CVSHealth®

Internal Audit Methodology

Revised October 2020

Table of Contents

Section A: Planning and Scoping Phase

Planning and Scoping Phase Overview

The Planning and Scoping Phase is performed to identify the scope and objective of the audit by refining the Audit Plan Strategy through discussions with the Business Area.

By the completion of the Planning and Scoping Phase, the Business Area (from key contact up to the appropriate members of Management) should understand and agree to the audit scope and objectives. The Audit Team should have a high-level understanding of the Business Area's business objectives, risks threatening those objectives, key processes, and have identified the process owners/subject matter experts.

A.1 Planning and Scoping Notification

Purpose

The purpose of the Planning and Scoping Notification is to inform the appropriate members of Business Area Management that IA is beginning the Planning and Scoping Phase of the audit and will be engaging with both them and their respective team. This process also confirms with the appropriate members of Business Area Management that IA identified the appropriate individual(s) to schedule planning and scoping meetings.

Instruction

The Audit Team emails the appropriate members of Business Area Management to notify that the Audit Team is ready to begin planning and scoping activities and confirm both the audit timeline and other key contact(s) to support the initial planning and scoping meetings. The Audit Team may modify the template as needed. Once sent, a copy of this email is documented within the applicable Audit Repository.

From the IIA (2200):
"Internal auditors must develop and document a plan for each engagement, including the engagement's objectives, scope, timing, and resource allocations. The plan must consider the organization's strategies, objectives, and risks relevant to the engagement."

A.2 Building Objective and Scope

Purpose

The purpose of establishing the scope and objective for the audit is to confirm IA focuses on providing assurance over the most critical risks within the enterprise. By effectively scoping an audit, IA ensures the audit is of an achievable size for the assigned Audit Team. Further, efficiently scoped audits focus on those areas that provide the most value-add to the Business Area.

Instruction

A.2.1 Background Review

The audit's scope and objective Phase begins with the high-level direction in the Audit Plan Strategy by IA Management during the Audit Planning process. Further refinement of the scope is facilitated through review of various documentation (see below examples) and meetings with the Business Area.

- Prior Audits
- Risk Monitoring Meetings

- SOX/SOC1
- External Guidance

A.2.2 Risk Stakeholder Input

Key stakeholders across the organization may have relevant information to assist in the assessment of the Business Area risks. The Audit Team should inform applicable business stakeholders of the audit and seek feedback to consider as part of planning and scoping. The Audit Team may use the below email template as a guide and should be maintained in the Audit Repository with any applicable responses.

Responses noting concern, or new information, should be discussed with the Audit Manager/Director to assess any impact to the audit, and dispositioned within the applicable Audit Repository.

Business Areas to consider engaging:

- SOX and Control Assurance
- Investigation Services
- Special Investigations Unit
- Legal
- Compliance
- Finance & Accounting
- Asset Protection

A.2.3 Planning and Scoping Meetings

The purpose of the Planning and Scoping Meetings is to obtain additional information from the Business Area to further develop the scope and objective. Auditors should be prepared to ask questions and facilitate the discussions with the business, such as:

- Key processes and sub-processes involved
- Relevant subject matter experts (SME) for each process
- Do any applications support these processes?
- Inherent risks within the processes and impact
- Mitigating controls/procedures

Notes and outcomes of these meetings should be retained within the Scope Document to support the scope and objective. The Audit Director communicates to and obtains CAE approval for any change needed in the Audit Plan Strategy due to any new information obtained during the Planning and Scoping Meetings.

A.2.4 Fraud Risk Assessment

The Audit Plan Strategy, scope, and objective focus on addressing the key risks facing the Business Area, including the inherent risk of fraud. Each audit is required to consider the potential risk for fraud by performing a Fraud Risk Assessment. This assessment considers the inherent risk of potential fraud within the Business Area under review. The Audit Team may refer to the Fraud Risk Assessment template as a guide and should be maintained within the Audit Repository with any applicable responses.

> ***From the IIA (2210.A2):***
> *"Internal auditors must consider the probability of significant errors, fraud, noncompliance, and other exposures when developing the engagement objectives."*

A.2.5 Scope Document

As information is gathered during the planning and scoping meetings, and the Audit Plan Strategy is refined into the audit scope and objective, this progression is retained centrally within the Scope Document. This documents the appropriate due diligence review performed by IA in planning the audit and understanding the key risks. Note the final scope and objective is documented in the Kick-Off Deck.

A.2.6 Drafting the Scope and Objective

Drafting the Scope: The scope includes the purpose of the audit. Items to consider may include:

- What lines of business will be included?
- What specific processes will be reviewed?
- What date range will be assessed?
- What outcomes will the audit seek to achieve?

The initial direction is set within the Audit Plan Strategy, which is further refined to the scope and objective. The scope is driven by the key risks that led to this audit being included on the Audit Plan. When drafting the scope, it is important to consider areas and functions that may be explicitly excluded. This could be due to an area having comparatively lower risk, a function being newer and not yet ready to be audited, or an area being recently audited through another audit.

> ***From the IIA (IG2220):***
> *"During planning, internal auditors typically draft a scope statement that specifically states what will and will not be included in the engagement (e.g., the boundaries of the area or processes, in-scope versus out-of-scope locations, subprocesses, components of the area or process, and time frame). The time frame may be based on a point in time, a fiscal quarter, a calendar year, or another predetermined period of time."*

> ***From the IIA (IG2210):***
> *"Internal auditors can formulate preliminary objectives of engagements through a review of the annual internal audit plan and prior engagement results, discussions with stakeholders, and consideration of the mission, vision, and objectives of the area or process under review. The preliminary objectives are further enhanced through risk assessment exercises to cover the governance, risk management, and controls of the area or process under review. The engagement objectives articulate what the engagement is specifically attempting to accomplish and determine the engagement scope."*

Drafting the Objective(s): The objectives are a more detailed breakdown of the areas within the audit and satisfy the scope. Like the audit scope, the objectives provide assurance over the design and effectiveness of management's control environment in mitigating the key risks.

> ***From the IIA (IG2220, cont.):***
> *"To ensure the scope is sufficient to meet the engagement objectives and aligns with the organization's annual internal audit plan, internal auditors must use sound professional judgment based upon relevant experience and/or supervisory assistance. When determining the scope, it is helpful for them to review the engagement objectives to ensure that each objective can be accomplished under the established parameters. Internal auditors generally consider and document any scope limitations, as well as any requests from the client or stakeholders for items to be included or excluded from the scope. If internal auditors encounter scope limitations, these must be reported in the final engagement communication.*
>
> *At times, internal auditors may place reliance on work performed by others — such as external auditors or compliance groups within the organization — and it may be useful to document such reliance in the scope statement. Standard 2050 – Coordination and Reliance and its Implementation Guide provide further guidance on the internal audit activity's reliance on such work."*

A.3 Data Analytics

Purpose

Data analytics is utilized during audit planning to drive an *effective scoping* and throughout testing to provide the *highest level of business assurance* within the riskiest areas of the audit. Through data analytics IA has the ability, and the creativity, to obtain relevant business data to perform intelligent and meaningful summarizations, to generate audit value.

Instruction

Audit Managers are responsible for ensuring appropriate time and effort are devoted during the audit process to leverage data analytics. Although the use of analytics is not required for each audit, the evaluation of using analytics should be performed for every audit.

In addition, the Analytics Team in IA is available for support throughout audit process, with expertise in data management, data science, analytics, and robotics.

<u>Descriptive Analytics</u>: Descriptive Analytics are executed during the audit planning and recommended be performed within three to four weeks prior to audit kick-off. Through descriptive analytics, the Audit Team obtains insight into the process to develop a better understanding of key risks. The Audit Team, with the assistance of the Audit Manager, should identify and develop and understanding of the data universe, or the transactional set of data in the area being audited.

A.3.1 Scoping and Planning Data Analytics

The Audit Manager should lead the business request to obtain basic and available information to assist in the execution of descriptive analytics. The transactions data should be readily available and may consist of adjudicated claims, vendor payments, or travel expenses. A data universe may have the following fields: transaction id, transaction date, transaction description, transaction type, member, amount, etc. The Audit Team should utilize CVS Health approved file transfer methods, such as KiteWorks and Audit Board, for the transfer and receipt of data. The type of analytics performed may include a summarization of transaction types, member or other key fields, monthly trending, stratifications, turn-around-times, outlier detection analysis and text analytics. Results of these high-level analytics may also help to target the Audit Team's testing efforts, as they build their RCA.

An email to applicable members of both Business and IT Leadership confirming use of Data Analytics should be sent to ensure alignment and facilitate the request of data. The Audit Team may modify the email template as needed. Once sent, a copy of this email should be documented within the applicable Audit Repository.

A.4 Audit Work Breakdown

Purpose

The purpose of the Audit Work Breakdown is to identify key milestones and accompanying target dates to facilitate the achievement of the target final report date. The Audit Work Breakdown also serves as an optional means of tracking audit progress and steps yet to be completed, as well as actual hours spent to forecasted hours.

It is important to select an achievable target final report date for the Audit Team while still completing the audit in a timely manner to provide relevant assurance to Senior Management and the Audit Committee. Further, the Audit Work Breakdown is designed with the expectation of audits being completed timely to allow sufficient time to complete all audits by the end of the annual plan (except for those intentionally designated as carry-over audits). As such, delaying the target final report date means delaying the completion of other audits.

Instruction

The applicable member of the Audit Team drafts a timeline that supports completing the audit by the target final report date. The Audit Team should collaborate with IA Management to appropriately set expectations for the timeline and level of detail to include. Dates should be set for key milestones: Kick-Off Meeting, RCA Validation, Testing Sign-Off, and Report Distribution. When designing the target dates for milestones, consideration should be given to the complexity of the audit, the number and experience of staff assigned to the audit, and other audits/responsibilities staff may have concurrently during the course of this audit.

A.5 Kick-Off Deck & Meeting

Purpose

The purpose of the Kick-Off Deck is to present the audit scope and objective to the Business Area and set expectations for the audit. At the discretion of the Audit Team, a Kick-Off meeting may be held to further discuss any feedback or questions they may have and facilitate the beginning of the Risk Control Analysis (RCA) Phase of the audit.

Instruction

A.5.1 Kick-Off Deck

The Kick-Off Deck presentation serves as the means of reaching alignment with the Business over the areas to be included within the scope of the audit, timeline, etc. Direct reports into the CAE are responsible for providing final approval of the Kick-Off Deck in advance of sharing with the Business and ensuring appropriate alignment with the CAE. For required components to be included in the Kick-Off Deck, refer to the Kick-Off Deck Template.

A.5.2 Kick-Off Meeting

As noted above, at the discretion of the Audit Team, a Kick-Off Meeting may be scheduled. The Kick-Off Meeting invitation is distributed by a member of the IA team. The invitees should include the appropriate level of both IA Management and Business Area Management. The invitees should also include any relevant supporting functions if necessary. The Kick-Off Meeting consists of the Audit Team discussing the materials in the deck. Following the Kick-Off Meeting, the deck should be documented within the applicable Audit Repository, noting any significant discussions held in the meeting and any subsequent changes or feedback.

The final version of the deck is issued in final form by a member of IA Management, along with a standard email, which summarizes the audit scope/objective and estimated completion date, to formalize the Kick-Off of the audit. A final copy of the Kick-Off Deck should also be stored in the central department file (i.e. SharePoint) to facilitate sharing with CVS external auditors.

A.6 Status Updates

Purpose

The purpose of providing status updates is to ensure key stakeholders are aware of the audit's progress and developments. As the Audit Team identifies items that may potentially lead to audit issues, they should be shared with IA Management and the Business Area for discussion and validation and to ensure appropriate alignment.

Instruction

A.6.1 Business Status Updates

Relevant business contacts and control owners should be kept informed of the status of the audit. At a minimum, key stakeholders identified in the "Business Line Contacts" table in the Kick-Off Meeting should be provided status updates throughout the audit. IA Management determines the frequency and format with which the meetings are to occur.

The goal of these updates is to inform the Business Area on the audit status, discuss outstanding questions and documentation requests, findings and potential audit issues and next steps. As a best practice, it is recommended to send a follow-up email to attendees summarizing the call and the agreed upon action items and/or deliverables discussed in the meeting. Providing this follow up helps ensure each attendee leaves the meeting with the same understanding regarding expectations and ownership.

A.6.2 Internal Status Update

IA Management should be regularly informed of the status of each audit, whether through recurring scheduled status meetings or ad-hoc as deemed necessary, and up to the discretion of IA Management. Topics to discuss during this meeting can include a discussion of the following: audit forecast to actual hours, roadblocks and challenges, potential control gaps identified, or testing exceptions observed and next steps. If audit progress is trending behind schedule, this is the time to discuss so that the cause of the delay may be assessed and addressed.

Section B: Control Analysis Phase

Control Analysis Phase Overview

The purpose of the Control Analysis Phase is to understand and document processes supporting key controls and to determine whether the control environment is adequately designed to mitigate key risks. Walkthrough meetings are held to obtain this detailed understanding and are documented through in a Process Narrative/Walkthrough Memo and Process Flow Chart. The key risks and related key controls are then summarized in the RCA document, where the team concludes on the effectiveness of the design of the controls at mitigating the related risk.

B.1 Walkthroughs

Purpose

The purpose of Walkthrough meetings is to “walk through” the step-by-step processes supporting the key controls. At the conclusion of the Walkthroughs, the Audit Team should be confident that all relevant key risks have been identified, as well as all related key controls and control gaps. The information gained in these meetings, along with any key documentation review, is the primary source for drafting the RCA document.

Instruction

The walkthrough meeting consists of reviewing an example of the process from end-to-end to confirm understanding of the process and relevant controls. Typically, this involves selecting an individual transaction and following it through the process and obtaining documentation of each key step. Walkthrough supporting documentation must be obtained for each key control and is the primary source for drafting the Process Narrative or Walkthrough Memos and Process Flow documents.

While initial planning and scoping discussions with business owners should have identified processes and given some idea of the high-level steps involved, walkthrough meetings expand the understanding of the key processes at a detail level, as well as identify the controls as either key or non-key. Understanding the step-by-step process, and observing it being performed, helps provide the information needed to assess whether the design of a control is sufficient to mitigate the related risk.

The Audit Team should prepare questions designed to facilitate their understanding of the process and identification of key controls. The best way to prepare these questions is by reviewing the policies and procedures for the process in advance. When reviewing, record the additional detail needed to support whether controls exist within the process, and whether such controls would mitigate the key risks. If policies and procedures are not available, review the collected documentation from the Planning & Scoping Phase.

B.2 Narratives & Process Flow

Purpose

The purpose of a process narrative or process flow with walkthrough memo is to document IA’s understanding of the process under review and identify the relevant controls with supporting evidence. The use of either a process narrative or a process flow chart and walkthrough memo to document controls is at the discretion of the Audit Manager. The narratives and flow charts serve as supporting documentation for the RCA.

Instruction

B.2.1 Narratives

Narratives document IA's understanding of the Business Area's control environment and rationale supporting the identification of key controls. The narratives should include sufficient detail and appropriate context for another auditor to be able to comprehend the step-by-step process and understand the controls without having attended the walkthrough meetings. Including screenshots and example reports obtained in the walkthrough meetings helps achieve this level of detail.

Controls identified within narratives should be noted using control statements which include the five components of a control listed below:

Five Components of a Control		
Component	**Description**	**Example Control Statement**
Frequency	How often is the control performed? The most common frequencies are daily, weekly, monthly, quarterly, and annually.	"On a monthly basis…"
Person / Application	Who or what is performing the control? If a person, use their title rather than name. If an application, use the proper name of the application.	"…the Claims Supervisor…"
Performing a Function	What is the act being performed? Be specific in how the control mitigates the risk.	"…reviews 10% of claims for compliance with the claims processing guidelines…"
Prevents / Detects	How does the control mitigate the risk? Does it prevent the risk from being realized? Or does it detect risks that have been realized in order to remediate? This is often evident in the nature of the control, and as such not explicitly stated like the other components.	(The example control is a detect control, as it is performed after-the-fact to identify any claims not processed in conformance with guidelines)
Evidence	What documentation exists to evidence control performance? How can the Business Area show how the control is performed and how well it is performed?	"…as evidenced by completing and signing off on the Supervisor Review Checklist. "

If a component is missing or if the identified risk is not mitigated, a control gap should be noted. The narrative should document which components of a control are in place as well as those that are missing. Any controls and control gaps identified within the narrative should be documented within the RCA and included in the audit repository.

B.2.2 Process Flows

Flowcharts are diagrams that show step-by-step progression through a process or system using connecting lines and a set of conventional symbols. Different types of symbols used in Internal Audit are included in the example and template listed below.

B.3 Risk Control Analysis (RCA)

Purpose

The Risk Control Analysis (RCA) refers to the aggregate risks, respective controls (and control gaps), any related test plan, and effectiveness conclusions of those controls. The purpose of the RCA is to summarize key controls and IA's assessment of the controls' design effectiveness and operating effectiveness.

Instruction

B.3.1 Drafting the RCA

The RCA provides a summary of the audit by laying out the objectives, risks, controls, and the test plan, along with the assessments of both the design effectiveness and operational effectiveness.

- Design Effectiveness: Was the control adequately designed to sufficiently mitigate the related risk, regardless of how well the control performer executes the control (which is assessed through the test plan). As described in the control section, the Audit Team assesses design effectiveness by verifying the inclusion of the five components of a control and that the control mitigates the related risk.
- Operational Effectiveness: Was the control adequately executed by the control performer to mitigate the related risk, which is assessed by executing the test plan. Typically, tests are only performed for controls with a design effectiveness assessment of effective (as no matter how well an ineffectively designed control is performed, it cannot mitigate the risk due to the design). However, Audit Teams may at times test ineffectively designed controls to assess the significance and impact of the control gap.

The RCA is composed of eight components, described below. Using the List View within Audit Board, these components provide an end-to-end view of the audit and serve as support for the conclusions presented within the audit report. After all controls and design assessments making up the RCA are drafted and reviewed internally, evidence of review must be indicated using the appropriate Work Step within the Audit Repository.

RCA Component	Description
Risk Number & Name	Include the risk statement identified during scoping or during the walkthroughs. Risks should be numbered in relation to their respective objective.
Control w/ Business Owner	Include the control statement identified during the walkthroughs. Be sure the control mitigates the assigned risk and that each control includes all five components of a control: 1. Frequency 2. Person/Application 3. Performing a Function 4. Prevents/Detects 5. Evidence If one or more of the five components is missing, verify the component is not otherwise addressed. If no control is present, then note the lack of a control for the relevant risk as a control gap.

	Include the identified control owner at the bottom of the control field in order to identify the business contact that can speak to any questions or issues identified regarding the control as well as provide requested test support documentation
Design Effectiveness	If all five components of a control are addressed and the control mitigates the risk, then it is an "Effective" control. If the control does not mitigate the risk, it might instead be a process. If it does not include all five, or if no control exists, this is a "Control Gap".
Type & Frequency	Determine whether the control is Automated or Manual • A = Automated Control (performed by a system) • M = Manual Control (performed by a person) Determine whether the control is Detective or Preventative • D = Detective (the control identifies instances of the realized risk after the fact) • P = Preventative (the control mitigates the risk from occurring) Determine how often the control is performed • Daily (once a day or more) • Weekly • Monthly • Quarterly • Annually
Key Control	Determine whether the control is a Key Control by assessing how well the control mitigates the related risk • Key Control: substantially mitigates the risk on its own • Non-Key Control: supports a key control but cannot wholly mitigate the risk on its own. General practice suggests to not include non-key controls in the RCA but only in the narrative / flow chart.
Test Plan	Describe the test steps to determine whether an effectively designed control is operating effectively. Include the sample size to be tested and attributes to be verified. If the control is not effective, note "No testing to be performed due to ineffective control design." The Audit Team designs tests for all controls with a design effectiveness assessment of effective as well as for any ineffective controls where the severity of the control gap must be assessed. The test plan includes the strategy of each test, including the sample size, test purpose, and test steps. Individual tests are performed over selected sample transactions or items as a representation of the control performance over the total population.
Operational Effectiveness	Describe the outcome of the test, clearly stating that the control either Effective or Ineffective the test.
Report Disposition	Describe the impact the design effectiveness and operational effectiveness results have on the audit report. List how the audit issues are included within any reportable issues. If issues were not reportable, explain the rationale for the non-reportable disposition.

When drafting the Test Plan, the use of data analytics should be considered. Data analytics procedures are best leveraged when large populations of data are available (thousands or millions of records). Rather than selecting a sample to gain assurance of a proper and adequate control environment, data analytics may be used to perform a test over the entire population, allowing for stronger supporting evidence for any issues that may be identified. Each Audit Team should perform analytics by directly leveraging standard analytics tools, such as Alteryx or ACL, as well as consider auto-executable analytics tools within the Self-Service platform.

Tool/Application	Description
Basic Desktop	
Microsoft Excel	A basic, popular, and widely used analytical tool. Analyzes and summarizes complex tasks, including preview of pivot tables for filtering of data.
Microsoft Access	Offers basic data analysis through queries, which can be filtered for further analysis.
Specialized Auditing Software	
Alteryx*	Advanced analytics tool that simplifies the process of accessing and blending data from multiple data sources.
ACL (2nd choice)	Combination of data access, data analysis, and integrated reporting, with immediate visibility into transactional data, and reading and comparing data.
Specialized DA Visualization Software	
Tableau Public and Power of BI	A data visualization software. Interactive tool that suggests labels, tools, column sizes, and dashboards and worksheets for data analysis and visualization.

The Audit should consider meeting with the appropriately assigned Data Analytics contact to identify potential tests to be performed. Data Analytic tests should be designed and documented within the RCA in the same manner as any other test, including details on the sample (potentially 100% in this case), period of sample, and test steps to be executed. Once tests are identified, verify applicable data to execute testing is available or requested from the Business Area, including evidence to support completeness.

B.3.2 Internal RCA Review

Due to the significance of the RCA, it must be reviewed by the Audit Manager prior to moving forward to fieldwork. If applicable, an Audit Lead may perform a preliminary detailed review prior to Audit Manager review. The Audit Manager’s review will be evidenced by signing off on the RCA Work Step within the audit repository.

If any audit issues are identified, those issues should be validated with internal audit management prior to formally sharing in writing with the Business Area as well. However, as previously noted, it is always encouraged to discuss initial observations with the Business Area as soon as possible after they are identified.

B.3.3 Business Area Validation of RCA or Process Flow

Validation of the controls to be tested with the Business Area is required to ensure controls are identified properly and control gaps on design effectiveness have been discussed. Alignment may be reached by sharing the Process Flows and confirming the process and key controls identified are appropriate, or by sharing controls included in the RCA.

When sharing the RCA and/or Process Flow with the Business Area, their input and validation should be focused on the accuracy of controls and control gaps, if any. The test plan portion of the RCA should not be shared with the Business Area. After sending the RCA to the Business Area, a meeting to discuss any questions or feedback may be warranted. The Business Area's validation of the RCA and/or Process Flow must be saved within the audit repository (within the Risk Control Analysis (RCA) Review Work Step). If the validation was provided during a meeting, include the calendar invite and/or note attendees providing validation.

Section C: Fieldwork and Testing Phase

Fieldwork and Testing Phase Overview

The purpose of the Fieldwork and Testing Phase is to assess the operational effectiveness of the key controls identified during the Control Analysis Phase. To execute testing to support this assessment, the Audit Team must request documentation, select test samples, prepare workpapers, and obtain management review.

Note: There are additional requirements for documentation related to audits being conducted under privilege and at the direction of Legal. Refer to Internal Audit's Attorney Client Privilege Procedures for further detail.

C.1 Leadsheets

A test leadsheet should be documented by the auditor to provide summarized testing results related to each control within the RCA. Each applicable control on the RCA should be referenced within the Audit Board Work Step with the following details: Control Number, Name & Description, Attributes Tested, Population, Sampling Methodology, and Conclusion.

From the IIA (2300):
"Internal Auditors must identify, analyze, evaluate, and document sufficient information to achieve the engagement's objectives."

In addition to details included within the Work Step, a *Testing Table* should also be included within a leadsheet, containing the sampled items, test attributes, and the test results. The testing table should summarize the results of each sampled item and whether the selection passed each attribute. The auditor is subject to using any tickmarks to help assist with documentation as needed.

Testing Column	Description
Sample Number(s)	Each sample on the test table should be uniquely numbered (e.g., 1, 2, 3, etc.) with a corresponding reference to the supporting workpapers.
Description(s)	Each item sampled should include relevant details describing the selected samples (transaction number, invoice date, account ID, etc.), to differentiate each sample. Any Personally Identifiable Information (PII) or Personal Health Information (PHI) should be de-identified and omitted from the leadsheet prior to management review.
Attribute(s)	The attributes are the key elements being tested (e.g., control points, accuracy of recorded account balance, etc.). Each sample selected should be tested against the test plan and align with the RCA.
Workpaper Reference(s)	All workpapers utilized for testing should be referenced in this column with appropriate Audit Board links utilized.
Comment(s)	Any additional comments for sampled items should be documented here with a tickmark or with commentary, up to the auditor's discretion.

Auditor Prepared by:
The leadsheet should be documented to show who prepared the supporting workpapers for a test.

Prepared by: The section should be dated and should list the auditor(s) who prepared the testing leadsheet and its workpapers.

Tickmark Testing Legend
The tickmark legend should define each tickmark used in the leadsheet. Tickmarks are used up to the auditor's discretion and can be used to make notations as necessary. Note additional tickmarks may be added to substantiate for testing.

From the IIA (2320):
"Internal Auditors must base conclusions and engagement results on appropriate analyses and evaluations."

C.2 Sampling Guidelines

There are two methods of sample selection: 1) statistical and 2) non-statistical. The method used requires auditor judgment and should be discussed with the Audit Team prior to testing.

Statistical sampling uses random numbers to select the sample, which ensures each item in the population has an equal or known chance of being selected. These techniques include independent random sampling, systematic or interval sampling, stratified sampling, to name a few.

Non-statistical sampling does not use random numbers to select the sample. Instead, the auditor uses judgment based on an understanding of the population. Such sampling may be done haphazardly. The Audit Team should assess whether the sample is representative of the population and whether sample results can be extrapolated across the entire population. The method of sample selection should be documented in the Audit Board Work Step and each applicable population file.

C.2.1 Sample Sizes

When applying any type of sampling, standard sample sizes are as follows:

Configurable	Annual	Semi-Annual	Quarterly	Monthly	Bi-Weekly	Weekly	Daily/Recurring
1	1	2	2	2	5	5	25

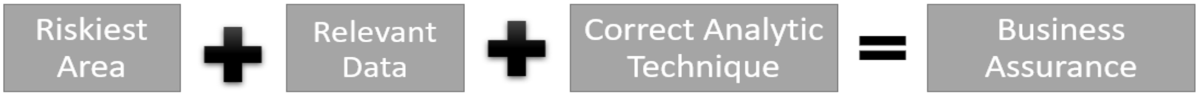
For daily/recurring populations of less than *250 items*, a sample size of 10% of the total population should be used and a minimum of 5 samples should be tested to gain comfort over the lower population. Any deviation from these standard guidelines should include sufficient documentation explaining the rationale for the deviation.

C.2.2 Additional Sample for Errors Identified

When an exception is identified within an original sample size of a daily, recurring, and as-needed control, the Audit Team may assess whether additional testing and sampling is necessary based on the original results of the testing performed. As such, additional samples may be tested to obtain comfort.

C.2.3 Data Analytics: Execution and Documentation

Data Analytics testing is similar to other testing and performed once process walkthroughs and risk assessments are executed. Using the audit risk and objective, the Audit Team with the support of the Audit Manager, should assess the analytics technique and relevant data for the greatest risk or critical area of the audit. The Audit Team should ensure the test is performed as intended in order to gain the desired assurance over the respective control. Prescriptive analytics may be performed in any control or substantive testing; however, the focus should be in the riskiest controls and most critical areas of the audit to maximize the value and impact of analytics during the audits.


Riskiest Area + Relevant Data + Correct Analytic Technique = Business Assurance

The Audit Team may perform analytics in less risky audit areas, as data may be easier to obtain and analyze. However, the time to confirm completeness and accuracy of data and perform the analytics may not prove valuable. Focusing on the riskiest areas often requires a multi-disciplinary team and complex data, which at times is unstructured, such as data within in contracts or invoices.

Once the initial test results are performed, the Audit Team should review the logic behind the scripts, particularly for potential false positives. The Audit Team should review the script and initial results and consider the need for modifications to the script to address false positives.

Once the script is finalized and the final testing results obtained, the Audit Team will document those results in a lead sheet and add to the Audit File. The Audit Team may need to provide additional language regarding the testing and results within the lead sheet to fully document the testing performed. In addition, due to the size constraints within the Audit Repository and sensitive information included within the data, the Audit Team may need to use discretion in the extent and types of information included to support procedures performed and results. As a result, deviations from the standard Workpaper Documentation Methodology may be deemed necessary and should be appropriately documented.

C.2.4 Data Analytics: Findings & Results

Due to the testing of an entire population rather than a sample, the number of identified exceptions may be higher than observed in typical sample testing. If the number of exceptions seems reasonable to address, then they should be vetted with the Business Area to provide further documentation to support the exceptions identified. However, if the number of exceptions is too high to provide to the Business Area, the Audit Teams may pursue one of the following approaches:

- May group the exceptions based on a specific criterion, or similarity, and inform the Business Area of the findings in the form of a summary for each grouping.
- May select a sample of exceptions at random or judgmentally, most commonly by taking a risk-based approach, to validate with the Business Area.

Auditors' judgment should be strongly expressed when determining the significance of the exception. Data analytics is designed to provide reasonable assurance that controls mitigate the key risks, not necessarily absolute assurance. For example, analytics may identify 2K exceptions, which may seem significant, but when identified within a population of 7M, means the control is 99.97% effective.

C.3 Audit Workpaper Documentation

Purpose

Each workpaper should be appropriately documented to demonstrate how each attribute was performed and how the auditor obtained assurance that the attributes were satisfied or failed. All documented final evidence is retained within the appropriate audit repository until the audit report is issued.

Instruction

C.3.1 Request Procedures for Supporting Documentation

The auditor is responsible for obtaining supporting documentation through their best applicable branch of communication. Best practice is to utilize the Workstream functionality within Audit Board to facilitate the Business Area to provide requested documentation directly into Audit Board. However, Audit Teams also have the option to send a request via email to the business area, or even consider using a Document Request List to consolidate and track document requests when sending to the business area. Please note that the template below is optional.

C.3.2 Workpapers

Please find the requirements for documenting workpapers below:

Clean Copies:

- Documentation regarding how the attribute(s) are appropriately satisfied.
- Header including control number, workpaper reference/sample number, and source of documentation.
- Footer including page number and preparer’s name.

> ***From the IIA (2330):***
> *“Internal Auditors must document relevant information to support the conclusions and engagement results.”*

Exceptions:

- Documentation describing only the failed attribute
- Header including control number, workpaper reference/sample number, and source of documentation
- Footer including page number and preparer’s name

For samples with the same failed attribute, only a single failed workpaper is required to represent all failed instances. Each unique instance of failing an attribute should be documented appropriately.

Note that regardless of the preparation by the core Audit Team or by the Internal Audit Data Analytics team, the same workpaper requirements are applied to all documentation.

Privacy

Certain information protected by privacy laws (e.g. PII, PHI, PCI) should **not** be included in the working papers, including credit card numbers, driver’s license numbers (or other government issued ID numbers), social security numbers, and bank account/routing numbers (both in combination). Other confidential identifying information should be expunged from the working papers unless the information was directly utilized in assessing one or more test attributes.

If information must be retained, certain security measures must be taken. The information should only be stored in approved Internal Audit documentation repositories and should not be stored within AuditBoard. If any confidential identifying information is required to be provided to external parties, the information must be encrypted during transit (i.e. encrypted email, etc.).

Any questions regarding confidential identifying information should be brought up to Internal Audit Management and directed to the Privacy Office at privacyoffice@cvs.com or 401-770-5713.

C.3.3 Naming Conventions

To ensure that all testing workpapers are easily referenced, the auditor is required to use a naming convention to ensure their workpapers are easily identifiable and referenced. The naming conventions may include:

[*Audit Number*] - [*Control Number*] – [*Type of Document i.e. leadsheet, clean copy, failed copy*]

C.4 Audit Review

Purpose

Each workpaper must be reviewed by an individual other than the preparer to ensure procedures performed are within the guidelines of the audit methodology. This review must be evidenced in the audit repository.

> ***From the IIA (2340):***
> *"Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed."*

Instruction

By the conclusion of the Fieldwork and Testing Phase, each workpapers should be documented and marked as prepared in the audit repository prior to final management review. If applicable, the Audit Team Lead may perform a preliminary review depending on the team size and the structure of the audit. Each workpaper should be reviewed by the appropriate level of management and uploaded within the appropriate workpaper repository prior to issuance of the final audit report.

Section D: Reporting Phase

Reporting Phase Overview

The purpose of the Reporting Phase is to create the formal output of the work performed in the Control Analysis and Fieldwork and Testing Phases, communicating both the results of the audit and any corrective actions to be implemented.

By the completion of the Reporting Phase, the Audit Team will have issued the audit report, after having received approval from Internal Audit management as well as the Business Area's management. All workpapers within the audit repository should be prepared and reviewed prior to issuing the final report.

D.1 Audit Report

Purpose

The purpose of the Audit Report or Audit Memo is to formally communicate the results of the audit. The Audit Report is the preferred and recommended document; however, the Audit Memo may be used if deemed to be more appropriate by the Audit Team (e.g. Special Projects, Proactive Assurance Projects, and Internal Audit Requirements).

Note: There are additional requirements for reports related to audits being conducted under privilege and at the direction of Legal. Refer to the Attorney Client Privilege section in the Appendix for further detail.

Instruction

D.1.1 Audit Summary Page

The first page of the audit report serves as a summary, providing a high-level audit background, objective and scope of the audit, and conclusion and findings summary. A "Draft" watermark should be included on the Audit Report until all applicable levels of review have occurred and the report is ready for Final Distribution.

Report Header: The top of the report includes the audit name and project number and identifies the document as either an Audit Report or Audit Memo. The report is addressed to the appropriate business management responsible for the areas being reviewed within the audit, with the level of management required to be a Vice President of above within the applicable business area.

Audit Background: Brief background on the business area under review to provide context, such as number of transactions, revenue, number of employees, etc. Background should provide context as to where we are within the organization, such as business segment or department, and rationale for why the audit is being performed. This may include details over which items or areas were in scope and which were out of scope for the audit. Information and language included in the Executive Summary section of the Kick-Off Deck can be leveraged when drafting the Background section of the Audit Report.

Objective and Scope: The scope, including period under review, and objective(s) from the Kick-Off Deck is included in the audit summary page.

Conclusion and Findings Summary: The section begins by providing the Overall Control Environment Opinion and includes a conclusion statement based on that opinion. The conclusion statement provides context to the reader to interpret the Control Opinion. The report template includes all four Control Opinion options; the non-applicable opinions should be deleted. The Audit Team should use discretion to determine the appropriate control opinion based on the scope of the audit, the number of findings and the business areas involved. Following the conclusion statement, each finding and observation should be listed within the Reportable Findings Table.

Control Opinion	Description
Effective	The control environment (design and execution) provides reasonable assurance that key risks are adequately mitigated. Any issues observed do not threaten the achievement of business objectives. Effective opinions usually involve only Low rated, or no, issues.
Mostly Effective	Except for the conditions noted, the control environment provides reasonable assurance that key risks are adequately mitigated. The achievement of business objectives *may* be threatened by either multiple issues throughout the process or a single critical issue within the process. Near-term action is suggested to assure adequate key risk mitigation. Mostly Effective opinions usually involve only Moderate and/or Low issues.
Improvement Needed	The control environment provides limited assurance that key risks are mitigated. The achievement of business objectives is *likely* threatened by multiple issues throughout the process or a critical issue(s) within a single portion of the process. Prompt action is necessary to prevent the process from becoming Ineffective. Improvement Needed opinions usually involve High and/or Medium rated issues.
Ineffective	The control environment provides little to no assurance that key risks are mitigated. The achievement of business objectives is currently threatened. Immediate management attention is needed to remediate the issue identified. An Ineffective opinion may include multiple High rated issues.

D.1.2 Findings & Management Action Plans

Findings are items identified during the audit (e.g. testing exceptions, control gaps identified) which have a risk impact to the organization and an associated Management Action Plan to remediate the issue. Findings and Management Action plans should be discussed with management to reach alignment prior to holding the Close Meeting. This section provides the details of the findings and management action plans, which include the following elements:

- **Finding Title** – Provides clarity as to the finding as well as to the area impacted.
- **Issue Details** – Describes the finding observed, the impact/risk to the business, the root cause and the exceptions supporting the finding.
- **Rating** – Provides clarity over the significance of a given finding based on the risk impact to the respective segment or enterprise. Each audit finding should be rated based on the criteria below.

Rating	Criteria
Low	Low Findings may not warrant immediate attention; however, management should still address the Finding to mitigate increased risk. The presence of a low Finding may not pose significant risk to the achievement of business objectives, but multiple Low Findings in a related area could pose such a risk. Controls are mostly in place and operating effectively, except for noted exceptions. Controls may need strengthening or other improvement opportunities may exist.
Medium	Medium Findings require near-term attention from management of the business, potentially including senior management and will be brought to the attention of the Audit Committee. Without timely resolution of a Medium Finding, the impact of the underlying problem could lead to increased risk. The presence of a Medium Finding may threaten the achievement of business objectives, and/or leave the business open to compliance concerns. Controls in place may only partially mitigate risks, or a key control may not exist at all.
High	High Findings require immediate attention from management and will be brought to the attention of the Audit Committee. The presence of a High Finding actively threatens the achievement of business objectives, and/or may pose a high likelihood for compliance violations or vulnerabilities. Current controls in place do little or nothing to mitigate key risks, or controls do not exist. The realization of the underlying risk, if left unmitigated, would have a noticeable impact on the enterprise, such as harm to a large number of stakeholders, material misstatements of financials, significant fines, penalties, and sanctions from regulatory bodies, or impact to the reputation of the company.
Deficiency	If SOX related, rating categories are assessed as Deficiency, Significant Deficiency, or Material Weakness. Audit Teams should perform appropriate due diligence over assessing the SOX impact, and outreach to the SOX and Controls Assurance Team may be necessary.
Observation	See Observation guidance in the following section.

- **Management Action Plan** – Describes specific management actions to address the root cause(s) of the finding and mitigate the risk(s) going forward. The specific language included within the Management Action Plan may be drafted by management, or by Internal Audit with information provided by management. Management's target completion date should also be noted within the Management Action Plan, as this date differs from the Target Completion Date noted below, which incorporates subsequent validation efforts by Internal Audit.
- **Remediation Owner** – The main point of contact and member of Management for the action plan, typically at the Director level or above.
- **Remediation Due Date** – Provides the estimated date for completion of the Management Action Plan and subsequent validation efforts by Internal Audit. Management Action Plans may be reflected as "Completed" within the report if they have been implemented by Management and validated by Internal Audit *prior to* Audit Report Issuance.

Refer to the Kick-Off Deck Template for guidance over the escalation protocol if challenges arise in reaching alignment with Management regarding Findings and Management Action Plans.

D.1.3 Observations

Audit Observations are those items that are not sufficiently significant to be deemed a reportable issue, but the Audit Team determines should be brought to Senior Management's attention. These items identify opportunities for improvement to business area processes. These may be items that have minimal risk impact and do not rise to the level of a Low issue (as per the finding rating guidance). A recommendation to Management to address each Observation may be included, if applicable; however, formal Management Action Plans are not prepared nor tracked. Additional context may be included to reflect steps Management has already taken or plans to take to address the Observation.

D.1.4 Standard Terminology

This section provides the standard definitions for the Overall Control Environment Opinions and Finding Ratings. This section should not be changed from the version included within the Audit Report Template.

D.1.5 Distribution List

This section notes the individuals to receive the report in addition to the addressee. Generally, business colleagues Manager and above should be included, however auditor discretion may be used to include additional contacts below the Senior Manager level. The Business Planning Committee (BPC) section is standard for all reports and should only be modified in the event there are additional BPC members who apply to the specific audit. Segment firewall and segregation of duties concerns should be considered when determining the Distribution List. Refer to Internal Audit's Audit Report Template for additional guidance.

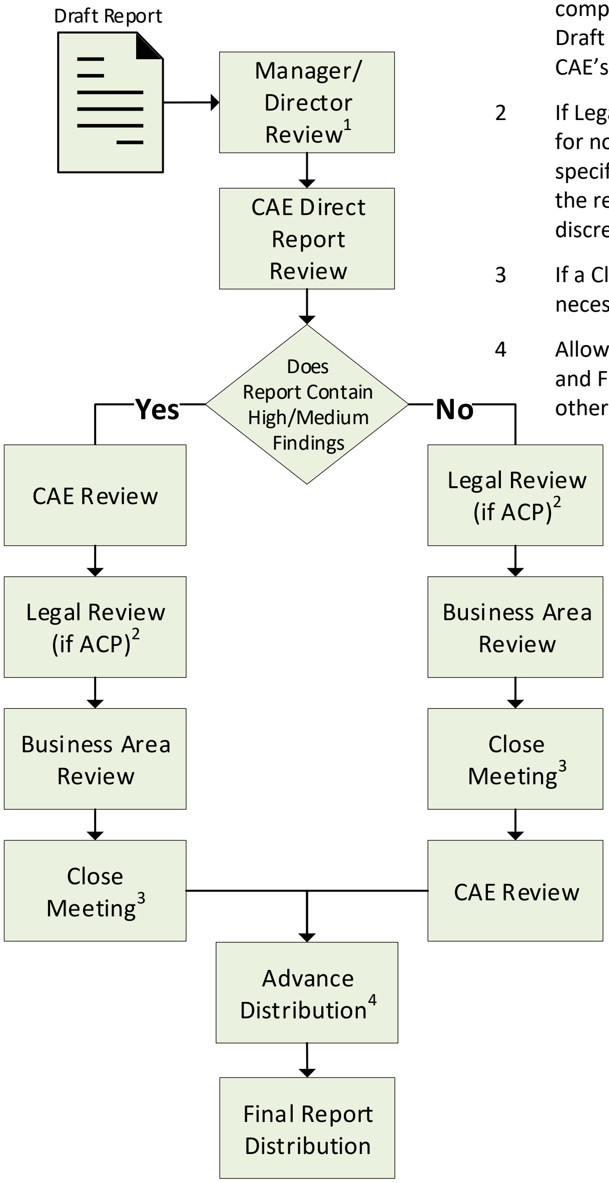
D.2 Audit Report Review and Close Process

Purpose

The purpose of the report review process is to ensure the quality and accuracy of the final Audit Report.

Instruction

D.2.1 Audit Report Review Workflow



1 All applicable levels of Internal Audit Management are responsible for completing their review before the Draft Audit Report is provided to the CAE's Direct Report for review

2 If Legal review is deemed necessary for non-ACP audits, based on a specific risk identified, Legal review of the report may be requested at the discretion of the Audit Team

3 If a Close Meeting is deemed necessary by the Audit Team

4 Allow two business days between AD and Final Distribution, unless directed otherwise

D.2.2 Closing Meeting

Once the draft audit report is reviewed within IA, a copy may be shared with business management to allow for review and confirmation of content.

At the discretion of Audit Management, a Closing Meeting may be scheduled. The draft Audit Report should be provided in advance, emphasizing management's review prior to the meeting to allow for targeted and impactful discussions. The Closing Meeting is scheduled by a member of the Audit Team, inviting applicable business owners as deemed necessary. Reportable findings should be discussed during the Closing Meeting to confirm action plans, responsible parties, and target completion dates for each issue.

If a Closing Meeting is not held, the Audit Team must obtain confirmation from management of the report's factual accuracy and their agreement to the Management Action Plans prior to moving forward to Advanced Distribution. At a minimum, positive confirmation must be obtained from the report addressee, or designated delegate, and applicable responsible parties for each Management Action Plan. Additional confirmations may be obtained from other members of management and/or stakeholders, at the discretion of Audit Management.

D.2.3 Final Review

All workpapers related to the Control Analysis and Fieldwork and Testing Phases should be completed and reviewed in the audit repository system *prior* to the issuance of the audit report. Audit Management evidences their oversight and involvement through their reviews evidenced across Work Steps, demonstrating their comfort obtained that the audit was performed in accordance with this methodology, particularly on the following Work Steps:

- Kick-Off Deck
- RCA Review
- Fieldwork and Testing Review
- Director and CAE Review of the Draft Audit Report

D.2.4 Advance Distribution

After the Close Meeting, or alignment with the business on the draft audit report, an Advance Distribution is made by a member of Internal Audit Management for *all* Audit Reports, regardless of opinion or rating of findings. This communication is sent to the applicable Senior Leaders, including direct reports of the CEO and other business contacts as deemed appropriate by the Audit Team. The Advance Distribution is designed to provide advance notice of the contents of the Audit Report to any colleagues, through the CEO's direct reports, who may not have attended the Kick-Off Meeting and/or Close Meeting. IA Management should utilize professional judgment when assessing the senior leaders to include on the Advanced Distribution. IA then issues the final report within two days of this distribution, unless directed otherwise.

D.2.5 Final Audit Report Distribution

Final Audit Reports are to be distributed by the CAE or the CAE's administrator/designee. Reports will be distributed to the applicable individuals based on the Distribution List. The "Draft" watermark should only be removed prior to the Final Audit Report Distribution. A final copy of the Audit Report should also be stored in the central department file (i.e. SharePoint).

Section E: Post-Issuance Phase

Post-Issuance Phase Overview

The purpose of the Post-Issuance Phase is to close out the audit and perform post-audit activities. The Post-Issuance Phase includes the procedures to record findings, close out the projects within the audit repository system, evaluation of auditor and audit performance, and the validation of Management Action Plans (MAPs) in accordance with the Audit Report.

Note: There are additional requirements for documentation related to audits being conducted under privilege and at the direction of Legal. Refer to the Attorney Client Privilege section within the Appendix for further detail.

E.1 Audit Findings

Purpose

The purpose of entering findings into the audit repository is to facilitate reporting and tracking and validation of remediation of audit findings.

Instructions

Following the issuance of the final Audit Report, a member of the Audit Team records reportable findings within AuditBoard to allow for the proper monitoring and tracking of Audit Findings. The details of each finding recorded within AuditBoard should match the details included in the respective Final Audit Reports. Findings should be entered into AuditBoard prior to the completion of the Audit Close Checklist and closing of the audit.

E.1.1 Completion Status

As findings are recorded within Audit Board, the Audit Team member entering the records the applicable "completion status" based on completed Action Plan steps. Please see the table below for the possible completion statuses in which a finding may exist.

Status	Meaning
Pending Remediation	• Business is aligned with the corrective MAP and the report has been issued • IA has not tested and validated the MAP
Closed *	• Business has completed their corrective MAP • Internal Audit has tested the business's MAP and concluded risk identified in the initial audit finding is successfully mitigated
** These statuses will be elaborated upon more in-depth within the Findings Follow-up section*	

Newly entered findings may include an open/on schedule status, as the Final Audit Report was issued with the business's agreed-upon corrective MAPs. However, instances may occur where the business instituted and carried out their corrective MAP prior to the issuance of the Final Audit Report. In these instances, the finding should be recorded with the appropriate completion status denoted.

E.1.2 Finding Follow-up

Once a finding has been recorded within Audit Board, it is the responsibility of the assigned member of the Audit Team to monitor and track the status of their findings. See the findings follow-up section for details on the steps to validate and close findings.

E.2 Audit Close Checklist

Purpose

The purpose of the Audit Close Checklist is to self-assess adherence to IA's internal procedures as defined by this Methodology document. Such self-review encourages compliance with the IIA Standards and allows the opportunity for continual improvement of individual auditors, audit teams, and the IA department as a whole.

Instruction

Upon issuance of the final Audit Report, a member of the Audit Team is required to complete an Audit Close Checklist. The Audit Close Checklist is comprised of a series of questions used to verify appropriate audit procedures were followed during the Planning, Fieldwork and Testing, and Reporting Phases of an audit. Questions may be answered with either a Yes, No, or Not Applicable response. All "No" and "N/A" responses should include a written comment elaborating why a deviation from the applicable standard/procedure occurred. Completed Checklists are submitted to the respective Managers for their review and sign-off prior to closing the Audit Project.

E.3 Closing Projects

Purpose

The purpose of closing the project audit repository is to ensure all documentation is closed for further editing.

Instruction

Following the issuance of the Final Audit Report, the Audit Team shall complete audit closing activities within five business days in the audit repository system. The Audit Team should verify the following and notify the assigned Manager that an Audit is ready to be closed.

- Pertinent workpapers were uploaded to the audit repository system
- Follow-ups, questions, and coaching notes are cleared or closed
- Superseded documents, drafts and duplicate documents are deleted
- Workpapers are reviewed and signed-off on by the appropriate level of oversight (Audit Lead, Audit Manager, Director, etc.)
- Reportable findings are appropriately entered into the system of tracking and retention

E.4 Audit Survey

Purpose

The purpose of Audit Surveys is to drive continuous improvement and help Internal Audit aggregate feedback from the respective business area(s) on what went well during the project and areas of opportunity for the team to reflect on going forward.

Instruction

Audit teams will be responsible for creating and sending audit surveys from AuditBoard within one week of the final report issuance. The audit survey seeks to collect feedback from the business area regarding aspects of the project that went well, as well as areas of opportunity for the team to consider going forward. The Internal Audit Administration Team is responsible for summarizing and anonymously sharing results of the surveys with the respective project team. The summarized results show general trends, both positive and negative and should be used to assess the project.

The audit survey recipients would typically include report addressee(s), as well as those business contacts the audit team worked most closely with throughout the project (such as any key contacts that assisted with walkthroughs and testing).

E.5 Audit Staff Evaluations

Purpose

The purpose of audit evaluation is to provide feedback and to reflect on the experience of the audit: areas done well and where opportunity exists for improvement.

Instruction

At the end of each audit the members of the Audit Team should reconnect as a group to reflect on their ability to meet the expectations set at the beginning of the Audit. Feedback may cover areas such as individual auditor performance, audit outcome, and Business Area feedback. Per management's discretion, formal written feedback may be collected at the end of audit. The assigned Audit Manager determines which members of the Audit Team are responsible for reviewing colleagues on the Team. A formal template/questionnaire is available to aide in the assessment of auditor performance. Written documentation is prepared and/or collected by the Manager upon completion, relayed to the appropriate individuals, and retained for performance evaluations.

E.6 Finding Follow-up

Purpose

The purpose of finding follow-up is to verify management completed the agreed-upon MAPs sufficiently and in a timely manner to address the findings identified during an audit.

Instruction

E.6.1 On-going Communication

To aid in verifying MAPs are completed on time and/or any potential threats to timing are noted, assigned "Audit Contacts" are responsible for monitoring finding due dates and reaching out to the business for status updates prior to the listed deadline. At a minimum, the auditor should contact the business 60 days in advance of the Target Completion Date in the report to ensure the MAP's completion is on schedule to be completed and validated by the assigned due date. As part of any finding follow-up communications with the business, the Auditor should confirm each responsible party up to, and including the VP, are copied. Any findings or important updates regarding MAPs noted during these communications should be logged and recorded within the finding's Audit Committee Status field.

E.6.2 Due Date Extensions

If the business is unable to complete management's agreed-upon MAP by the initial due date, the assigned Audit Contact must obtain an explanation for the delay, assess management's process to correct the issue, and when they expect the updated MAP to be completed. Any changes to MAPs, or their due dates, must be presented to and approved by the assigned Audit Manager on the finding. Due date extensions should not be common occurrence and only allowed in one-off situations. If a finding includes a Medium or High-risk rating, it is the assigned Audit Contact's responsibility to verify the CAE is copied on any communication of revised due dates. In addition, if a Medium or High finding is past due 30 days or greater from the original due date, IA Management is responsible for determining the level and extent of involvement required by the CAE.

E.6.3 Finding Validation Procedures

Auditors should exercise professional judgment in determining the approach and extent of testing procedures needed to validate MAPs and close out the related finding. Test plans and sample sizes should be designed to ensure supporting documentation is sufficient to verify, with reasonable assurance that the MAP is appropriately completed, and the underlying risk mitigated. Supporting documentation must be obtained, reviewed, and approved by the Audit Team for each recorded finding, regardless of risk or deficiency classification. See examples of different validation procedures that could be taken in the scenarios below:

	Issue	Action Plan	Validation
1	The vendor names entered into Mainframe do not match the vendor names on the Vendor Information form.	The business will retrain AP vendor setup employees on the appropriate setup process. An additional level of review will be added to ensure all vendor setups are checked for accuracy.	IA will obtain evidence of the employee retraining process (i.e. meeting invite, training documents, etc.). For a sample of new vendor set-ups (post action plan), IA will verify that vendor information agrees between Mainframe and the vendor form, as well as inspect for evidence of the additional level of review was performed.
2	Omnicare Pharmacies are not completing their required monthly Prescription Validation self-assessments.	The business will recommunicate the respective policy, send out a reminder to all pharmacies a week prior to the due date, and follow-up with any pharmacy that does not submit an assessment on time.	IA will obtain a copy of the policy recommunication email, a copy of the reminder email sent to all pharmacies, and for a sample of pharmacies that did not complete the self-assessment on time – a copy of the business's follow-up communications with said pharmacies.

Auditors should follow the appropriate general documentation and naming conventions outlined in the Fieldwork and Testing Phase methodology when compiling workpapers as part of validation testing. Note variations to the standard Fieldwork & Testing methodology may exist, due to the nature of validation testing as opposed to normal fieldwork; those differences are noted below.

- ***Leadsheets:***

  A specialized narrative based leadsheet exists for documenting the results of validation testing. The validation leadsheet outlines the following areas:

  - **Objective** – describes the MAP
  - **Procedures** – steps being taken to validate the MAP
  - **Results/Observations** – descriptive results of validation testing
  - **Conclusion** – MAP is complete and validated, or has failed

  This leadsheet is used in place of the standard leadsheet template but does not replace the need to include accompanying supporting workpapers.

- ***Naming Convention***:

  The following naming convention is required for validation supporting workpapers:

  [*Audit Number*] - [*Finding Number*] – [*Type of Document i.e. leadsheet, clean copy, failed copy*]

E.6.4 Failed Validation Testing

In instances where validation testing of a MAP failed, the assigned audit contact should document the exception as follows:

- Record the failure on the validation leadsheet
- Document the exception sample
- Update the Audit Committee Status for the failure accordingly (i.e. Status log)

Testing documentation noting the failure (validation lead sheet & examples) should be kept in the audit repository system for retention purposes.

Upon confirmation of a MAP's failure, the assigned audit contact should notify the respective Audit Manager of the finding. The assigned audit contact and manager should work with the business to determine whether the current MAP needs to be modified and the appropriate next steps. For Medium and High rated findings with failed validation, IA Management should notify the CAE of the failure and the extent of involvement required.

In most instances when validation testing fails, the corresponding due date for the MAP is extended to allow for the appropriate corrective action. As such, the assigned audit contact shall follow the same Due Date Extension process noted in the standards above.

E.6.5 Closing an Audit Finding

Upon completion of effective validation testing, the assigned Audit Contact uploads supporting documentation to the respective audit repository system, updates any necessary statuses to denote the results of the testing, and inform the respective IA manager that is ready for their review and sign-off. Once the IA Manager reviews and approves the audit validation workpapers, the finding record is closed.

Note: There are additional requirements for finding follow-up actions related to audits being conducted under privilege and at the direction of Legal. Refer to the Attorney Client Privilege section in the Appendix for further detail.

Appendix

Overview

The appendix contains materials which support auditors and the audit process in executing the Internal Audit Methodology.

AP.1 Quality Peer Review (QPR)

Purpose

The purpose of Internal Audit (IA) Quality Peer Review (QPR) is to provide guidance around the IA Peer Review process ensuring quality of the IA output. Selected audits will be assessed on adherence to internal procedures as defined by the methodology guidance. IIA standards recommend periodic reviews with continuous feedback and proactive improvements. The peer review process allows continual improvement of individual auditors and project teams.

QPR Roles include:

- QPR Reviewer – the individual assigned a project to review, the project will be from a different team than this individual is on to provide independence
- QPR Manager – the manager of the QPR Reviewer
- Manager Under Review – the manager whose project is being reviewed
- QPR Coordinator – the individual assigned to coordinate the QPR process, including compiling the list of completed projects each review period and assigning the QPR Reviewers

Instruction

AP.1.1 Initiating the QPR

On a semi-annual basis, the Chief Audit Executive (CAE), or the applicable designee, will select a completed audit for each Manager for QPR testing. The review will take place in both the first half of the year and the second half of the year, for a total of two audits reviewed annually per Manager.

The CAE, or the applicable designee, will make the selections for review, ensuring each Manager is selected for review at least twice annually. All audits and other projects are eligible for review. The QPR Coordinator will provide a list of completed audits by Manager during the time period being reviewed to the CAE. Certain types of audits will be excluded from the selection process including proxy reviews, or audits performed by an outside auditor since these audits would not be performed in accordance with CVS IA Methodology. Also, certain other projects may have several elements of the Methodology that are not applicable; in these situations, an additional audit may need to be selected for review to accurately assess the Manager's compliance with the Methodology.

AP.1.2 Performing the QPR

The review is performed using the Quality Peer Review Checklist, which includes the attributes a QPR Reviewer will verify were appropriately addressed and included within the respective audit file. Each attribute has a related score, which drives the overall QPR score at the end of the review. Attributes are assessed using the following attributes.

QPR Attribute	Description
Attribute Met (AM) [1pt]	The attribute was consistently met as supported by the documentation retained within the audit file. An attribute may not have been traditionally met within the documentation but was adequately supported with other documentation within audit file that explicitly states this attribute was not followed for this project, the rationale for the variance, and any related approval by IA management, if necessary. All applicable components must be met and consistently applied across relevant workpapers.
Inconsistently Satisfied (IS) [0.5pt]	The attribute was inconsistently met by documentation within the audit file. They might have met the attribute for a portion of the workpapers but not consistently. For example, eight leadsheets met the Methodology, but two did not. The QPR reviewer should add rationale as to why they assessed this attribute as such.
Improvement Opportunity (IO) [0pt]	The attribute was consistently not supported by documentation retained within the audit file. Critical components are not included, or attributes are applied in limited instances. The QPR reviewer should add rationale as to why they assessed this attribute as such.
Not Applicable (N/A) [1pt]	This attribute does not apply for the given project. Rationale for why the attribute did not apply should be added by the QPR reviewer within the checklist. Attributes that do not apply for the project should be explained by documentation within the audit file, providing contemporaneous explanation and rationale for why that attribute was not followed. If several elements are identified as N/A, an additional project may be selected to appropriately assess the Manager Under Review.

The review may be performed by a Staff or Senior Auditor with at least a year of experience but must require oversight by a QPR Manager. The QPR Manager must agree with the opportunities identified by the Staff or Senior performing the review, and responsible for providing the results to the Manager Under Review.

Once the initial review is completed and agreed to by the QPR Manager, the QPR Manager will share the results of the review with the Manager Under Review to discuss the results and any questions. Given the complexity of many IA Audits, some of the initial review results may be explained by one of the Audit Team Members; however, Auditors should always strive to include high quality documentation that can be easily and readily understood by a reasonably educated individual who was not associated with the specific audit. In this situation, the QPR Reviewer should note an observation regarding how the Audit Team may enhance the attribute going forward, even if it does not result in a QPR score deduction for this Audit.

After the QPR Reviewer and their QPR Manager discuss the initial results with the Manager Under Review, they will make any necessary updates and add their Observation Disposition for each Inconsistently Satisfied and Improvement Opportunity Observation. The Observation Disposition includes the specific actions for the IS or IO Observation. Following the discussion with the Manager Under Review and completion of the Peer Review Checklist, the QPR Reviewer and QPR Manager sign off on the completed template, which is provided to the Manager Under Review's applicable CAE Direct Report for their acknowledgement and sign-off.

Any disagreements with the QPR Reviewer's assessment should be discussed and mutually resolved between the Manager Under Review and the QPR's Manager. Consultations with the Methodology Team for interpretation and clarity regarding the methodology guidance should occur, as needed. If the Manager Under Review and QPR Manager cannot come to an aligned consensus, the matter should be referred to the QPR Coordinator. If the matter needs further escalation, it should be provided to the respective Direct Report of the Manager Under Review. If the Direct Report and QPR Manager cannot come to an agreement, the disagreement should be noted within the QPR Peer Review Checklist and is referred to the CAE for final determination. Following resolution, such situations should be referred to the Methodology Team to consider possible updates to the Methodology to address the noted disagreement.

AP.1.3 Communicating QPR Results

Following the semi-annual completion of QPRs, the results are compiled and formally documented via an Audit Memo for review by the Methodology Team and the CAE. Once reviewed, the CAE will share the results and opportunities with the IA Department, noting areas for continued focus and improvement. Audit Managers should strongly consider discussing these results with their teams when results are distributed.

AP.2 Attorney Client Privilege Audits

Purpose

Legal may request IA conduct certain reviews to facilitate the Legal Department's (or outside counsel's) representation of CVS Health and its subsidiaries ("the Company") in connection with a pending or anticipated litigation or other circumstances. Such reviews are intended to help the Company's Legal counsel understand technical controls/issues in the relevant areas. When selected projects on the Audit Plan are performed at the direction of Legal counsel in connection with the seeking or rendition of Legal advice and services, some portions of the audit process, reporting, and workpapers are enhanced to ensure these projects are protected by the attorney client privilege and/or work product.

Instruction

AP.2.1 Identification, Planning and Scoping

IA and Legal will periodically discuss areas for review. Legal will identify projects needed to facilitate the provision of Legal advice and services. The following steps apply to each project Legal has requested to facilitate the representation of the Company. Otherwise, there is no change from defined departmental standards.

IA and Legal shall meet periodically to review potential topics for the IA Audit Plan. During those discussions, or at other points during the year, Legal may identify areas for review that are needed to facilitate Legal's representation of the company. To initiate a review that is necessary to facilitate Legal's representation of the Company, Legal will send a request to IA outlining the reason the review is needed and its scope. This request should be maintained with the workpapers. Based on Legal's request, IA will send a draft Kick-Off deck to the respective in-house attorney for review prior to distribution.

IA will add "Prepared at the Request of Legal Counsel: Privileged & Confidential Communication" ("the Legend") to the header of each page of the Kick-Off deck and in the Kick-Off meeting request.

Other relevant stakeholders may receive a copy of the Kick-off materials as directed by Legal. IA will keep the in-house attorney apprised with the status of the audit, including inviting the respective attorney to the Kick-Off meeting, and any other applicable meetings, to discuss the status of the project.

AP.2.2 Communications

Intra-department (within IA): Communications relating to conclusions, findings, and action plans (whether they be final or still in the vetting process) will include the Legend in the body of the email and attached documents. All other IA internal communications regarding the project are to be executed based on departmental standards.

Inter-department: Communications relating to conclusions, findings, and action plans (whether they be final or still in the vetting process) will include the Legend in the body of the email and attached documents and the designated in-house attorney should be copied on each of these communications. All other communications will be marked "Privileged & Confidential; Prepared at the request of Legal; Attorney Work Product." This may include, but is not limited to, the following: meeting invitations, information requests etc.

Audit Reports & Memos: Audit Reports and Memos should be addressed to the designated in-house attorney with business owners listed in the cc: section. Audit Reports and Memos (draft and final versions) should include the Legend in the footer of all pages, including the cover page, and the body of the email when distributing the report.

Any draft report circulated for comments should be sent to both the designated in-house attorney and the relevant business employees as directed by Legal. The emails containing the draft report should prominently state: "If responding via email, please Reply to All or copy [attorney] as this project has been directed by Legal and [attorney] is reviewing these materials as well. Do not copy others or forward this email to others."

After confirmation with the designated attorney, which should be retained in the workpapers, the final Audit Report or Memo should be distributed by the Chief Audit Executive, and the designated attorney should be the primary recipient on the email, consistent with the Audit Report or Memo distribution. The email should prominently state: "This audit was performed at the direction of legal counsel and/or in connection with the seeking or rendition of legal advice and services."

Departmental Reporting Containing Audit Findings

Audit Committee Reporting: Materials are required to be approved by Legal in advance of distribution as part of the enterprise Audit Committee process. Audit findings will include the Legend in the footer of each page. Work product may be uploaded to Diligent, the Company's electronic board book system, and should be appropriately restricted, including from third parties (i.e. External Auditors).

Inter-department Reporting: Compliance Committee Meetings and other meetings with management: ACP Findings should be excluded from meetings which contain attendees that were not included in the Audit Report distribution. Audit findings will include the Legend in the footer of each page. Distribution of ACP Audit findings outside IA may only be done by or at the direction of Legal.

Third Parties: Any documents related to a privileged audit, or otherwise privileged, should be reviewed by Legal prior to sharing the documents outside of the Company, including the external auditors. Any distribution of privileged documents will be done by or at the direction of Legal. IA may provide the external auditors with a verbal update related to any pertinent findings in support of the external auditor's role.

AP.2.3 Audit Workpapers

Electronic Workpapers

SharePoint: Draft workpapers may be maintained in a separate electronic folder in SharePoint with access limited to team members working on the review. Once working documents are completed and included within the department's system of record, any working files should be deleted from SharePoint, as well as local drives. Workpapers shall include the Legend.

Audit Board: Workpapers stored in Audit Board will be restricted to team members working on the review and IA Management via role-based security. Audit Projects shall be updated to ensure the project is denoted as ACP, the appropriate legal contact is noted, and the IA staff is appropriately assigned. Properly denoting as ACP will ensure the appropriate legal Legend is applied; however, all workpapers shall also include the legal Legend. Audit issues should be denoted in Audit Board as "under privilege" and denote the appropriate Legal contact. Supporting documentation obtained for closing and validating audit findings and uploaded to Audit Board should be noted with the Legal footer.

Hard Copy Workpaper Binders: The binder cover will contain the Legend. Workpapers contained within should be documented consistent with departmental standards.

AP.3 Patient Safety Work Product Audits

Purpose

Internal Audit ("IA") conducts reviews of activities performed by CVS business unit providers ("CVS Providers"). Certain of those reviews could improve patient safety and/or the quality of health care delivery by the respective CVS Provider. Those reviews, referred to herein as "Patient Safety Internal Audits," are conducted in accordance with, and subject to the protections of, the Patient Safety and Quality Improvement Act of 2005, 42 U.S.C. 299b-21 through 42 U.S.C. 299b-26 (the "Patient Safety Act").

A Patient Safety Internal Audit is conducted by IA operating within the patient safety evaluation system ("PSES") of the CVS Provider whose activities are the subject of the review and constitutes the deliberations and analysis of the PSES of that provider. The information developed and/or assembled in a Patient Safety Internal Audit is confidential and privileged patient safety work product ("PSWP") and shall be labeled accordingly. All information developed and/or assembled in connection with a Patient Safety Internal Audit shall be reported by IA to Enterprise Patient Safety Organization, L.L.C. ("EPSO").

PSWP developed and/or assembled in connection with a Patient Safety Internal Audit may be disclosed to individuals outside of the CVS business unit provider within whose PSES the review is conducted for the following limited purposes: (1) enterprise patient safety activities; (2) enterprise risk management and compliance; (3) legal advice and consultation; and (4) education and training.

All recipients of such PSWP shall maintain it securely and in strict confidence, and may not further disclose it; however, any failure to comply with these obligations shall not alter the confidential and privileged nature and character of such PSWP.

Instruction

AP.3.1 Identification, Planning and Scoping

IA will consult with the CVS Providers to discuss areas for review, consulting Legal as needed to determine whether a review will be a Patient Safety Internal Audit. The following steps apply to each Patient Safety Internal Audit. Otherwise, there is no change from defined departmental standards.

- IA, CVS Provider designees (those with direct responsibility over the patient safety evaluation system for the respective business unit), and Legal shall meet periodically to review potential topics for the IA Audit Plan. During those discussions, or at other points during the year, a CVS Provider, in consultation with Legal, may designate areas for review that should be performed as a Patient Safety Internal Audit. This designation should be maintained with the workpapers.
- Based on the designation of a review as a Patient Safety Internal Audit, IA will send a draft Kick-Off Deck to the respective CVS Provider designee and in-house attorney for review prior to distribution.
- IA will add "*PRIVILEGED & CONFIDENTIAL: PATIENT SAFETY WORK PRODUCT UNDER FEDERAL LAW* ("the PSWP Label") to the footer of each page of the Kick-Off Deck and in the Kick-Off meeting request.
- The Kick-Off Deck and final drafts of other documents created in connection with a Patient Safety Internal Audit must be reported to Enterprise Patient Safety Organization ("EPSO") by sending the document to a representative of EPSO.
- IA will keep the CVS Provider designee and in-house attorney apprised with the status of the audit, including inviting the respective attorney to the Kick-Off meeting, and any other applicable meetings, to discuss the status of the project and advise on matters related to the Patient Safety Act.

AP.3.2 Communications

Email Communications

- All communications, both internal and amongst departments, exchanged in connection with the Patient Safety Internal Audit should include the PSWP Label.

Audit Reports & Memos

- Audit Reports and Memos should be addressed to the CVS Provider designee and business owner directly responsible for the process under audit with the designated attorney and EPSO, or a representative thereof, listed in the cc: section. External parties, such as external auditors, should not be a recipient of the report or memo.
- Audit Reports and Memos (draft and final versions) should include the PSWP Label on all pages, including the cover page, and the body of the email when distributing the report.
- Audit Reports and Memos should include the following language within section II. Scope & Objective:

> *"This audit was conducted by Internal Audit within the [CVS Retail/Caremark Mail/Caremark Specialty/Omnicare/MinuteClinic] Patient Safety Evaluation System ("[Retail/Caremark Mail/Caremark Specialty/Omnicare/MinuteClinic] PSES") and*

constitutes the deliberations and analysis of the [Retail/Caremark Mail/Caremark Specialty/Omnicare/MinuteClinic] PSES. The information contained herein is confidential and privileged patient safety work product ("PSWP") and has been labeled accordingly. The distribution of this PSWP to individuals outside of [CVS Retail/Caremark Mail/Caremark Specialty/Omnicare/MinuteClinic] is for the following limited purposes: (1) enterprise patient safety activities; (2) enterprise risk management and compliance; (3) legal advice and consultation; and (4) education and training. All recipients of this PSWP shall maintain it securely and in strict confidence, and may not further disclose it; however, any failure to comply with these obligations shall not alter the confidential and privileged nature and character of this PSWP."

- Draft Audit Reports and Memos should be shared with both the CVS Provider designee and designated attorney prior to distribution and confirmation of alignment should be retained in the workpapers.
- The final Audit Report or Memo should be distributed from the IA mailbox or via the Chief Audit Executive, and the designated attorney and EPSO should be included as recipients on the email, consistent with the Audit Report or Memo distribution. The email should include the PSWP Label.

<u>Departmental Reporting Containing Audit Findings</u>

- Audit Committee Reporting
  - Materials are required to be approved by Legal in advance of distribution as part of the enterprise Audit Committee process.
  - Audit findings will include the PSWP Footer on each page.
  - Work product may be uploaded to Diligent, the Company's electronic board book system, and should be appropriately restricted for purposes other than those permitted under the limited purpose disclosures, including from third parties (i.e. External Auditors).
- Inter-department Reporting
  - Compliance Committee Meetings and other meetings with management: PSWP should be excluded from meetings which contain attendees that were not included in the Audit Report distribution.
  - Audit findings will include the PSWP Label on each page.
  - Distribution of PSWP outside IA may only be done by or at the direction of the CVS Provider designee, in consultation with Legal.

<u>Third Parties</u>

Any documents related to a privileged audit, or otherwise privileged, should be reviewed by Legal prior to sharing the documents outside of the Company, including the external auditors. Any disclosure of PSWP for purposes other than as described herein, shall only be done by or at the direction of the CVS Provider designee, in consultation with Legal.

AP.3.3 Audit File & Electronic Workpapers

- Audit Projects shall be updated to ensure the project is labeled as PSWP, the documentation managed as PSWP, the appropriate legal contact is noted, and the IA staff is appropriately assigned.

- Draft workpapers may be maintained in a separate electronic folder in SharePoint or the applicable Audit Repository (e.g. AuditBoard) with access limited to team members working on the review and IA Management.
- Documents should be handled in accordance with Internal Audit document retention policies and procedures.
- Workpapers shall include the PSWP Label.

AP.3.4 Issue Management

- Audit findings should be denoted with the Patient Safety Label in the respective audit repository (e.g. AuditBoard) with the appropriate Legal contact listed.
- Supporting documentation obtained for closing and validating audit findings and uploaded to the respective audit repository should be labeled with the PSWP Label.

AP.4 Proactive Assurance Projects

Purpose

The purpose of Proactive Assurance Projects is to provide assistance to business partners regarding control design considerations in advance of control operation, and retrospective auditing. This type of project applies when management implements or changes the design of a control, process, or system, usually characterized by a designated business project, to achieve a critical business objective. Depending on the size and nature of the change, IA may evaluate the design of proposed control(s) or critical phase(s) of a multiple stage project and provide an opinion to in advance of implementation.

Instruction

Projects should follow the standard audit life cycle as outlined in the Planning and Scoping, Control Analysis, Fieldwork & Testing, Reporting, and Post-Reporting Phases. However, due to the varying types of projects performed, the core audit methodology approach may be customized to accommodate each type of audit performed. Audit strategy and procedures should be appropriately discussed and agreed upon between IA and business management, with deviations in methodology and accompanying rationale documented within the workpapers as well as in the Audit Close Checklist.

AP.4.1 Planning & Scoping

The purpose of a Proactive Assurance Projects is to provide an independent opinion over specific aspect(s) of an operational process or project through testing procedures agreed upon between business and IA management. As IA generally does not review, or participate in, the entire process or project, involvement and objectives may vary depending on the nature of the agreed upon work. Proactive Assurance project are targeted to specific control(s) or business project phase(s), with IA providing an independent opinion on the evaluation of controls. Details of the extent and limitations of IA involvement should be evidenced within the appropriate documents within the Planning & Scoping Phase.

AP.4.2 Testing Procedures

Either the Risk Control Analysis, or the Audit Program Template, may be used to document the fieldwork procedures performed, depending on scope and extent of testing as determined by the IA Manager. Audit Programs are may be used in place of an RCA where testing is not risk and/or control based. Audit Programs list the objective, scope, and procedures to be performed for the applicable project. Similarly, Test Summaries may be used in place of a Test Leadsheet to document test procedures and results. A Test Summary includes the objective, procedure, results/observations and conclusion.

AP.4.3 Reporting

The Audit Memo is the preferred and recommended document for Proactive Assurance Projects. Generally, for Proactive Assurance Projects, a paragraph conclusion should be used in lieu of the traditional opinion rating, issued to business management. In lieu of Findings, Observations may be provided as opportunities for management to continue enhancing controls, to ensure they are appropriately designed and operating effectively. Observations may also include recommendations and/or monitoring items that, while not necessarily risk-based, may otherwise add value to management. Observations should be shared in real time with management, allowing for timely remediation, if applicable. In addition, it is recommended the Audit Team consider performing a post implementation review. Refer to the Reporting Methodology Standard for additional guidance on Reporting.

AP.5 Other Projects

Purpose

Other Projects may be performed to assist management in the implementation and assessment of controls as business projects are implemented or include a review of a narrowly defined scope and objective specific on business process.

Instruction

Other Projects should follow the standard audit life cycle as outlined in the Planning and Scoping, Control Analysis, Fieldwork & Testing, Reporting, and Post-Reporting Phases. However, due to the varying types of projects performed, the core audit methodology approach may be customized to accommodate each type of audit performed. Audit strategy and procedures should be appropriately discussed and agreed upon between IA and business management, with deviations in methodology and accompanying rationale documented within the workpapers as well as in the Audit Close Checklist.

AP.5.1 Types of Projects

Participation: Project Participation requires IA to advise management on controls related matters with respect to all relevant phases of a business project. IA's main objective is to identify key control points and ensure controls are implemented. Involvement and objectives can vary greatly depending on the nature of the project. IA is involved in all applicable portions of the business project life cycle and provide an opinion based on observation or inspection of testing performed by the business. When involved in Project Participation, it is critical for IA to maintain their independence and objectivity in both fact and appearance. The Audit Team must remember that while they are providing input and recommendations, management continues to own the work and IA may not perform or own any portion of management's process.

Review: A review provides limited assurance over the design and effectiveness of business controls and may include a more narrow and focused scope and objective, which will vary depending on the project.

AP.5.2 Testing Procedures

Participation: As requirements are defined, IA should work with business management to determine IA's level of involvement and any or all business meetings IA should attend. In many instances, IA may not be able to assess control objectives until the project requirement documents, where applicable, are completed and provided by the business.

The following are high-level activities IA should consider performing for each selected project:

- Understand the scope, business benefit, and strategic vision of the business project
- Understand the business project process flows and data flows
- Identify risks, key control points or objectives, and discuss control design in light of risks identified with business
- Confirm key control points/objectives are included in the project scope or business process
- Obtain evidence that the identified control points/objectives are included in project testing and documented appropriately
- Review test results of identified control points or objectives with business and confirm any critical issues are resolved
- Determine completeness and accuracy of relevant data transfers or migrations, if any
- Partner with the Sarbanes Oxley & Control Assurance (SCA) team, including communication with appropriate business and SCA Managers

Review:

Consistent with a Proactive Assurance, either a Risk Control Analysis Template, or the Audit Program Template, may be used to document the fieldwork procedures performed, depending on scope and extent of testing as determined by the IA Manager. Similarly, Test Summaries may be used in place of a Test Leadsheet to document test procedures and results.

AP.5.3 Reporting

The product of a Participation Project or Review is the Audit Report or Audit Memo, depending on scope and extent of testing, which is issued to management. The Audit Report is the preferred and recommended document; however, the Audit Memo may be used if deemed to be more appropriate by the Audit Team. Findings and Observations should be shared in real time with management, allowing for timely remediation. Refer to the Reporting Methodology Standard for additional guidance.

AP.6 Sarbanes Oxley Integrated Audit Procedures

Purpose

Provide guidance over the procedures for collaboration and execution of audits including a focus area or assessment of key or significant processes to the financial reporting process under the scope of SOX Sections 404 and 302.

Instruction

AP.6.1 Planning

As part of planning, auditors should connect with the applicable SCA Manager and/or Senior to obtain an understanding of any available SOX process documentation that can be leveraged as part of the planning phase and discuss any potential SOX concerns, if applicable. The Risk Stakeholder Input Email Template can be utilized to document the request. Supporting documentation for in scope SOX processes, consisting of process flows and related testing, can be found in the SOX Audit Repository. In the event a control that would otherwise be tested in an audit, is included in the SOX Framework for testing, the control should be carved out of the audit, unless management determines there is incremental value in also testing the control in the audit. If controls are carved out, this should be disclosed in the Kick-Off deck with a reference to reliance on the related SOX testing. For audits related to in scope SOX processes, the applicable SCA Manager should be copied on the distribution of the Kick-Off Deck.

AP.6.2 Finding

In the event a Finding is related to a SOX control or in scope SOX process, details of the Finding should be shared with the applicable IA SCA Manager upon identification. The SCA Team is responsible for assessing the information provided and determining whether the Finding should be classified as a SOX deficiency as well as confirming alignment with the SCA Senior Director. This assessment includes the completion of the "Summary of Deficiencies" document. The Audit team should provide the SCA team with any available documentation and/or knowledge to aide in the SCA Team's completion of the document. Both the SCA and core audit teams, should be comfortable with the proposed Management Action Plan.

AP.6.3 Reporting and MAP Validation

In the event an Audit Report contains a SOX deficiency, the SCA Director and Manager should be copied on the distribution of the Audit Report. The core Audit Team will add the deficiency to the Audit Repository as part of the Post Issuance process and will include the applicable SCA colleague who will be responsible for validation efforts. In the event changes are made to the Management Action Plan, including timing, the SCA Team should keep the applicable Audit Team Director and Manager informed.

AP.7 Methodology Review and Update

Purpose

The IA Methodology is the framework by which the IA Department conducts day-to-day activities. The Methodology reflects the process-oriented approach from managing audit activities to documenting the work product and were developed internally and based on industry best practices, such as the Institute of Internal Auditors (IIA).

Instruction

AP.7.1 Annual Internal Methodology Review & Reassessment

This annual review and reassessment of the Methodology is typically performed in Q3 to allow for implementation aligned with the coming audit plan year. The Methodology Team will be responsible for reviewing the Methodology, offering input to modify existing Methodology or create additional standards within the Methodology, as well as leading the effort to gather feedback from the various core audit teams. A Lead Coordinator from the Methodology Team will solicit feedback from colleagues, centrally track recommendations and discuss proposals with the Methodology Team. Conclusions reached on whether to incorporate proposed changes will be documented and communicated back to colleagues.

Modifications or additions to the existing Methodology should be the result of any changes in the audit industry, changes to the Retail, PBM, Insurance or Healthcare industries, or changes to CVS Health. Documentation to support Methodology changes will be retained for seven years. The Annual Methodology Review template should be utilized to ensure various aspects are considered when reassessing the Methodology, and conclusions reached are adequately documented.

The Lead Coordinator will compile and present proposed Methodology changes to the CAE for consideration, and any feedback will be incorporated into the proposed changes prior to final approval by the CAE. Once changes are approved by the CAE, notification of updates will be distributed to colleagues through the IA Methodology shared mailbox, and a training will be held on such updates, dependent on the depth of the changes.

AP.7.2 Internal Assessment of IIA Standards Conformance

At least annually, the audit methodology should be assessed for conformance with the IIA's International Standards for the Professional Practice of Internal Auditing, commonly referred to as the "IIA Standards", as documented within the IIA's International Professional Practices Framework (IPPF). Performing this assessment concurrently with the above Review and Reassessment helps ensure that any changes to the methodology will still provide for conformance with the IIA Standards. Each standard should be considered, with the method of conformance recorded (i.e. how the internal audit activity demonstrates conformance with the standard). Any instances of non-conformance should be considered for revision within the methodology. This assessment will be recorded within the IPPF Conformance template and maintained for at least seven years, to support the external review described below.

AP.7.3 External Assessment

Per Standard 1312 of the IPPF, "External assessments must be conducted at least once every five years by a qualified, independent assessor or assessment team from outside the organization." The scope of the external assessment should include, at a minimum, the following three core components:

- The level of conformance with the IIA Standards and Code of Ethics
- The efficiency and effectiveness of the internal audit activity
- The extent to which the internal audit activity meets the expectations of the board, senior management, and operations management, and adds value to the organization

The assessment should conclude with the external assessor's report. In addition to concluding on the level of conformance with the IIA standards (generally conforms, partially conforms, or does not conform), this report should include recommendations from the external assessor and management action plans to improve internal audit quality, efficiency, and effectiveness, which may provide new ideas or ways for the internal audit activity to better serve CVS's stakeholders and add value.

Depending on the significant of opportunities identified within the external assessor's report, formal action plans should be considered to address these items. At a minimum, all opportunities for improvement identified should be considered as part of the next Annual Internal Methodology Review & Reassessment, if not sooner.