High-Impact Audit Reporting

Participant Guide

The Institute of
Internal Auditors

Elevating Impact

COURSE INTRODUCTION

NOTES TO THE PARTICIPANT

About This Guide

This Participant Guide (PG) is designed to provide a basis for learning this course material. Please follow the guide closely and make sure to take notes throughout. Participants are encouraged to have a copy of the Global Internal Audit Standards readily available for the duration of the instruction of this course.

Participant Involvement

This course is intended to be highly interactive. Participants' involvement and motivation is crucial to their success and essential to the success of the course.

This page intentionally left blank.

This page intentionally left blank.

TABLE OF CONTENTS

INTRODUCTION

This course will provide you with the fundamental steps needed to develop a sufficient audit report. You will focus on developing the audit report using five components in a way that successfully evaluates the significance of an issue.

You will also learn how to determine reportable items and assemble audit reports in a manner that appropriately (accurately, objectively, clearly, concisely, constructively, completely, and timely) communicates the observations.

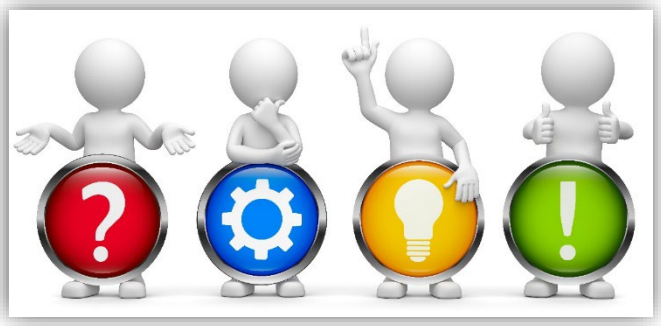
This course is designed to help those who write audit reports analyze their current report format for its effectiveness in eliciting management to take action.

LEARNING OBJECTIVES

- Discuss the importance of delivering results that utilize business acumen disciplines.
- Explain how audit results impact an organization's business objectives and operating processes.
- Recognize the importance of critical thinking when developing and communicating audit results.
- Recognize the communication needs of audit report readers and writers.
- Review the components of the audit report.
- Explore various reporting methods and formats.

PARTICIPATION

Discussion Questions



Activities

PARTICIPANT GUIDE

- Aligns with the course structure.
- Includes blank lines or space for taking notes.
- Will be used to record new ideas or insights.
- Is a resource to recall concepts learned and organize ideas and actions to be taken.

ACTIVITY: PERSONAL LEARNING OBJECTIVES

Instructions

- Document your personal learning objectives in the space provided.
- Be prepared to share your response.

_____

_____

_____

_____

_____

_____

_____

WORKING AGREEMENT

Learning is a process, and much of the success of this course depends on creating an effective learning environment that enhances the learning process. To nurture this environment, we want to establish a working agreement following the acronym PROCESS. Using this working agreement, we agree to demonstrate:

- P = Participation – This course is highly participatory. By agreeing to actively participate in discussions and exercises, you will get the greatest benefit from the program.

- R = Respect – There will be times when we will "agree to disagree" on the significance of issues, possible solutions, and best practices. We agree to show respect by actively listening to other viewpoints and not "forcing" our views on others.

- O = Openness – We will share our experiences and provide constructive feedback. By agreeing to such openness, you can expand your perspectives and build your skills.

- C = Confidentiality – Confidential matters should not be discussed outside class. Be aware that information of this kind may have consequences for others.

- E = Enthusiasm – Be enthusiastic about this learning experience!

- S = Sensitivity – You should be sensitive to the feelings and perspectives of others.

- S = Sense of fun – This course should be an enjoyable experience for everyone. If we approach the discussions, exercises, and other learning tools with the right mindset, we will not only have more fun but also will learn more.

UNIT WRAP-UP

Key Takeaway:

Questions and Answers:

Action Plan:

UNIT 1

THE PURPOSE OF AUDIT REPORTING

INTRODUCTION

This unit covers:

- Audit reporting guidance.
- Purpose of audit reporting.
- Audiences for audit results.
- Audit reporting limitations.

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:
  - 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, Principle 14, Principle 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:
  - Resolve the differences between the established criteria and the existing condition.
  - 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 varies across organizations. 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 customized 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.

This page intentionally left blank.

ACTIVITY: AUDIENCES FOR AUDIT RESULTS

Instructions

- Review the background information.
- Complete the table for each of the identified readers (audience) that receive audit results:
  - For each audience identified, describe what portions of the audit report pertain to them, how familiar they are likely to be with the audited activity area, and how they will use the details of the results provided in the audit report.
- Be prepared to share your results.

Background Information

Audit communications serve multiple purposes, and the audience will vary based on organization, type of engagement, and audit topic. Internal auditors should understand their audience before drafting the results of an engagement. Knowing how the report will be used — and the readers' levels of knowledge of and management level over the area being audited — will help guide the internal auditor in drafting the final communication.

Reader's Title (Audience)	How will the reader(s) use the information in the audit report?	**Reader's Role in Area Audited (e.g., Executive, Manager, Process Owner, etc.)**
Activity under review		
Management over the activity under review		
Executive management (CFO, CEO, etc.)		
External auditor		

Reader's Title	How will reader(s) use the information in the audit report?	Reader's Role in Area Audited (e.g., Executive, Manager, Process Owner, etc.)
Peers (Audit Colleagues)		
Board of directors		
Regulators		
Media (in the public sector)		
Other stakeholders (e.g., politicians, competitors, or benchmarking organizations)		
Other: _____		

This page intentionally left blank.

ACTIVITY: LIMITATIONS ON RESULT COMMUNICATION

Considering the importance of audit report readership and the varied response responsibilities to audit reporting that we established in the previous activity, it makes sense that an internal auditor should consider organizational limitations when it comes to audit result communication.

Instructions

- Respond to each of the questions.
- Be prepared to share your response.

Questions

1. What policies and procedure requirements have been developed to guide your audit result communications?

_____

_____

_____

_____

2. What governing body enforces the results communication policies and procedures?

_____

_____

_____

_____

3. What audience considerations should be considered during audit result development and communication?

_____

_____

_____

_____

This page intentionally left blank.

UNIT SUMMARY

In this unit, we established the importance and purpose of audit reporting. We reviewed the guidance related to audit reporting and written communications. We also explored the differences in audiences for audit reports and the limitations associated with various audit report readership.

This unit provided internal auditors with several activities to consider how audit reporting occurs in their own organization and be exposed to the processes and procedures involved in other internal auditor's organizations as well.

UNIT WRAP-UP

Key Takeaway:

Questions and Answers:

Action Plan:

UNIT 2

AUDIT REPORTING TASKS

INTRODUCTION

This unit covers:

- An overview of the audit reporting process.
- The tasks associated with the audit reporting process, including:
  - Writing the first draft of the audit report.
  - Obtaining observation/finding vetting and supervisory review.
  - Socializing the report with the activity under review.
  - Incorporating management's response and action plans.
  - Finalizing the audit report.

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.

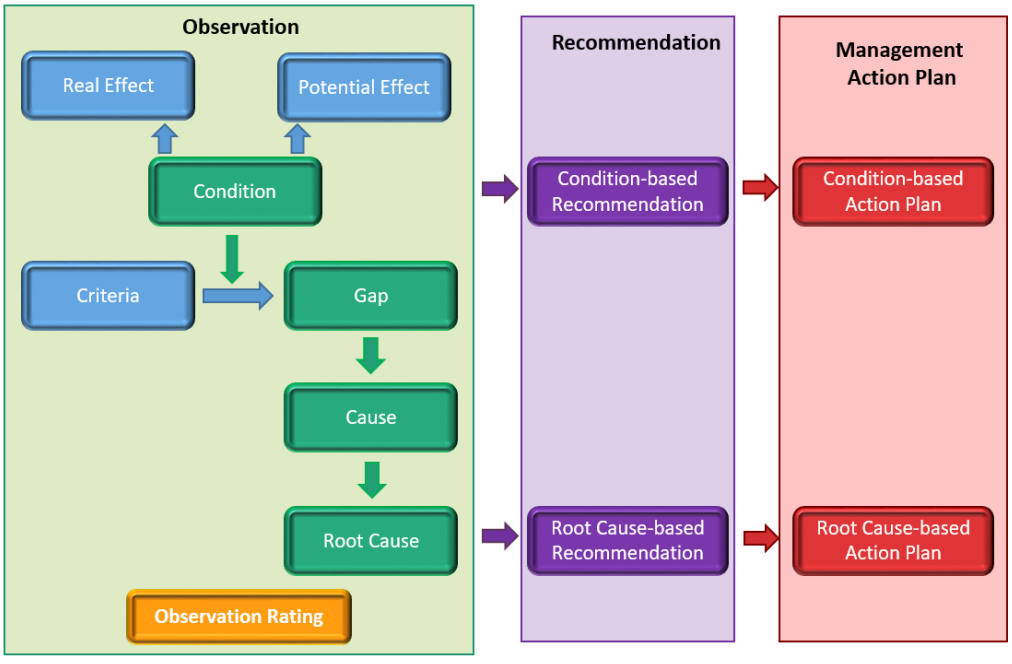
WRITING THE FIRST DRAFT

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.
- A purpose (objective).
- A scope.
- The whole report rating.
- Conclusions.
- Observations/Findings.
- Action plans.
- Release and confidentiality notifications.
- Distribution list.
- 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.

This page intentionally left blank.

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 un-actionable 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.

This page intentionally left blank.

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).

ACTIVITY: AUDIT REPORTING TASKS

Instructions

- Review each of the task scenarios below.
- Place them in the correct order to demonstrate an understanding of the flow of information during audit reporting tasks.
- Be prepared to share your response.

Task Order	Task Scenario
	a. Jeffery asks Audrina, another staff auditor, if she is willing to conduct a round of observation/finding vetting on his first draft of the audit report. She agrees and provides comments and suggestions via track changes in the MS Word document draft that Jeffery provided to her.
	b. Jeffery makes changes to the draft based on observation/finding vetting feedback, then submits the draft to Raquel, his audit manager. Raquel reviews the draft and informs Jeffery that he may move on to the next task in his audit report development process.
	c. Jeffery incorporates Nikolai's responses and action plans into the audit report draft and adds the associated headers/footers and necessary appendixes. He also verifies that a final conference has been scheduled with Nikolai.
	d. Jeffery utilizes the observations/findings and recommendations from the workpapers to begin developing the executive summary, as well as the conclusion and recommendations.
	e. Jeffery emails a PDF copy with the "draft" watermark to Nikolai, the manager of the activity under review for his consideration.
	f. Nikolai emails Jeffery his responses to the recommendations and associated action plans.

This page intentionally left blank.

UNIT SUMMARY

In this unit, we established an overview of the tasks associated with the audit reporting process. We examined the primary tasks at a high level, including:

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

This unit provided internal auditors with several activities to practice applying their knowledge of the tasks associated with audit reporting. It also exposed participants to the processes and procedures in other internal auditors' organizations regarding audit reporting tasks.

UNIT WRAP-UP

Key Takeaway:

Questions and Answers:

Action Plan:

UNIT 3

AUDIT REPORTING STRUCTURE

INTRODUCTION

This unit covers:

- Audit reporting elements.
- Communication of audit results.
- Other reporting considerations.

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.

ACTIVITY: UTILIZING IIA STANDARDS 14.5 AND 15.1

Instructions

- Review the provided sample statements from an audit report.
- Identify one or more examples where the tone could be improved for objectivity and clarity.
- Rewrite the identified examples to improve the tone.
- Be prepared to share your response.

Sample Statements

a. The assessment identified several internal control deficiencies that require management's attention.
b. The assessment identified several internal control failures that could subject the organization to a security breach.
c. The assessment identified several internal control issues that were not effectively addressed during remediation after the last audit.
d. The assessment identified several internal control gaps that would not exist if the IT department had followed its own policies.

Statement Rewrites

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

This page intentionally left blank.

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.

This page intentionally left blank.

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.

This page intentionally left blank.

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.

This page intentionally left blank.

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 number of controls deemed satisfactory.
B = Total number of controls assessed divided by number of controls deemed needs improvement.
C = Total number of controls assessed divided by 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, colors (e.g., traffic light colors 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.

This page intentionally left blank.

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 health-related 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.	
4. Critical systems, in-house or cloud-based, may not be recovered in a timely fashion leading to regulatory, legal,	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.	

financial, and/or reputation loss.		
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.	

Conclusion

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.

ACTIVITY: BUILD AN EXECUTIVE SUMMARY

Instructions

- Place the statements in an order representative of developing an executive summary.

Order	Statement
	a. The process was recently automated as part of the organization's digital transformation initiative.
	b. The audit engagement focused on ensuring the controls continue to be effective after the automated process was completed and was specifically focused on the membership engagement objective.
	c. Due to the high-risk observation/finding and the number of unaddressed repeat observations, the report rating is unsatisfactory.
	d. There were three repeat observations/findings where manual process-related controls were not improved as a part of digital transformation.
	e. The audit was performed using the waterfall methodology and conducted in 90 days.
	f. There were three observations/findings that were considered medium risk and one considered high risk, as the organization currently does not have an automated reminder process before memberships expire and no longer triggers electronic or physical reminder emails.

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 a prior audit finding was not sufficiently addressed from 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 generally elevated quickly to executive management, the audit committee, and the board because they may signify a compliance culture issue within the organization. This could, based on the industry, open the organization 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 organization'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 organization 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		

This page intentionally left blank.

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.	

This page intentionally left blank.

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 and 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

This page intentionally left blank.

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's process from achieving a higher level of program maturity, such as moving from a manual to an automated control.
- May currently pose limited risk to the organization, 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 organization 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 organization 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.

ACTIVITY: WRITE A CONSIDERATION FOR IMPROVEMENT

Instructions

- Review the provided telecommuting policy narrative.
- Draft a consideration for improvement memo based on the information in the narrative.
- Be prepared to share your response.

Telecommuting Policy Narrative

The old telecommuting policy explicitly states that certain activities should not be performed remotely. Those items include:

- Conducting wire transfers.
- Performing router, switch, and firewall configurations.
- Accepting credit card numbers from clients over the phone.
- Performing access administration.
- Using emergency/system IDs.
- Using public cloud collaboration tools.
- Contract engineers, technicians, and programmers accessing production systems remotely.

During the review, the auditor noted that the policy had been updated, stating that the entire employee and consultant base is allowed to perform all job duties from home, including IT network administration and wire transfers. The auditor verbally confirmed with management that all the processes described in the prior policy are being performed remotely; however, the new policy did not remove the paragraph above.

Consideration

_____

_____

_____

_____

_____

_____

_____

_____

_____

This page intentionally left blank.

APPENDICES

Common inclusions in appendices are:

- Definitions of whole-report and observation ratings, if used.
- Glossary and/or definitions of acronyms and abbreviations.
- Supporting details:
  - Additional background.
  - More detailed methodology information.
  - More granular-level data related to the observations.
  - Charts, graphs, and pictures.
  - Links to prerecorded videos.

Background
A background section within the appendix may be used for observations/findings and/or presented within the executive summary section to provide background on the audit project. It may also be incorporated into the appendix for audits that are shared to a larger or public population.

Some observations/findings call for explanatory background information to place the observation/finding in context. For example, observations/findings related to highly technical issues or areas experiencing significant changes may call for background information that is particular to the observation/finding.

Consequently, some organizations include a background section as a lead-in to each observation/finding.

A background section within the executive summary provides information that helps the reader understand the key messages of the report. If included, this section should:

- Provide a description of the process or processes being audited by using appropriate metrics.
- Describe any significant changes within the audited area or that affect the audited area.

This section also may list previous audits conducted and summarize their results.

Example:
Accounts payable processed US $410 million in 2019 and has processed US $489 million in 2020. In Q1 2021, the accounts payable activity was moved to another physical location following the merger with Company X.

Methodology
A methodology (or approach) section describes in a general way how the audit was performed. It may list general audit activities and include special tools used (e.g., data analysis tools).

Methods that are specific to the work done on a particular observation/finding should not be described in the executive summary. Rather, they should be described in the observation/finding itself, generally along with the condition.

Example:
This audit was conducted in accordance with the Internal Auditing Standards for the Government of [country where audit occurred] and The Global Internal Audit Standards.

The following methodologies and techniques were used during the examination phase of this audit:

- Interviews with key project management stakeholders across the agency.
- Review of documentation related to project management processes.
- Review and analysis of data from various sources, including project documentation.
- Review of project documentation for sampled projects.

OTHER REPORTING DETAILS

Audit reports typically also include additional details, including release and confidentiality notifications, distribution lists, and/or a list of auditors that varies by organization and audit reporting stage.

Release and Confidentiality Notifications
This section specifies how release and confidentiality of the report are controlled and what is necessary for release of the report externally. These details may be in the body of the report, as a watermark, on a title page, or as a header or footer.

Distribution
This section describes who receives the report and can be organized in a number of ways depending on the organization.

- Internal recipient – The activity under review.
- Internal copies – Senior management or the audit committee.
- External copies – External audit, regulators, or the public.

Auditors ("Audit Performed By" Information)
This may include:

- Auditor or auditors who performed the engagement.
- Auditor in charge or audit team leader (if appropriate).
- Others in audit management (if appropriate).

This page intentionally left blank.

CONFORMANCE AND NONCONFORMANCE DISCLOSURE

The internal audit process, including reporting, should follow the International Professional Practices Framework (IPPF). The report should be written in a way that demonstrates conformance and discloses nonconformance. **Standard 15.1 Final Engagement Communication** includes guidance to address these topics:

The Considerations for Implementation remind internal auditors that "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 eh Standards is appropriate only if supported by the results of engagement supervision and the quality assurance and improvement program."

One of the requirements of Standard 15.1 states that "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."

Example 1:
This audit was conducted in conformance with The Global Internal Audit Standards.

Example 2:
This audit was conducted in conformance with the Treasury Board Policy and Directive on Internal Audit and The Institute of Internal Auditors' (IIA's) International Professional Practices Framework (IPPF). Sufficient and appropriate evidence was gathered through various procedures to provide an audit level of assurance. The agency's internal audit function is independent and internal auditors performed their work with objectivity as defined by The IIA's Standards.

This page intentionally left blank.

UNIT SUMMARY

In this unit, we examined common audit reporting elements, including the executive summary, risk ratings, recommendations, etc. We also discussed the communication of audit results, including variety in readership and response. Finally, we explored other reporting considerations, including the usage of appendices and conformance and nonconformance disclosure.

This unit provided internal auditors with several activities to practice the skills associated with audit reporting structure and engage with other participants to discuss the variety of ways audit reporting can occur.

UNIT WRAP-UP

Key Takeaway:

Questions and Answers:

Action Plan:

UNIT 4

COMMUNICATING AUDIT RESULTS

INTRODUCTION

This unit covers:

- Methods to develop and present audit results.
- Developing an interim report or memo.
- Audit reporting formats.
- Comparisons of audit reporting structures.
- Conducting supervisory reviews.

WAYS TO PRESENT AUDIT RESULTS

Organizations may select from several options when it comes to presenting the results of an audit engagement.

Traditionally, the internal auditor will provide a memo to discuss interim results — or to summarize a consulting engagement — and the formal audit report is the final product provided to the activity under review and board upon completion of the engagement. In this traditional method, most memos and reports are written in MS Word and then saved to a PDF to reduce the ability of the activity under review modifying the report (or seeing the metadata created during the MS Word document editing process).

While these traditional methods hold merit, internal auditors may also utilize technology in presenting the audit results, including PowerPoint presentations, video reviews, and interactive storyboarding.

Additionally, closing conferences may be in person or virtual using a collaboration tool.

This page intentionally left blank.

REPORT FORMATS AND DELIVERY METHODS

Let's further explore the most common formats and delivery methods used today.

Report Formats

- Written reports.
- PowerPoint presentations.
- Video reports.
- Using visualization tools and strawman or storyboard approaches.

Delivery Methods

- Oral – Live using a collaboration tool.
- Oral – In-person.
- Video – Prerecorded with live Q&A.
- Video – Live.

Selection Considerations
The selection of the format and delivery method is going to be based on several factors, including the industry, organizational culture, preferences of audit client and audit (supervisory) committee, and significance of the message being conveyed.

DEVELOPING MEMO AND INTERIM REPORTING

During the course of the audit, the audit team may create a memo — or interim report — to ensure transparency and quickly communicate observations that have the potential to significantly impact the activity under review. Two common intermediate communication documents are the memo and interim report.

Memo

The memo can take the form of MS Word document or email communication depending on the message, ability to maintain the chain of communication, and anticipated actions required.

Interim Reporting

Auditors could utilize interim reports for one of several purposes, including:

1. Communicate material observations of a high priority in a timely fashion.
2. Communicate results from a sprint, when conducting an Agile audit using Scrum methodology.
3. Communicate satisfactory audit findings.
4. Communicate consulting engagement results or engagement updates.

OBSERVATION/FINDING FORMATS

Formal observations/findings can be included in a memo or report. Determining the content and tone of the observation will be based on the culture of the organization and severity of the finding.

Common Formats for Displaying Observations/Findings

Observation Format	Strengths	Weaknesses	Useful Writing Skills
Paragraph	• The relationship of the components is explicit. • A coherent, logical case can be built. • The relative severity of the risks can be more easily described.	• The components are not explicitly identified. • One "best" reading sequence is implied. • The report is potentially longer. • The reading takes longer. • The writers and the audit client may spend more time discussing the wording of the report.	• Paragraph organization. • Paragraph coherence. • Readable, clear sentences. • Punctuation.
Table	• Components can be explicitly identified, improving clarity and understanding for the reader. • The reader selects the reading sequence. • Draws attention to parts reader might be most interested in. • Makes for an effective appendix.	• Coherence among components is limited. • The physical constraints of the table may frustrate the writers.	• Conciseness. • Consistent use of terms.
Bullets	• The report is generally shorter. • The report can be used as a presentation. • The reading is quick. • Critical information can be emphasized through the short, isolated presentation of the elements and their sequencing on the list. • Useful in compliance audits.	• Coherence among components is severely limited. • Readers must derive the connections among the elements. • Lack of parallel structure and overly shortened items may make the meaning cryptic.	• Categorizing and prioritizing. • Conciseness. • Parallel structure. • Consistent use of terms.

Source: *Designing and Writing Message-Based Audit Reports*. Internal Audit Foundation. Reprinted with Permission. Copyright © 2001.

While this rather traditional formatting for effectively displaying observations has remained constant over time, it is important to note that the delivery has shifted into a way to share audit observations/findings in a real-time, value-added manner.

This page intentionally left blank.

ACTIVITY: DEVELOPING THE EXECUTIVE SUMMARY

Instructions

- Review the scenario.
- Develop an executive summary based on the scenario.
- Use one of the three observation/finding formats (paragraph, bullets, or table) when developing at least one audit observation/finding in your executive summary.
- Be prepared to share your results.

Audit Objective: Validate that access to network resources is appropriately granted and revoked in a timely manner based on the access management policy and procedures.

Audit Scope: The scope includes the employees that were transferred or terminated in the last four weeks before the date of the audit. The contractors were excluded from the scope of this audit.

Scenario: Auditing Active Directory Access

Your organization uses active directory to provide appropriate access to their systems based on job function. When a new associate or contractor is hired, he or she receives a user ID with access to the appropriate areas. When an associate is transferred, his or her access is adjusted as needed.

When an associate is terminated, his or her access is disabled or deleted. The procedure requires that access must be altered as employees terminated or disabled by the close of business on the day that the employee terminates.

During a review of active directory access for 55 employees who had been transferred or terminated during the audit period, it was found that 12 of the transferred employees' access were changed later than required, ranging from two to 23 days after transfer. In addition, accesses had not been disabled or deleted for five employees who were terminated within the last four weeks before the date of audit testing.

Audit Executive Summary

This page intentionally left blank.

ACTIVITY: BUILDING THE REPORT BODY DRAFT

Instructions

- Review the email from the manager of the activity under review, Nadine, in response to your socialized observation/finding draft.
- Using the observation/finding you developed in the previous activity, add the management's response and action plans to create the report body draft.
- Be prepared to share your results.

Scenario: Email from the Manager

Hello there internal audit team member,

Thank you for sharing your observations regarding the badge access audit.

Below you will see my responses to your observations and my proposed action plans.

Observation 1: It was found that 12 of the accesses were changed later than required, ranging from two to 23 days after transfer.
Risk Rating: Needs Improvement.
Response: Accept.
Action Plan: Review the transfer process to ensure that access is changed within the stated time frame, as documented in the organization's policy.

Observation 2: Accesses had not been changed for four employees who were terminated, ranging from two to four weeks before the date of testing.
Risk Rating: Needs Improvement.
Response: Accept.
Action Plan: Review the current process of communicating employee termination to ensure terminated employees' access is revoked. Review the termination process to ensure that access is changed within the stated time frame, as documented in the organization's policy.

Please let me know if you have any additional questions or concerns.

Looking forward to our time together at the closing conference!

Have a nice day,
Nadine

Audit Report Body Draft

This page intentionally left blank.

ACTIVITY: OBSERVATION/FINDING VETTING OR SUPERVISORY REVIEW

Instructions

- Conduct a mock observation vetting (or supervisory review):
  - Trade your executive summary and report body drafts with another participant.
  - Use the provided observation/finding vetting/supervisory review question checklist and guide to review your fellow participant's executive summary and report body drafts.
  - Provide them with feedback, as needed, to improve their drafts.
- After you trade your drafts back to their original author, review the feedback you were provided and make adjustments to your draft accordingly.
- Be prepared to share your results.

Observation Vetting or Supervisory Review Checklist

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

- ✓ Read the draft completely before making any comments regarding content.
- ✓ Balance any critical feedback with positive feedback and 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 un-actionable comments like "this does not make sense," "it's unclear," "avoid using…," or "it's vague."
- ✓ Include in your comments any questions that came to mind as you read the document.
- ✓ Keep your supervisory review process free of bias and fallacies. Do not criticize if you do not agree or fully understand because you do not have technical expertise in a particular area. A good process to consider when conducting observation/function 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 back to your teammate to ensure they are easy to follow, are free of bias, and are written in a mentioning, non-critical voice.

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 a 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?

Observation/Finding Vetting and Supervisory Review Notes

_____

_____

_____

_____

This page intentionally left blank.

UNIT SUMMARY

In this unit, we examined methods to develop and present audit results. We also discussed the purpose of, and how to develop, a memo or interim report.

This unit provided internal auditors with several activities to practice the skills associated with audit reporting structure and engage with other participants to conduct practice observation vetting and supervisory reviews of draft audit reports.

UNIT WRAP-UP

Key Takeaway:

Questions and Answers:

Action Plan:

COURSE SUMMARY

LEARNING OBJECTIVES

You have studied content based on the following learning objectives:

- Discuss the importance of delivering results that utilize business acumen disciplines.
- Explain how audit results impact an organization's business objectives and operating processes.
- Recognize the importance of critical thinking when developing and communicating audit results.
- Recognize the communication needs of audit report readers and writers.
- Review the components of the audit report.
- Explore various reporting methods and formats.

PLAN FOR ACTION

Review the topics that were discussed during the program. Select concepts and techniques you learned or ones that were reemphasized for you that will help you accomplish the challenges you face. Be specific as to how you will use the information you have learned.

What You Want to Change	Preliminary Action Steps to Accomplish	Results Expected for Success

WRAP-UP

Thank you for your participation!

Related Course Recommendations

- Critical Thinking — A Vital Auditing Competency.
- Root Cause Analysis for Enhancing Internal Audit Effectiveness.

APPENDIX: SAMPLE AUDIT REPORTS

APPENDIX: TABLE OF CONTENTS

Note: All example documents in this appendix have been submitted by volunteer IIA members. Identifying information has been redacted. Thank you to all who contributed submissions.

EXECUTIVE SUMMARY

Background

Introduce the reader to the area, department, process where the work was performed. (typically one paragraph or less in length).

Objectives

Between 3-5 objectives, which must be covered in the testing segment.

Scope

The selected period for the review.

Limitations

Issues that have prevented a full scope of the engagement.

Summary of Key Findings

Pay attention to the word **KEY**, not all. These are findings/observations of higher risk and/or matters that would concern management.

Risks Identified

Actual risks that emanated from the findings/observations that must be addressed in the shortest possible time by implementation of corrective action.

Engagement Opinion

An overall opinion based on elements of facts which surfaced during the engagement. An engagement opinion is not to be confused with a finding.

Rating

An overall risk rating of the report (if this is the culture of the organization). This must be based on the overall view of the audit team and discussed with the activity under review. Ratings should be keyed and color-coded, e.g.,

1-2 LOW

3-4 MEDIUM

5-6 HIGH

7-8 SEVERE

OBSERVATIONS/FINDINGS AND RECOMMENDATIONS

A. Findings of Satisfactory Performance

As outlined in the Global Internal Audit Standards.

B. Findings Requiring Corrective Action

For each finding: Two short paragraphs of two sentences each:

- Paragraph 1. Condition (1 sentence) and Criteria (1 sentence).
- Paragraph 2. Cause (1 sentence) and Consequence (1 sentence).

Corrective Action – One or two sentences of the final decision between the internal audit function and activity under review for risk reduction.

Action Plan – This is included in the report as an appendix with dates for each implementation. This would be used to conduct Follow-Up audits (Monitoring).

INTERNAL AUDIT DEPARTMENT

AUDIT REPORT RATINGS, COMMENT PRIORITIES & CATEGORIES

Audit Report Ratings

Audit ratings have been developed for the purpose of indicating the overall level of performance, from an internal audit perspective, for the function audited. The ratings relate to internal operations, administrative and financial controls, and auditee performance relative to plan/policy/procedures in each function audited and are based on established guidelines. The ratings do not address the issue of profitability.

The ratings are used to accomplish the following objectives:

- Provide management with an indication of the relative competence with which functions covered by the audit were performed.
- Measure any change in performance of the functions since the previous audit.
- Provide incentive to area management to improve their operations.
- Help to determine the frequency and extent of audit coverage which should be provided in the future.

The rating criteria is intended to be used as a set of guidelines to lend to conformity, not as inflexible rules which must be interpreted literally as such interpretations may not always give appropriate consideration to all relevant factors. The Auditor's judgment is an essential ingredient of the ratings and should take precedence over a literal interpretation of the guidelines.

Some examples of conditions which relate to each of the rating classifications are presented in the *Audit Ratings - Examples* List. Note that these conditions are examples and do not address every condition which can exist. Also note that all conditions do not have to exist in order to generate a particular rating. One condition can be the reason for the rating issued. The possible ratings are Excellent, Good, Satisfactory, Needs Improvement and Unsatisfactory. An "Unsatisfactory" rating would require a targeted follow-up review within six months to determine if significant progress had been made toward correction of problems and implementation of audit recommendations.

Additional factors or conditions which should be considered in determining an audit report rating are:

- An increase in the number of report comments can result in a decline in the rating issued from audit to audit. The scope of the audit and nature of the comments should be taken into consideration.
- Generally, the more high priority comments that are included in the report, the lower the rating will be. Likewise, an increase in the number of audit report comments from year-to-year will usually have a negative impact on the audit report rating. The mix of high and moderate priority ratings will be taken into consideration.
- An excessive number of low priority or exit conference comments, which individually may not be included in the audit report, can negatively impact the audit report ratings. If such a situation exists, an audit report comment will be included to highlight and explain the nature of the excessive low priority or exit conference comments.

- Repeat audit report comments can cause ratings to decline and fall into the needs improvement or unsatisfactory category.

- If the overall performance of one department, area, or aspect of the audit varies significantly from all others, it may be necessary to issue multiple ratings.

The audit report language, recommendations, opinions, and conclusions should be consistent with the rating(s) issued.

Audit Comment Priorities

Audit comments will be assigned a priority rating to assist management and the audit committee in directing resources and monitoring resolution of the comments. The assigned priorities, *High*, *Moderate*, or *Low*, are determined from an internal audit perspective and do not correspond directly to criteria relating to materiality for the financial statements or classification of deficiencies for Sarbanes-Oxley (404) internal control considerations. In order to promote operational efficiencies and encourage above average performance within the company, more stringent standards are applied to an internal audit perspective for assigning priorities. The internal auditor's judgment is an essential ingredient of the priority rating and will take precedence over any literal interpretation of the guidelines. See the *IAD Audit Comments – Priority Ratings Guidelines* for examples of the considerations for determining a priority rating.

All high and moderate rated audit report comments that are not corrected or resolved prior to the next regularly scheduled Audit Committee meeting will be tracked as a pending item and the status of resolution reported to the Audit Committee until resolved. Comments or observations included in audit reports that are "potential improvement opportunities" will not be considered pending items or included on the Audit Committee Pending Items Report. Such comments and observations are included as a service to management and do not represent issues or problems requiring Audit Committee attention.

IAD Audit Comments – Priority Ratings Guidelines

PRIORITY	CONDITION
High	**Management should initiate immediate action to address the comment.** 1 Major internal control weakness 2 Major policy or procedure exceptions 3 Significant risk exposure 4 Major financial exceptions – loss, misstatement, errors, fraud 5 Significant law or regulatory violations 6 Significant potential opportunity – revenue, savings, efficiencies, improvements
Moderate	**Management should initiate timely action to address the comment.** 1 Substantial internal control weakness 2 Substantial policy or procedure exceptions 3 Substantial risk exposure 4 Substantial financial exceptions – loss, misstatement, errors, fraud 5 Substantial law or regulatory violations 6 Substantial potential opportunity – revenue, savings, efficiencies, improvements
Low	**Management should initiate reasonable action to incorporate a plan to address the comment in the normal course of business.**

1 Minor internal control weakness
2 Minor policy or procedure exceptions
3 Limited risk exposure
4 Minor financial exceptions – loss, misstatement, errors, fraud
5 Minor law or regulatory violations
6 Limited potential opportunity – revenue, savings, efficiencies, improvements

---

Audit Comment Categories

Audit comments will be categorized as to the nature or type of comment. The categories include: law & regulatory violations, policy & procedure exceptions, internal control weaknesses, documentation exceptions, financial exceptions, written procedure (lack of or outdated), and miscellaneous. Technical exceptions and normal or expected levels of errors, especially related to law & regulatory violations, policy & procedure exceptions and documentation exceptions that are minor in nature will usually not be included as audit report comments. An audit report comment in one of these categories will usually involve systemic issues, excessive occurrences or serious problems that warrant inclusion in the audit report. The following comments summarize the general nature of comments that will fall into each category:

- Law & regulatory violations – relates to violations of FDIC, FRB, KOFI, SEC or other applicable regulations that govern activities of THE COMPANY. Report comments relate to substantial problems, issues or violations and do not include technical violations or expected levels of errors that occur in the normal course of business.

- Policy & procedure exceptions – relates to systemic issues, major or substantial deviations from policy or procedure or excessive occurrences or exception levels. Report comments will not normally include technical violations or expected levels of errors that occur in the normal course of business.

- Internal control weaknesses – relates to identified weaknesses and uncontrolled risk exposures that could potentially create unacceptable levels of errors, losses, reputation risk, contingent liabilities or lead to other major problems for THE COMPANY.

- Documentation exceptions – relates to failures to develop, maintain or retain appropriate documentation to support compliance with laws, regulations, contracts, policies, procedures or internal control requirements of THE COMPANY. Report comments relate to substantial problems, issues or violations and do not include technical violations or expected levels of errors that occur in the normal course of business.

- Financial exceptions – relates to accounting errors, operational losses, unnecessary or excessive expenses, lost revenue, unrecorded assets or liabilities, un-balanced or out-of-balance accounts and other financial matters affecting THE COMPANY's financial statements or condition. Typically such comments involve actual or potential losses to the organization.

- Written procedures – relates to lack of or outdated written procedures requiring substantial effort to develop or correct.

- Miscellaneous – relates to all other comments not categorized into one of the areas described above.

Potential Improvement Opportunities

Internal audit reports may also include observations and comments related to potential improvement opportunities for management's consideration. Such comments are not considered to be issues or problems from an internal audit perspective and will not impact audit report ratings. These items will not be included or tracked as pending items.

Audit Ratings – Examples List

RATING	CONDITION
Excellent	**Overall performance exceeds the expected level.** 1) No report comments combined with very few technical exceptions or exit conference memo exceptions. 2) Comments in report require no response and relate to suggestions for improving efficiency, as opposed to improving internal controls.
Good	**Overall performance meets the expected level.** 1) Few moderate priority report comments which are minor In nature. 2) One, or possibly two, high priority comments which were corrected during the audit and which did not create a liability or loss to the client. 3) Relatively few technical exceptions and exit conference memo comments which are easily corrected in a short period of time, combined with only a few moderate priority report comments.
Satisfactory	**Overall performance does not consistently meet the expected level.** 1) Several moderate priority report comments. 2) Average number of technical exceptions and exit Conference memo comments. 3) Combination of #1 and #2. 4) Two or more high priority report comments. 5) Report comments which require routine efforts (reorganization, time or resources) to correct in the normal course of business. 6) Report comments which were disclosed by an exit conference memo during the previous audit.
Needs Improvement	**Overall performance is weak and frequently falls below expected levels.** 1) Numerous moderate priority report comments. 2) Three or more high priority report comments. 3) Combination of #1 and #2. 4) Above average number of technical exceptions or exit conference memo comments combined with several report comments. 5) Internal control weaknesses that create above average exposures. 6) Report comments which require substantial effort (reorganization, time or resources) to correct. 7) Internal control weaknesses or other conditions which created unnecessary losses or liabilities for the client. 8) Repeat audit report comments.

Unsatisfactory	**Overall performance is unacceptable.** 1) Excessive number of report comments. 2) Several major report comments. 3) Unacceptable number of technical exceptions and/or exit conference memo comments. 4) Unresolved report comments. 5) Unreasonable deadlines for correction of report comments. 6) Previously reported, unresolved report comments. 7) Significant violations of law, regulations, or established policies. 8) Internal control weaknesses or other conditions which created unnecessary losses or liabilities for the client, if the loss or liability is significant. 9) Significant findings such as fraud, embezzlement, or misappropriation of funds which occurred as a result of failure to maintain proper controls or follow established policies and procedures.

Sample Bank

Accounting Department
Internal Audit – 20xx

Sample Bank
Accounting Department
Internal Audit – 20xx

March 17, 20xx

To the Audit Committee of the Board of Directors
Sample Company:

We have completed our internal audit of the Accounting Department of Sample Bank ("Bank") as of January 31, 20xx Our report includes background information, an executive summary, audit objectives, audit scope, and audit findings/recommendations.

To assist you in analyzing our findings/recommendations, we have provided our suggestions for corrective action based on the finding's exposure (impact and likelihood of occurrence) to loss, as follows:

High-----Impact-----Low	5	4	3	2	1
1	**M**	**M**	**H**	**H**	**H**
2	**M**	**M**	**H**	**H**	**H**
3	**L**	**L**	**M**	**H**	**H**
4	**L**	**L**	**L**	**M**	**M**
5	**L**	**L**	**L**	**M**	**M**

Low----------Likelihood----------High

High (H) - Management should quickly remedy the situation to prevent significant risk of loss.

Moderate (M) - Timely remedy by management is suggested.

Low (L) - Does not appear to represent an immediate risk but improvements are still possible.

Best Practice Recommendation (BP) – An observation to improve operational effectiveness or efficiency.

We would like to express our appreciation to the management of the Accounting Department for their cooperation throughout our audit.

Very truly yours,

Mary Smith

Mary Smith
General Auditor

Sample Bank
Accounting Department
Internal Audit – 20xx

Table of Contents

Sample Bank
Accounting Department
Internal Audit – 20xx

Background

Internal Audit has conducted an audit of the Accounting Department of Sample Bank ("Bank"). The Accounting Department's processes include such accounting functions as account reconciliation, financial reporting, management reporting, security portfolio, and tax planning. Details of testing and procedures performed are included in the audit scope below.

Executive Summary

There are three findings reported, of which two are repeated from the prior audit, as follows:

		Relative Importance
1.	Several accounts contain stale-dated reconciling items. ***(Repeat Finding)***	High
2.	Suspense accounts were not being validated. ***(Partial Repeat Finding)***	Moderate
3.	The supply inventory accounts have not been reconciled.	Low

The internal control environment has remained stable since the prior internal audit. Management should quickly address the stale-dated reconciling items to reduce the possibility of future loss.

Audit Objectives

Our audit objectives were:

To determine the system of internal controls were operating adequately, effectively and efficiently.

To determine procedures were in place to identify and correct differences in applicable general ledger and in-house demand deposit accounts.

To verify operating procedures related the company's portfolio securities were effective.

To ensure regulatory reports were accurately prepared.

Sample Bank
Accounting Department
Internal Audit – 20xx

Audit Scope

We performed the following tests and procedures:

- Reviewed the system of internal controls (operational, financial reporting and compliance) by interacting with management throughout the business process to evaluate objectives, risks, and the appropriate level of control. Performed tests, where appropriate, to determine if established controls were in place and functioning effectively.
- Identified all general ledger and in-house deposit accounts relating to the business process and ensured a reconcilement was prepared and approved in a timely manner. For all suspense accounts and other accounts with balances of $25,000 or more, performed the following:
    - ensured mathematical accuracy and completeness;
    - verified subsidiary and general ledger totals; and
    - determined reconciling items were adequately described and traced selected items (selection based on dollar amount, stale date or unusual nature) to determine validity and proper/ timely clearance.
- Tested the company's procedures to agree portfolio securities to safekeeping list(s).
- Selected portfolio securities and recalculated accruals, accretion and amortization.
- Verified a sample of portfolio security purchases and sales.
- Obtained the company's most recent Regulatory Report and tested a sample of items to ensure accuracy.
- Reviewed and tested procedures related to income tax planning and preparation.
- Determined the current status of prior audit recommendations.

Sample Bank
Accounting Department
Internal Audit – 20xx

Audit Findings and Recommendations

Finding #1: Several Accounts Contain Stale-Dated Reconciling Items
Relative Importance: High
Repeat Finding

Reconciling items for due from accounts should normally clear within thirty days and, for suspense accounts, items should generally clear within five days. In rare instances, due from reconciling items may take longer to clear, but always within six months. Several accounts as of 1/31/00 contained stale-dated reconciling items. Management was aware of the level of stale dated items and had already begun the process to clear them. We noted the following:

- The General Due From account contained five stale (over six months old) items, and one of these items is a "we debit" for $500,000. The $500,000 relates to a matured Treasury note that was pledged as collateral, but the Trustee will not release the proceeds to Company without written consent of The Court. The Company has tried numerous times to contact the Court and has been unsuccessful.
- The Special Due From account contained four stale (over six months old) items.
- The In Process account contained thirty-two items greater than five days old.
- The Checking Account contained four stale items (over six months old).
- The Interdepartmental Transfers account contained forty-one items greater than five days old.
- The Special In Process account contained forty debits totaling $4,078,321, and thirty-six credits totaling $4,591,059 over thirty days old.

Unless due from and suspense account reconciling items are cleared in a timely manner, unnecessary losses may occur. In addition, the longer items are outstanding, the more difficult and time consuming they are to clear.

Recommendation

Although management reported that, as of 2/28/00, the level of stale items had been significantly reduced, we recommend management continue to allocate the necessary resources to clear and/or charge-off stale reconciling items in all affected accounts. In addition, we recommend management follow its policy to charge off stale (over six months old) due from reconciling items.

Management Action Plan

The Accounting Department has allocated the necessary resources to follow up and clear all unreconciled items. The outstanding item for $500,000.00 on the General Due From account was cleared on 2/15/00. Management was aware of and had begun taking corrective action on this finding prior to the audit. Management will follow its policy to charge-off stale reconciling items over six months old.

Individual(s) Responsible: John Doe, Accounting Manager

Completion Date: Completed

Finding #2: Suspense Accounts Were Not Being Validated
Relative Importance: Moderate
Partial Repeat Finding

Suspense accounts, by their nature, have increased risk of fraudulent or erroneous activity since the outstanding items are not reconciled to a control total. Therefore, periodic validation is necessary to reduce the risk of loss.

In the prior two audits, we noted the Accounting Department reconciles and follows outstanding items in several suspense accounts (interdepartmental transfers, cash suspense, in-process, special in-process); however, no periodic validation of outstanding items was performed. As a result of the prior recommendations, a procedure to validate all items each month was initiated, but was discontinued due to turnover in the department.

Unless suspense accounts are periodically validated, losses may occur due to error or intent.

Recommendation

We again recommend management periodically validate all or a sample of outstanding items in suspense accounts. This validation could be performed quarterly or semi-annually to reduce the workload.

Management Action Plan

The Accounting Department has allocated the necessary resources to perform periodic validations in the suspense accounts. Management will validate all or a sample of outstanding items in suspense accounts on a semi-annual basis.

Individual(s) Responsible: John Doe, Accounting Manager

Completion Date: Completed

Finding #3: The Supply Inventory Accounts Have Not Been Reconciled
Relative Importance: Low

The supply inventory accounts (an asset account and a contra-asset account) are used to track current supplies on hand. These accounts net to zero each month, since supplies are expensed when purchased. Due to a system deficiency, the supply inventory accounts have not been reconciled. Therefore, the balances in these accounts may not accurately reflect the current supplies on hand. Without proper periodic reconcilements, errors and/or inappropriate activity may occur and remain undetected.

Recommendation

We recommend management ensure proper periodic reconcilements are prepared for the supply inventory accounts.

Management Action Plan

We determined that the purchasing software had a corrupted file that was causing a malfunction making reconcilement impossible. The file has been fixed and the purchasing department is currently re-keying all prior data. When this process is completed, a physical inventory will be taken and the general ledger will be adjusted accordingly. A monthly reconcilement of the supply inventory and contra accounts will be prepared thereafter.

Individual(s) Responsible: Jane Smith, Facilities & Purchasing Officer

Completion Date: April 30, 20xx

Audit of Enterprise Risk Management

1.0 Introduction

Risk management is an explicit and systematic approach to identify, assess and address risks associated with objectives. It facilitates the sharing of risk information, which enhances informed decision-making and improved planning. As such, risk management increases organizational resilience by improving predictability in achieving outcomes, protecting corporate assets and maintaining stakeholder trust. Enterprise Risk Management (ERM) promotes a continuous, proactive and systematic process to understand, manage and communicate risk information from an organization-wide perspective.

Core risk management principles are articulated in the Treasury Board Secretariat (TBS) 2010 *Framework for the Management of Risk* (*TBS Framework*). Accompanied by the TBS *Guide to Integrated Risk Management* (*TBS Guide*), the *TBS Framework* guides deputy heads on the implementation of effective risk management practices at all levels of their organization.

The [redacted] ERM Policy designates the Chief Risk Officer as the process owner for the risk management self-assessment function and for providing assurance that the organization is operating effectively from a risk perspective. The Chief Risk Officer is responsible for ensuring that the *TBS Framework* and *Guide* are reflected in the [redacted]'s policies, guidance, and tools.

The Enterprise Risk Management and Transformation Initiatives Division (ERMTID) in the Corporate Affairs Branch supports the Chief Risk Officer through the development and implementation of the ERM Framework, which includes risk-related policy, processes, tools, resources, services and training. The Division provides horizontal support and leadership for risk management to all branches and programs on risk-related matters. Vice-presidents and direct reports to the President are ultimately accountable for managing risks

2.0 Significance of the Audit

Risk management makes a significant contribution to strengthening the departmental capacity to recognize, understand, accommodate and capitalize on new challenges and opportunities. It prepares an organization to respond to change and uncertainty, contributes to improved decision making and better allocation of resources. Risk management is recognized as a core element of effective public administration.

With the current fiscal environment of deficit reduction and limited resources, key decisions and resource allocation rely on effective risk management and analysis. Risk management enables organizations to respond proactively to change and uncertainty by using risk-based approaches and information to enable more effective decision-making.

The audit is timely as changes are being made to the Management Accountability Framework (MAF). MAF 2014–2015 has a new core area of management: Management of Integrated Risk, Planning and Performance. Its objective is to strengthen integration and alignment of planning in departments and agencies. It is also responding to a need for coordinated and consistent TBS-wide guidance on planning and risk management, and better alignment between integrated risk management, planning and performance functions within departments and agencies.

The audit objective was to provide assurance that the Agency's ERM Framework is in place,that key Agency risks are identified, assessed and managed effectively for achieving its objectives, and that risk information is integrated into planning and decision making. The audit scope covered the ERM control framework and processes at both the corporate level and within selected branches and programs, in addition to how information was utilized for integrated business planning and decision making.

Given the [redacted]'s mandate of providing integrated border services that support national security and public safety priorities and facilitating the free flow of persons and goods, operational risk management activities occur on a daily basis. The audit did not examine activities supporting operational risk management, such as the targeting and intelligence programs. The audit focused on the process for developing the Enterprise Risk Profile (ERP), which is part of the risk management process and control framework. Observations are based on the 2013 ERP, which was the most recent version at the time of the audit.

Further details of the audit scope and criteria can be found in Appendix A.

3.0 Statement of Conformance

The audit conforms to the *Internal Auditing Standards for the Government of Canada*, as supported by the results of the quality assurance and improvement program. The audit approach and methodology followed the *International Standards for the Professional Practice of Internal Auditing* as defined by the Institute of Internal Auditors and the *Internal Auditing Standards for the Government of Canada*, as required by the Treasury Board's *Policy on Internal Audit*.

4.0 Audit Opinion

The Agency's ERM Framework is aligned with the key principles of the *TBS Framework* and *Guide* to identify, assess and manage risks. Opportunities for improvement relate to reviewing the [redacted] Framework to continuously mature risk management practices. The Agency is identifying, assessing, mitigating and monitoring its risks at the corporate level with the consistent application of the [redacted] ERM Policy and associated guidance. Opportunity exists to further strengthen risk management practices below the corporate level by developing mitigation strategies for identified risks. Regular monitoring of risks, risk drivers, and the mitigation plans at all levels of the Agency would ensure that changes affecting the Agency's environment are identified in a timely manner. A process has been defined for integrating risk information into planning and decision making.

This translates to a medium risk exposure to the Agency.

5.0 Key Findings

The Agency's risk management approach and process have been well defined and documented in the CBSA ERM Policy, Framework and Handbook, which are communicated across the organization. Together, these documents describe an ERM program that is generally in line with TBS principles for risk management. Exceptions noted relate to the absence of periodically reviewing the Agency Framework and defining risk tolerance.

An analysis of the 2013 Enterprise Risk Profile and associated Branch and Program Risk Profiles indicated that significant risks are identified and assessed, and respect the process defined in the [redacted] ERM Handbook. Risk mitigation plans were developed and documented for the corporate risks, and identified appropriate risk sponsors and mitigating activities to address enterprise risks. Opportunity exists to further strengthen risk management practices below the corporate level, by developing mitigation strategies for identified risks.

Corporate level risks were being monitored annually; however, risks identified below the corporate level were not monitored as required by the [redacted] ERM process. Regular monitoring of risks, risk drivers, and risk mitigation strategies at all levels of the organization would allow the Agency to identify changes affecting its environment in a timely manner.

The audit also noted that corporate risk information was generally integrated in corporate planning documents and integrated business plans (IBP). The IBP integrated business planning process is currently being revised to further integrate risk information. Corporate risk management practices are also regularly monitored by governance bodies within the Agency.

At the [redacted], risk is managed on a daily basis at the operational level. While ERM practices continue to mature, without a more structured and integrated approach to risk management below the corporate level, the Agency cannot be assured that the identified risks are being properly managed, reduced or eliminated.

6.0 Summary of Recommendations

The audit makes two recommendations relating to:

- periodically reviewing the [redacted] ERM Framework and program to identify and address gaps and opportunities for improvement;
- ensuring that formal mitigation plans at below the corporate level are developed implemented and monitored.

7.0 Management Response

The Corporate Affairs Branch agrees with the recommendations of the Audit of Enterprise Risk Management. The principal means by which the Branch will respond to the audit recommendations is through a comprehensive review and update of the ERM Framework, including the ERM Policy and related tools, and through the further integration of risk management within the business planning and performance measurement processes.

In that context, the Branch has already taken steps to begin to improve and mature the ERM Program, and will continue to work in collaboration with key stakeholders across all branches to complete this work. The Branch is also working on establishing contacts with counterparts in other government departments and in [redacted] and [redacted] customs and immigration administrations, to explore opportunities to share best practices with key partners. This consultative approach will inform the new strategic direction for moving the ERM Program forward. The Branch will implement its action plan by the end of July 2015.

8.0 Audit Findings

8.1 Risk Management Framework

Audit Criteria:

- The [redacted]'s risk management framework and processes are documented, complete and communicated across the Agency.

8.1.1 TBS Risk Management Framework and Guide

The TBS *Framework for the Management of Risk* (*TBS Framework*) is a key policy instrument that outlines a principles-based approach to risk management for all departments and agencies. The Framework describes Deputy Heads' responsibility in the effective management of their organizations in all areas of work and at all levels of their organization, including risk management and describes the expectations for an effective risk management practice. It is supported by the TBS *Guide to Integrated Risk Management* (*TBS Guide*) which outlines practical guidance and considerations for operationalizing these principles. The principles represent the minimum requirements and encourage departments to focus on areas that will assist them in progressing towards a cohesive and consistent approach to risk-informed decision-making. The *TBS Framework* does not provide specific requirements to integrated risk management to departments as their mandate, risk exposure, and management capacity vary.

The *TBS Guide* further outlines a framework and process for risk management that includes risk management principles, framework elements, and process steps such as ongoing communication, risk assessment and risk treatment, and monitoring and review.

8.1.2 The Agency's ERM Framework is aligned with TBS Framework

The Agency has documented its approach to risk management in the [redacted] ERM Policy; the CBSA ERM Framework – Process and Tools; and the [redacted] Risk Management (RM)Handbook.

Our review of the [redacted] ERM Framework, Policy and Handbook found that the Agency has a fully documented risk management framework and process. The risk management framework and process are modelled after the *TBS Framework* and *Guide*, and capture most of the key elements, including a:

- demonstrated mandate and commitment to ERM through a defined and endorsed ERM Policy, and assigned roles and responsibilities for risk management consistent with TBS guidance;
- framework design that is generally aligned with TBS guidance (i.e. an understanding of the Agency and its environment, an established ERM Policy, integration into organizational processes such as planning, and resources allocated to ERM); and
- risk management process that has been designed to include all of the key activities outlined by TBS (i.e., process activities such as communication and consultation, establishing the context, the risk assessment process, risk treatment processes, and guidance for monitoring and reviewing identified risks and mitigation strategies).

However, the [redacted] ERM Framework did not include the following elements from the TBS guidance:

- ongoing monitoring and continuous improvement of the ERM Framework, and
- risk tolerance definition and guidance.

Ongoing Monitoring and Continuous Improvement of the ERM Framework

Continuous improvement of the culture, capacity and capability of risk management encourages organizations to continually monitor, review and improve their risk management approach and processes to ensure their effectiveness, efficiency and relevance in supporting the organization's overall performance.

An Integrated Risk Management Framework was approved by the Executive Committee in November 2008, and was replaced by a new ERM Policy, including the process and tools, in August 2010. In addition, an ERM Strategic Plan was developed which included two main objectives as well as performance indicators in 2010. Since the development of the ERM Policy and the ERM Strategic Plan, ongoing monitoring of the [redacted]'s ERM Framework by ERMTID has not been implemented. Monitoring and reporting against the performance indicators, as envisioned in the ERM Strategic Plan, did not take place. An update and assessment against performance indicators was prepared at the time of the audit. Without regular review of the Agency's risk management framework, risk management practices may not sufficiently evolve to address the Agency's needs at all levels of the organization.

Risk Tolerance Definition and Guidance

The TBS Framework defines risk tolerance as "the willingness of an organization to accept or reject a given level of residual risk (exposure). Risk tolerance may differ across the organization, but must be clearly understood by the individuals making risk-related decisions on a given issue. Clarity on risk tolerance at all levels of the organization is necessary to support risk-informed decision making and foster risk-informed approaches". Although not a specific requirement, TBS suggests that guidance be provided on setting risk tolerance levels for identified risks.

Existing risk documentation did not include processes and guidance around establishing risk tolerances for identified risks.

Management indicated that risk tolerance was expressed in the Agency through management's response to identified risks (i.e., accept and watch or mitigated) and that it was difficult to define and set Agency tolerance level.

Defining risk tolerance and developing a methodology for expressing tolerance levels would strengthen integrated risk management practices in the Agency. This, in turn, would facilitate risk-informed decision-making in regards to the acceptance of risk, senior management engagement when tolerance levels are exceeded, and the prioritization of resources related to risk mitigation and business planning.

Recommendation 1:

The Vice-President of the Corporate Affairs Branch should periodically review the [redacted] ERM Framework and program in order to identify and address gaps and opportunities for improvement to further mature Agency risk management practices.

Management Action Plan	Completion date
The Corporate Affairs Branch agrees with this recommendation. The Branch is currently in the process of undertaking a formal review of the [redacted] ERM Policy, the RM Handbook, the ERP document and the ERP process to identify gaps and make the necessary changes to reflect the improvements that will mature the Agency's ERM program. In updating the current ERM Policy, the Branch will commit to conducting a review of the ERM Framework and Program	July 20xx

8.2 Risk Management Practices

Audit Criteria:

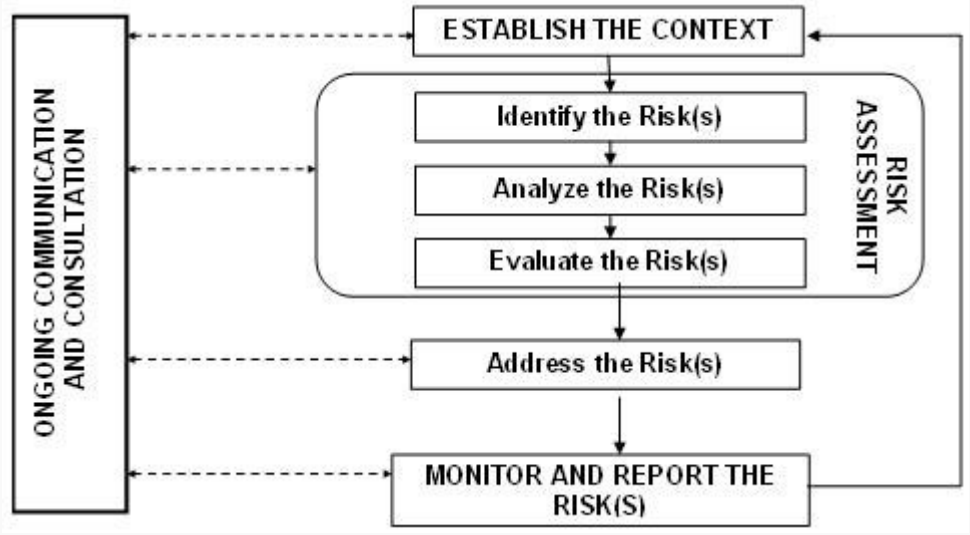
- Management identifies and assesses significant risks that may preclude the achievement of its objectives.
- Management identifies and assesses the existing controls that are in place to manage its risks.
- Management formally responds to its risks, and communicates both risks and risk management strategies to appropriate stakeholders across the organization enabling the Agency to carry out its responsibilities.
- Risk information is integrated in and used for planning and decision-making purposes.
- Risk management practices are regularly monitored by oversight bodies within the Agency.

8.2.1 Background

As outlined in the ERM Framework and the ERM Policy, the [redacted]'s risk management process contains the following elements, and outlined in Figure 1 below:

- 1. Establishing the risk context
- 2. Risk assessment
  - Identify and analyze risks
  - Identify and analyze the controls
  - Evaluate the risks
- 3. Addressing risks
- 4. Monitoring, reporting, and re-evaluating risks; and
- 5. Ongoing communication and consultation regarding risks

Figure 1: The [redacted]'s Enterprise Risk Management Process



- 1.0 The [redacted]'s Enterprise Risk Management Process
  - 1.1. Establishing the risk context
  - 1.2. Risk assessment
    - 1.2.1. Identify and analyze risks
    - 1.2.2. Identify and analyze the controls
    - 1.2.3. Evaluate the risks
  - 1.3. Addressing risks
  - 1.4. Monitoring, reporting, and re-evaluating risks; and
  - 1.5. Ongoing communication and consultation throughout the process.

[redacted] facilitated risk assessment exercises below the corporate level, at the various Branch Management Teams (BMT) and Program Management Tables (PMT). The facilitated risk assessment exercise included conducting interviews with BMT and PMT members, creating and validating the BMT/PMT risk inventories, assessing the risks identified, and the creating and validating of the BMT/PMT risk profile. These risk profiles provide input into the corporate risk identification, which in turn is presented to vice-presidents and

members of the Executive Committee. The ERP 2013 also considered additional information sources, such as the [redacted] Environmental Scan, the [redacted] Risk Assessment, the [redacted] Plan, the [redacted] Risk Profile, and the Agency Performance Summaries, among others.

Even though [redacted] facilitates the risk identification process, the Vice-Presidents are ultimately accountable for managing risks for their areas of responsibility.

8.2.2 Establishing the Context

The purpose of establishing the context of risk management activities is to define the scope of the risk identification exercise, key stakeholders, and operating environment. Furthermore, this allows an organization to identify and gather information regarding facts and trends impacting its operating environment that may create risks to meeting its objectives. The audit found that the sampled risk profiles provided a detailed background and context of the Branch/Program/Area being assessed.

8.2.3 Risk Identification and Analysis

The [redacted] ERM Handbook outlines the process to identify and assess significant risks. The audit found that the identification and assessment of significant risks that may preclude the achievement of objectives was completed through the Branch and PMT Risk Profiles as well as the ERP 20xx. These risk identification and assessment documents followed the process outlined in the ERM Handbook. Risks were identified, documented and assessed, and associated with the achievement of one or more business objectives, and also included considerations related to fraud.

The audit selected four out of thirteen Branch/PMT Risk Profiles and the 20xx ERP to determine whether identified risks included the expected attributes, such as the following:

- both internal and external sources and/or risk drivers are considered;
- potential consequences are considered;
- identified risks are relevant to the branch/program/area;
- the achievement of one or more specific objectives is considered;
- identified risks are assessed using the Agency's published scales for impact, likelihood and trends; and
- the residual risk as final risk exposure assessment is considered.

The selected Branch/PMT Risk Profiles and the ERP were aligned with the [redacted] guidance in terms of the approach and methodology used in the risk assessment process. For example, in the sample selected, the risk statements were consistent and used similar language; internal and external sources of drivers of risk were taken into consideration; and potential consequences were considered for each risk.

The ERP risks are identified by [redacted] from various information sources, such as the Branch and PMT Risk Profiles, the [redacted] Plan, the [redacted] Risk Assessment, the [redacted] Environmental Scan, and the [redacted] Risk Profile. The ERMTID did not have a formal process or documentation, such as a central risk register to indicate how and to what extent the Agency's various sources were considered in developing the ERP. The audit reviewed the process and roll-up of information from these sources to determine whether significant risks were captured in the Agency's ERP.

[redacted] facilitated the risk assessment exercise for the branch and PMT risk profiles, which included key branch and PMT personnel. Through discussions with the directors general, directors and regional directors, risks were identified and subsequently validated through voting.

Overall, risks are being identified, analyzed and assessed across the Agency with the consistent application of the [redacted] ERM Policy and associated guidance.

8.2.4 Risk Evaluation

The [redacted] ERM Handbook requires that once risks have been identified and assessed, controls in place are to be identified and analyzed. The effectiveness of the controls is assessed against the five-point Control Effectiveness Evaluation Scale and Matrix provided in the ERM Handbook. Additional guidance to the management team undertaking controls self-assessment is provided in the [redacted] Management Control Framework.

The risk profiles included in our sample identified the relevant controls whose effectiveness was self-assessed using the appropriate [redacted] guidance. When requested, documentation to substantiate the assessment of control effectiveness was not provided for our review. Documenting the process of how controls are identified and assessed for effectiveness would further mature the control assessment step within the risk assessment process at the branch/PMT level.

Following the results of the controls assessment, risks were evaluated on likelihood and impact. For the 20xx ERP cycle, Executive Committee members evaluated the enterprise risks by voting on the exposure from a likelihood and impact perspective. Following the voting, risk sponsors and risk responses were identified for each risk.

The audit concluded that the risk evaluation step of the ERM process was completed and followed Agency guidance.

8.2.5 Addressing Risks

The [redacted] ERM Policy requires the development of mitigating strategies/plans by management to prioritize the risks when it is not feasible to address all risks. Once risks have been identified, and control effectiveness evaluated and risk responses have been determined (e.g., mitigate, accept and watch), mitigation plans are required for risks whose response is identified as 'mitigate'.

For ERP 20xx, risk mitigation plans were developed and documented, and identified appropriate risk sponsors and mitigating activities to address the risks as per the [redacted] process guidance. Of the 20 key corporate risks identified, the 'mitigate' risk response was identified for 13 risks. Our analysis of the risk response strategies provided in the Annex B of the ERP 20xx indicated that the mitigation strategies were identified and documented.

Below the corporate level, the [redacted] ERM process requires assigned risk sponsors to develop risk response strategies for the risks where the risk response was identified as 'mitigate'. For the four risk profiles selected, risk sponsors were identified. However, documented risk mitigation strategies did not exist, unless the risk was rolled-up into the ERP and mitigated through the ERP mitigation plan by default. It was found that [redacted] does not request or receive copies of the mitigation plans below the corporate level.

Without a more structured and integrated approach to risk management below the corporate level, the Agency cannot be assured that the identified risks are being properly managed, reduced or eliminated.

8.2.6 Integration of risk into planning and decision-making

Once risks have been identified, assessed and addressed, the risk management process should be integrated within planning and decision-making. By including risk information into decision-making, resource allocation and prioritization, the Agency can allocate its resources, both financial and non-financial, more effectively and efficiently.

At the corporate level, one form of integration of risk information into planning was identified in the Report on Plans and Priorities (RPP) and Departmental Performance Report (DPR). The audit reviewed the RPP 20xx–20xx, RPP 20xx–20xx and DPR 20xx–20xx and found that ERP risk information had been incorporated into these planning documents and was linked to priorities.

At the branch level, detailed guidance was developed on integrated business planning that includes templates on how risk information is to be integrated into planning and decision-making. Although some ERP risk information was included in the integrated business plans reviewed, the level of detail related to risk was inconsistent. While the plans were primarily based on core activities and/or key branch commitments, it was not evident how risk was considered in the final decision to allocate resources.

Further integrating risk into the planning process would allow the Agency to make more informed decisions around resource prioritization and allocation. [redacted] has indicated that the integrated business planning process was being revised for fiscal year 20xx–20xx.

8.2.7 Monitoring and Oversight

Monitoring, reporting, and re-evaluating risks

The [redacted] ERM Policy defines risk monitoring as the process of monitoring risks and associated mitigation/action plans to ensure that risk exposure levels remain within acceptable ranges. As such, risk monitoring is expected to occur at all levels within the Agency.

At the corporate level, the Director, [redacted], is responsible for developing and implementing a monitoring and performance measurement process to monitor Agency risks and corporate response strategies. The audit found that ERP risks and risk mitigation strategies are monitored by ERMTID on an annual basis through the development of the ERP (which is completed every two years) and through the ERP status updates (which are conducted in the interim years). The ERP Status Update prepared in even-numbered years provides information on changes to the Agency's risk environment and on progress made in these mitigation efforts. To some degree, risk responses identified as part of the ERP are monitored by [redacted] through these ERP Status Updates. As part of this process, risk sponsors are consulted and various corporate documents (e.g. Environmental Scan) are reviewed. The updated risks are then presented to and validated by the vice-presidents. The implementation status of the planned mitigation activities is self-reported by the risk sponsors. With the exception of the ERP and ERP Status Update, no further monitoring of ERP risks and associated mitigations strategies is being conducted by [redacted] at the corporate level. During the course of the audit, [redacted] indicated that ERP monitoring results would be presented to the Executive Committee bi-annually.

Below the corporate level, vice-presidents, direct reports to the President, and managers are responsible for monitoring risks within their area of responsibility. As mitigation strategies did not exist for branch and PMT risks, they could not be formally monitored. Branch and PMT stakeholders involved in the risk assessment process described that risks, issues and controls are discussed at PMT and management meetings; but documentation was not provided to support these discussions.

Without regular monitoring of risks, risk drivers, and risk mitigation strategies, including updates on control effectiveness at all levels of the organization, changes affecting the Agency's environment may not be identified in a timely manner. This could impede the achievement of Agency objectives/priorities and cause inefficiencies (e.g., expending resources to control a risk that no longer exists).

Oversight of CBSA Risk Management Practices

The audit expected to find governance structures that promote a risk informed culture and management practices throughout the Agency. As indicated in the [redacted] ERM Policy and various committees' terms of references, the following committees and positions have been delegated the responsibility of reviewing the Agency's risk management practices:

- The Agency Departmental Audit Committee;
- The Executive Committee;
- The Director of [redacted]; and
- The Chief Audit Executive.

The Audit Committee is responsible for providing objective advice and recommendations to the President regarding the sufficiency, quality and results of assurance on the adequacy and functioning of the Agency's risk management, control and governance frameworks and processes; and for periodically reviewing the Enterprise Risk Profile and Agency risk management arrangements, and to document any significant concerns in relation to the Agency's risk management framework and processes. The Audit Committee Charter requires the Committee to provide the President with objective advice on recommendations pertaining to adequacy and functioning of the Agency's risk management framework and processes. The audit confirmed that the Audit Committee executes its responsibilities by periodically reviewing the ERP. Program updates, along with the ERP, are presented by [redacted] and are generally shared with the Audit Committee members on an annual basis.

In addition, the Executive Committee is required to identify key risks, prioritize Agency activities and identify, monitor and report on expected results, ensuring appropriate linkages to key management accountability documents. The audit found that status updates were provided to Executive Committee for the 20xx ERP and mitigation plans, the ERP 20xx Status Update, and the 20xx ERP, but not the 20xx ERP mitigation plans.

According to the [redacted] ERM Policy, the Chief Audit Executive is responsible for providing an independent and objective assessment of the application of the ERM framework and ERM strategies and practices. The Chief Audit Executive's responsibilities for ERM are being carried out through the conduct of this audit.

To conclude, the audit found that risk management practices at the corporate level are regularly monitored by oversight bodies within the Agency.

Recommendation 2:

The Vice-President of the Corporate Affairs Branch should adhere to the [redacted] ERM Policy and Guidelines to ensure that formal mitigation plans below the corporate level are developed, implemented and monitored.

Management Action Plan	**Completion date**
The Corporate Affairs Branch agrees with this recommendation. The Branch has fully integrated risk management considerations into the 20xx–20xx integrated business plan templates at the branch level. This includes requests for information from branches to develop their formal risk mitigation plans to identify key directorate-level commitments that will help mitigate specific risks and risk drivers identified in the 20xx ERP. The updated ERM Policy will clarify the responsibilities and accountabilities of all vice-presidents to ensure that formal branch-level risk mitigation plans are developed, implemented and monitored, and will further clarify the role of the Vice-President, Corporate Affairs Branch in monitoring and reporting on the implementation of the ERM Policy.	November 20xx

Appendix A – About the Audit

Audit Objectives and Scope

The audit objective was to provide assurance that the Agency's Enterprise Risk Management Framework is in place, that Agency risks are identified, assessed and managed effectively for achieving objectives, and that risk information is integrated into planning and decision making.

The audit scope covered the ERM control framework and processes at both the corporate level and within selected Branches and Programs, in addition to how information was integrated into existing management activities including business and operational planning and decision-making. It focused on the Agency's ERM Policy, procedures, and tools and also considered how other risk management documents, including but not limited to, the National Border Risk Assessment, the Departmental Security Plan, the Strategic Emergency Management Plan and Major Projects, were used in the ERM process.

The audit was conducted from February 20xx to August 20xxand focused on the process for developing the Enterprise Risk Profile, which is part of the ERM process and control framework. Observations are based on the 20xx ERP, which was the most recent version at the time of the audit.

Finally, the audit examined whether the ERM process is being properly integrated with strategic and operational plans across the Agency at the branch and PMT level.

An audit of Enterprise Risk Management was approved by the Agency's Audit Committee as part of the Risk-Based Audit Plan 20xx–20xx to 20xx–20xx.

Risk Assessment

Our risk assessment conducted during the planning phase identified the following key risk areas:

- If the Agency's ERM process, including monitoring, does not align with an appropriate risk management framework (i.e. *TBS Framework for the Management of Risk*, etc.) and is not appropriately communicated, the effectiveness of ERM across the Agency could be reduced.

- If the ERM process is not informed by the appropriate individuals across the Agency, there is a risk that risk profiles and decisions resulting from them will not be reflective of current and actual risks threatening the achievement of Agency objectives.
- If ERM is not fully integrated into planning and decision-making practices and risk information is not shared across the Agency, there is a risk that the identified vulnerabilities may not be used for planning and resource allocation purposes, and may not be managed and mitigated effectively for achieving objectives.

Approach and Methodology

The examination phase of this audit was performed using the following approach:

- Reviewing key risk management documents;
- Conducting interviews on ERM processes, roles and responsibilities, oversight function and monitoring, etc.;
- Reviewing management committee terms of reference and records of decision;
- Reviewing documents relating to ERM monitoring processes and reports;
- Reviewing a sample of risk assessments; and
- Reviewing a sample of key organizational planning documents.

Audit Criteria

Given the preliminary findings from the planning phase, the following criteria were chosen:

Lines of Enquiry	Audit Criteria
1. Risk Management Framework	• 1.1 The [redacted]'s risk management framework and processes are documented, complete and communicated across the Agency.
2. Risk Management Practices	• 2.1 Management identifies and assesses significant risks that may preclude the achievement of its objectives. • 2.2 Management identifies and assesses the existing controls that are in place to manage its risks. • 2.3 Management formally responds to its risks, and communicates both risks and risk management strategies to appropriate stakeholders across the organization enabling the Agency to carry out its responsibilities. • 2.4 Risk information is integrated in and used for planning and decision-making purposes. • 2.5 Risk management is regularly monitored by oversight bodies within the Agency.

Appendix B – List of Acronyms

BMT

Branch Management Team

CBSA

Canada Border Services Agency

CRO

Chief Risk Officer

DPR
Departmental Performance Report

ERM
Enterprise Risk Management

ERMTID
Enterprise Risk Management and Transformation Initiatives Division

ERP
Enterprise Risk Profile

MAF
Management Accountability Framework

PMT
Program Management Table

TBS
Treasury Board Secretariat

RPP
Report on Plans and Priorities

2020 | INTERNAL AUDIT MEMORANDUM

Subject: 2020 Enterprise Risk Management Gap Analysis
Date: January 20, 2021
To: [redacted]
Cc: [redacted]
From: [redacted]

Company Logo Here

Drafted: 2/4/2021

BUSINESS DESCRIPTION

The Enterprise Risk Management (ERM) [redacted]

The ERM department [redacted]

ENGAGEMENT OVERVIEW

Our main objective of was to conduct [redacted]

The two risk frameworks are well aligned with similar components, however the COSO ERM Framework provides more extensive guidance and implementation documentation.

CONCLUSION

The existing risk management processes [redacted]

SCOPE

January 2020 – October 2020

The primary components of the NA CRO Council ERM Framework are:

- Risk Appetite and Limits;
- Identify and Assess Risks;
- Risk Measurement;
- Monitoring and Reporting;
- Stress and Scenario Testing;
- Risk and Capital Management; and
- Link to Business Strategy.

This memo is intended for the exclusive use of [redacted] management and the Board of Directors.

2020 | INTERNAL AUDIT MEMORANDUM

KEY METRICS

Each principle in both the COSO ERM Framework and the NA CRO Council is comparable to one or more principles in the corresponding framework.

Governance & Culture
- Exercises Board Risk Oversight
- Establishes Operating Structures
- Defined Desired Culture
- Demonstrates Commitment to Core Values
- Attacks, Develops, and Retains Capable Individuals

Strategy & Objective-Setting
- Formulates Business Objectives
- Analyzes Business Context
- Defines Risk Appetite
- Evaluates Alternative Strategies

Performance
- Identifies Risk
- Assesses Severity of Risk
- Prioritizes Risk
- Implements Risk Responses
- Develops Portfolio View

Review & Revision
- Assesses Substantial Change
- Pursues Improvement in Enterprise Risk Management
- Reviews Risk and Performance

Information, Communication, & Reporting
- Communicates Risk Information
- Reports and Risk, Culture, and Performance
- Leverages Information and Technology

COSO ERM Framework

North American CRO Council ERM Framework

Risk Culture & Governance
- Underpinned by Company Values
- Interaction with Board of Directors
- Incentive Compensation Oversight
- Employee Survey Process
- RF&I, Audit Committee

Risk Appetite & Limits
- Aligned with Corp Strategy, financial & capital mgmt & segment plans, incentive comp
- Setting of limits, thresholds and tolerances
- Categories - enterprise, segment earnings, insurance, capital & liquidity, market and credit, and operations

Identify & Assess Risks
- Techniques/Involvement to Assess and Risks
- Updating Risk Factors
- Year-end Risk & Uncertainties in MD&A
- Assessing & Prioritizing Risks

Risk Measurement
- 3 Lines Model
- Company and Board Committees
- Independent Oversight of Enterprise Risks

Stress & Scenario Testing
- Enterprise Stress Testing performed on a semi-annual basis
- Ad hoc Analysis throughout the year

Monitoring & Reporting
- Identify, Measure & Monitor Material Exposure
- Monitor the Effectiveness of Risk Management
- Report on Risks Relative to the Company Risk Appetite
- Assess Capital Adequacy Relative to Known Risks
- Provide Timely, Useful & Actionable Info

Risk & Capital Management
- Managing Relationship between Risk, Profit & Capital
- Robust Enterprise Financial Model

Link to Business Strategy
- ERM Roles in Company's Strategic, Capital & Business Planning Processes

NA CRO Council information does not list out specific principles, but the principles listed were derived from component descriptions in [redacted].

Enterprise Risk Management Gap Analysis

Area Reviewed	Key Framework Components Considered	Testing Results	Conclusion
Risk Appetite is Approved Annually	• Defines Desired Culture • Risk Appetite and Limits • Link to Business Strategy • Formulates Business Objectives • Demonstrates Commitment to Core Values	[redacted]	**Effective**
Adequacy of Risk Assessment	• Identifies Risks • Assesses Severity of Risks • Risk Measurement • Assesses Substantial Change • Attracts, Develops and Retains Capable Staff	[redacted]	**Marginal** **Recommendation – ERM** [redacted]
Risk Environment is Monitored	• Identifies Risks • Assesses Severity of Risks • Assesses Substantial Change • Reviews Risk and Performance • Monitoring and Reporting	[redacted]	**Effective**

Enterprise Risk Management Gap Analysis

Area Reviewed	Key Framework Components Considered	Testing Results	Conclusion
Involvement in Setting of Corporate Strategy, Objectives and Capabilities	• Establishes Operating Structures • Defines Desired Culture • Demonstrates Commitment to Core Values • Formulates Business Objectives • Link to Business Strategy	[redacted]	**Effective**
Inherent Risk Levels are Established	• Identifies Risk • Assesses Severity of Risks • Prioritizes Risks • Develops Portfolio View • Assesses Substantial Change	[redacted]	**Marginal** **Recommendations –** [redacted]
Board and Management Committee Involvement	• Exercises Board Risk Oversight • Risk Culture and Governance • Evaluates Alternative Strategies • Implements Risk Responses • Communicates Risk Information	[redacted]	**Effective** **Recommendations–** [redacted]

Enterprise Risk Management Gap Analysis

Area Reviewed	Key Framework Components Considered	Testing Results	Conclusion
Coordination with Management	• Analyzes Business Context • Formulates Business Objectives • Implements Risk Responses • Develops Portfolio View • Assesses Substantial Change	[redacted]	Effective
ORSA Report is Completed Annually	• Assesses Severity of Risks • Reviews Risk and Performance • Pursues Improvement in Risk Management • Communicates Risk Information • Reports on Risk, Culture and Performance	[redacted]	Effective **Recommendation –** [redacted]
Risk Reporting	• Assesses Severity of Risks • Reviews Risk and Performance • Leverages Information and Technology • Communicates Risk Information • Reports on Risk, Culture and Performance	[redacted]	Effective **Recommendation –** [redacted]
Scenario and Stress Testing	• Evaluates Alternative Strategies • Assesses Severity of Risks • Assesses Substantial Change • Pursues Improvement in Risk Management • Communicates Risk Information	[redacted]	Effective

2021 | WORKFORCE MANAGEMENT AND BUSINESS ANALYTICS INTERNAL AUDIT REPORT

To: [redacted]
CC: [redacted]
Audit Team: [redacted]

Company Logo Here

Issued: 7/16/2021

BACKGROUND

Workforce Management [redacted]

SCOPE

June 2020 – February 2021

Designed to ensure [redacted]

- [redacted]

CONCLUSION

3 Reportable Findings

[redacted]

Our audit work is conducted in conformity with the *International Standards for the Professional Practice of Internal Auditing* promulgated by *The Institute of Internal Auditors*.

KEY RISKS

Operational

- Data Integrity
- Poor Customer Service
- Competency/Training
- Business Disruption & System Failures

Strategic

- Inefficient Use of Resources
- Inadequate/Incorrect Internal Reporting

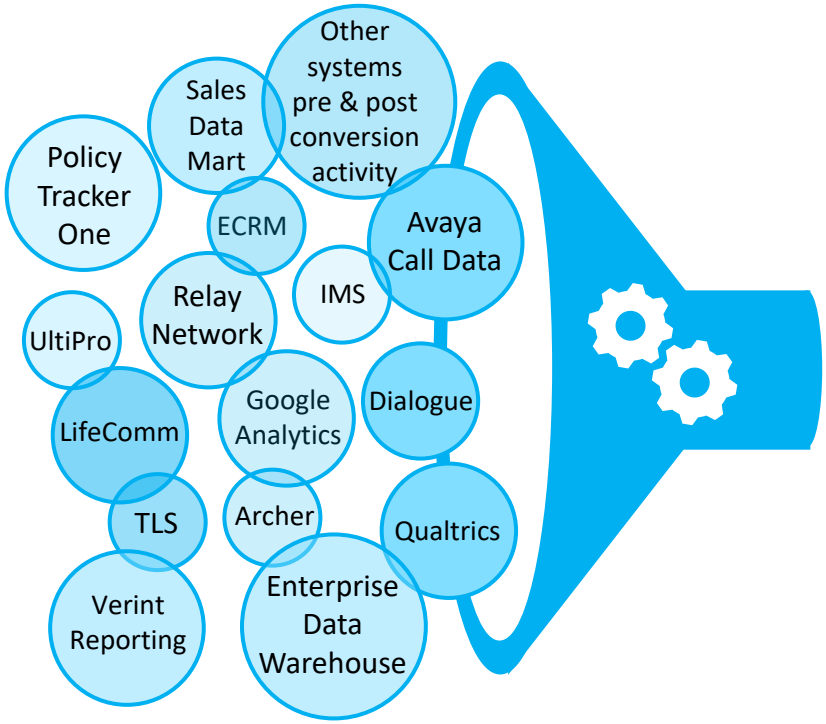
Due to the effectiveness of 15 controls tested, average inherent risk score of 3.17 dropped

↓ 32 %

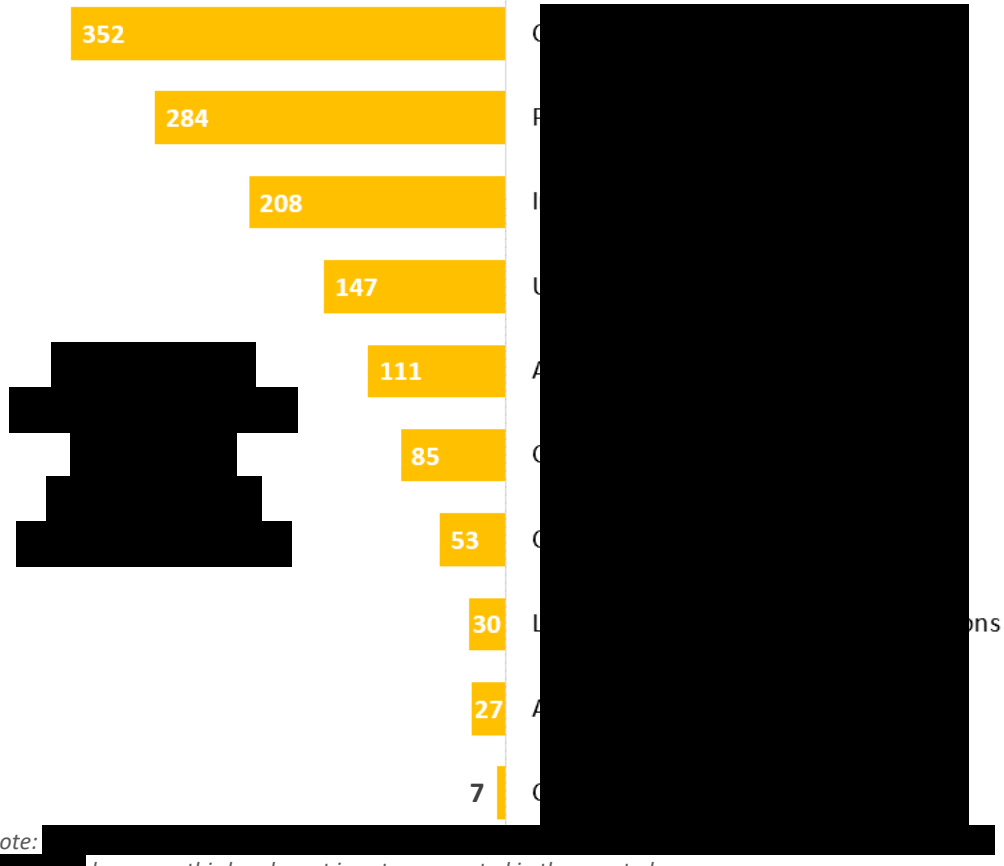
to an average residual risk score of 2.17

This report is intended for the exclusive use of [redacted] management and the Board of Directors.

Sources Used by Workforce Management and Business Analytics Group



Areas and Employee Count supported | As of April 2021



Note: [redacted] *however, this headcount is not represented in the count above.*

The Team

[redacted]
Full Time Active Employees

[redacted] Business Analytics

[redacted] Workforce Management

Tenure at [redacted]

Min	Average	Max
[redacted] Years	[redacted] Years	[redacted] Years

Min	Average	Max
[redacted] Years	[redacted] Years	[redacted] Years

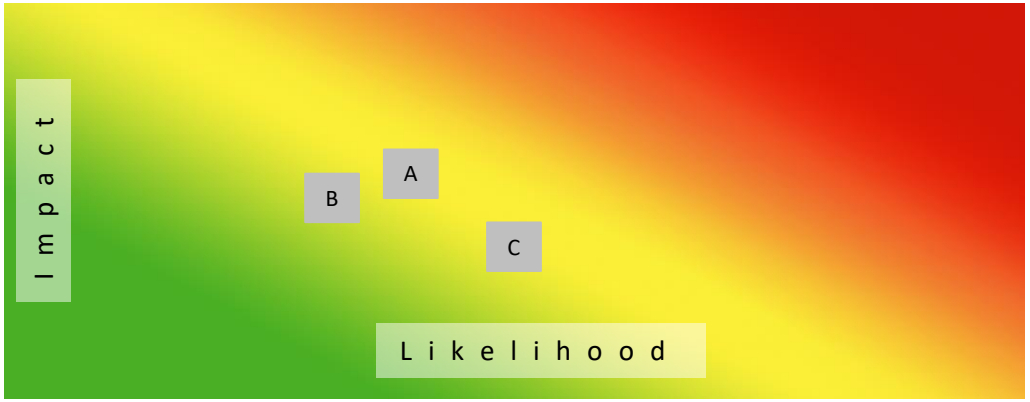
Full Time Employee Locations

[redacted]

2021 | WORKFORCE MANAGEMENT AND BUSINESS ANALYTICS INTERNAL AUDIT REPORT

FINDINGS:

Finding Level	Number of Findings (1st risk-based audit)
1 | Severe	0
2 | Major	0
3 | Moderate	3



LEGEND:

In Process

Completed

Legend	Level	Observation	Business Response	Estimated Completion Date & Owner
A	3	SQL Server Reporting Services ("SSRS") Report Changes [redacted]	[redacted]	9/30/2021 [redacted]
B	3	Staffing Model Changes [redacted]	[redacted]	12/31/2021 [redacted]
C	3	Report Management [redacted]	[redacted]	9/30/2021 [redacted]

This report is intended for the exclusive use of [redacted] management and the Board of Directors.

2021 | OPERATIONAL ACCOUNTING TARGETED CONTROL REVIEW

Control Owners: [redacted]
CC: [redacted]
Audit Team: [redacted]

Company Logo Here

DRAFT: 05/28/2021

BACKGROUND

The [redacted]

This [redacted]

CONCLUSION

Four level 3 findings [redacted]

Our audit work is conducted in conformity with the *International Standards for the Professional Practice of Internal Auditing* promulgated by *The Institute of Internal Auditors*.

FINDINGS

Finding Level	Number of Findings
1 | Severe	0
2 | Major	0
3 | Moderate	4

LEGEND:

In Process

Completed

SUMMARY OF TESTING

[redacted]

SUMMARY OF TESTING

Control Tested	Testing Procedures	Evaluation Results	Level	Legend
Process: [redacted] Operational Accounting Risk: Amounts reported to Corporate are incorrect				
Schedule S Control Checks	Review the [redacted] preparation and review process documentation to ensure the process is adequately documented, reviewed, and approved prior to implementation and amounts reported agree to supporting documentation.	Finding Noted: [redacted] Business Response/Owner: [redacted]	**3**	**A**
Process: [redacted] Operational Accounting Risk: Incorrect or Missing Transactions				
[redacted] Reasonableness Analysis	Review [redacted] analysis documentation to ensure the process is adequately documented, reviewed, and approved prior to implementation and amounts reported agree to supporting documentation.	Findings Noted: [redacted] Findings Noted: [redacted] Business Response/Owner: ([redacted])	3 3	B C
Operational Accounting control checks	For a sample of control documentation in the [redacted] Operational Accounting area, verify control checks are accurate and adequately support the control purpose.	The control appears to be in place and operating effectively.		

Continued on next page

SUMMARY OF TESTING

Control Tested	Testing Procedures	Evaluation Results	Level	Legend
Process: [redacted] Operational Accounting Risk: Incorrect or Missing Transactions				
[redacted] quarterly settlement review	From a sample of [redacted] Quarterly Settlements, choose a sample of key balances ([redacted]) and agree to supporting documentation and the general ledger; Verify wires are accurate and appropriately reviewed by management; Obtain review support evidencing the quarterly review of the [redacted] and assess review procedures for reasonableness.	Findings Noted: [redacted] Findings Noted: [redacted] Business Response/Owner: ([redacted])	3 3	B C
[redacted]	[redacted]	The control appears to be in place and operating effectively.		