Topic 6 Internal Auditing

AUDIT REPORT GUIDANCE

The Global Internal Audit Standards provide relevant, mandatory guidance regarding audit reports. **Domain IV: Managing the Internal Audit Function** provides communication guidance for the chief audit executive, and **Domain V: Performing Internal Audit Services** provides guidance for the completion of audit engagements, including composing the final audit report.

Within Domain IV, Principle 11 and Standard 11.2 describe the tenets of effective communication. **Principle 11 Communicates Effectively** states, "The chief audit executive guides the internal audit function to communicate effectively with its stakeholders."

- **Standard 11.2 Effective Communication**

The chief audit executive must establish and implement methodologies to promote accurate, objective, clear, concise, constructive, complete, and timely internal audit communications. Methodologies, such as supervisory reviews, should enhance the degree to which engagement communications are: o Accurate: free from errors and distortions and faithful to the underlying facts.

- Objective: impartial, unbiased, and the result of a fair and balanced assessment of all relevant facts and circumstances.
- Clear: logical and easily understood by relevant stakeholders, avoiding unnecessary technical language.
- Concise: succinct and free from unnecessary detail and wordiness.
- Constructive: helpful to stakeholders and the organization, and enabling improvement where needed.
- Complete: relevant, reliable, and sufficient information and evidence to support the results of internal audit services.
- Timely: appropriately timed, according to the significance of the issue, allowing management to take appropriate corrective action.

Within Domain V, Principles 14 and 15, and the relevant Standards provide mandatory guidance regarding engagements and communication.

Principle 14 Conduct Engagement Work states, "To implement the engagement work program, internal auditors gather information and perform analyses and evaluations, collectively referred to as 'evidence.' These steps enable internal auditors to provide assurance and identify potential findings; determine the causes, effects, and significance of the findings; develop recommendations and/or collaborate with management to develop management's action plans; and develop conclusions."

- **Standard 14.4 Recommendations and Action Plans**

Internal auditors must determine whether to develop recommendations, request action plans from management, or collaborate with management to agree on actions to: o Resolve the differences between the established criteria and the existing condition. o Mitigate identified risks to an acceptable level.

- ❖ Address the root cause of the finding.
- ❖ Enhance or improve the activity under review.

- **Standard 14.5 Engagement Conclusions**

  Internal auditors must develop an engagement conclusion that summarizes the engagement results relative to the engagement objectives and management's objectives. The engagement conclusion must summarize the internal auditor's professional judgment about the overall significance of the aggregated engagement findings.

Principle 15 Communicate Engagement Conclusions and Monitor Action Plans states, "Internal auditors communicate the engagement results to the appropriate parties and monitor management's progress toward the implementation of recommendations or action plans."

- **Standard 15.1 Final Engagement Communication**

For each engagement, internal auditors must develop a final communication that includes the engagement's objectives, scope, findings, recommendations, and/or action plans, and conclusions.

The final communication for assurance engagements also must include:

- The findings and their significance and prioritization.
- An explanation of scope limitations, if any.
- A conclusion regarding the effectiveness of the governance, risk management, and control processes of the activity reviewed.

The final communication must specify the individuals responsible for addressing the findings and the planned date by which the actions should be completed.

When internal auditors become aware that management has initiated or completed actions to address a finding before the final communication, the actions must be acknowledged in the communication.

The final communication must be accurate, objective, clear, concise, constructive, complete, and timely, as described in Standard 11.2 Effective Communication.

If the engagement is not conducted in conformance with the Standards, the final engagement communication must disclose the following details about the nonconformance:

- Standard(s) with which conformance was not achieved.
- Reason(s) for nonconformance.
- Impact of nonconformance on the engagement findings and conclusions.

The **Considerations for Implementation and Evidence of Conformance** for Standard 15.1 add:

A statement that the engagement is conducted in conformance with the Global Internal Audit Standards should be included in the final engagement communication. Indicating that the internal audit engagement conformed with the Standards is appropriate only if supported by the results of engagement supervision and the quality assurance and improvement program.

The style and format of final engagement communication vary across organisations. The chief audit executive may provide templates and procedures.

Multiple versions of a final communication may be issued, with formats, content, and level of detail customised to address specific audiences, based upon how much they know about the activity under review, how the findings and conclusions impact them, and how they plan to use the information.

THE REPORTING PROCESS

As discussed in Unit 1 and according to IIA Standard 11.2 Effective Communication, communication should provide value to the audit client. Communication should be "accurate, objective, clear, concise, constructive, complete, and timely."

In order to demonstrate conformance with Standard 11.2 Effective Communication, internal auditors should be aware of the various communication touchpoints that occur during the reporting process.

The internal audit function begins an engagement with the production of a planning document, which occurs during engagement planning and outlines the objectives and scope of the engagement (Principle 13 Plan Engagements Effectively, including Standard 13.1 Engagement Communication). During engagement fieldwork, the internal audit function prepares a preliminary draft report noting observations/findings and recommendations (Principle 14 Conduct Engagement Work). After the fieldwork phase, the internal audit function composes the executive summary, which provides a review of the objectives, scope, and results. An engagement report is also developed, which consists of the details regarding engagement observations/findings, recommendations, and management response (Standard 15.1 Final Engagement Communication). The last stage of the information flow of audit report elements occurs during follow-up. This happens through status tracking of management action plans (Standard 15.2 Confirming the Implementation of Recommendations or Action Plans).

To ensure the information flow of the audit report elements occurs as described and timely, actionable results can be delivered to the activity under review, the internal auditor should focus on:

1. Writing the first draft of the audit report.
2. Obtaining observation/finding vetting and supervisory review.
3. Socializing the report with the activity under review.
4. Incorporating management's response and action plans.
5. Finalizing the audit report.

WRITING THE FIRST DRAFT

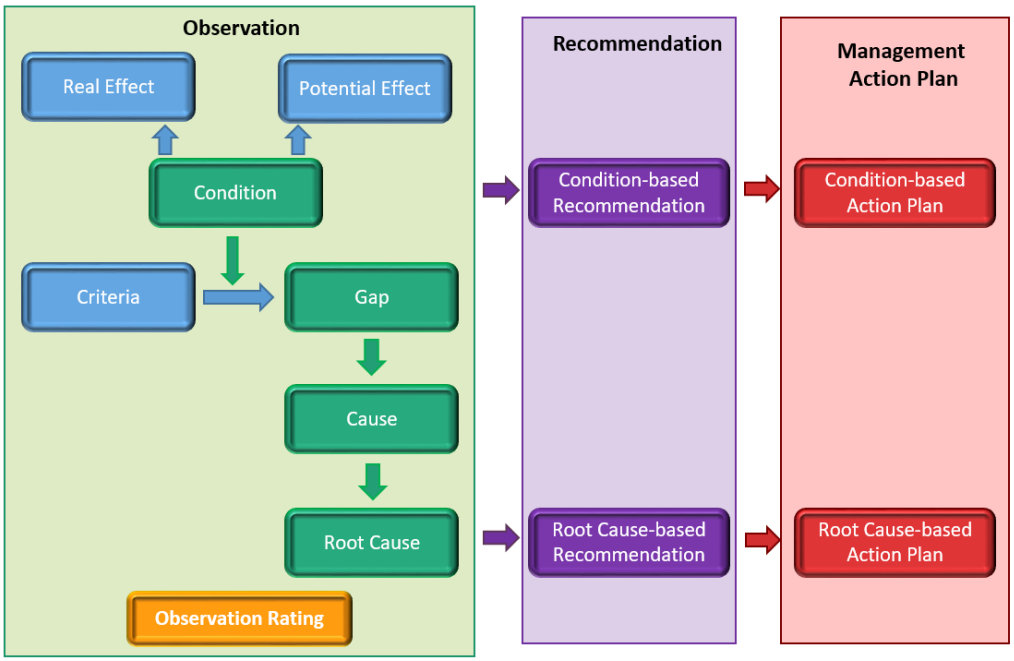
The internal auditor should use the observations/findings and recommendations from the workpapers to construct the first draft of the report. Report formats vary from organization to organization.
However, a typical audit report includes:

- An executive summary.
- Observations/Findings.
- A purpose (objective).
- Action plans.
- Scope.

- Release and confidentiality notifications.
- The whole report rating.
- Distribution list.
- Conclusions.
- Internal Auditors.

Observations/findings, recommendations, and management's action plans (responses) make up the core of a written report. These components enhance communication between the internal audit function and stakeholders and are linked together as illustrated in the figure below.

Figure 2: Observation, Recommendation, and Management Action Plan



Source: Writing An Audit Report – IIA Writing Toolkit

Source: IIA Audit Tool: Writing an Audit Report. The Institute of Internal Auditors, Inc. Audit Report Tool Kit. 2021.

OBTAINING OBSERVATION/FINDING VETTING & SUPERVISORY REVIEW

Prior to presenting a draft memo, observation/finding, or report to audit management for review, it is common first to have the document reviewed by another auditor in the department; this process is known as observation/finding vetting.

The observation/finding vetting process is designed to not only look for spelling, punctuation, and grammatical errors but also to ensure the message will be correctly received by the activity under review, senior leaders, the audit committee, and the board of directors. As internal audit function teammates are generally more familiar with the content under review than audit management, it is a good practice to start by conducting the observation/finding vetting process before the supervisory review process. The supervisory review would be conducted by the lead internal auditor/internal audit function manager and/or the chief audit executive (CAE).

Internal auditors should consider the following tips when conducting the observation/finding vetting review process:

- Read the draft completely before making any comments regarding content.
- Respond to the draft in a timely manner — consider the entire audit review cycle.
- Ensure you are aware of the method and tools used to document feedback if you are not using an edit tracking function, such as that in MS Word.
- Balance any critical feedback with positive feedback, along with considerations for improvement.
- Ensure the report tone is polite, professional, and mentoring (not blunt, rude, or offensive).
- Develop comments that are actionable and specific to content. Avoid using generic and unactionable comments like, “this does not make sense,” "it’s unclear,” “avoid using…,” or “it’s vague.”
- Include in your comments any questions that come to mind as you read the document.
- Remain free of bias and fallacies. Do not criticize if you do not agree or fully understand because you may not have technical expertise in a particular area. A good process to consider when conducting observation/finding vetting is determining if you can reasonably follow the evidence and come to the same conclusion as the reporting authoring auditor.
- Proofread your comments before providing them to your teammate or subordinate to ensure they are easy to follow, free of bias, and written in a mentoring, non-critical voice.

The internal audit function may develop a guide or checklist to aid in observation/finding vetting and/or supervisory reviews.

Review the sample observation/finding vetting guide for reviewing for The Five Cs:

OBSERVATION/FINDING VETTING GUIDE: REVIEWING FOR THE FIVE C'S

Criteria

- Does it answer the question "What ought to be?"
- Is the relevant standard, policy, procedure, or principle cited to give the observation/finding an authoritative tone?
- Is there a best practice or industry standard that can stand in for written policy, procedure, etc.?

Condition

- Does it answer the question "What is?"
- Does the condition state the factual evidence that the internal auditor found in the course of the examination (the current state)?
- Is the present or past situation described in a clear and concise manner?
- Did the condition contain high-level, mid-level, or granular detail?
- Is the condition quantified, wherever possible?

Cause

- Does it answer the question "Why?"
- Do the causes explain why the conditions do not agree with the criteria?
- Do proximate, intermediate, and root causes logically delve deeper to keep answering the question, "Why?"
- Are the actionable causes identified?

Consequence (Effect)

- Does it answer the question "So what?"
- Do the effects persuasively explain the risks and benefits by stating supportable facts? • Are effects logically differentiated from one-time direct impact? The systemic impact?
- If possible, has the writer quantified the effects?

Corrective Action Plan (Recommendations)

- Does it answer the question "What is to be done?"
- Does at least one of the recommendations and/or action plans effectively address and eliminate the cause?
- Are the recommendations and/or action plans practical, logical, cost effective, and actionable?

Every organization will differ, and after the observation/finding vetting process is complete, a supervisory review conducted by the lead internal auditor/internal audit function manager, and/or the chief audit executive (CAE) should be performed to comply with IIA Standard 12.3: Ensuring and Improving Engagement Performance, "The chief audit executive must ensure that engagements are properly supervised, quality is assured, and competencies are developed."

The guidance and suggestions provided for observation/finding vetting also apply to supervisory reviews.

SOCIALIZING THE REPORT WITH THE ACTIVITY UNDER REVIEW

After any revisions have been made to the audit report draft, and after the observation/finding vetting and supervisory review, the report should be shared as a draft with the activity under review. This is often referred to as "socializing the report."

The intention of socializing the report in its draft form is to share results in as close to real time as possible, while also reducing the possibility of "surprising" the activity under review with any findings during the closing conference. This also provides the activity under review and/or management time to review the observations/findings, respond to each of them, and develop action plans in response to the observations/findings.

INCORPORATING RESPONSE & ACTION PLANS

After the preliminary report (draft) is delivered to management in the previous step of socializing with the activity under review, management responds to each observation/finding. Management will develop an action plan for items requiring remediation, including identifying the responsible party, actions to be taken, and estimated delivery date.

Management may share the response and corresponding action plan in any format that is convenient to them, with comments made to the provided draft of the report, an email, a separate document, etc. It is then the internal audit function's responsibility to incorporate the responses and action plans into the final draft of the internal audit report.

FINALIZATION OF THE AUDIT REPORT

Once the internal auditor has incorporated the action plans obtained from the management of the activity under review, the last tasks that remain are adding any necessary materials to the appendix, creating version control headers/footers/watermarks as needed, and other document housekeeping type actions. The internal auditor should also schedule the closing conference/exit conference at this time (if it was not previously scheduled).

AUDIT REPORTING STRUCTURE

ASSOCIATED STANDARDS

The value of any audit engagement is defined by the quality of the assessment results. An internal auditor's ability to clearly articulate the intent and conclusion of an assurance or advisory engagement in the correct context and tone is paramount. Its importance is enforced by The IIA's Global Internal Audit Standards.

Standard 14.5 Engagement Conclusions

Internal auditors must develop an engagement conclusion that summarizes the engagement results relative to the engagement objectives and management's objectives. The engagement conclusion must summarize the internal auditor's professional judgment about the overall significance of the aggregated engagement findings.

Assurance engagement conclusions must include the internal auditor's judgment regarding the effectiveness of the governance, risk management, and/or control processes of the activity under review, including an acknowledgement of when processes are effective.

Standard 15.1 Final Engagement Communication

For each engagement, internal auditors must develop a final communication that includes the engagement's objectives, scope, findings, recommendations and/or action plans, and conclusions.

The final communication for assurance engagements also must include:

- The findings and their significance and prioritization.
- An explanation of scope limitations, if any.
- A conclusion regarding the effectiveness of the governance, risk management, and control processes of the activity reviewed.

TYPICAL AUDIT REPORT ELEMENTS

Report formats vary from organization to organization. However, a typical format includes:

An executive summary, including:

- Audit purpose (objective).
- Audit scope.
- Whole report rating.
- A conclusion.
- Observations/Findings, including:
  - Risk Ratings – Low, medium, high, critical, or material.
  - Recommendations.
- Action plans, including:
  - Management responses – General agreement/disagreement and action plan.
- Release and confidentiality notifications.
- Distribution list.
- Auditors.

ADDITIONAL REPORTING ELEMENTS

Depending on the organization or the audit project, some reports also include:

- Considerations for improvement – Lower significance/risk; could be verbally conveyed.
- Background information – About the area being audited.
- Business profile – Brief description of the business unit/agency being audited, such as location, sales volume, amount of inventory carried or products produced, etc.
- Methodology – How the audit fieldwork was accomplished.
- Standards – Conformance statements.
- Commendation – General appreciation for their cooperation during the audit.
- Management accomplishments.

THE EXECUTIVE SUMMARY

The executive summary should be a stand-alone document that provides high-level information for those readers who only want or need a big picture of the audit. Content and format may vary depending on audience, regulatory requirement, or organizational standards.

Common content that may be provided in the executive summary includes:

- A conclusion with high-level causes and effects.
- Audit objective (purpose).
- Audit scope.
- Observation/Finding summaries.
- Ratings.
- Release and confidentiality.

Some executive summaries also include:

- Background, including high-level risk drivers.
- Standards-compliance statement.

It is important to take the key stakeholders and other readers into consideration when writing the executive summary. Choice of words, tone, and technical complexity will all impact the reaction of the recipient. Today's executive summaries are typically a blend of affirming what was satisfactory at the time of the review and where an opportunity for improvement exists. Taking time in the report to recognize collaboration and cooperation can make even unsatisfactory reviews more palatable to the recipient.

Let's review an example of an executive summary for an emerging topic audit engagement:

Executive Summary

The purpose of the audit engagement was to provide management and the audit committee with an independent assessment of the organization's controls regarding the use of its remote management tool (RMT) and is based on the recent cyberattacks known to have targeted and adversely affected this technology.

Scope
This engagement focused on access management, the remote management tool (RMT) system security and monitoring, patching and vulnerability scanning of the RMT solution, and the playbook for validating the incident management program. The time period covered is the last six months.

Conclusion
One finding with a needs improvement rating and three findings with unsatisfactory ratings were noted. Recommendations have been made for these findings are summarized in the table.

Area	Rating	Overall Opinion	Audit Recommendation
Logging, Alerting, and Monitoring	Needs Improvement	Although all three elements are present, the organization is using the vendor's default alerts.	Consider developing additional alerts specific to organizational behavior (time of day, day of week, size/volume, etc.).
Patching and Vulnerability Scanning	Unsatisfactory	Patching is performed quarterly and vulnerability scans are performed monthly. All patching is based on N-1. Audit discovery is not enabled on the vulnerability scanner.	Consideration should be made to patch based on the National Vulnerability Database (NVD) criticality score vs. date. Vulnerability scanning should be performed as frequently as possible to identify newly identified vulnerabilities. The vulnerability scanner should be set to audit the discovery of new devices.
Zero-day Playbook	Unsatisfactory	A Zero-day playbook does not exist nor is Zero-day discussed in the incident management program.	Consider developing a process for monitoring zero-day exploits and analyzing their possible impact to the organization, as well as addressing the impact, if necessary.
RMT Playbook	Unsatisfactory	A playbook exists for unapproved access, malware, data breaches, and advanced persistent threat (APT), but nothing specific to RMT.	Consider developing a process to identify, assess, and respond to a cyber incident that impacts the organization's RMT solution.

THE EXECUTIVE SUMMARY: AUDIT OBJECTIVES

The audit objectives, or purpose, section of the executive summary describes what the audit aimed to achieve. Essentially, the objectives state why the audit was conducted.

The high-level audit objective is typically developed during the annual internal audit planning process and approved by the internal audit committee. During planning, the internal auditors and activity under review may expand or adjust the audit objectives. The organization's culture and regulatory environment will determine whether changes in objectives must be first approved by the chief audit executive (CAE) and audit committee.

Common verbs used in writing objectives include evaluate, assess, or determine.

Example: The objectives of the audit were to assess the accuracy and timeliness of accounts payable, including determining the sufficiency of systems used to support the accounts payable process.

THE EXECUTIVE SUMMARY: AUDIT SCOPE

The audit scope section of the executive summary describes what the audit covered; it sets the boundaries of the audit.

The high-level audit scope is normally developed during the annual audit planning process and approved by the audit committee. During planning, the auditors and auditee may expand or adjust the audit scope. For some organizations, the scope continues to evolve into the engagement fieldwork. The organization's culture and regulatory environment will determine whether changes in audit scope must first be approved by the CAE and audit committee.

The scope is written using inclusion and, when necessary, exclusion statements.

- Inclusion states the bounds of the audit.
- Exclusion states what the audit did not cover; this is important if the reader might otherwise expect such coverage.

Common reasons for exclusion include:

- The scope area was or is being covered by another audit.
- Some aspect of the area being audited (e.g., a sub-process or a system) has recently changed or is about to change significantly.
- Some activity of the area being audited is newly implemented and no auditable records have been created.
- Some activity of the area being audited was deemed a low risk and removed from fieldwork.
- The time to accomplish the assessment exceeded the time allowed for that aspect of the engagement.

In describing any exclusion, you should explain *why* the area is being excluded.

Example: The audit covered accounts payable activity during the first three quarters of 2022. All payments to vendors were included, with the exception of payments related to the construction of the West Overland facility; that project will be audited comprehensively in a separate Q1 2022 project audit.

THE EXECUTIVE SUMMARY: OBSERVATIONS/FINDINGS

It is common to include a summary of current and repeat findings within the executive summary, whereas detailed observations/findings and their risk rankings are found in the observations/findings section of the report. In the executive summary, references to observations/findings should be written with a message-first approach; include the main point of any substantial observations/findings up front rather than at the end or in the middle of the report.

Example: The internal audit team noted that the same business units, including IT, continue to purchase subscriptions to web services through their personal credit cards and are reimbursed through the T&E system. These actions continue to violate both the procurement and T&E policies as stated in the audit reports from 2022 and 2023, despite the remediation efforts put forth following the two prior-year engagements.

THE EXECUTIVE SUMMARY: RISK RATINGS

Many organizations rate each observation/finding. Typically, the rating is assigned based on risk — the inherent risk of the audited activity coupled with what the auditors found (the condition) and concluded (the cause and effect) about the design and operation of the controls (the current risk).

The ratings may be expressed in several ways using:

- The words low, medium, or high (often with low-rated observations/findings omitted from the audit report or listed without elaboration).
- The "traffic light colors" — red, yellow, and green (sometimes with orange inserted between red and yellow, and often with observations/findings rated green omitted from the audit report or listed without elaboration).
- Words such as critical, significant, major, and minor (often omitting observations/findings rated as minor from the audit report or listing without elaboration).

Each observation/finding is typically risk-rated before the audit report is written, and the observations/findings identified as high or critical are incorporated into the executive summary.

THE EXECUTIVE SUMMARY: WHOLE-REPORT RATING

The whole-report rating is a rating that typically places the results of the engagement as a whole on a scale using a combination of objective criteria and professional judgment. A whole-report rating may be included as an aspect of the conclusion section, or as its own stand-alone section of the executive summary.

Example:

Overall Rating: Needs Improvement (where A=7; B=4; C=5)

Calculation:

A = Total number of controls assessed divided by the number of controls deemed satisfactory.

B = Total number of controls assessed divided by the number of controls deemed to need improvement. C = Total number of controls assessed divided by the number of controls deemed unsatisfactory. If A > (B+C) = Satisfactory.

If A > B < C = Needs Improvement.

If (A+B) < C = Unsatisfactory.

Rating systems may use words, colours (e.g., traffic light colours of red, yellow, and green), or numbers. Such systems typically offer three ratings, but some offer as few as two and as many as five.

- Unsatisfactory, satisfactory (red, green).

- Unsatisfactory, needs improvement, satisfactory (red, yellow, green).

• Unsatisfactory, needs significant improvement, needs improvement, satisfactory (red, orange, yellow, green).

Example:

Accounts Payable: Needs Significant Improvement.

Be aware that some organizations would fail the audit (unsatisfactory rating) if any control received an unsatisfactory rating.

ACTIVITY: RISK RATING

Instructions

- Read the provided scenario.
- Use the provided rating system for the report.
- Review the five provided observations/findings and rate them based on the rating system.
- Write a conclusion that incorporates your rating results.
- Be prepared to share your response.

Scenario

Your audit team has just completed fieldwork on a continuity audit, focusing on plan maintenance and testing. The team requests your assistance with completing the risk rating.

Rating System

Unsatisfactory	Needs Significant Improvement	Needs Improvement	Satisfactory

Risk	Observation/Finding	Risk Rating
1. Out-of-date business continuity plans could impede recovery, causing financial and reputational damage to the organization.	The organization has a documented business continuity plan (BCP). Annually, each business owner reviews their plan, makes adjustments, and confirms it is current. The marketing department was the only department that failed to perform last year's annual review and confirmation.	
2. Plans may not address healthrelated emergencies that could impact the workforce.	Neither the business continuity plan nor the disaster recovery plan included provisions for pandemic planning so the organization was not prepared for its entire employee base to work from home long term.	
3. Not having current content details at the onset of an incident could slow the organization's abilities to recovery key systems or obtain key resources.	During the last audit, it was noted that the employee and vendor call library had not been updated since the previous audit. The department updated the observation/finding and, after validation, the observation/finding was closed. During this audit, the auditor also noticed the call library had not been updated since the observation/finding was closed 15 months ago.	

Risk	Observation/Finding	Risk Rating
4. Critical systems, in-house or cloud-based, may not be recovered in a timely fashion leading to regulatory, legal, financial, and/or reputation loss.	The disaster recovery plan does not reflect the changes in technology nor vendors introduced since the onset of work-from-home over a year ago.	
5. Recovery of critical infrastructure may be delayed if critical resources are not authorized in implement recovery proceedings.	The disaster declaration process has not been updated to reflect the personnel changes nor the addition of the Disaster Recovery as a Service (DRaaS) provider.	

THE EXECUTIVE SUMMARY: CONCLUSION

The executive summary conclusion summarizes the observations/findings and communicates the outcome in context for executive readers. It is written at a high level and in plain, candid language.

Example:

Risks in the accounts payable process were not routinely assessed by management, and management did not sufficiently monitor accounts payable activity. As a result, the organization may not be getting the best value for its purchases.

Two areas present the greatest risks:

1. Untimely payments to vendors.
2. Confusing and potentially inaccurate reporting to executive management on accounts payable activity.

Management has committed to taking the necessary steps to improve its oversight, including assigning resources appropriately, updating systems, and enhancing reporting.

Some organizations may also incorporate the whole report risk rating as part of the conclusion section, instead of a stand-alone section in the executive summary.

REPORT BODY: OBSERVATIONS/FINDINGS

Once the executive summary is complete, the focus shifts to providing the supporting detail in the main body of the results reporting. This section contains the details behind each observation/finding.

Observations/Findings Section

The detailed findings are presented in the observations/findings section of the report or in an appendix.

Observations/findings fall into three categories:

1. Observations/findings that signify a control failure – Items discovered and validated during fieldwork signify a control has failed to meet its objective.
2. Repeat findings – Findings that were present in prior audits that still exist or have resurfaced.
3. Considerations for improvement – Observations/findings that are low risk or gaps in current controls that would prevent the activity under review from improving their maturity level.

There are several formats used for the observations/findings section, depending on the type of information being presented, the audience, and the presentation format. The observation/finding format varies from organization to organization and from one audit shop to the next.

Some of the more common observation/finding formats are:

- Paragraphs.
- Tables.
- Bullets.

REPEAT FINDINGS

Periodically, the auditor will discover that a prior audit finding was not sufficiently addressed in the last audit report period, or the action item and remediation date agreed upon during the last audit report period had been postponed.

These findings are typically escalated quickly to executive management, the audit committee, and the board because they may indicate a compliance culture issue within the organisation. This could, based on the industry, open the organisation to additional scrutiny by regulators and external auditors. In addition, if the failed or postponed remediation can be tied to a successful security incident, the organisation's insurance claim could be denied.

Repeat findings are normally stated first in the executive summary and then further defined in the body of the report.

The internal audit function of the organisation may choose to detail repeat findings in a separate portion of the observations/findings section, adding columns for the original finding, risk ranking, recommendation, and management's action plan in addition to the new observation/finding statement, updated risk ranking, and new recommendation and management action plan.

Internal auditors should also document "partial repeat" findings. A partial repeat finding is one where some of the prior issues have not been fully addressed.

RECOMMENDATIONS, RESPONSES, AND ACTION PLANS

Beyond writing the observation/finding, some internal audit functions also provide a non-perspective recommendation. Internal auditors should use intentional word choice and tone when writing recommendations as it is management's role to decide how to respond to an observation/finding.

Recommendations

Recommendations, if used, follow each observation/finding and describe possible solutions to address root cause(s) and correct adverse conditions.

Example:

Observation/Finding	Recommendation	Rating	Management Response	Action Plan
A repository of active vendors is not maintained. New vendors are manually added to the accounts payable system once the procurement department confirms a PO was sent to the vendor and that the product requested arrived. In the last 60 days, the organization has had to pay a late penalty six times, three times regarding new vendors not yet set up in the accounts payable system.	Procurement should develop a process to communicate new vendors to the accounts payable department to ensure timely payment of merchant invoices.	Needs Improvement		

MANAGEMENT'S RESPONSE

After the observation/finding and recommendation have been approved by internal audit management and presented to the activity under review, the activity under review will consider the observation/finding and recommendation (if provided) and determine whether or not they are in agreement. Generally speaking, management will either agree, challenge, or disagree with each observation/finding, recommendation, and/or rating.

Management Responses (for each observation/finding).

- Agree.
- Refute (challenge) or ask for the observation/finding to be explained.
- Disagree/argue the:
  - ❖ Observation/finding conclusion (opinion).
  - ❖ Ratings.

Example:

Observation/Finding	Recommendation	Rating	Management Response	Action Plan
A repository of active vendors is not maintained. New vendors are manually added to the accounts payable system once the procurement department confirms a PO was sent to the vendor and that the product requested arrived. In the last 60 days, the organization has had to pay a late penalty six times, three times regarding new vendors not yet set up in the accounts payable system.	Procurement should develop a process to communicate new vendors to the accounts payable department to ensure timely payment of merchant invoices.	Needs Improvement	10/04/21: Challenge – The process is for accounts payable to call if they do not have the vendor details, which is the process they follow.	

ACTION PLANS

Management is responsible for developing action plans describing what the activity under review has committed to do to address the root cause(s) and to correct existing deficiencies and gaps. The action plan should not only discuss what will be done but also by whom and in what time frame. The internal auditor and management should agree on the action plan prior to closing the audit.

The internal auditor should also place the action plan into a tracking tool to verify timely remediation, appropriate audit follow-up testing, and validation.

Example:

Observation/Finding	Recommendation	Rating	Management Response	Action Plan
A repository of active vendors is not maintained. New vendors are manually added to the accounts payable system once the procurement department confirms a PO was sent to the vendor and that the product requested arrived. In the last 60 days, the organization has had to pay a late penalty six times, three times regarding new vendors not yet set up in the accounts payable system.	Procurement should develop a process to communicate new vendors to the accounts payable department to ensure timely payment of merchant invoices.	Needs Improvement	10/04/21: Challenge – The process is for accounts payable to call if they do not have the vendor details, which is the process they follow. 10/15/21: Agree. Reviewed audit findings with the internal auditor and have obtained a better understanding.	Procurement will work with accounts payable to ensure new vendors are established in the accounts payable system at time of PO submission. **Plan assigned to:** Procurement Manager **Accountable Party:** Chief Operations Officer (COO) **Due:** 12/31/2021

CONSIDERATIONS FOR IMPROVEMENT

The considerations section — which may be an appendix or separate limited distribution memo — is used to inform the activity under review of observations/findings that have minimal risk at the present time. This section is typically omitted from the final board package. However, these risks should be considered because they:

- May impede their ability to meet their objectives in the future.
- May keep the activity under review to achieve a higher level of program maturity, such as moving from a manual to an automated control.
- May currently pose a limited risk to the organisation, with the potential to become a bigger issue in the future.

The primary characteristics of a consideration for improvement include:

1. The issue is not significant enough to be included in observation(s)/finding(s).
2. Management is not required to respond to the issue.

Example:

The organisation plans to migrate all their systems from passwords to password-less authentication using FIDO2 security keys next year, once they thoroughly test the new authenticator app. Internal audit recommends that the organisation develop a process to manage the security keys before the keys are distributed to the employee population, and adjust their existing password policy and help desk knowledge database before they begin the migration.