CHAPTER 2

The Why and How of Risk Assessment

Are auditors leaving money on the table by avoiding risk assessment? Does risk assessment lead to better peer review results? In this chapter, you'll see that understanding risk assessment is a key to greater profit and positive peer review results.

Audit Risk Assessment as a Friend

Audit risk assessment can be our best friend, particularly if you desire efficiency, effectiveness, and profit—and who doesn't? Risk assessment tells you what to do—and what to omit. In other words, risk assessment is the doorway to maximum impact with minimal effort.

Why do some auditors avoid audit risk assessment?

- We don't understand it
- We are creatures of habit

Too often auditors keep doing the same as last year (commonly referred to as SALY), no matter what.

But what if SALY is faulty or inefficient?

Working Backward

The old maxim "Plan your work, work your plan" is true in audits. Audits—according to professional standards—should flow as follows:

1. Determine the risks of material misstatement
2. Develop a plan to address those risks
3. Perform substantive procedures
4. Issue an opinion

Some auditors sometimes go directly to step three and use the prior year audit programs to satisfy step two. Later, before the opinion is issued, the documentation for step one is created "because we have to." In other words, they work backwards, because they don't *really* plan.

Is there a better way?

A Better Way

Audit standards call us to do the following steps:

1. Understand the entity and its environment
2. Understand the transaction level controls
3. Use planning analytics to identify risks of material misstatement
4. Perform fraud risk analysis
5. Assess the risks of material misstatement (identify where risk exists)

While we might not complete these steps in this order, we do need to first perform our risk assessment and *then* assess risk.

Okay, so what risk assessment procedures should we use?

Audit Risk Assessment Procedures

AU-C 315.06 states:

The risk assessment procedures should include the following:

1. Inquiries of management, appropriate individuals within the internal audit function (if such function exists), others within the entity who, in the auditor's professional judgment, may

have information that is likely to assist in identifying risks of material misstatement due to fraud or error
2. Analytical procedures
3. Observation and inspection

I like to think of risk assessment procedures as detective tools used to sift through information and identify clues. Just as a good detective uses fingerprints, lab results, and photographs to paint a picture, we use walkthroughs, planning analytics, fraud inquiries, and the understanding of the entity to create a risk portrait.

Understand the Entity and Its Environment

The audit standards require that you understand the entity and its environment.

You might start by asking management this question, "If you had a magic wand that you could wave over the business and remove one problem, what would it be?" The answer tells you a great deal about the entity's risk.

You want to know what the owners and management *think* and *feel*. Every business leader worries about something. And understanding fear illuminates risk. Think of risks as threats to objectives. Your client's fear tells you what the objectives are—and the threats.

To understand the entity and its threats, ask questions such as:

- How is the industry faring?
- Are there any new competitive pressures or opportunities?
- Have key vendor relationships changed?
- Can the company obtain necessary knowledge or products?
- How strong is the company's cash flow?
- Has the company met its debt obligations?
- Is the company increasing in market share?
- Who are the key employees and why?

- What is the company's strategy?
- Are there any related party transactions?

Once you know your client's risks, relate them to the risks of material misstatement. After all, the audit opinion is in relation to whether material misstatements are present.

As with all risks, we respond based on severity. The higher the risk, the greater the response.

We'll respond to the risks of material misstatement at two levels: financial statement and transaction.

Responses to the risk of material misstatement at the financial statement level are general, such as appointing more experienced staff for complex engagements. Responses to risk of material misstatement at the transaction level are more specific such as a search for unrecorded liabilities. But before we determine responses, we must first understand the entity's controls.

Understand the Transaction Level Controls

We must do more than just understand transaction flows (e.g., receipts are deposited in a particular bank account). We need to understand the related controls (e.g., who enters the receipt in the general ledger, who reviews the receipting activity, etc.).

As we perform walkthroughs or other risk assessment procedures, we gain an understanding of the transaction cycle, but, more importantly, we gain an understanding of controls. Why? To see if controls are properly designed and implemented.

The use of walkthroughs is probably the best way to understand internal controls. As you perform your walkthroughs, ask questions such as:

- Who signs checks?

- Who has access to checks (or who has electronic payment ability)?
- Who approves payments?
- Who initiates purchases?
- Who can open and close bank accounts?
- Who posts payments?
- What software is used? Does it provide an adequate audit trail? Is the data protected? Are passwords used?
- Who receives and opens bank statements? Does anyone have online access? Are cleared checks reviewed for appropriateness?
- Who reconciles the bank statement? How quickly? Does a second person review the bank reconciliation?
- Who creates expense reports and who reviews them?
- Who creates the monthly financial statements? Who receives them?

As we perform walkthroughs, we ask the payables clerk (for example) certain questions. And, as we do, we make observations about the segregation of duties. Additionally, we inspect documents such as purchase orders.

This combination of inquiries, observations, and inspections allows us to determine if a risk of material misstatement is present. A weak control is a risk indicator.

As you perform your walkthroughs, gain an understanding of the entity's information technology and related controls.

Information Technology Risks

Depending on the size and complexity of the business, information technology can be simple or quite elaborate. Regardless, gain an understanding of the application and general computing controls.

When you perform your accounts payable walkthrough, for example, review application controls. Some systems make

payments based on purchase orders. Others pay when the purchase order, the receiving document, and the invoice agree (commonly known as a three-way match).

Additionally, review the entity's general information technology controls. Ask questions such as:

- Are passwords required to access each software component (e.g., accounts payable)?
- Who has the ability to make changes to the company's software? What is the process for testing and tracking software changes?
- How are technology changes documented? Who does this?
- What are the physical security requirements for computer and network systems?
- Is cloud-based technology used? If yes, how?
- Is software access limited to persons that must have permission? Is access assigned so that proper segregation of duties is ensured? Who provides access to software and when? Is access discontinued upon an employee's termination?
- What are the backup procedures? Who is responsible for this duty? Has recovery been tested? If yes, when?
- Does the entity use antivirus software? If yes, what and how is it updated? How often? Who is responsible for this duty?
- Are firewalls in use? If intrusions occur, who is notified? Who is responsible for protection of the company's information? Have the entity's personnel been trained with regard to phishing and malicious emails?
- Are periodic technology reports provided to management and those charged with governance?
- Does the company have written technology policies? Who monitors those?
- Have there been any significant technology problems?
- What is the educational background and experience of the

information technology personnel?
- Does the entity outsource technology duties?

Complex information technology systems may require the auditor to use a specialist.

As you review the information technology system, remember the purpose for gaining this understanding: to see if the application or general controls create a risk of material misstatement.

Another risk identification tool is planning analytics.

Planning Analytics

Planning analytics assist in identifying risks of material misstatement. I like to use multiple-year comparisons of key numbers (at least three years, if possible), and key ratios.

Unexpected variations in numbers can signal that fraud or error is present.

(See Appendix A for a detailed look at preliminary analytics.)

Fraud Risks

In every audit, inquire about the existence of theft. And while performing walkthroughs, look for control weaknesses that might open the door to fraud.

We should also consider management override of controls and intentional overstatements of revenue

Fraud risk is addressed in the next chapter, so, this is all I will say about theft for now.

Sometimes the greater risk is not fraud but errors.

Same Old Errors

Have you ever noticed that some clients make the same mistakes every year? Usually it's your smaller clients—those with poorly trained staff.

One way to identify potential misstatements due to error is to maintain a summary of the larger audit entries made over the last three years. If your client tends to make the same mistakes, you'll know where to look for potential errors.

Now it's time to pull all of the above together.

Creating the Risk Picture

Once you complete the risk assessment procedures, synthesize the disparate pieces of information into a composite image. You are, at this point, bringing the information into one distilled risk snapshot. What are you bringing together? Examples include:

- Control weaknesses
- Unexpected variances in significant numbers
- Entity risk characteristics (e.g., level of competition)
- Large related-party transactions
- Occurrences of theft

And why do you do this? As a basis for your audit strategy and audit plan.

With the risk snapshot in hand, you can now assess risk. How? By using the risk of material misstatement (RMM) formula.

Assess the Risk of Material Misstatement

Understanding the RMM formula is key to identifying high-risk areas.

What is the RMM formula?

Simply put, it is:

Risk of Material Misstatement = Inherent Risk X Control Risk

Using the RMM formula, we are assessing risk at the assertion level. While audit standards don't require a separate assessment of inherent risk and control risk, consider doing so anyway. Why? For a better understanding of risk.

Once we complete our risk assessment process, control risk can be assessed at high—simply as an efficiency decision. Alternatively, you can assess control risk below high and test controls for effectiveness.

The cash risk assessment might appear as follows (if control risk is assessed at high for all assertions):

ASSERTION	INHERENT RISK	CONTROL RISK	RMM
Existence	High	High	High
Completeness	Low	High	Moderate
Accuracy	Moderate	High	Moderate
Rights and Obligations	Low	High	Moderate
Cutoff	Moderate	High	Moderate

The cash risk assessment might appear as follows (if controls related to existence are tested and found to be effective):

ASSERTION	INHERENT RISK	CONTROL RISK	RMM
Existence	High	Moderate	Moderate
Completeness	Low	High	Moderate
Accuracy	Moderate	High	Moderate
Rights and Obligations	Low	High	Moderate
Cutoff	Moderate	High	Moderate

RMM is based on inherent risk and control risk. So, we consider the risk of each component in arriving at RMM as a whole. I

commonly use the lower of inherent risk and control risk, but there is no requirement to do so. Other auditors use something other than the lower of the two. For instance, if inherent risk is low and control risk is high, they might assess the RMM at moderate or high. RMM depends on risk. Some high risk assessments are "really high" and others are "somewhat high." Thus, RMM depends on the actual risk for each assertion.

Some auditors use percentages in assessing risk, though I am not a fan of doing so. But if you are mathematically inclined, percentages may work better for you. Personally, I like using categorical values: low, moderate, and high.

(See appendix B for *Understanding the Audit Risk Model*.)

The Inputs and Outputs

Audit planning inputs come from risk assessment procedures such as walkthroughs and planning analytics.

What are the outputs of risk assessment? The audit strategy and the audit plan (audit programs).

In chapter four, I'll show you how to create your audit strategy and audit plan.

Risk Assessment - A Simple Summary

- Risk assessment is your friend
- Determine the risks of material misstatement *prior* to developing your audit plan
- Your risk assessment tools include:
  - Understanding the entity and its environment
  - Walkthroughs
  - Planning analytics
  - Fraud inquiries
- Gain an understanding of the entity

- Understand the internal controls of the business and determine whether they are properly designed and whether they have been implemented
- Use planning analytics to uncover unexpected changes in numbers
- Inquire of management, other employees, and those charged with governance regarding fraud
- Based on the evidence gathered, develop your risk picture (a snapshot of where the financial statements might be misstated)
- The risk of material misstatement = inherent risk X control risk (use this formula to assess the risk of misstatement)
- Develop your audit strategy and audit plan to address identified risks of misstatement

Next we'll take a look at how to perform risk assessment procedures related to fraud.