1

THE EVALUATION APPROACH

CHAPTER SUMMARY

Overview of the SEC rules requiring management's assessment of the effectiveness of the entity's internal control over financial reporting

Description of a risk-based, top-down approach to the evaluation of an entity's internal control and disclosure controls and procedures

Summary of the external auditor's responsibilities and how management can work with its auditors to create an efficient internal control audit

MANAGEMENT'S EVALUATION OF INTERNAL CONTROL

The Sarbanes-Oxley Act of 2002 (SOX) made significant changes to many aspects of the financial reporting process. One of those changes is a requirement that management provide a report that contains an assessment of an entity's internal control over financial reporting.

Securities and Exchange Commission (SEC) rule 13a-15 (f) defines internal control over financial reporting in this way:

> The term internal control over financial reporting is defined as a process designed by, or under the supervision of, the issuer's principal executive and principal financial officers, or persons performing similar functions, and effected by the issuer's board of directors, management and other personnel, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles and includes those policies and procedures that:
>
> **(1)** Pertain to the maintenance of records that in reasonable detail accurately and fairly reflect the transactions and dispositions of the assets of the issuer;
>
> **(2)** Provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the issuer are being made only in accordance with authorizations of management and directors of the issuer; and
>
> **(3)** Provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the issuer's assets that could have a material effect on the financial statements.

When considering the SEC's definition, you should note these points:

- The term "internal control" is a broad concept that extends to all areas of the management of an enterprise. The SEC definition narrows the scope of an entity's consideration of internal control to the preparation of the financial statements—hence the use of the term "internal control *over financial reporting*."
- The SEC intends its definition to be consistent with the definition of internal controls that pertain to financial reporting objectives that was provided in the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Report. (See Chapter 2 of this book for a detailed discussion of the COSO Report).

This book, unless otherwise indicated, uses the term "internal control" to mean the same thing as "internal control over financial reporting," as defined by the SEC rules.

Management files its internal control report together with the annual 10K. The internal control report must include:[1]

> **(A)** *Management's Annual Report on Internal Control Over Financial Reporting.* Provide a report on the company's internal control over financial reporting that contains:
>
> **(1)** A statement of management's responsibilities for establishing and maintaining adequate internal control over financial reporting;
>
> **(2)** A statement identifying the framework used by management to evaluate the effectiveness of the company's internal control over financial reporting;

(3) Management's assessment of the effectiveness of the company's internal control over financial reporting as of the end of the most recent fiscal year, including a statement as to whether or not internal control over financial reporting is effective. This discussion must include disclosure of any material weakness in the company's internal control over financial reporting identified by management. Management is not permitted to conclude that the registrant's internal control over financial reporting is effective if there are one or more material weaknesses in the company's internal control over financial reporting; and

(4) A statement that the registered public accounting firm that audited the financial statements included in the annual report has issued an attestation report on management's assessment of the registrant's internal control over financial reporting.

(B) *Attestation Report of the Registered Public Accounting Firm.* Provide the registered public accounting firm's attestation report on management's assessment of the company's internal control over financial reporting

(C) *Changes in Internal Control Over Financial Reporting.* Disclose any change in the company's internal control over financial reporting that has materially affected, or is reasonably likely to materially affect the company's internal control over financial reporting.

Overview of the Evaluation Process

Management must have a "reasonable basis" for its annual assessment. To provide this reasonable basis, management must perform an annual evaluation of internal control.

SEC Release Nos. 33-8810 and 34-55928 provide important interpretative guidance for management regarding its evaluation of internal control. The SEC rules on evaluating internal control are objective driven and principles-based, and they start with a description of the overall objective of management's evaluation. Having a clear understanding of the overall objective of your evaluation is vital if you want that process to be as effective and efficient as possible.

According to the SEC, the primary objective of management's evaluation is to

> Provide management with a *reasonable basis* for its annual assessment as to whether any *material weaknesses* in internal control exist as of the end of the fiscal year

The phrases in italics are of critical importance in planning and performing an evaluation of internal control.

- *Reasonable basis.* A reasonable basis is "such level of detail and degree of assurance as would satisfy prudent officials in the conduct of their own affairs." The notion of "reasonable" does not imply an

unrealistic degree of precision or a single conclusion or evaluation approach. By setting a threshold of "reasonableness" to its guidance, the SEC acknowledges that management can and should exercise judgment in how it complies with its rules and that there is a full range of appropriate ways to evaluate internal control.

- *Material.* An amount is material to the financial statements if it would change or influence the judgment of a financial statement user. Note that the SEC rules direct management to identify "material" weaknesses," not all weaknesses or deficiencies in internal control. Having a clear understanding of what is and is not material will help you design a more efficient evaluation approach.

Even though the SEC has provided detailed interpretative guidance, ultimately this guidance not only allows for but actively encourages management to exercise its judgment in the design and execution of the procedures it performs to meet the overall objective for evaluating internal control.

Material Weakness

The SEC states that overall objective of the evaluation of internal control is to determine whether a material weakness exists as of the fiscal year-end. In order to meet this objective, it is critical you have a working definition of the term.

A *material weakness* is a *deficiency*, or combination of deficiencies, in internal control such that there is a *reasonable possibility* that a material misstatement of the annual or interim financial statements will not be prevented or detected in a timely basis.

A control *deficiency* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

There is a *reasonable possibility* of an event when the likelihood of the event is more than remote.

With these definitions in hand, you have a sound basis for choosing the nature, timing and extent of procedures necessary to support your evaluation of internal control.

RISK-BASED JUDGMENTS

Underlying the SEC guidance is the idea that management's assessment of risk is central to its process for evaluating internal control. Within this context, there are two types of risks. Although they are related to each other, it is

important for you to distinguish between the two of them as you plan your evaluation process.

- *Misstatement risk* is the risk that the financial statements could be misstated, irrespective of the entity's internal controls. For example, consider a high-technology manufacturing company. The nature of its business means that the company is vulnerable to rapid advances in technology, which could make its products obsolete. This obsolescence must be reflected in the company's financial statements (in the way inventory is valued). Because of the materiality of inventory to its financial statements and due to the high degree of judgment in making an estimate of the value of high-tech inventory in a constantly changing business environment, you might consider misstatement risk related to inventory to be high.
- *Risk of control failure* is the risk that a failure in the design or operation of a control could lead to a material misstatement of the financial statements.

  The risk of control failure is a function of misstatement risk and the likelihood of a control failure. If this combination of factors is high, then the risk of control failure increases. If this combination of factors is low, then the risk of control failure decreases.

For example, consider the high-tech manufacturing company, as discussed. The circumstances of the company's business lead to a relatively high misstatement risk. But what about the risk of control failure?

Assume that the company conducts an annual physical count of this inventory to determine the quantity of items on hand. This control procedure is critical if the company is to accurately report the valuation of its year-end inventory and its cost of sales throughout the year. Obtaining a proper count by inventory item is critical not only for determining the gross amount of the inventory balances, but also for identifying the amount of inventory that may be subject to obsolescence. Put another way, if this control procedure were to fail (i.e., the company did not get an accurate inventory count), there would be a high risk that the failure could lead to a material misstatement.

Suppose that the nature of the inventory required a high degree of specialized knowledge to determine precisely what the item was (i.e., all processing chips look the same to the untrained eye). Further, the company had a 100% turnover of personnel assigned to conduct the inventory count. Given these circumstances, the likelihood of a control failure (i.e., an inaccurate inventory count) would be relatively high.

In this situation, the combination of a high misstatement risk and a high likelihood of control failure results in a high overall risk of control failure.

As the combination of misstatement risk and likelihood of control failure decreases, however, so does control risk.

For example, suppose that the high-tech manufacturer changes its policy for reimbursing employees for their cell phone usage. The company raises the amount it will reimburse employees from $50 per month to $75 per month. The sales manager knows from past experience that most salespeople will fail to read the e-mail announcing the change in policy, and as a result, it will take months before the new policy is universally endorsed. Once the salespeople realize that the reimbursement has been raised, they will be reimbursed retroactively. That is, as of a given point in time, the company technically has a liability to all its salespeople who have not yet figured out the new policy.

Thus, there is a risk that the company's accrued liabilities may be understated. But how significant is this risk to the financial statements as a whole? Most likely, the total amount of this liability is inconsequential to the company's financial position.

Because misstatement risk is low, the risk of control failure also should be small. Remember that by definition, the risk of control failure is the risk that a failure of the control could lead to a "material" misstatement. In this case, even if there was no control over reimbursing employees for cell phone usage, the company could not materially misstate its financial statements. The risks related to control failure are nonexistent.

Given this combination of high likelihood but extremely small significance, there is probably a low overall risk that a material misstatement of the financial statements would occur as a result of this circumstance. With such a low risk, you probably would not include controls related to capturing unpaid cell phone reimbursements within the scope of your internal control evaluation.

Why Understanding Risk Is Important

The proper design and efficient performance of an evaluation of internal control depends greatly on management's assessment of risk. The fundamental principle is that you should focus your attention where the risk is the highest, where there is a relatively high likelihood that a significant misstatement of the financial statements could result. The nature and extent of the procedures you perform to document and test controls should be commensurate with the risk that a failure of those controls could result in a material misstatement of the financial statements. The opposite also is true: You do not need to spend a great deal of time on those areas where risk is the lowest.

Management's decisions should be driven by an evaluation of the risk in three areas:

1. *Identifying controls to include in the assessment.* A control where there is a low risk that its failure could lead to a material misstatement is scoped out of the evaluation; that is, it is not included in the documentation, testing, or evaluation of controls.
2. *Evaluating the operating effectiveness of the controls.* The procedures management uses to obtain evidence about the operating effectiveness of controls should be based on an assessment of risk. For those controls where the risk of material misstatement is highest, the procedures performed should produce highly reliable evidence about operating effectiveness; if the controls have a lower risk, then the evidence does not have to be as reliable.
3. *Documenting the evidence related to testing of the controls.* When the risk associated with a control is relatively high, the documentation of the tests performed should be extensive. The converse also is true—if the risk is low, then the documentation need not be as extensive.

Exhibit 1.1 illustrates how risk-based judgments affect each of these three decisions.

Later chapters of this book will provide more guidance on how to make risk-based judgments in each of these areas.

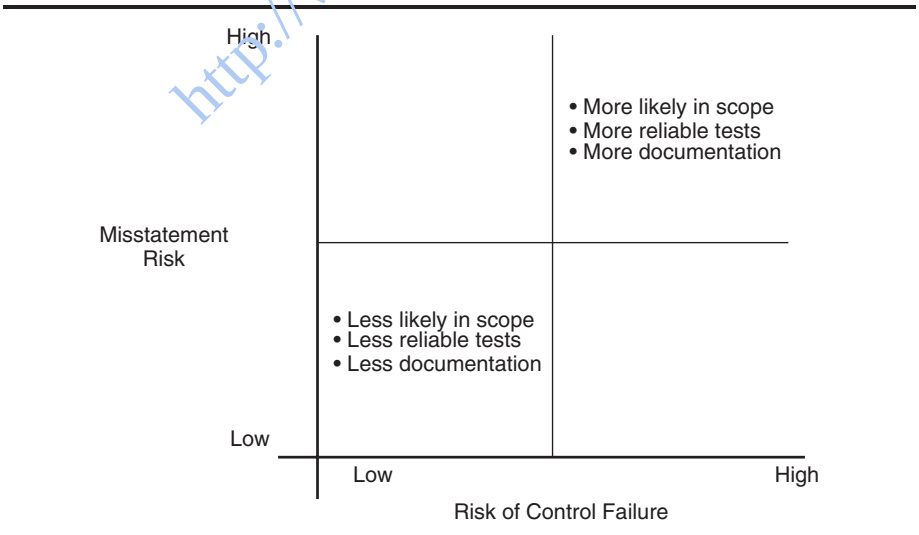

EXHIBIT 1.1 RISK-BASED JUDGMENTS

RISK-BASED, TOP-DOWN EVALUATION APPROACH

In the years immediately following the effective dates of SOX 404, many companies adopted an evaluation approach that started by identifying all (or nearly all) of the company's controls and then documenting and testing each one to determine whether internal control as a whole was effective. As you can imagine, this approach was extremely time consuming and costly. Moreover, this bottoms-up approach was unnecessary to achieve the overall objective of management's evaluation.

In 2007, the SEC revised its rules to clarify its original intent and any ambiguity about management's evaluation approach that may have existed. Of primary importance was providing direction on how to properly scope the engagement or scale it to account for different circumstances between entities.

The resulting rules explicitly state that there is no requirement for management to include all controls in its evaluation. Instead, management should use a "risk-based, top-down" approach to plan and perform its evaluation of internal control.

In general, the key steps in this approach include:

- *Identification of misstatement risk.* Management should use its knowledge of the business, external events, and circumstances and the application of generally accepted accounting principles (GAAP) to identify risks that the entity's financial statements could be misstated.
- *Assessment of misstatement risk.* Management should assess the relative magnitude of the identified misstatement risks. This assessment is made without regard to internal controls. Negligible or immaterial risks require no further consideration; that is, the controls related to these risks do not need to be part of management's evaluation process.
- *Identify controls that mitigate misstatement risks.* The entity should have controls in place to mitigate those misstatement risks that are of some significance. This process of identifying controls should begin at the top with the broadest, most pervasive controls and then proceed downward to more direct, specific controls.

Identification of Misstatement Risk

Evaluating internal control properly requires a deep understanding not only of the entity's operations but, just as important, of how those operations and the types of transactions and arrangements the entity enters into should be accounted for. For example, it's not enough for the board of a community

bank to know that the bank holds a portfolio of derivatives in order to hedge interest rate risks. In order to identify risk and evaluate internal control, management also must have a working knowledge of how to account for derivatives and hedging transactions.

In many instances, the operations management of an entity may not be particularly knowledgeable about the accounting principles that apply to the company's business, especially when those principles are complex or evolving. In those instances, it is important to add someone with the requisite accounting expertise to the team responsible for evaluating internal control.

Sources of Risk

Management uses its knowledge of the entity to identify sources of misstatement risk—that is, what could go wrong—in the preparation of the financial statements. The risk of misstating the financial statements is different from the business risks faced by the company. However, business risks can create financial reporting risks, so the consideration of business risks can be a good starting point. For example:

- In a declining economy with rising interest rates, the default rate on mortgages and other consumer debt will rise. Lenders must take this trend into account when estimating bad debt allowances; if they don't, there is a risk that the valuation of the loan portfolio will be overstated.
- Consider ABC Hotel, which has a virtual monopoly on a certain section of a city and so operates near capacity. Inevitably, new hotels will enter the marketplace. If the demand for rooms does not keep pace with the expanding supply, occupancy and room rates will drop at ABC. To determine the proper value for the asset (i.e., the hotel), its owners must consider the estimated future cash flows to be generated by the property, and that estimate should consider the effect of increased competition.
- In order to meet the demands of its customers, a software company begins to offer consulting systems integration and ongoing support services. The bundling of these services with the licensing of its software can significantly complicate the accounting for revenue, which, in turn, creates a risk of misstating revenue in the financial statements.

It may be helpful to think of risks as coming from two main sources: those external to the company and part of the business environment, and those internal to the entity and its own operations.

External sources of risk might include:

- *Industry conditions,* such as the competitive environment, seasonal or cyclical activity, technology considerations, or the cost and availability of material or labor.
- *Regulatory environment,* such as industry-specific regulations or accounting practices, legislation and regulation that affect the entity's operations, taxes, regulatory supervision, and accounting standards.
- *Other external factors,* such as general economic conditions, interest rates, the availability of capital, or inflation.

Internal sources of risk might come from:

- The nature of the entity's business operations
- Investment activity
- Financing structure and activity
- The accounting for normal, day-to-day transactions, including how those transactions are:
  - Initiated
  - Authorized
  - Captured
  - Processed

Managing Change

Change to external or internal factors is a primary source of risk. In the community bank example discussed, it was not interest rates per se that created the misstatement risk; it was the change to those rates. A company may operate successfully for years using the same software. Although this software may be inelegant and slightly flawed, over time the company has learned to create little work-arounds so management still can receive reliable information. Upgrading that system—even if the new one is more efficient and modern—will create risks that were not present with the old system.

Conditions that frequently serve as a source for risk include:

- *Changes in the operating environment.* Changes in the regulatory or operating environment can result in changes in competitive pressures and significantly different risks.
- *New personnel.* New personnel may have a different focus on or understanding of internal control. When people change jobs or leave the company, management should consider the control activities they performed and who will perform them going forward. Steps should be taken to ensure that new personnel understand their tasks.

- *New or revamped information systems.* Significant and rapid changes in information systems can change the risk relating to internal control. When these systems are changed, management should assess how the changes will impact control activities. Are the existing activities appropriate or even possible with the new systems? Personnel should be adequately trained when information systems are changed or replaced.
- *Rapid growth.* Significant and rapid expansion of operations can strain controls and increase the risk of a breakdown in controls. Management should consider whether accounting and information systems are adequate to handle increases in volume.
- *New technology.* Incorporating new technologies into production processes or information systems may change the risk associated with internal control.
- *New lines, products, or activities.* Entering into business areas or transactions with which an entity has little experience may introduce new risks associated with internal control.
- *Restructurings.* Corporate restructurings, which usually are accompanied by staff reductions, can result in inadequate supervision, the lack of necessary segregation of duties, or the deliberate or inadvertent elimination of key control functions.
- *Foreign operations.* The expansion of a company outside of the United States will introduce new and unique risks that management should address.
- *Accounting changes.* Although not mentioned in the COSO Report, Statement on Auditing Standards No. 55 (as amended), *Internal Control in a Financial Statement Audit*, includes changes in GAAP as a circumstance that requires special consideration in the entity's risk assessment process.

How to Identify Risk

The process management uses to identify risk will vary. Larger, more complex companies may require a more formal system for identifying risk. Smaller, less complex entities may be able to rely on management's daily involvement with the business to identify risk. No requirements dictate the procedures management should perform to identify risk. As a practical matter, those responsible for conducting the evaluation of internal control should make sure that, collectively, the team has an appropriate level of knowledge about GAAP and the entity's operations (including information technology systems) to be able to reasonably identify risks of misstatement.

Periodically, you will want to challenge your risk identification process to see if it is still adequate to identify risks of misstatement because if risks are not identified, they cannot be controlled or otherwise managed.

The results of the financial statement audit or communications from others about the entity's internal control should cause management to reevaluate its risk identification process. For example, consider the ABC Hotel example. Suppose that the independent auditors determined that the value of the asset had been impaired and recommended that management adjust its financial statements accordingly. In addition to determining whether to record the adjustment, management also should understand the difference between how it valued the asset and how the auditors valued the asset.

It's possible that the auditors and management, working with the same set of facts, made different assumptions underlying the projected cash flows from the hotel. In that case, the difference between management and the auditors was related to two different, highly subjective judgments.

However, the difference in valuations may be due to management being unaware that the change in market conditions requires it to project future cash flows and determine whether the asset has been impaired. Under these circumstances, the difference between the auditors' valuation of the asset and management's was caused by management's failure to identify a risk of misstatement and to design a control to address that risk.

Fraud Risk

The SEC explicitly states that management's evaluation of risk should include consideration of the vulnerability of the entity to fraudulent activity. The risk of misstatement due to fraud ordinarily exists in any organization.

An entity's vulnerability to fraud is a function of three factors: opportunity, incentive/motivation, and rationalization. Consider the simple (but unfortunately quite common) example of the bookkeeper who embezzles funds simply by writing a company check to himself. In order for this fraud to occur, all three factors must be in place.

1. *Opportunity.* Lax controls create the biggest opportunity for fraud. At a small business, there usually is a lack of adequate segregation of duties. The same person who enters transactions into the general ledger also reconciles the bank and has the authority to disburse funds. This lack of a fundamental control allows the person to: disburse funds to him- or herself, hide the disbursement in an expense account where it won't be questioned, and cover up the fraud during the preparation of the bank reconciliation.

2. *Motivation/incentive.* When the opportunity to commit fraud presents itself, the chances of a fraud occurring increase dramatically if the person in a position to commit the fraud is highly motivated to do so. For example, if the bookkeeper was having financial difficulties, she would be motivated to embezzle funds.
3. *Rationalization.* Even with an opportunity and a motivation, many people will not commit a fraud because they know that stealing is wrong. In order for them to embezzle funds, they have to rationalize their act, convince themselves that what they are doing is okay. For example, one of the common rationalizations is "I'll pay it back." The bookkeeper does not believe he is stealing; only that he is borrowing money from the company for a short period of time.

An organization's vulnerability to fraud is greatly reduced when even one of these factors is diminished. Chapter 5 provides more details on the controls an organization should have in place to reduce its risk due to fraud.

Assessment of Misstatement Risk

Assessing misstatement risk means determining relative significance of the misstatement to the financial statements. Management's assessment of misstatement risk includes considering both quantitative and qualitative aspects of the account, class of transactions or disclosures that would be affected by the misstatement.

Materiality

Because the materiality of a financial reporting element increases in relation to the amount of misstatement that would be considered material to the financial statements, management's assessment of misstatement risk for the financial reporting element also increases. For example, a risk affecting revenue probably would be more important than one affecting prepaid assets.

Qualitative Aspects

In assessing risk, you should consider the qualitative aspects that would make the account, class of transactions, or disclosure more prone to material misstatement. These factors should be considered when assessing risk:

- *The extent to which the financial statement reporting element involves judgment in determining the recorded amount.* The more judgment involved, the higher the risk.

- *Whether the reporting element or the underlying asset is susceptible to fraud.* The more susceptible to fraud, the higher the risk.
- *The relative complexity of the related accounting requirements.* The more complex the accounting requirements, the higher the risk of misstatement.
- *Whether the nature or volume of the underlying transactions have changed significantly.* The greater and more recent the changes, the higher the risk.
- *The extent to which the recognition or measurement of the item is sensitive to changes in environmental factors, such as technological and/or economic developments.* The more sensitive the item is to environmental changes, the higher the risk.

With these general principles in mind, the SEC explicitly states that these items generally would be assessed as having a higher misstatement risk:

- Related party transactions
- Critical accounting policies (those policies that are most important to the financial statement presentation and which generally "require management's most difficult, subjective, or complex judgments" because they often "require estimates abut the effect of matters that are inherently uncertain")

Likelihood of Control Failure

Assessing the risk of control failure requires the consideration of two factors:

1. *The* significance *of the misstatement that would result from the control failure*. This factor addresses the questions: "If a failure in the control occurred, and a misstatement of the financial statements resulted, how big would that misstatement be? Would it be material? Inconsequential? Or somewhere in between?" Your assessment of misstatement risk (discussed earlier) provides the answer to these questions.
2. *The* likelihood *that the control will fail*. This factor addresses the question: "What is the chance that the control will fail?" By considering the likelihood of a control failure, you will direct the focus of your evaluation on those controls that represent the highest risk.

When considering the likelihood that a control might fail to operate effectively, you should consider:

- The type of control (i.e., manual or automated) and the frequency with which it operates
- The complexity of the control

- The risk of management override
- The judgment required to operate the control
- The competence of the personnel who perform the control or monitor its performance
- Whether there have been changes in key personnel who either perform the control or monitor its performance
- The nature and materiality of misstatements that the control is intended to prevent or detect
- The degree to which the control relies on the effectiveness of other controls (e.g., information technology general controls)
- The evidence of the operation of the control from prior year(s)

For example, management's judgment of the risk of control failure would be higher for controls whose operation requires significant judgment than for noncomplex controls requiring less judgment.

Top-Down Approach to Identifying Relevant Controls

The consideration of the risk of material misstatement is crucial when planning and performing an evaluation of internal control. It is this consideration that helps direct management's focus to the most critical areas of the company's internal control system. In a similar fashion, beginning at the top of the system and working down will help drive efficiency and direct the focus of the evaluation.

But where is the top of an internal control system? And once you're there, what direction is down? Answering these questions requires an understanding of three key principles of internal control design. (Chapter 2 discusses these principles in more detail.)

1. Within any organization, controls operate at two distinct levels: the broad, general entity level and the more focused and specific activity level.
2. Controls are designed to mitigate risks. Some controls address risks *directly*; other controls address the same risks *indirectly*.
3. At the activity level, controls can be designed to either:
   a. Prevent errors from entering the financial information system,
   b. Detect and correct errors that have already entered the system.

Exhibit 1.2 illustrates this internal control design.

At the top of this structure are the entity-level controls. For example, these controls might include the company's hiring and training policies and the firewall protecting its network. Notice that there are relatively few entity-level

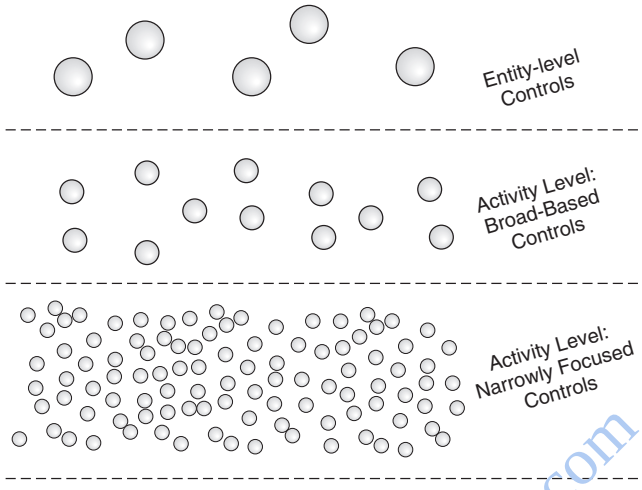

EXHIBIT 1.2 INTERNAL CONTROL DESIGN

controls. This is because, by their nature, entity-level controls have a broad (though indirect) effect on the company's financial reporting risks (as indicated by the relative size of the sphere). For example, a firewall might cover the company's inventory system, billing and receivables, and general ledger system all at once.

Entity-level controls have a very indirect effect on the financial statements. For example, the quality of the company's training can improve job performance and reduce the risk of misstatement, but training alone is not sufficient to prevent or detect an error.

At the lowest level of the pyramid are the company's most specific, narrowly focused activity-level controls. An edit check to ensure that a date is formatted mm/dd/yyyy is an example of such an activity-level control. This control is directed specifically to one field on a single data entry form. The control is designed to *prevent* an error from entering the information, and it is typical for controls at this level of the pyramid to be preventive ones, designed to be performed on every transaction.

Notice how many more activity-level controls exist in a typical internal control system. There are two reasons for this relative abundance of preventive activity-level controls.

1. *Activity-level controls address very specific risks and have a very narrow (but direct) effect on financial reporting risks.* Entities enter into many different types of transactions. In our example, paying suppliers

is just one of dozens of different types of financial activities, and an organization will have activity-level controls for each of these activities. Additionally, for each transaction type, the company may face many different kinds of risk, each requiring a different kind of activity-level control. For example, not only will companies want to make sure that they pay only approved suppliers, they also will want to make sure they pay the correct amount.

2. *Many internal control systems include redundant controls, multiple controls that achieve the same objective.* For example, the company may use a purchase order system to make sure that its buyers are approved to enter into transactions. In addition, a manager may periodically compare actual purchases to budget to make sure that company buyers are staying within their approved limits.

In between the entity-level controls and preventive activity-level controls are the broad-based activity-level controls. A bank reconciliation is a good example of such a control. A bank reconciliation does not prevent the bookkeeper from entering an incorrect amount as a cash disbursement. But if such an error were made, a properly performed bank reconciliation should detect and correct it. Many broad-based activity-level controls are detective in nature and usually performed periodically rather than on every transaction.

A top-down approach to internal control evaluation means that you start with entity-level controls, which have the broadest span but most *indirect* effect on reducing financial statement misstatements. Once you have evaluated entity-level controls, you then proceed down to the more specific activity-level controls. At the activity level, you again begin at the top, with those controls that are farthest along in the information processing stream. Usually these are *detective* controls.

After evaluating detective controls, you may then proceed back down the information processing stream, back to the inception of the transaction, evaluating controls along the way.

The key to applying the top-down approach is to ask—at each step of the evaluation: Are the controls I've evaluated so far capable of appropriately addressing the related risk of material misstatement?" If the answer is yes, there is no need to evaluate more controls. If the answer is no, then you should continue to evaluate more controls farther down in the structure until you reach a point where you have evaluated enough controls to evaluate the risk.

Exhibit 1.3 and 1.4 describe the top-down process.[2] We start with the control design described in Exhibit 1.2, and we "drop" a risk in at the top.

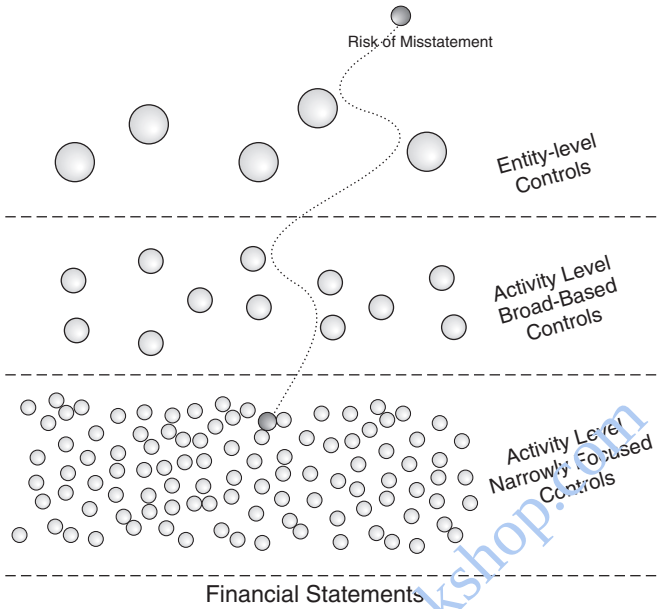

EXHIBIT 1.3 TOP-DOWN APPROACH RISK NO. 1

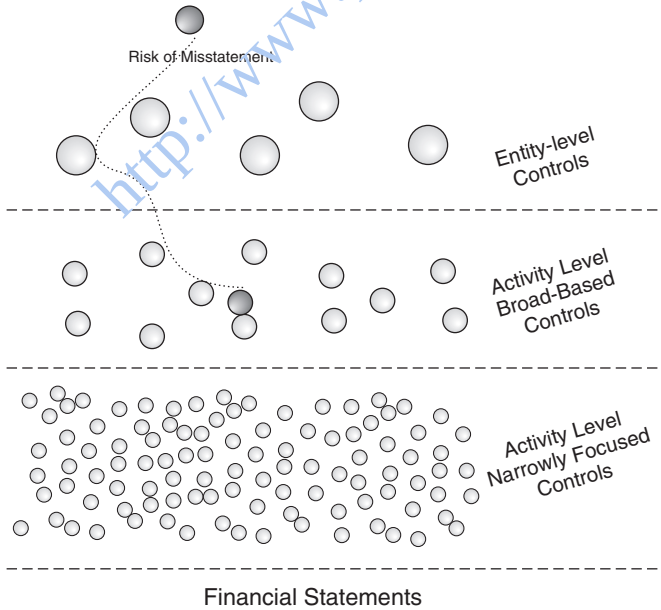

EXHIBIT 1.4 TOP-DOWN APPROACH RISK NO. 2

That risk (represented by a darker ball) will interact with the controls, starting at the top, with entity-level controls. At each interaction you will ask: "Is the control capable of stopping the risk from making its way to the financial statements?"

If the answer is no, then the risk "bounces" off the control and continues unimpeded until it encounters another control, and the same question is asked. It is hoped that some control (or combination of controls) will eventually stop the risk from reaching the financial statements.

Exhibit 1.3 shows an example where the risk is stopped by a combination of activity-level controls. Exhibit 1.4 shows another risk, one for which a broad-based activity-level control is sufficient.

The top-down approach to evaluating internal control says that the only controls you should evaluate are the ones that are necessary to mitigate the risk. In Exhibit 1.3, the control interacts with and ultimately is stopped by a combination of six controls. All the other controls in the diagram—though they might address the risk—do not need to be included in the evaluation of internal control.

In Exhibit 1.4, you can stop your evaluation at the broad-based activity-level controls. For example, the reconciliation between the subledger and the general ledger account total (a broad-based activity-level control) would be evaluated. The specific, narrowly focused controls (e.g., edit checks) do not need to be included in the evaluation.[3]

You will want to use a top-down, risk-based approach for the following reasons:.

- *Audit Efficiency.* Understanding the strengths and weaknesses of entity-level controls will allow you to develop more targeted tests of application-level controls. You will be better able to anticipate weaknesses that may be identified in application-level testing, and you will do a better job of following up on application-level control weaknesses.
- *Better Remediation of Control Deficiencies.* If control deficiencies are discovered, they should be corrected. If the deficiencies are corrected and new controls are functioning as of year-end, then the company will be able to report that its internal control was effective. The remediation of entity-level control deficiencies typically takes longer than the remediation of activity-level control deficiencies. Therefore, you will want to identify entity-level deficiencies as early in the process as possible to increase the chance that they can be corrected successfully by year-end.

- *Improved Audit Effectiveness.* Many times, the root cause of an activity-level control problem is a deficiency in an entity-level control. For example, suppose that you are testing controls over cash, and you discover that the bank reconciliations are prepared improperly. Someone else on the project team discovers that control procedures relating to the payment of vendor invoices are deficient, and someone else finds inventory controls are not applied in a consistent manner. Are these three observations isolated activity-level control deficiencies?

  Sometimes they are not. It may be that the company does a poor job of communicating job responsibilities to its employees and supervising their work (entity-level controls). As a result, control activities are performed sporadically or incorrectly. What the project team observed at the activity level are symptoms, not underlying causes. If the company only addresses the symptoms, the underlying cause will go untreated and will only cause more problems in the future.

The Overall Objective of the Auditor's Engagement

The auditor's objective in an audit of internal control is to express an opinion about management's assessment of the effectiveness of the company's internal control over financial reporting. This objective implies a two-step process:

Step 1. Management must perform its own assessment and conclude on the effectiveness of the entity's internal controls

Step 2. The auditors will perform their own assessment and form an independent opinion as to whether management's assessment of the effectiveness of internal control is fairly stated.

Thus, internal control is assessed twice, first by management and then by the independent auditors. That the auditors will be auditing internal control—and in some cases, reperforming some of the tests performed by the entity—does not relieve management of its obligation to document, test, and report on internal control.

To form his or her opinion, the auditor will:

- Evaluate the reliability of the process used by management to assess the entity's internal control.
- Review and rely on the results of *some* of the tests performed by management, internal auditors, and others during their assessment process.
- Perform his or her own tests.

Use of Work of Internal Auditors and Others

Both the SEC and Public Company Accounting Oversight Board (PCAOB) recognize that external auditors should be able to use, to some degree, the work performed by management in its self-assessment of internal control in their audit. To do otherwise, to completely prohibit external auditors from using some of management's work, would make the cost of compliance quite steep. At the same time, the primary objective of an audit is to obtain an objective, independent opinion. To form and take responsibility for such an opinion, auditors must do some of their investigation independently from the company.

Thus, the SEC must balance two competing goals: objectivity and independence of the parties involved versus the use of management's work by the external auditor as a means of limiting the overall cost of compliance.

External Auditor's Use of the Company's Internal Control Testing and Evaluation

Ultimately, the auditor is responsible for determining the extent to which he or she will rely on management's work in the audit. PCAOB Auditing Standard No. 5 provides guidance to auditors on the principles they should use to make that determination.

Paragraph 19 of the auditing standard provides extensive guidance on the degree to which the company's work on internal control can be used by the external auditors. The relevant section is titled "Using the Work of Others." The standard indicates that the work of "others" includes the relevant work performed by:

- Internal auditors
- Other company personnel
- Third parties working under the direction of management or the audit committee

In general, the auditor's determination about using the work of others is a risk-based judgment: The greater the risk, the more the auditor will want to use his or her own work to form an opinion. As the risk decreases, the auditor can begin to rely more on the work of the company.

The external auditor's ability to rely on the work of others has its limits. Paragraph 35 of the standard states that the procedures performed to achieve certain audit objectives should be performed by the auditor him- or herself. The objectives are:

- Understanding the flow of transactions related to the relevant assertions, including how there transactions are initiated, authorized, processed, and recorded.
- Identifying the points within the company's processes at which a misstatement—including a misstatement due to fraud—could arise that, individually or in combination with other misstatements, would be material.
- Identifying the controls that management has implemented to address these potential misstatements.
- Identifying the controls that management has implemented over the prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could result in a material misstatement of the financial statements.

To achieve these objectives, the auditor typically performs a walk-through for each of the company's significant accounts and disclosures. As part of its evaluation, management also may perform walk-throughs of these same accounts, but the auditing standard makes it clear that auditors must perform their own walk-throughs.

The standard also identifies two areas that are highly important to internal control and financial reporting. As such, auditors typically will want to rely primarily on their own work in testing:

1. The control environment
2. Controls over the period-end financial reporting process

Assessing Competence and Objectivity

Auditors will have to assess the competence and objectivity of those people whose work they plan to use. The higher the degree of competence and objectivity, the greater use auditors may make of the work.

Competence means the attainment and maintenance of a level of understanding and knowledge that enables that person to perform ably the tasks assigned to them.

Objectivity means the ability to perform those tasks impartially and with intellectual honesty.

Competence and objectivity go hand in hand. The auditor will not use the work of someone who has a low degree of objectivity, regardless of the person's level of competence. Likewise, the auditor should not use the work of someone who has a low level of competence, regardless of his or her objectivity.

To allow the company's external auditors to make as much use as possible of the company's own assessment of internal control, company management should have a clear understanding of the conditions that must be met for the external auditors to use the work. To help the external auditors determine that those criteria have been met, you may wish to *document your compliance with the key requirements* of the auditing standard and make this documentation available to the external auditors early on in their audit planning process. For example, you should consider:

- Obtaining the biographies or resumes of project team members showing their education level, experience, professional certification, and continuing education
- Documenting the company's policies regarding the assignment of individuals to work areas
- Documenting the "organizational status" of the project team and how they have been provided access to the board of directors and audit committee
- Determining that the internal auditors follow the relevant internal auditing standards
- Establishing policies that ensure that the *documentation* of the work performed includes:
  - A description of the scope of the work
  - Work programs
  - Evidence of supervision and review
  - Conclusions about the work performed

WORKING WITH THE INDEPENDENT AUDITORS

To render an opinion on either the financial statements or the effectiveness of internal control, the company's independent auditors are required to maintain their independence, in accordance with applicable SEC rules. These rules are guided by certain underlying principles, which include:

- The audit firm must not be in a position where it audits its own work.
- The auditor must not act as management or as an employee of the client.

For example, with regard to internal controls, the auditor could not design or implement internal controls and still be allowed to perform an audit.

The auditor's rules of independence require the audit committee to preapprove nonaudit services related to internal control over financial reporting. In seeking this preapproval, the auditor will:

- Provide a written description of the scope of the internal control–related services to the audit committee.
- Discuss with the audit committee the potential effects of the service on the independence of the firm.
- Document the substance of its discussion with the audit committee.

NOTES

1. See Regulation S-K, Item 308 (17 CFR § 229.308).
2. Shawn O'Brien was the first to describe this analogy.
3. During the initial implementation of SOX 404, many entities took a bottoms-up approach to their evaluations. Rather than starting with entity-level controls, they began by documenting and testing all or nearly all of the specific, narrowly focused activity-level controls. As a result, they performed a great deal of work of negligible incremental value. The proper application of a risk-based, top-down approach will lead to increased efficiency with only a marginal loss of effectiveness, if any.