avoid undesirable outcomes. However, although management by instinct has proven to be generally effective throughout the ages, in today's competitive environment companies cannot afford to rely solely on instincts for success. The Sarbanes-Oxley Act of 2002 ("Sarbanes-Oxley") necessitates that management have a more structured, focused understanding of the key risks facing a company, particularly relating to financial reporting. In 2004, the Committee of Sponsoring Organizations (COSO) issued its Enterprise Risk Management Integrated Framework ("COSO ERM Framework"). This framework is helping to provide the impetus for more companies to implement enterprise risk management (ERM).

This chapter focuses on understanding of risk and how risk management concepts have evolved. It discusses risk, enterprise risk management, and corporate governance. This overview serves as a basis for concepts used throughout the entire book. It provides the foundation for understanding enterprise risk management, and how auditors can effectively add value when auditing in an ERM environment.

RISK DEFINED

Businesses must deal with risks, many of which have the same characteristics as those encountered elsewhere in life. To put risk in the proper business context, the COSO ERM Framework defines *risk* as follows:

> Risk is the possibility that an event will occur and adversely affect the achievement of an objective.

A few key, fundamental points are embedded in this definition:

- Risk begins with strategy. A company is in business to achieve particular strategies and objectives, and risks represent the barriers to successfully achieving those. Therefore, companies with different strategies will face different sets of risks.
- Risk does not represent a single point estimate (i.e., the most likely outcome). Rather it represents a range of possible outcomes. Because many different outcomes are possible, the concept of a range is what creates uncertainty when understanding and evaluating risks.
- Risk encompasses both opportunities and threats. Most people focus only on the downside of risk, that is, a hazard or negative outcome that needs to be mitigated or eliminated. While many risks do in fact present a threat, failure to exploit an opportunity or competitive advantage can be considered a significant risk as well.

Using this definition of risk, one begins to comprehend the extensive number of risks that businesses face as they try to execute their strategies. This extensiveness can be somewhat overwhelming, which brings greater appreciation for the need to have a process to effectively understand and manage the risks across an organization. This need can be addressed through enterprise risk management.

> **PRACTICE POINTER:** There are also definitions describing the nature of risks (i.e., the reasons risks exist). These typically fall into three categories: inherent risk, control risk, and detection risk. Statement on Auditing Standards No. 107 (SAS-107), *Audit Risk and Materiality in Conducting an Audit*, defines these three categories as follows:
>
> 1. *Inherent risk* is the susceptibility of a relevant assertion to a misstatement that could be material, either individually or when aggregated with other misstatements, assuming there are no related controls. The risk of such misstatement is greater for some assertions and related account balances, classes of transactions, and disclosures than for others. For example, complex calculations are more likely than simple calculations to be misstated. Cash is more susceptible to theft than is an inventory of coal. Accounts consisting of amounts derived from accounting estimates that are subject to a significant measurement of uncertainty pose greater risk than do accounts consisting of relatively routine, factual data. External circumstances giving rise to business risks also influence inherent risk. For example, technological developments might make a particular product obsolete, thereby causing inventory to be more susceptible to overstatement. In addition to those circumstances that are peculiar to a specific relevant assertion, factors in the entity and its environment that relate to several or all of the classes of transaction, account balances, or disclosures may influence the inherent risk related to a specific relevant assertion. These latter factors include a lack of sufficient working capital to continue operations or a declining industry characterized by a large number of business failures.
> 2. *Control risk* is the risk that a misstatement that could occur in a relevant assertion and that could be material, either individually or when aggregated with other misstatements, will not be prevented or detected on a timely basis by the entity's internal control. That risk is a function of the effectiveness of the design and operation of internal control in achieving the entity's objectives relevant to preparation of the entity's financial statements. Some control risk will always exist because of the inherent limitations of internal control.
> 3. *Detection risk* is the risk that the auditor will not detect a misstatement that exists in a relevant assertion that could be material, either individually or when aggregated with other misstatements. Detection risk is a function of the

which risks are most likely to significantly affect their ability to achieve their strategies (i.e., present the greatest exposure).

> **OBSERVATION:** The COSO ERM Framework makes reference to both inherent and residual risks. Although organizations must ultimately understand the inherent likelihood of a risk occurring at a given impact level in order to ensure optimal risk management, organizations with less risk experience tend to find residual risk, which evaluates likelihood after giving consideration to existing risk management activities, intuitively easier to understand.

Finally, it is necessary to understand the organization's tolerance for each risk. This assessment leverages off of the risk tolerance input discussed in the previous section. Because tolerance levels will vary from risk to risk, this assessment will help define how much tolerance management has for the specific risk scenarios. Risks with exposure beyond management's tolerance are prime candidates for focused risk management actions.

Filtering Risks

After completing the risk assessment stage, it is time to filter the risks. The spectrum of risk will include many more risks than an organization can focus on at a given point in time. Therefore, it is necessary to filter the risks down to a small, manageable number of *key* risks before proceeding to the risk analysis stage. The focus is on assuring that risks with a tolerable likelihood of significant impact are filtered out at this time, and that only those risks with an intolerable likelihood of significant impact are analyzed in the next stage.

RISK ANALYSIS STAGE

In the risk analysis stage management learns more about the key risks that filtered down from the risk assessment stage. The risk analysis stage covers the deeper analysis of risks alluded to in the Risk Assessment component of the COSO ERM Framework. In the risk analysis stage, the following primary questions need to be answered for each risk:

- Where does the risk occur (i.e., external to the organization, or internally within one of the business units, locations, functions, or processes)?
- What causes the risk to occur and why; that is, what are the key risk drivers?

- How can the risk be measured; that is, how will the organization know the risk is occurring and to what extent?

Answering these questions may be somewhat involved, therefore it is important to focus on only the *key* risks in the risk analysis stage.

Sources of Risk

Understanding the source of each risk helps to manage the risk at its source instead of some other point. If the source of a risk is not identified, the risk may not be managed as effectively and efficiently as desired by management. For example:

- External risks, those arising outside the organization, may not be fully manageable by the organization. Although there may be ways to influence and prepare for external risks (e.g., lobbying for legal and regulatory change, or continually scanning the market for competitor or other emerging industry changes), failure to recognize the external source of these risks may result in the organization devoting unnecessary resources toward attempting to manage these risks internally.
- Internal risks that are not managed at the source may result in ineffective deployment of valuable resources. For example, if an organization's products are not selling as expected due to a perception that the price is too high, there may be increased focus on managing price risk within the sales and marketing areas. However, if the real source of the risk is in the inability to effectively allocate costs among products, the risk may need to be managed in the accounting area.

Drivers of Risk

Once the source of a risk is understood (the "where"), the next step is to understand the cause of the risk (the "why"). Frequently, there are multiple reasons a risk might occur, ranging from inherent vulnerabilities to specific control deficiencies. These reasons are referred to as risk drivers. Drivers may be as follows:

- Specific events or incidents; examples include a natural disaster causing business continuity risk to increase, or a production problem causing defects, which, in turn, result in customer satisfaction risk increasing.
- Pervasive problems that accumulate to cause a risk; examples include inadequate screening of new hires causing an

- Whether stated or not, management has varying tolerance levels for each of the risks. Even if the tolerance is not clearly articulated, it is important to understand what management considers acceptable, relative to exceptions and errors.
- Audits are historical in nature; that is, they evaluate the effectiveness of activities based on how they operated in the past. However, understanding how performance and risks are measured, and how management monitors those measures, gives the auditor greater assurance regarding risk management effectiveness in the future as well.
- Not all activities focus on controlling or mitigating risks. Some activities allow an organization to exploit a competitive advantage and achieve key strategic objectives. Failure to do so may have more significant ramifications than failing to mitigate a risk. Therefore, considering risk optimization as part of an overall audit plan is extremely beneficial.

Applying a risk management-based audit approach does not preclude the auditor from performing earlier generation-type audits. The following examples describe situations when a risk management-based audit approach may dictate that specific audit projects follow one of the more traditional approaches:

- *Compliance Audit* Companies subject to regulation (e.g., banks, utilities) must comply with certain regulations. These companies typically have a stated or unstated objective to comply with applicable regulations. Therefore, because the potential impact of non-compliance can be significant, it is important to ensure that the risk management activities related to regulatory compliance risk are operating effectively. A compliance-focused, control-based audit may be the most appropriate way to provide that assurance. Management probably has little or no tolerance for non-compliance with such regulations.
- *Financial Audit* A consumer products company is heavily dependent on effective marketing campaigns to achieve its market share objectives. Because these marketing programs run for periods of time that do not necessarily correspond with the company's fiscal year, the accounting for marketing costs can have a material financial effect on an interim basis. Therefore, a financial audit at the completion of a key marketing program may be appropriate to ensure that the risk management activities relative to managing the financial aspects of marketing risk are operating as designed. Estimates and judgments may be required, therefore management may tolerate variability up to a certain percentage of the account balance.

- *Control Audit* The same consumer products company may have several marketing programs at any point in time. Because no single program is individually significant, yet, in the aggregate, programs operating during a given quarter are material, a control audit can provide assurance that the financially focused risk management activities are designed and operating effectively to manage marketing risk to an acceptable level for each of the marketing programs. Management probably has little or no tolerance for errors or inconsistent operation of the process and controls.
- *Process-Based Audit* A manufacturing company operates in a very competitive market where the quality of products is the primary difference between companies. Although warranty claims do not present a material financial risk, any perceived degradation in quality may adversely impact the company's market share. Because the company's success is highly dependent on optimizing its current capability to produce high-quality products, an operational audit, focusing on the efficiency and effectiveness of its quality control risk management activities, can help determine if the company is managing its quality assurance risk to an acceptable level. Similar to the control audit example, management probably has little or no tolerance to errors or inconsistent operation of the quality control process.
- *Risk-Based Audit* A consulting company inherently has a high degree of legal risk. Litigation relating to the services it provides could significantly erode the capital of its partners, therefore it is critical to mitigate legal risk to a relatively low level (e.g., the value of fees paid for the services). A risk-based audit can help provide assurance that the contracting process effectively limits the company's exposure in the event of a dispute with a customer. Management would probably have no tolerance to exceptions, due to the potential exposure of not effectively mitigating the risk.

Each of these examples illustrates how risk management-based audit needs can be met by performing an audit following the approach from one of the previous audit generations. While the approaches vary among them, they all have the following risk management-based audit characteristics:

- All audits are based on the need to achieve a business objective, whether formally stated or not.
- All are performed to determine whether the underlying risks are effectively mitigated or optimized to an acceptable level.

Define Risks

Risks may be defined in a variety of formats, based on the source from which each risk was derived. However, these definitions may not be clear to all parties involved in the risk assessment. Therefore, the next key step is to define the risks in a consistent manner, and create a common risk language for the organization. The following tips have proven effective when preparing a concise, customized risk universe:

- *Define the risks in a cause-and-effect format.* That is, begin each definition with a brief description of the risk and end it with the consequence. For example, a definition of human resources risk might be "Failure to attract, develop, and retain competent individuals inhibits the organization's ability to execute, manage, and monitor key business activities."
- *Keep the definitions brief (preferably one sentence).* The initial assessment of risks is a very involved process, and preparing detailed definitions may "put people in a box" in terms of how they think of a risk. Having brief, high-level definitions allows participants to think broadly about a variety of causes and effects. The discussion and analysis during risk assessment will provide the needed input to make the definitions more specific, if necessary.
- *Customize the definitions by using the language the organization speaks.* A risk universe should provide a common risk language, ensuring that when one individual refers to a risk by name, everyone knows what that individual is referring to. Customizing generic risks to incorporate the organization "lingo" helps ensure this common language is created and understood.

PRACTICE POINTER: Don't underestimate the importance of consistent risk definitions. One of the greatest barriers to successful risk assessment is lack of a common understanding of what each risk means. Failure to utilize a consistent definition format will result in different interpretations of risk and, ultimately, more confusion when trying to assess the risks.

Link Risks to Strategies

Risks are uncertainties that an organization faces as it executes its strategies. Therefore, each risk must be put in a context of how it can affect the strategies. Chapter 4, "Strategy: The Beginning of The Journey," discussed the importance of linking risks to strategies.

The following is an example illustrating how the strategic and value objectives defined in Chapter 4 can be linked to three specific risks, which are defined below:

AfterMath Example

Strategic Objective A—Enhance shareholder value by consistently delivering operating earnings growth (currently 25%).
Strategic Objective B—Penetrate 60% of the top 1,000 school districts, and 40% of the next tier of 1,500 school districts.
Strategic Objective C—Be recognized by educators, institutions, and associations as a significant contributor to the advancement of education objectives in the United States.
Strategic Objective D—Achieve a ranking in the top 50 of *Business Today Magazine's* "Best Companies to Work For".
Value A—Always act with integrity when dealing with fellow employees, customers, vendors, or other parties to whom you are representing the company.
Risk A—*Competitor Risk:* Failure to effectively monitor and understand competitor actions may result in diminished market share and, ultimately, questions about the viability of AfterMath's business model.
Risk B—*Policies and Procedures Risk:* Lack of compliance with established policies and procedures may result in unacceptable performance by employees, which, in turn, may cause an inability to achieve financial, operational, or customer objectives.
Risk C—*Health and Safety Risk:* Failure to protect the health and safety of employees and third parties on company property may result in claims, fines, low morale, or reduced productivity.

Each organization's business model is unique and, therefore, its risk universe is unique. Linking all of the identified business risks to strategies will help validate the inclusion of each risk in the universe. If a risk cannot be linked to a strategic objective, operational objective, financial objective, or value, it may not be properly defined or even relevant for the organization. That is why it is important to link risks to strategies before proceeding with the formal business risk assessment.

When first working through this exercise, many of the risks may appear to affect more than one objective, indicating these risks are somewhat pervasive. For example, Policies and Procedures risk may have a direct effect on several objectives, because lack of well-defined and consistently followed policies and procedures will have an effect on one or more of the direct drivers.

However, some of the other risks may appear to affect several objectives, but with further analysis comes a realization that the correlation is not as strong, so these risks are not shown as linked.

Scales such as those in Illustration 6-4 can be used for a single vote on significance and likelihood.

Illustration 6-4: Examples of Scales for a Single Vote on Significance and Likelihood

Simple Scale

1 **Low Threat** Not likely to be a significant threat to the organization.
5 **Moderate Threat** May occasionally prove to be a significant threat to the organization.
9 **High Threat** Likely to be a significant threat to the organization.

Enhanced Scale

1 **Very Low Threat** Virtually no chance of significantly threatening the organization.
3 **Low Threat** Not very likely to significantly threaten the organization.
5 **Moderate Threat** May occasionally prove to be a significant threat to the organization.
7 **High Threat** Likely to be a significant threat to the organization.
9 **Extremely High Threat** Is, or certainly will be, a significant threat to the organization.

Specific Scale

Refer to the significance criterion section for examples of specific threats (strategic or financial).

Computation/Combination

If separate significance and likelihood assessments have been completed, these two assessments may be combined to determine the level of risk. Examples of these combinations are as follows:

- **Simple Average** The significance and likelihood votes are averaged to determine level of risk. This is the simplest and most common method of computing level of risk. When using this method, it is advisable to eliminate risks with an average below a predetermined level (e.g., 5 on a scale of 9) to reduce the number of assessments going forward.
- **Weighted Average** Some people believe the significance criterion should carry more weight than the likelihood criterion. This can be accomplished by weighting the significance factor more heavily in the computation. For example, multiplying significance by 1.2, adding the likelihood, and dividing by 2 determines a weighted average with greater emphasis on the significance criterion. When using this method, it is advisable to eliminate risks with an average below a predetermined level (e.g., 6 on a scale of 9) to reduce the number of assessments going forward.

OBSERVATION: Other techniques (such as multiplying significance by likelihood and dividing by the top scale value) may be applicable, but caution is encouraged because the mathematical relationships become less intuitive and may cause confusion among the participants.

Separate Assessment

Another approach is to perform a separate assessment through a combined vote on significance and likelihood as depicted in the following nine-box map. The definitions of significance and likelihood may be similar to the ones previously discussed.

Each participant votes *one* box for every risk (e.g., if the participant believes the risk has high significance and moderate likelihood, they would vote an "8"). The average for each risk determines the group's consensus for level of risk, and is represented by that risk's placement in one of the nine boxes.

6 High Significance/ Low Likelihood	**8** High Significance/ Moderate Likelihood	**9** High Significance/ High Likelihood
3 Moderate Significance/ Low Likelihood	**5** Moderate Significance/ Moderate Likelihood	**7** Moderate Significance/ High Likelihood
1 Low Significance/ Low Likelihood	**2** Low Significance/ Moderate Likelihood	**4** Low Significance/ High Likelihood

OBSERVATION: Although this can be a very efficient means of determining level of risk, facilitators must help the participants identify and understand divergence in votes caused by differences in opinion on *either* significance or likelihood. For example, if one group believes a risk is high significance and low likelihood (box 6), and another group believes it is low significance and high likelihood (box 4), the average (box 5—moderate significance and moderate likelihood) may

3. Combine similar barriers into groups that may reflect a single risk.
4. Create risk definitions for each group and other individual barriers.
5. Link all of the risks to the objectives to ensure comprehensiveness of the risk listing. (This can be completed using a matrix similar to the example provided in Chapter 5.)
6. Validate the risks with appropriate process management to ensure:
   a. The definitions make sense and "speak their language."
   b. All risks that can be combined have been.
   c. The list is complete.

PRACTICE POINTER: Although the audit team typically completes this exercise, it is preferable to involve process management in the brainstorming of risks. Even if management is unwilling to participate in a formal brainstorming session, a survey of key process individuals can assist in the identification of events, scenarios, issues, or circumstances that might cause objectives to fail. At a minimum, the resultant list of risks should be shared with and agreed to by process management.

PRACTICE POINTER: It is important to have a consistent format for defining risks. Because process-level people are typically less experienced with risk concepts, they tend to perceive stated risks as current issues. Care should be taken to utilize a definition format that makes it clear that each risk is an inherent risk in the process, and not the audit team's judgment of where potential issues will arise from the audit.

Illustration 8-1 is an example of this approach.

Illustration 8-1: AfterMath Example

Accounting Objective—Post all journal entries accurately and timely.

Barriers—The following represent potential barriers to achieving this objective.

- Accounting processes are not formally designed and documented to provide direction on how to process journal entries.
- The general ledger system does not provide edit checks and other systematic checks to flag journal entries that are not input accurately.

- Systems security is inadequate to prevent journal entries from being inappropriately modified.
- Accounting personnel are not adequately trained and supervised in how to execute the journal entry process.
- There is no management review of journal entries to validate the appropriateness of journal entries.
- There are no performance measures to motivate the timely and accurate processing of journal entries.

Risks—The potential barriers can be summarized and defined as the following risks.

- **Policies and Procedures Risk** Polices and procedures that are ineffective, insufficient, unclear, or outdated may result in poorly executed processes.
- **Human Resources Risk** Inadequate training, development, and supervision of personnel may result in the inability of employees to effectively and consistently perform key processes.
- **Systems Risk** Outdated, inadequate, or non-interfacing systems may inhibit the ability of personnel to execute key processes.
- **Performance Measurement Risk** Lack of defined metrics, and inability to gather relevant information for measurement purposes, may impair management's ability to monitor individual and team performance.

Although there may be additional risks inherent in achieving the above accounting objective, this illustration demonstrates how to perform the process of identifying and defining process-level risks. Additional examples can be found in the audit project case studies, beginning in Chapter 19, "Case Study: Close the Books."

Risk Assessment

The approach to assessing and prioritizing risks at the process level is similar to, but simpler than, the assessment at the business level. This step aligns with the Risk Assessment component of the COSO ERM Framework. The focus is on impact and likelihood for each process-level risk. Since there are typically fewer risks at the process level than the business level and precision is less important (the actual impact and likelihood can be validated as part of the audit process), the simple scales discussed in Chapter 6 can be used effectively.

Evaluating impact and likelihood at the process level must be both consistent and focused. The following provides guidance for evaluating these criteria:

- Impact should focus on the potential exposure over a specific period of time, typically one year. Because risks may occur

As with the process design evaluation, it is important to have a consistent way of communicating the conclusions being made. The same terms are utilized, with modifications made to reflect the effectiveness of the operation of the process:

- **Strong Operation** The key controls are operating effectively to ensure all key risks are managed to an acceptable level. While there may be some opportunities to improve the efficiency and effectiveness of the process operation, there are no significant shortcomings relative to the management of the key risks.
- **Moderate Operation** The key controls are operating effectively to ensure most of the key risks are managed to an acceptable level, but there are gaps for certain key risks. These gaps probably will not cause the overall process to fall significantly short of achieving the desired result, but there may be impacts (e.g., financial, customer, reputation) that process-level management would consider unacceptable.
- **Weak Operation** Several of the key risks have gaps in operation that will likely result in the process not achieving the desired result on a consistent basis. There are typically actions that must be pursued immediately to improve the operation of the process to ensure those risks can be managed to an acceptable level.

These terms can be used in audit reports to articulate the auditor's judgment regarding control effectiveness or risk management effectiveness. Refer to Chapter 12, "Action Planning Phase: The Real Value," where reporting the results of audits is discussed.

> **OBSERVATION:** "Acceptable level" and "desired results" are judgments that vary from company to company, and even process to process. However, if the process is integral to a company's evaluation of its internal controls over financial reporting, the acceptable level may be defined relative to the guidance in professional standards as to what constitutes a material weakness or significant deficiency.

SUMMARY

The testing phase of an audit is conducted to (1) validate whether the process is operating as designed to ensure the desired results are achieved or (2) determine the impact if the process is not designed or operating adequately. In this phase the auditor answers

the following questions that arise after completing the process design phase:

1. What tests should be performed to validate that the process is operating as designed? Typically, attribute tests are most appropriate to corroborate that the process is operating as designed as such tests determine that relevant attributes of key controls are being consistently executed. The attribute tests to be performed are documented in the audit matrix.
2. What tests should be performed to determine the impact when portions of the process are not adequately designed? Typically, quantitative tests provide the information necessary to compute or extrapolate the impact of a process that is not effectively designed or is not consistently operating as designed. The quantitative tests to be performed are documented in the audit matrix.
3. Based on the results of testing, how effectively is the process operating? After testing is completed, the evaluation of the testing results is documented in the audit matrix. This documentation includes conclusions about how effectively the process is operating.
4. If the process is not consistently operating as designed, why isn't it and what opportunities for improvement exist? The auditor must identify the root causes of inadequate operation and possible solutions to improve the operation of the process to a level that will assure the risks are managed to an acceptable level. This is documented as audit findings in the workpapers (refer to Chapter 12 for additional discussion).

A well-designed and well-operating process provides assurance that the key risks are managed to an acceptable level. When the process is not consistently operating effectively, the auditor must determine the impact of the operational shortcomings and possible solutions.

EXHIBIT 10-1
TESTING PHASE
WORK PROGRAM

Program Step	Target Date	Completion Date	Completed By
1. What is the overall focus of audit testing?			
a. To validate that a well-designed process is operating as intended.			

- The auditor must ensure that findings are discussed with appropriate management. Typically, findings should be discussed with both the individual(s) responsible for implementing solutions and the process owner.
- Management may have a different idea on how to best address the finding. The auditor should be open to such ideas as management's solution maybe more effective and viable than the auditor's original recommendation.
- If management disagrees with the auditor on the finding or recommendations, the auditor may not fully understand management's risk tolerance. The auditor should thus revisit with management their tolerance level to reach an agreement on the validity of the finding, the need to address it, and the appropriate recommendations.

OBSERVATION: When an "agreed-upon solutions" approach is utilized for reporting audit results (versus the "recommendations and management's response" approach), the cycle time for issuing the final report is typically reduced. This is due to it being easier for management to edit the agreed-upon solutions as compared to creating specific responses to the recommendations.

Disposition

Up until this point in the audit, all findings were considered candidates for the final audit report. Now that the auditor has articulated the finding, determined the potential impacts, identified the root causes, developed recommendations, and received management's comments, it is time to decide whether the finding will be

1. Included in the final audit report;
2. Modified or combined with other findings to better state the issues and provide more actionable solutions;
3. Discussed with management and delivered informally as an opportunity for improvement, but not included in the final audit report due to its relative low risk; or
4. Removed from consideration for the audit report, due to subsequent facts or considerations from management that render it inappropriate or unnecessary.

Helpful Hints

- The judgments applied in determining the disposition of an audit finding are some of the most important judgments an auditor makes; therefore, these judgments should be documented in the workpapers.
- Decisions on which findings to include in the final audit report are influenced by the audit department's reporting protocol and objectives—that is, some audit departments include all valid findings in a detailed audit report, while others filter out and exclude the less important findings.
- When valid, but less significant, findings are excluded from a formal audit report, management may still appreciate a summary of those excluded findings as a reminder of other opportunities identified in the audit.

Owner

Each audit finding must have an owner who is ultimately responsible for ensuring that the corresponding recommendations are implemented. This assignment of authority and accountability is necessary to avoid confusion over responsibility for the actions and provide a point of contact for monitoring implementation progress. (Refer to Chapter 13 for a discussion of follow-up and monitoring procedures.)

Helpful Hints

- The owner should be an individual with both the knowledge and ability to implement the required actions.
- While other individuals may help with implementing the solutions, identifying a single point person makes it easier for both the process owner and auditor to follow up on the recommendations.
- The owner must acknowledge and accept the responsibility and accountability that has been granted him or her. Therefore, the auditor should not simply work with the process owner to assign ownership, but should also talk directly with the action owner about the finding and recommended actions to ensure they understand what needs to be done and why.

Target Date

Reportable audit findings must be acted upon in a timely manner to limit the period during which the key risks are not being managed to an acceptable level. Therefore, target dates should be agreed to with the owners to ensure timely implementation.

- Lack of formally articulated risk tolerance levels may result in:
  - — Risks that are managed to levels that are not consistent with the organization's overall risk appetite risk taking philosophy; or
  - — Confusion among individuals regarding what the boundaries and limits are for key risk-related activities and decisions.
- An inadequately defined or positioned risk management function may impair the abilities of the individuals involved in the function to carry out their responsibilities effectively.

RISK ASSESSMENT

Once the foundation is established with the inputs into the funnel, risk assessment is the starting point for specific ERM activities. There are several key attributes that are necessary to effectively execute the risk assessment process.

Key Questions

The following questions will help to address the key risk assessment attributes:

- Has a risk universe been developed that captures all key risks the organization faces?
  - — Have risk events or scenarios been identified?
  - — Have areas and categories been created to establish a formal risk model that is customized for the organization?
  - — Are each of the risks defined using words and thoughts that are consistent with how the organization speaks (i.e., has a common risk language been created)?
  - — Have the risks been linked to the organization's strategy?
- Has the impact of each risk been formally assessed?
  - — Have both financial and nonfinancial impacts been considered (e.g., strategic, reputational, legal, health and safety)?
  - — Have realistic worst-case scenarios been identified and considered?
  - — Is there a consensus on the risk impact?

- Has the likelihood of that impact been determined for each risk?
  - — Is the likelihood inherent or managed (residual)?
  - — Is there a consensus on the risk likelihood?
- Has management's tolerance relative to their acceptance of each risk's exposure been determined?
  - — Does the tolerance correspond with the likelihood assessment, allowing for a meaningful assessment of the gap between current and tolerable likelihood?
  - — Is there a consensus on the risk tolerance?
- Are there other assessment criteria (e.g., manageability, efficiency) utilized by management to assess risks?
  - — Is the assessment of these criteria appropriately related to the other criteria utilized in the assessment?
- Have the key or primary risks been identified for the company?

Potential Exposures

Failure to adequately address the key risk assessment attributes might create the following exposures:

- Inadequate identification, categorization, and definition of all key business risks into a comprehensive risk universe may result in
  - — Lack of recognition and management of certain key risks;
  - — Confusion and misunderstanding when discussing risks among individuals within the company; or
  - — An overly cumbersome, unorganized risk listing that cannot be effectively understood and managed.
- Ineffective assessment of risk impact may result in
  - — Lack of recognition regarding how significantly risk occurrences will impact the organization, causing under-management of key risks; or
  - — Over-allocation of resources toward risks with less potential impact.
- Ineffective assessment of risk likelihood may result in
  - — Lack of recognition regarding how likely significant risk occurrences will be, causing under-management of key risks; or

such methods perceive each of the attributes being rated at that particular point in time. However, such perceptions may vary from one individual to the next based on the scenarios they choose to think about when making their judgments as well as their own biases and tolerances to risk. As a result, the information gathered, while valuable, may not be as comprehensive or reliable when compared to the information gathered in a facilitated risk assessment session. Such sessions offer the following advantages:

- The results of initial judgments (typically gathered by some form of voting method) can be compiled and discussed among the entire group involved in the session. This discussion helps to bring alignment among the group; not so much in terms of agreeing on ratings but ensuring consistency about what scenarios are being considered that support the judgments used when rating the individual risks. This discussion is frequently more valuable to management than the actual ratings themselves.
- If the discussion indicates that the participants did in fact view the risks from different and incongruous perspectives, it is easy to re-vote the rating at that time. Once again, this will not ensure consensus, but it will increase the validity of the resultant average.
- Once all of the risks are rated, the group can look at the ranking or order of the risks and discuss whether such rankings make sense. This is important because, throughout the course of a facilitated session, some bias, or vote creep, may subtly occur without it being recognized. By taking a step back and looking at the resultant rankings, the group may be able to detect anomalies in the rankings that require re-voting.

Question: **What factors or outcomes should be considered when devising risk scales?**

Answer: The most common and obvious factor—financial impact—typically is the easiest to measure and generally is the most quantifiable. However, other factors or risk outcomes may prove to have a greater impact and, thus, should also be considered. Examples of risk occurrences whose impact may exceed the financial impact are as follows:

- A threat to the health or safety of employees or customers may be more significant than the fine resulting from the occurrence.
- Damage to the reputation of the organization may have a more adverse effect on share price or future sales than the financial impact of the event.
- An event that results in the downgrading of an organization's credit rating may cause severe liquidity problems in the future that far exceed the financial impact of the event.
- A fraud or some other action by management may diminish the trust employees have in management, causing profound changes in the culture and diminished reliance on entity-level controls (e.g., tone at the top).

The assessment of risks should not be limited by the financial impact. Doing so may result in a failure to identify other key risks or underassessing the impact of such risks, resulting in the misallocation of risk management efforts.

Question: **When using voting equipment or surveys, should the averages be used as the final assessment results or should additional judgment be applied?**

Answer: Risk assessment is, by nature, a very judgmental process and, as such, quantitative information must always be balanced against qualitative judgments. The quantitative information can be very valuable in helping management prioritize risks. However, one should be careful to avoid relying solely on these quantitative results. The quantitative ratings still involve a great deal of judgment, and defaulting to the ratings may result in management inadvertently ignoring bias that may have existed when ranking the risks. Therefore, it is important to look at the relative placement of the risks and evaluate whether this placement may result in a misallocation of risk management resources.

Question: **How do organizations assess strategic risks that may put the company out of business?**

Answer: This is one of the most difficult aspects of risk assessment; however, it should not be ignored as the

Desired Stage

The average score for the Desired Stage was 7.8, reflecting the executive team's view that, as a technology company, they needed to be at or above the *managed* stage for this capability. Failure to effectively execute its technology capabilities might diminish the company's competitive advantage. Specifically, this assessment was due to the following factors:

- AfterMath must continue to maintain a competitive advantage with the technology embedded in its products. The financial and supporting systems were considered to already be at an acceptable stage.
- The company should take a more proactive approach to enhancing financial and other supporting systems. This was deemed necessary to ensure the quality and costs of its products remained acceptable.
- The current security infrastructure is considered to be acceptable as is; no enhancements were seen as necessary at this time.

Gap Analysis

Because the technology capability is currently approaching the *managed* stage, with a relatively small gap of 1.2, opportunities to close the gap are somewhat limited. However, the executive team did agree to the following action.

- The CIO agreed to establish a more consistent approach to identifying potential options for enhancement. He will assemble a steering team to ensure system needs are discussed on a regular basis, and to support the prioritization of systems enhancement initiatives.

INFORMATION

Overall, the consensus was strong that information is available when needed from the company systems; however, information from external sources was not as consistent. This feeling was stronger in areas that deal with some outsiders more than others.

Current Stage

The average score for the current stage was 6.2, reflecting the belief that the company currently had characteristics from both the *defined* stage and the *managed* stage. This assessment was due to the following factors:

- Information within the company's systems is accurate, relevant, and generally easy to obtain. However, AfterMath does not have good sources of market and competitor intelligence; therefore, external information is not as timely and accurate.
- Reports are generally timely, relevant, and accurate. The design of key reports has not been reviewed in some time, but most participants indicated that the reports were probably still appropriate.
- Access to critical and confidential data is well protected, with an appropriate level of access restrictions in place. Monitoring of access violations is generally a manually intensive process.

Desired Stage

The average score for the desired stage was 7.5, reflecting the executive team's view that information needed to be at or above the *managed* stage for this capability. There was little tolerance to information shortcomings with internal systems, but greater acceptance of the challenges in obtaining reliable external information. Specifically, this assessment was due to the following factors:

- Information from the company's systems must remain accurate, relevant, and accessible. Improved availability of relevant information on the market and competitors was perceived to be valuable to maintain the company's competitive advantage.
- While reports are considered timely, relevant, and accurate the design of certain key reports could be enhanced to improve their usability.
- Access to critical and confidential data should be maintained at the current level, although greater use of on-line monitoring techniques would be desirable.

Gap Analysis

Since the information capability is currently between the *defined* and *managed* stages, and the gap is relatively small at 1.3, opportunities to close the gap are somewhat limited. However, the executive team did identify some opportunities worth pursuing.

- An individual reporting to the Vice President—Strategic Planning will be assigned the responsibility of establishing formal information sources of market and competitor

Risk Name and Definition	Risk Box	Key Control	Design Gap Analysis
Systems Risk—Outdated, inadequate, or non-interfacing systems (e.g., inventory management and accounting) may inhibit AfterMath's ability to manage and monitor inventory levels, resulting in excessive carrying costs or production delays.	9	• Since the Inventrix system is critical to AfterMath's success, an IT project leader is assigned full-time to work with users on ongoing enhancements and updates. • Inventrix automatically interfaces with the general ledger as part of nightly batch processing.	The process and systems design appear to be adequate to manage this risk to an acceptable level.
Vendor Performance Risk—Inadequate assembly of component parts by outsourcing vendors, untimely or misleading communications from vendors relative to parts on hand or delivery dates, and insufficient means of measuring and monitoring vendor performance, may result in substandard quality or delays in receiving necessary component parts.	6	• There is not a formal process to monitor whether vendors are consistently complying with performance expectations. • There have been incidents where vendors were late in delivering assembled units or such units were of substandard quality. In such cases, AfterMath typically works around the problem with in-house resources instead of communicating and rectifying the problem with the vendors.	The process design does not appear to be adequate to manage this risk to an acceptable level since there are no formal procedures to monitor and address vendor performance issues (***Audit Finding #4***).

EXHIBIT 20-3
AUDIT MATRIX: OPERATION OF RISK MANAGEMENT CAPABILITIES

The section of the audit matrix relating to the Inventory audit documents the testing approach and test results, which provides the basis for assessing the operation of risk management capabilities.

Risk Name	Testing Approach	Test Results	Conclusion
Accounting Risk	1. Test monthly reconciliations as of the most recent month-end to validate that Inventrix balances agree with the general ledger. 2. Observe the 4th quarter inventory count and test to ensure quantities on hand agree with Inventrix.	1. All balances per Inventrix agreed with the general ledger. 2. The 4th quarter inventory count was conducted in accordance with company procedures, and resulting adjustments were less than .5.	The design and operation of the Accounting process appear to be sufficient to manage this risk to an acceptable level.
Budgeting and Forecasting Risk	1. Review end-of-month unit balances for finished units, motherboards, viewable screens, plastic outer casings, and protective carrying cases to ensure the unit quantities were consistently within acceptable ranges.	1. While the ending balance was never lower than the computed acceptable level, unit levels were excessive for motherboards (two months), viewable screens (six months), and plastic outer casings (five months).	While Inventrix is flagging excessive inventory balances, AfterMath is not effectively managing and outsourcing vendors to ensure their production and shipment of assembled components is consistent with the Company's standards (***Audit Finding #2***).
Contract Risk	1. Considering the effective process design, no testing of this risk is considered necessary.	N/A	The design and operation of the contracting process appear to be sufficient to manage this risk to an acceptable level.
Health and Safety Risk	N/A	N/A	N/A
Human Resources Risk	1. Considering the effective process design, no testing of this risk is considered necessary.	N/A	The design and operation of the Human Resources process appear to be sufficient to manage this risk to an acceptable level.
Integrity Risk	N/A	N/A	N/A
Obsolescence Risk	1. Discuss with personnel in Research & Development	1. The only change Research & Development was concerned	The design and operation of Obsolescence risk management

As described in Chapter 17, Exhibit 17-3, inventory management is a key process to manage supply chain risk. The procurement process is an integral part of the inventory management process and, thus, is a key to manage supply chain risk. Therefore, a procurement audit was scheduled in the upcoming year.

The objective of this audit was to *"Determine AfterMath's capabilities to manage the procurement process to the desired level (including supplier selection, bidding, contracting, and product or service receipt)."* Since more than just inventory items are procured by the procurement function, this audit will cover all procurement activities for AfterMath. This chapter outlines the background, process, and results of the audit.

BACKGROUND INFORMATION

The following provides relevant information about AfterMath's procurement activities, which information is necessary for effectively conducting this procurement audit.

- The Director of Procurement has overall responsibility for running the Procurement department. Two Purchasing Agents assist him in carrying out procurement activities. The Director of Procurement reports to AfterMath's General Counsel.
- The Director of Procurement and two Purchasing Agents are the only authorized agents of the company; that is, they are the only individuals with the authority to bind the company for purchases over $10,000. Purchases under $10,000 can be executed through the use of a purchase order by managers and above.
- AfterMath utilizes company-authorized credit cards (procurement cards) for small purchases (under $1,000). Over the last 12 months, approximately $1.6 million has been purchased with procurement cards.
- The Procurement department processed approximately $125 million of purchases over the last year.
- AfterMath currently has almost 1,000 vendors, of which approximately 450 have recurring activity throughout the year. The Procurement department is responsible for vendor selection, and setup and maintenance within the system.
- The general ledger system contains a purchase order module that is utilized to process all purchase orders and contract information. This module directly interfaces with the accounts payable module in the general ledger.

KEY OBJECTIVES

After discussion with the Director of Procurement, it was clear that the area has formal, well-defined strategic and operational objectives. The Director took great pride in the annual exercise he executes with the Purchasing Agents to update the objectives and ensure alignment with AfterMath's overall strategic objectives. Through discussions with key internal customers during the annual budgeting process, the Director believes his function will continue to meet the needs of the Company over the upcoming year.

Following are the key procurement objectives that have just been finalized for the next year.

1. **Best Purchase** Ensure purchases meet the needs of the company; that is, the right goods or services are at the right place, at the right time, and at the best price (supports AfterMath's Earnings Growth and Market Share objectives).
2. **Legal** Ensure all purchases appropriately protect the company's legal interests and do not create potential legal exposures (supports AfterMath's Earnings Growth, Market Share and Reputation objectives).
3. **Vendor Relations** Create and foster positive relationships, which will help ensure vendors cherish their relationship with AfterMath and will offer the company the best available terms (supports AfterMath's Earnings Growth and Integrity objectives).
4. **People** Make the Procurement department a positive and rewarding place to work by providing development and advancement opportunities, either within the area or in other areas of the company (supports AfterMath's People objective).

The Director of Procurement also indicated that he had developed specific key performance indicators (KPIs) to measure and monitor how effectively the department was achieving its objectives. The KPIs for each of the objectives are as follows:

1. **Best Purchase**
   a. Costs of recurring purchases grow at less than the CPI (Consumer Price Index) for all major procurement categories (e.g., inventory, office supplies, services).
   b. Costs of new purchases represent the lowest of qualifying bids.
   c. Internal customer surveys, which cover quality and timeliness of procurement services, average more than 4.0 on a 1–5 scale.

However, in order to validate that these risk management capabilities are designed properly and operate effectively, management agreed that a risk management-based audit would be appropriate for key processes surrounding cash flow/liquidity and supply chain activities.

In addition to the inventory management (Chapter 20, "Case Study: Inventory") and procurement (Chapter 21, "Case Study: Procurement") processes, as indicated in Chapter 17, Exhibit 17-3, the accounts payable and disbursements processes are key processes utilized to manage the cash flow/liquidity and supply chain risks. Therefore, an accounts payable and disbursements audit was scheduled in the upcoming year.

The objective of this audit was to *"Determine AfterMath's capabilities to manage the disbursements and accounts payable processes to the desired level."* This chapter outlines the background, process, and results of the audit.

BACKGROUND INFORMATION

The following provides relevant information about AfterMath's disbursement activities and accounts payable department, which is necessary for effectively conducting this accounts payable and disbursements audit.

- The Accounts Payable department processed $127 million of disbursements transactions over the last year.
- The average month-end accounts payable balance was $11 million, with month-end balances ranging from $7 million to $17 million over the last 12 months.
- AfterMath strives to take advantage of discounts on the $64 million of invoices eligible for discounts per the payment terms. The discount terms are typically 2% discount if paid within 10 days of the billing date (i.e., 2%, net 10).
- The objective is to pay bills not subject to discount when due (typically 30 days after the billing date). There is a strong desire to avoid being charged penalties or interest on late payments.
- The Accounts Payable department is led by the Accounts Payable Manager, with two supervisors and four clerks reporting up to the Manager. The Accounts Payable Manager reports to the Controller.
- The accounts payable module in the company's general ledger system is utilized to process all accounts payable transactions. This module directly interfaces with the accounting records in the general ledger and the purchase order system.

KEY OBJECTIVES

After discussion with the Accounts Payable Manager, it was clear that the area does not have formally stated strategic or operational objectives. The Manager had little interest in working with the audit team on developing such objectives because she believes, "Everybody knows what we are here to do." Therefore, the audit team had to determine what they believed the objectives were to provide the foundation for this audit.

The audit team brainstormed potential operational objectives related to the accounts payable and disbursements processes. In addition, the audit team considered AfterMath's strategic and value objectives to identify other relevant objectives. After clarifying and combining the ideas, the team agreed that the following are the key strategic and operational objectives for the area.

1. **Accuracy** Ensure payments to vendors are accurate and amounts recorded in the general ledger accurately reflect the obligations of the company (supports AfterMath's Earnings Growth objective).
2. **Timeliness** Pay all invoices timely to take advantage of discounts where available, and avoid penalties or interest on late payments (supports AfterMath's Earnings Growth objective).
3. **Vendor Relations** Respond to vendor inquiries and deal with vendors in a respectful manner to foster positive relationships, which will help ensure vendors cherish their relationship with AfterMath and will offer the company the best available terms (supports AfterMath's Earnings Growth and Integrity objectives).
4. **People** Develop Accounts Payable employees for advancement opportunities, either within the area or in other areas of the company, and promote acting with integrity in all internal and external dealings (supports AfterMath's People and Integrity objectives).

While information is available to measure some of these objectives, the Accounts Payable Manager indicated that she has not established and does not currently monitor any key performance indicators (KPIs). She agreed that KPIs might be helpful, but would like more information about what would be measured and monitored before agreeing to formalizing KPIs **(Audit Finding #1).**

The audit team next discussed tolerance levels with the Accounts Payable Manager, who believed that, generally, any errors or delayed payments were unacceptable in her mind; however, she would "defer to the experts" (i.e., the auditors) on what would be considered a significant risk management issue. The audit team decided that it

management agreed that a risk management-based audit would be appropriate for key processes surrounding quality assurance activities.

As indicated in Chapter 17, Exhibit 17-3, the production cycle and quality assurance processes are key to managing quality assurance risk. The sub-processes relating to quality assurance for internally produced and outsourced parts are integral to managing this risk. Therefore, a quality assurance audit was scheduled in the upcoming year.

The objective of this audit was to *"Validate the effectiveness of AfterMath's quality assurance capabilities to help manage product failures to an acceptable level."* This chapter outlines the background, process, and results of the audit.

BACKGROUND INFORMATION

The following provides relevant information about AfterMath's quality assurance activities, which is necessary for effectively conducting this procurement audit:

- The Director of Quality Assurance reports directly to the Vice President—Production.
- Reporting to the Director of Quality Assurance are two Quality Control Auditors, one focusing on internally produced parts and units and the other focusing on the assembled components received from the outsourcing vendors.
- The company's philosophy is that quality should be built in at all stages in the production process, rather than inspected and detected later. Therefore, the Quality Control Auditors spend a portion of their time working with and training production line employees on techniques to build in quality.
- Any defects or problems identified during the Quality Control Auditor's inspections are immediately sent back to the production line for rework.
- The Quality Assurance department also takes on quality initiatives in other parts of the company (however, these other initiatives are not within the scope of this audit).

KEY OBJECTIVES

The Director of Quality Assurance emphasized that the area has formal, well-defined strategic and operational objectives. She believes her department serves a very focused and vital role in supporting the company's strategic objectives. In fact, having a

name in the marketplace for consistently high-quality products gives AfterMath a competitive advantage. She also believes that, throughout the course of the audit, it will become evident to the audit team that her two Quality Control Auditors clearly understand and embrace these objectives.

Following are the key quality assurance objectives:

1. **Zero Defects** Ensure that products being shipped to customers have no defects (supports AfterMath's Earnings Growth, Market Share, and Reputation objectives).
2. **Quality Mindset** Provide education, training, and advice throughout the company to promote a mindset of high quality in all employees (supports AfterMath's Earnings Growth, Market Share, Reputation, and People objectives).

The Director of Quality Assurance also stated that she had developed specific key performance indicators (KPIs) to measure and monitor how effectively the department was achieving its objectives. The KPIs for each of the objectives are as follows:

1. **Zero Defects**
   a. No logic, wiring, display, or memory defects are subsequently discovered in products shipped to customers.
   b. Quality control inspections discover 98% of all structural defects (e.g., casing, straps, viewable screens) in finished products.
2. **Quality Mindset**
   a. All new employees on the production line receive quality control training within one week of commencing employment.
   b. The department receives at least a 4.2 average score on internal customer surveys conducted to assess the quality of educational, training, and advisory efforts.

The audit team next discussed tolerance levels with the Director of Quality Assurance, who believed that any results outside of the established KPIs would be considered unacceptable to both her and the Vice President—Production.

Finally, the audit team discussed organizational considerations with the Director of Quality Assurance. The Quality Assurance department is small and centralized, and she closely supervises the activities of the department on an ongoing basis. The success of the department is dependent on effective communications with the production line. She was not aware of any other organizational or cultural considerations that would impact the audit and the audit team's assessment of risk management effectiveness.