal auditors with the opportunity to bring the engagement to closure and finalize some or all aspects of the engagement:

- **To confirm understanding by discussing the draft audit report.** This is an important objective when the findings have been discussed preliminarily and action plans have been solicited as findings were discussed during the engagement. When this communication during the engagement has occurred, the draft report—provided to business management before the exit meeting—should hold no surprises. In fact, using this methodology, the internal audit team can issue the report shortly after the exit meeting, sometimes as rapidly as within 24 to 48 hours. This is a preferred approach.
- **To confirm understanding and solicit action plans by discussing the draft audit report.** If internal auditors communicate findings during the engagement but do not solicit action plans until the draft report is issued, this meeting can be used to obtain management's action plans.
- **To reach agreement on audit findings and solicit action plans by discussing the draft report.** Some internal audit functions do not communicate findings as they are identified during the engagement. When this is the case, this meeting can be used to discuss the findings and solicit action plans. Note that when finding discussion is delayed until the exit meeting, it often leads to more contentious exit meetings and extends the issue time for the report.
- **To close the fieldwork but not to discuss the draft audit report.** Some internal audit functions draft the report after the exit meeting. In this case, the objective of the exit meeting is narrowly limited to confirming some details of the testing performed during fieldwork or as a formal closure to the fieldwork. A methodology such as this often extends the issue time for the report but may be inevitable for some internal audit functions.

Engagement Reporting

Audit reports are key deliverables for internal audit functions. As such, internal audit should give careful consideration to readership of the report as well as its structure, the drafting process, and report quality. Furthermore, internal audit functions should communicate throughout the engagement—namely through status communication, exit meetings, and the assessment of management action plans—to ensure that engagement results are fully communicated and understood. When delivering a report on an advisory engagement, internal audit should customize the communication based on agreed-upon process and format with management. Communicating advisory engagement results is discussed in detail in chapter 16, "Advisory Services."

Readership

The final engagement report has a broad readership, which may include:

- The recipients of the assurance services provided
- Business unit management
- Senior management
- Other assurance providers, including second line of defense professionals
- The board
- External readers, such as external auditors and, for some organizations, regulators, legislators, the news media, and interest or advocacy groups

This broad readership has differing needs and levels of understanding. For example, some of these readers will primarily be interested in the overall rating of the report and other pertinent facts included in the executive summary of the report. Others may be interested in the more detailed aspects of the report: some may have an interest in all of the findings while others will be interested in only some; some will need more explanation while others will find such explanations unnecessary; and some will want more detail while others will want less. Identifying the readers and assessing their needs and levels of understanding are essential to developing and structuring the final engagement report.

Engagement Report Structure

Aspects of audit communication are required by The IIA's *International Standards for the Professional Practice of Internal Auditing*. Specifically, Standard 2410 states, "Communications must include the engagement's objectives, scope, and results." However, audit report structures are variable; they reflect the internal audit function's mission, the needs of the report's primary readers, and the culture of the organization. Furthermore, the *Standards* does not specify a report structure; that is, it does not mandate how the required elements—objectives, scope, and results—are to be sequenced. In addition, it neither precludes other elements nor stipulates how such other elements might be named and sequenced. In fact, Implementation Guide 2410 notes that "the format and content of such communications may vary by organization or type of engagement." It is important to note that aspects of communication may not be formalized in a written report. In some cases, it may be better to communicate some items orally in person or via telephone or video conference. For example, some "soft" topics, such as culture, may be more effectively communicated this way. Even when communicating outside a written report, however, all such communication must be documented in audit workpapers to maintain a record that it occurred.

While there is no prescribed report format, the following items are frequently included in audit reports in varying sequence:

- Executive summary
- Objective
- Scope
- Rating
- Standards conformance statement
- Background
- Findings, recommendations, and action plans
- Report distribution
- The internal audit team that performed the engagement
- To whom the report is addressed and other parties receiving the report

Executive Summary

The executive summary of the report typically includes:

- The purpose statement
- The scope statement
- The rating

Purpose Statements

Effective purpose statements should be definitive about what the engagement set out to achieve; that is, what the engagement sought to conclude on or determine. It serves as the internal audit function's objective for the engagement. The purpose statement may be drawn from the annual audit planning documentation. If the engagement was not included in the audit plan, the purpose statement should include an explanation of what prompted the engagement, be it an event or a request by business management, senior management, or the board.

Some internal audit functions opt for standardized (boilerplate) purpose statements if the purpose of every audit is the same. Such a statement uses the same wording for every engagement report, inserting the name of the business area being audited. An example of a standardized purpose statement is, "The objective of this audit was to determine the effectiveness of internal controls to manage risks in [the process or activity]."

Scope Statements

The scope statement, in conjunction with the purpose statement, sets context to orient and prepare readers. IIA Practice Guide, Audit Reports – Communicating Assurance Engagement Results, defines scope statements this way: "scope statements may indicate period covered, the type of internal audit being conducted (assurance engagement, advisory/consulting engagement, or follow-up audit), specific risks, relevant systems, and/or the departments or functions assessed."

The level of detail in scope statements varies among internal audit functions. Some list at a high level the activities or processes covered by the engagement, while others go one level deeper and list the sub-activities or sub-processes. In addition, some describe their methods—that is, they include the nature and extent of engagement work performed—while others omit this information from the scope statement, incorporating relevant methods in each finding or adding a separate report section to cover methods.

An important component of the scope statement is the identification of any activity or process excluded from the scope when a reasonably knowledgeable reader would otherwise expect that activity or process to be included. The scope statement should not only identify such an exclusion but also explain why the activity or process was excluded.

The opinion is the critical location for communicating high-level conclusions. Because of its importance, the opinion should be prominent and readily identifiable in the report structure.

Engagement Opinions

Engagement opinions (or conclusions) are an optional component in communicating engagement results. Such opinions are called *micro* opinions to distinguish them from *macro* opinions. As defined in IIA Practice Guide, Formulating and Expressing Internal Audit Opinions, "Macro opinions generally are based on the results of multiple audit projects, whereas micro opinions are typically based on the results of a single audit project or a few projects performed over a limited period of time." Internal auditors should give particular attention to whether an opinion is a desirable component of the audit report and, if so, how the opinion is developed, considering various rating types and assessing rating benefits and drawbacks within their organization.

Opinion Development

When included in the report, engagement opinions likely hold the highest interest for the largest number of readers, and opinions should be developed to address the needs of those with a primary stake in the engagement results: business management, senior management, and, in many organizations, the board and outside regulators. Furthermore, such opinions should communicate crucial conclusions to these stakeholders—conclusions that these readers want and need to hear from the internal audit function.

IIA Standard 2410.A1 leaves open the option of not rendering an opinion. Internal audit functions should carefully examine their primary stakeholders' expectations before deciding whether or not to render an opinion. In some organizations, like health care and public education, management prefers for the internal audit function to focus communication on the insights identified based on where the audited business area is in terms of governance, risk management, and control (GRC) maturity rather than providing an opinion that could be perceived as a black and white stamp of approval or disapproval. Other organizations, however, like banks and financial services, have regulators that require opinions, and many boards prefer their use because they focus the attention on the areas of the organization needing the most attention based on the results of assurance services provided across the organization.

Conclusions and opinions are the internal audit function's evaluations of the effects of the findings and recommendations on the objectives of the engagement. They usually put the findings and recommendations in perspective based upon their overall implications. Internal audit functions should clearly state engagement conclusions in the engagement report. Conclusions may cover, but are not limited to, whether operating or program objectives and goals conform to those of the organization, whether the organization's objectives and goals have a reasonable probability of being met, and whether the activity under review is functioning as intended.

When the preference is for inclusion of an opinion, internal auditors should examine not only each finding but also the relationships among the findings. Sometimes a single finding by itself is prominent and drives the opinion. In this case, the opinion focuses almost exclusively on the overall implications of that finding. However, findings often compound each other, resulting in effects that raise the internal auditors' opinion to another level. For example, one finding may focus on a poorly designed process while another may focus on insufficient data security. Taken together, these findings may lead to a more significant risk than each represents individually. Furthermore, the root cause leading to that risk may be that, at a high level, processes are not aligned with the organization's data security needs.

The components of an opinion are described in the Interpretation of Standard 2410.A1, "Opinions at the engagement level may be ratings, conclusions, or other descriptions of the results." Thus, internal audit functions have flexibility in how to present opinions.

When opinions are rendered, a best practice is to combine a rating with an opinion description. As described above, the rating provides a limited number of conclusions. The opinion description is uniquely developed for each engagement: it provides the rationale for the rating. Combining a rating with an opinion description offers the benefits of an unambiguous rating—a conclusion open to consistent interpretation—with the benefits of text that illuminates the nuances of the engagement.

Engagement Ratings

Engagement ratings may be one element of the opinion or they may stand alone when opinions are not included as part of the engagement communication. Ratings are typically seen as a desirable way to communicate the business's overall achievement status of the engagement objectives. For example,

a rating of "satisfactory" means that GRC processes are adequately designed and operating effectively to provide reasonable assurance regarding the achievement of control and/or business objectives under review. In deciding whether to include a rating as part of the communication, internal audit functions should consider the advantages and disadvantages of ratings. In developing ratings, internal auditors examine the finding-by-finding results and apply both objective criteria and subjective professional judgment.

Including an engagement rating has multiple advantages:

- Senior management and boards have a strong preference for ratings because of the clarity that ratings offer. Furthermore, ratings facilitate engagement-to-engagement comparisons for these high-level readers. For many in senior management, the rating influences how much of the report is read—or whether it is read at all. That is, those in senior management may put aside reports with positive ratings, trusting that their management team is addressing the findings and that senior management intervention is unnecessary.
- For business area management, ratings limit ambiguity. In the absence of ratings, management interprets significance or severity solely by relying on other clues in the engagement report. These clues are the wording of the opinion, if one is rendered; the number, tone, and length of the findings; and the number and nature of the recommendations—all of which are open to different interpretation than is a rating. By limiting ambiguity, ratings can help business management prioritize actions.
- For other stakeholders, ratings focus attention. For example, ratings alert the external auditor to areas of particular concern. Similarly, ratings may alert the media to areas more likely to impact the public and may alert interest groups to areas impacting their constituencies.
- For the internal audit function, ratings make it easier to summarize results for senior management and the board. Furthermore, ratings contribute to the internal audit function's planning and may be a component of the function's measurements of its own work.

On the other hand, there are several disadvantages to including ratings in audit communication:

- Disagreements and negotiations over the rating may become the sole focus of discussions between business area management and internal auditors. A narrow focus on improving the rating may distract management from focusing on the substance of the engagement results.
- Some organizations use engagement ratings as a factor in assessing management performance. The internal audit function may not intend ratings to be used in this way, but they should consider the consequences of such a management practice.
- The internal audit function may not use its rating system effectively. In particular, internal audit may overwhelmingly default to one rating, rendering the rating system itself ineffective as a communication tool.

When ratings are used, many internal audit functions use a three-point rating system: satisfactory, marginal or needs improvement, and unsatisfactory. However, some use a system with four or more points—for example, unsatisfactory, marginally unsatisfactory, marginally satisfactory, and satisfactory. Splitting the "marginal" rating into two—leaving no midpoint—has two advantages:

- Splitting the midpoint communicates a clearer message to readers.
- Splitting the midpoint can help prevent the internal audit function from developing a pattern of defaulting to the midpoint rating.

These rating schemes may be enhanced by adding traffic light colors or graphic elements. The aim of including such elements is to communicate the rating vividly.

Many internal audit functions find it helpful to expand the rating criteria definitions by describing or providing examples across the range of risk categories, such as financial, operational, compliance, and reputational. **Exhibit 13-1** shows this approach. Such definitions support the internal audit function's ability to deliver clear messages through the engagement rating.

Exhibit 13-1
Example of Rating Criteria Definitions by Category

	Financial Exposure	Maximum Operational Exposure	Maximum Reputational Exposure	Maximum Regulatory Exposure
Rating: Satisfactory	< $200 million	Not meeting non-customer-facing operational objectives for < 24 hours	Organization mentioned negatively in the media but in a limited way	Increased regulatory attention but no penalties or sanctions
Rating: Needs Improvement	$200 million to $1 billion	Not meeting non-customer-facing operational objectives for > 24 hours OR Not meeting customer-facing operational objectives for < 12 hours	Organization's reputation publicly questioned, for example, in the media or through legal testimony	Regulatory penalties but no sanctions
Rating: Unsatisfactory	> $1 billion	Not meeting customer-facing operational objectives for > 12 hours	By the media or through legal testimony, organization associated with or found responsible for malfeasance, environmental damage, and/or injuries or deaths	Regulatory sanctions, up to and including revocation of licensing

Body of the Report

Following the executive summary is the main body of the report: the findings and recommendations and the action plans. The findings describe the criteria, summarize the conditions found, provide pertinent details, and offer finding-by-finding conclusions about causes and effects.

Findings should be sequenced and their length managed to reflect their relative severity. The sequencing should be based on the severity of the finding (typically, the level of residual risk), and finding ratings help in this regard. The sequencing of findings with identical ratings should be evaluated carefully to place them in the appropriate sequence. Finding length likewise should be managed. A best practice is to ensure that less severe findings are not significantly longer than more severe findings due to readers' tendencies to see length as an indicator of importance.

Additional report sections may be included; some may be distinct from the executive summary and findings, and some may be incorporated into those broad sections:

- **Table of contents.** Lengthy reports may benefit from such a table. If the report will be read electronically, this table may offer hyperlinks.
- **Background.** A general background section may be included in the executive summary or elsewhere in the report to provide context around the purpose and scope statements.
- **Audit methods.** Methods may not call for a separate section; they may be included in the scope section, and finding-specific methods can naturally and smoothly be woven into each finding as the conditions are described.
- **Finding summary.** Some complex reports benefit from this section, which is placed between the executive summary and the findings.
- ***Standards* conformance statement.** This statement may be placed anywhere within the report structure, but commonly it is placed at the end of the executive summary or at the end of the report.
- **Efficiency or improvement recommendations.** Some internal audit functions include such a section to separate findings and recommendations that do not address internal control weaknesses but that the internal auditor is offering for business management's consideration. Alternatively, this can also be included as an appendix to the report.

Additionally, appendices may be desirable for or even expected by readers, depending on the organization's culture. Appendices serve secondary readers, often providing more detailed or technical information. Some typical appendices are:

- Rating definitions and explanations of how they are derived
- Supporting details for more technical secondary readers
- A glossary
- Detailed explanations of audit methods

Finally, the report structure should include:

- A way to identify the report by title, business area, location, report date, report number, and/or status (draft or final)
- Report distribution
- Appropriate release and confidentiality notifications
- The internal auditor(s) who performed the engagement

Engagement Findings

Engagement findings form the body of the engagement report. They typically are among the first report sections developed.

As previously discussed, readership extends beyond those involved in the engagement itself, and internal auditors must keep the readership in mind when developing the findings. The key attributes of findings are well defined in IIA Practice Guide, Audit Reports – Communicating Assurance Engagement Results. These attributes are the criteria, condition, cause, effect, and recommendation. Sound findings contain these attributes and management's action plan.

Decisions regarding how to document findings in audit reports are based on:

- Expectations of business area management, senior management, and the board
- Level of work performed during the engagement
- What level of detail is appropriate for the criteria and condition
- What levels of cause and effect are expected
- In what order attributes will be presented in the finding
- What type of recommendation and action plan to include, and what style is used for these
- Whether background is included in each finding and, if so, how
- How the findings are structured, including whether attributes are named, and, if so, how

Finding Development

Engagement findings are developed and structured in various ways by internal audit functions, taking into consideration the readers' needs and levels of understanding. Defining a consistent approach to finding development and structure helps the internal audit function communicate clearly and efficiently.

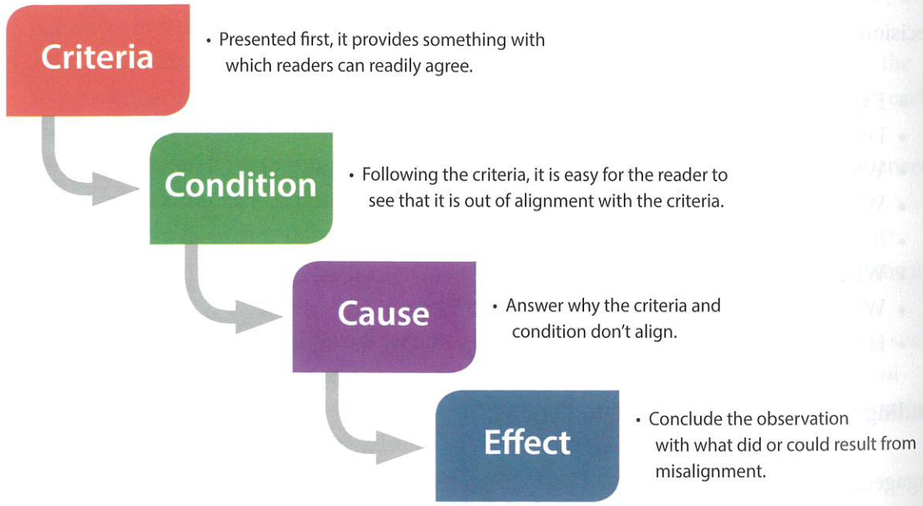
As previously discussed, communication of findings is easier when internal audit functions discuss findings with business area employees during the engagement. These discussions serve as the starting point for documenting the findings in final communications.

Finding Structure

Internal audit functions have numerous options. Decisions about finding structure include:

- **Attribute sequencing.** Attribute sequencing refers to the order in which attributes are presented in the finding. This decision has an impact on how readers process the information within the finding. As previously discussed, findings often resonate with the reader better when the attributes are presented in a way that is logical to them. See **exhibit 13-2** for optimal finding attribute sequencing.
- **Attribute naming.** Attribute naming refers to whether each attribute is named (identified) and whether to retain standard internal audit terms (criteria, condition, cause, effect, recommendation, and action plan) or to use synonyms.
- **Finding formatting.** Format refers to how the finding looks; format considerations include layout, fonts, and use of color.

Exhibit 13-2
Optimal Observation Attribute Sequencing



Finding Ratings

As previously discussed, it may be desirable to use finding ratings to communicate the importance of each finding and the priority management should place on actions to address it. Such a rating typically categorizes the level of residual risk associated with the finding. In deriving such ratings, internal auditors apply professional judgment to a set of rating criteria.

The rationale for including finding ratings is four-fold:

- **They are desirable for senior management and the board.** Ratings provide unambiguous conclusions about the residual risks associated with each finding. Readers can skim the findings and gain an overview of the engagement results.
- **They are desirable for business area management.** Ratings help management prioritize actions.
- **They contribute to the development of an engagement rating.** The internal audit function can use the finding ratings to help determine the overall engagement rating (if such a rating is used). This determination can include certain parameters based on the finding ratings. Additionally, when readers of the audit report understand the ratings of the individual findings, they can more readily understand the overall rating or opinion presented, if any.
- **They help guide the internal audit function's post-engagement efforts.** Finding ratings may be used to determine the nature and extent of follow-up. In addition, ratings may contribute to audit planning.

The most common rating scheme has three levels: high, moderate, and low. However, some internal audit functions find four levels more appropriate for their environment, splitting the "moderate" rating into two. Additionally, some internal audit functions present the ratings using elements such as traffic light colors (red, yellow, and green) or graphics. **Exhibit 13-3** shows a set of rating criteria for a three-level rating scheme.

Exhibit 13-3
Example of a Finding Rating Scheme

Finding Ratings and Criteria	
High-Level Risk	• A financially material loss or misstatement • A failure to meet operating objectives • Damage to the organization's reputation • Likelihood of regulatory fines and sanctions
Moderate-Level Risk	• A financially less-than-material loss or misstatement • Risk of a delay in or an impediment to meeting operating objectives • A negative effect on the organization's reputation • Likelihood of regulatory concern but without fines or sanctions
Low-Level Risk	• A non-material loss, which may be recoverable • Inefficiencies in meeting operating objectives, which may be recoverable • A temporary effect on the organization's reputation, which is recoverable • A regulatory-related finding but one not likely to be cited as a regulatory concern

In determining the finding rating, internal auditors should apply the rating criteria using professional judgment. The rating process is not a formula; it is the process of reaching a conclusion based on evidence, criteria, and judgment. To this end, internal auditors typically consult with internal

audit management in determining the rating of each finding. Internal auditors—supported by internal audit management—should be prepared to support the rating conclusion if challenged by business area management.

Some internal audit functions do not include recommendations in their findings; they include management action plans only. These internal audit functions communicate recommendations during the engagement status meetings and solicit management's action plans in advance of formally documenting the findings. Provided the action plan is responsive—as described below—these internal audit functions eliminate the recommendations from the findings and go directly to presenting the action plans. This approach eliminates redundancy and creates a forward-looking, action-oriented tone. Additionally, it eliminates the appearance of conflict if the recommendations and action plans do not align exactly.

A final decision in developing the finding is how much background to include. For most findings, some background information can be smoothly integrated into each attribute. For example, when and how a criterion changed may be integrated into the criteria; likewise, why a unit was reorganized may be integrated into the condition or cause. However, for large and complex engagements, each finding may benefit from a distinct background section, often presented to introduce the finding. For example, a finding covering a highly technical process—whether in IT, finance, or some other area—may benefit from a distinct background section.

Thus, overall, internal audit functions make a number of decisions about how findings are developed, structured, and formatted. Each of these decisions is made using judgment, internal auditors' understanding of internal audit methodology, and the culture of the organization.

Incorporation of Management Action Plans

Internal auditors should assess management action plans to determine their responsiveness and sufficiency in addressing the audit findings. Depending on the internal audit function's methodology for soliciting action plans during status meetings, this assessment may take place as internal auditors develop and present findings during these meetings. In contrast, this assessment may take place only after the draft report has been delivered and, possibly, after the findings have been reviewed during the exit meeting. Whenever it takes place, in collaborating on action plan development, internal auditors and the internal audit function must maintain independence. In particular, internal auditors should not dictate what is to be done, how it is to be done, when actions are to be taken, or who is to be responsible.

Regardless of when management supplies action plans, internal auditors should ensure that, at a minimum, the action plans include these elements:

- **The business's proposed actions.** The proposed actions should address the specific exceptions covered by the finding and be precise in defining the actions to be taken.
- **Action plan ownership.** Business management should specify who has ownership for implementation. This ownership should be at a high enough level to make decisions about the resources needed to implement the action.
- **Proposed completion date(s).** Business management should commit to when the action plan will be completed.

In assessing the action plan, internal auditors should evaluate the types of actions proposed to ensure that the action plan addresses the causes identified. In fact, a cause-focused action plan may be the only type required. Condition-focused and recovery-focused action plans may follow the cause-focused action plan, providing a more detailed response to individual conditions identified. However, internal auditors should not accept condition-focused and recovery-focused action plans as sufficient in the absence of a cause-focused action plan.

Particularly complex findings may call for management to collaborate with other parties—for example, other business units or external resources—to resolve a finding. (A typical instance is when a business unit requires collaboration with the IT unit to close a finding.) When this is the case, internal auditors should evaluate whether action plans describe how business management will actively engage other parties. In fact, some internal audit functions require action plans to show that business management has negotiated joint ownership with appropriate other parties, even when those parties are outside the audited business area.

Audit Report Distribution

Internal audit functions must control the distribution of engagement reports. This includes the CAE's decisions regarding how and to whom reports are distributed as well as legal considerations and considerations involving the communication of sensitive information. Making these decisions may involve consulting legal counsel and compliance areas within the organization.

The CAE decides who should receive the report. As required by IIA Standard 2440 - Disseminating Results, and in particular by IIA Standard 2440.A1, this decision is based on ensuring that results are disseminated "to parties who can ensure that the results are given due consideration." Thus, the CAE should consider not only the scope of the engagement but also the span of the actions and the level at which actions are required. While most internal audit functions adopt a standard distribution list, the CAE should be willing to expand that distribution when necessary to achieve the desired actions. This may mean distributing the report to those whose support the audited business area needs to remediate the findings, or it may mean distributing the report to higher-than-usual levels within the organization when high-level involvement is needed.

The communication of some engagement results may involve legal considerations. In this regard, CAEs are encouraged to consult their organization's legal counsel. Moreover, they are strongly encouraged to develop policies and procedures regarding handling such matters and to form close working relationships with areas such as legal counsel and compliance.

For some organizations, dissemination of results outside the organization is mandated by law, statute, or regulation. For example, in many countries, government bodies are required to make reports available to the public. When the organization is not subject to such mandates, the CAE must take steps before disseminating results outside the organization. Namely, as required by IIA Standard 2440.A2, the CAE must "assess the potential risk to the organization; consult with senior management and/or legal counsel as appropriate; and control dissemination by restricting the use of the results."

A best practice is for the CAE to help the organization develop guidelines for disseminating information outside the organization. Such guidance may be codified in the internal audit function's charter, the board's charter, or the organization's policies.

Report Quality

Standard 2420 - Quality of Communications states, "Communications must be accurate, objective, clear, concise, constructive, complete, and timely."

The Interpretation to this standard elaborates that:

- Accurate communications are free from errors and distortions and are faithful to the underlying facts.
- Objective communications are fair, impartial, and unbiased and are the result of a fair-minded and balanced assessment of all relevant facts and circumstances.
- Clear communications are easily understood and logical, avoiding unnecessary technical language and providing all significant and relevant information.
- Concise communications are to the point and avoid unnecessary elaboration, superfluous detail, redundancy, and wordiness.
- Constructive communications are helpful to the engagement client and the organization and lead to improvements where needed.
- Complete communications lack nothing that is essential to the target audience and include all significant and relevant information and observations [findings] to support recommendations and conclusions.
- Timely communications are opportune and expedient, depending on the significance of the issue, allowing management to take appropriate corrective action.

Reporting of Disagreements

Disagreements between the audited business area and internal auditors may not always be resolved, even when internal auditors communicate throughout the engagement and aim to confirm or reach understanding at the exit meeting. When this is the case, internal auditors should escalate disagreements in an effort to resolve them, and the internal audit function should have a well-defined escalation process aligned with the organization's normal escalation process.

If disagreements remain, the engagement report should overtly describe their nature, scope, and significance. While not a best practice, leaving such disagreements unresolved but described may be the most rational course of action for internal auditors. Approaches vary based on the nature of the disagreement:

- The disagreement may be over the facts (the conditions) or their significance (the effects or the risks); if so, the engagement report may include a management response describing the disagreement in brief.
- The disagreement may be over the responsiveness of the action plan; if so, the engagement report should overtly state that the internal auditor has concluded the action plan is nonresponsive.

Senior Management and Board Reporting

Senior management and the board (or its equivalent) are important stakeholders for communicating results. Internal audit functions adopt various approaches to delivering such communications. In particular, internal audit may provide these stakeholders with whole reports, executive summaries only, multi-report summaries only, or some combination of these approaches.

Internal auditors should consider various approaches to senior management and board reporting, including the use of multi-report summaries. Furthermore, internal auditors should explore expectations for a macro opinion—which may cover internal controls surrounding governance, risk management, and compliance—and explore how the internal audit function may meet these expectations.

Approaches to Senior Management and Board Reporting

The internal audit function decides on the appropriate approach by assessing the needs and expectations of senior management and the board and getting their input. There are many items that the internal audit function can report to senior management and the board. Preferences of senior management and the board, as well as the culture of the organization, dictate which items are included. Common information that is reported includes:

- Results of assurance and advisory engagements, either individually or aggregated
- Summarized and trending finding information
- Finding remediation efforts
- Annual audit plan
- Audit plan status
- Resource adequacy
- Resource competency in terms of ongoing professional training, licensure, and certification
- Annual financial budget
- Financial budget updates

While any or all of this information can be requested by and provided to senior management and the board, at the minimum, almost all want to receive engagement results. Some members of senior management and some boards want to see every engagement report. Such members of senior management may be in any size organization, but such boards typically are those in smaller organizations where the volume of reports is manageable as board reading. For this audience, well-constructed executive summaries are essential. For one thing, a well-constructed executive summary communicates high-level messages; for another, it may influence whether these readers will read the entire report or have received enough information to stop after reading the executive summary.

Some boards want to see only a portion of the engagement reports. For example, they may want to see all the executive summaries, but want to see full reports only for those with certain ratings. Or they may want to see executive summaries only and no full reports at all.

Multi-Report Summaries

Providing multi-report summaries serves most members of senior management and most boards, as the internal audit function is able to highlight trends and themes represented by individual engagements. Even boards that see every engagement report typically will benefit from multi-report summaries as well.

In developing multi-report summaries, the internal audit function should have a clear understanding of what is relevant for senior management and the board. Most importantly, multi-report summaries should not be used to describe the work done by the internal audit function; such descriptions can and should be provided through other means. Rather, multi-report summaries should focus on the results of the work—results that address what senior management and the board need to know. For example, if multiple engagements have identified a lack of coordination among business units, the multi-report summary should highlight that theme. Likewise, if engagement ratings reflect improvement or deterioration in the control environment, the multi-report summary should highlight that trend.

Rated engagements are inherently easier to summarize than are nonrated engagements. For this reason, internal audit functions that are expected to provide multi-report summaries are likely to opt for engagement ratings. Trending may be by processes, locations, or other relevant parameters.

Internal audit functions that rate each finding are also better positioned to summarize engagement results. In this case, summaries can be readily developed around themes that cut across engagements. Such themes may be developed around high-risk findings, with further theme development by types of risks or processes.

The internal audit function should adopt presentation approaches that highlight what is relevant. Specifically, multi-report summaries should use text and graphics so that themes and trends are presented vividly. Multi-row and multi-column tables, cluttered graphics, and dense text do not help the internal audit function deliver high-level messages clearly.

Entitywide (Macro) Opinion on Internal Controls Surrounding Governance, Risk Management, and Compliance

The board may ask the internal audit function to provide an overall opinion on internal controls surrounding some or all of the following: governance, risk management, and compliance. As previously discussed, such an opinion is called a *macro* opinion to distinguish it from a *micro* opinion. Again, as defined in IIA Practice Guide, Formulating and Expressing Internal Audit Opinions, "Macro opinions generally are based on the results of multiple audit projects, whereas micro opinions are typically based on the results of a single audit project or a few projects performed over a limited period of time."

The rationale for this request is clear: the board looks to internal auditors to offer reasoned conclusions based on their work, potentially taking into consideration work performed by other assurance providers. In rendering such an opinion, the internal audit function contributes its unique perspective to the board's oversight of the organization. An overall opinion is not required by the *Standards*. However, Standard 2450 - Overall Opinions states, "When an overall opinion is issued, it must take into account the strategies, objectives, and risks of the organization; and the expectations of senior management, the board, and other stakeholders."

Internal audit functions should consider a number of factors in deciding if such an opinion can be rendered, what its scope will be, how it will be derived, and how it will best be presented. IIA Practice Guide, Formulating and Expressing Internal Audit Opinions, highlights these considerations:

- The purpose for which the opinion will be used
- Whether the opinion can be rendered based on the audit period and testing timelines
- A clear understanding of what the organization considers "overall" satisfactory performance
- The organization's risk appetite and the criteria for the opinion
- The sufficiency of audit work and audit evidence (including the work of others and informal evidence) to support the opinion requested

The Interpretation of Standard 2450 also highlights that the reasons for an unfavorable macro opinion must be stated. An unfavorable opinion—while it may be expressed through a one- or two-word rating—calls for the CAE's explanation of how it was reached.

As when issuing individual engagement results, the CAE should examine the legal considerations involved as well as considerations related to the communication of sensitive information. Both of these issues are addressed by Implementation Guides 2400-1 and 2440.

With these considerations in mind, internal audit functions intending to render a macro opinion should develop a process for formulating the opinion based on:

- Audit evidence built up over time
- The results of an aggregation of engagements

- Work performed by others
- Informal evidence

This last may include insights gained by the CAE through involvement in organizational committees and initiatives as well as trends and themes identified by examining the results of engagements, especially as these are discussed with senior management. IIA Practice Guide, Formulating and Expressing Internal Audit Opinions, provides expanded discussions of all these considerations.

Finding Follow-Up and Closure

Internal auditors follow up on findings to gain assurance that management actions have been implemented as planned and have sufficiently resolved the findings. Internal audit functions use varying approaches to follow up and have varying requirements for closure. However, these follow-up and closure activities are an essential component of internal auditing and are required by Standard 2500 - Monitoring Progress (which states, "The chief audit executive must establish and maintain a system to monitor the disposition of results communicated to management") and by Standard 2500.A1 (which states, "The chief audit executive must establish a follow-up process to monitor and ensure that management actions have been effectively implemented or that senior management has accepted the risk of not taking action"). Internal auditors should adopt effective practices for following up on and closing audit findings.

Approaches and Mechanisms

Finding follow-up may be handled in various ways. Some internal audit functions follow up on all findings, while others follow up selectively (for example, by not following up on low-risk findings). In addition, some internal audit functions prioritize following up on high-risk findings (for example, by scheduling more frequent communications with the business to check on progress toward closure).

Selective follow-up is enabled when the internal audit function rates findings. Regardless of the follow-up approach, the internal audit function should develop mechanisms for tracking findings, including defined, periodic communication with the business. All such follow-up activity should be documented, especially when follow-up extends over a period of time and calls for periodic updates from management. Many internal audit functions use a database to store findings, facilitate follow-up, document follow-up activities, and analyze trends in findings.

If management opts to accept the risk represented in a finding rather than to address and close it, the CAE must decide if such risk acceptance is within the risk tolerance of the organization. As previously discussed, if the CAE decides that it is not, it must be escalated to the board.

Level of Effort to Validate Closure

Internal audit functions decide what level of effort is required to validate finding closure. In doing so, they should examine the sufficiency of the closure actions and seek evidence that the closure is sustainable.

Some internal audit functions perform all such validation themselves. When they do, they determine the level of testing required to validate closure. They may accept testing performed by management or others (for example, other second line of defense functions), or they may perform testing themselves at the same level performed during the engagement.

Some internal audit functions accept management's assertion that findings are closed, at least for some findings. Specifically, some internal audit functions accept management assertion of closure for low-risk findings. Typically, findings closed in this way are included for coverage in subsequent audit engagements.

Adding Value to the Business

The communication from the internal audit function is critical in terms of the value it can provide to the business. Communication before, during, and after the annual risk assessment process enables the internal audit function to coordinate with other assurance providers, including second line of defense professionals, and senior management on risk assessment and assurance engagements, and contribute to the risk and control culture of the organization. Communication during engagement performance provides opportunities for the internal audit function to contribute to strengthening the specific control environments assessed. Providing micro and macro opinions positions the internal audit function to engage in conversations with all levels of management regarding the current state of individual control environments and the state of the overall organizational system of internal controls when the micro opinions are aggregated into a macro opinion. Finally, communication to the board regarding the various activities undertaken by the internal audit function provides an opportunity to have a dialogue regarding the value the board and senior management receive from those activities and allows for identification of additional value-adding activities the internal audit function can engage in to maximize the overall value it can provide the organization.