- Resource allocations are increased or decreased as appropriate to ensure the ERM activities are achieving the desired results.

Innovative Level

- ERM objectives are a driving force behind strategic planning.
- Resource allocations are increased or decreased as appropriate to optimize the costs of the different ERM activities relative to the benefits derived.

Value Creation Stage

- The ERM system evolves from enabling success to being recognized as a competitive advantage.

Framework Design

Foundation Level

- The external and internal context is understood, documented, and articulated to those involved with the ERM system.
- The structure and organizational positioning of ERM is established.
- A risk management policy is developed, approved, and communicated.
- ERM considerations are linked to the performance appraisal process.

Proficient Level

- Changes to the external and internal context are monitored, updated, and communicated as needed.
- The ERM structure is assessed at least annually to ensure it is enabling the ERM objectives. This assessment includes, at a minimum, the roles and responsibilities of the highest risk officer and any risk committees.
- The risk management policy is periodically reviewed and updated, and supporting training is conducted for any substantive changes.
- The performance appraisal process drives the right behaviors related to ERM.

Innovative Level

- The ERM structure evolves to ensure ERM is embedded into all areas of the business; i.e., it is instilled in everything the organization does and every decision that is made.
- The policy is streamlined to eliminate requirements that do not ultimately support value protection or creation.

Value Creation Stage

- The framework measurably drives value creation.

Risk Criteria

Foundational Level

- Governance risk criteria (risk capacity, risk attitude, risk appetite, and risk tolerance) are defined and documented.

- Assessment risk criteria are analyzed and appropriate criteria are included in the risk assessment process.

Proficient Level

- Governance risk criteria are reassessed periodically and adjusted in response to business changes.
- Assessment risk criteria are reevaluated periodically to remove those that are not enhancing the risk assessment process and to add others that will enhance the process.

Innovative Level

- Risk appetite statements begin to increase the focus on upside risks.

Value Creation Stage

- The risk attitude becomes more risk embracing, and risk appetite statements evolve to optimally pursue value creation opportunities.

Risk Assessment

Foundational Level

- A risk universe has been developed that captures all known risk events and uses terms understandable by people in the organization.
- Causes, sources, and interdependencies among risks are generally understood.
- The risk universe has been assessed and prioritized, based on appropriate risk assessment criteria.

Proficient Level

- The risk universe is updated periodically to reflect new, emerging, or changing risks, as well as increased knowledge about existing risks.
- The results of risk events are used to enhance the organization's risk analysis.
- The prioritized risk portfolio is updated periodically, reflecting both changes in the organization's context and its success in managing certain risks to a tolerable level.

Innovative Level

- The organization is more effective at identifying, analyzing, and evaluating unusual, black swan-type events, particularly those with multiple interdependencies.

Value Creation Stage

- The organization becomes adept at developing strategies for exploiting certain risk events to create new value, giving it a competitive advantage.

Risk Treatment

Foundational Level

- Risk treatment options have been evaluated and treatment approaches determined for all key risks in the risk portfolio.

an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

To support that definition, the IIA has developed its International Standards for the Professional Practice of Internal Auditing. These standards, which fall into two categories, attribute standards and performance standards, cover fundamental characteristics of any audit project. The IIA standards discuss the following.

Attribute Standards

- Purpose, authority, and responsibility
- Independence and objectivity
- Proficiency and due professional care
- Quality assurance and improvement program

Performance Standards

- Managing the internal audit activity
- Nature of work
- Engagement planning
- Performing the engagement
- Communicating results
- Monitoring progress
- Communicating the acceptance of risks

With this basic understanding of auditing and the fundamental auditing standards, it is now time to consider how the different auditing approaches have evolved over the years.

CONTROLS-BASED AUDITING

The first generation of internal auditing can be described as controls-based auditing, which includes traditional audit activities that were prevalent prior to the 1980s. This type of auditing typically is an extension of the independent, external audits that organizations have been undergoing for many years to evaluate and opine on the fairness of financial statements and disclosures. These audits primarily rely on the results of substantive testing to validate, with reasonable assurance, that account balances are fairly stated.

Controls-based internal audits evolved to serve one of three primary purposes:

1. To validate compliance with established laws, regulations, policies, principles, etc. These audits, which are still common and relevant today, are typically referred to as "compliance" audits.
2. To test and validate recorded financial balances, utilizing a lower scope than the external audit. Organizations perform these audits (commonly referred to as "financial" audits) to gain assurance that the specific financial accounts are accurate on an interim basis, reducing the likelihood of adjustments at year-end.

3. To verify that key controls supporting the initiation, authorization, recording, processing, and reporting of transactions are operating as designed. The focus of these audits is on the underlying controls and procedures, as opposed to the account balances themselves. They are referred to by a variety of names, such as "controls" audits, "transaction flow" audits, and "procedural" audits.

OBSERVATION: The evaluation and testing of internal controls over financial reporting as required by the Sarbanes-Oxley Act typically follow a controls-based audit approach.

Controls-based audits have the following characteristics:

- *Objective* Determine compliance with underlying guidelines, such as laws and regulations, company policies, established charters, promulgated standards, principles (e.g., generally accepted accounting principles), etc.
- *Approach* Understand the underlying guidelines and audit for compliance and conformance with those guidelines.
- *Focus* Identify and correct compliance exceptions and errors.
- *Testing Approach* Use statistical-based predictive and substantive testing, although controls audits may use some compliance testing.
- *Recommendations* Relate exceptions or errors to the relevant guidelines and recommend how to correct the exceptions or errors.

The controls-based audit generation is still common because compliance, financial, and controls audits continue to support audit functions' general governance responsibilities. Additionally, because the methodologies for these types of audits are well documented, most audit departments have charters that incorporate these audit approaches.

PROCESS-BASED AUDITING

Process-based auditing, commonly called "operational" auditing, became more prevalent in the 1980s. Internal audit functions were looking for ways to provide more of the value that outside consultants were touting. These functions began experimenting with new audit approaches to deliver that type of value. Although controls-based auditing was still the cornerstone of most of these functions' charters, they also performed projects that evaluated the design, effectiveness, and efficiency of key processes in the organization. Best practices were typically used as the benchmark for this new evaluation. This shift in approach became known as the second generation of internal auditing.

Process-based audits have the following characteristics:

- *Objective* Determine how effectively and efficiently the process under review is meeting specific business or operational objectives.

- *Approach* Understand the specific business or operational objectives, re search best practices for achieving those objectives, and determine how effectively and efficiently the process was currently meeting those objectives.
- *Focus* Identify gaps between the current process and best practices.
- *Testing Approach* Typically, use a consulting-focused evaluation of best practices and the current process, supplemented with compliance testing to evaluate the current process.
- *Recommendations* Relate gaps to the specific business or operational objectives and provide potential impacts of not closing the gaps.

The process-based audit generation allowed auditors to use greater creativity and provide additional value relative to traditional controls-based audits. A more consultative methodology evolved to help auditors perform these audits. However, since process-based audits did not typically address the key compliance, financial, and control requirements that are a fundamental part of most audit functions' fiduciary responsibilities, audit functions typically used process-based audits to "fill out" an audit plan, with controls-based audits still being the primary focus for the majority of the audit hours.

RISK-BASED AUDITING

In the 1990s, a third generation of auditing developed, commonly called risk-based auditing. As the major public accounting firms became more active in consulting with and performing internal audits for organizations, they needed to develop methodologies that provided greater focus and value to justify the higher cost per hour that they were charging. Risk-based auditing provided them with a compelling selling point. By starting with a thorough understanding of the business and its various business risks, auditors were able to make scope reductions that ensured the key risks were addressed in the audit, without devoting valuable resources to other areas that had relatively lower risk. The public accounting firms, as well as forward-looking audit functions that quickly developed and followed a risk-based approach, found that they could provide management with greater comfort regarding risk-related controls and activities, while typically spending fewer hours.

Risk-based audits have the following characteristics:

- *Objective* Determine the primary business risks and evaluate how effectively the controls and procedures are mitigating the risks to an acceptable level (i.e., how much residual risk remains).
- *Approach* Understand the business, identify and evaluate the key business risks, and assess how effectively existing controls and procedures are mitigating these risks to an acceptable level. Controls and procedures relating to other risks (i.e., non-key risks) are not assessed in risk-based audits.
- *Focus* Identify controls and procedures that are not operating effectively to mitigate the key business risks to an acceptable level.

- *Testing Approach* Typically, a combination of substantive and compliance testing is utilized. The testing approaches used in both controls-based and process-based auditing may be appropriate; however, testing will only focus on key risks.
- *Recommendations* Relate exceptions or errors to the key risks, and provide potential impacts of not effectively mitigating each risk to an acceptable level.

The risk-based audit approach firmly positioned the audit function as a valuable part of the organization. Most audit functions now use risk as the foundation for determining which projects should be conducted, and how the projects will be performed. This approach makes sense to many executives and provides management with greater assurance that the audit resources are being deployed in an appropriate manner. Controls-based and process-based audits are still being performed, but they are scheduled and executed based on the underlying risk, as opposed to some standard frequency or formula for conducting audits.

RISK MANAGEMENT-BASED AUDITING

In the late 1990s, Enterprise Risk Management (ERM) began to evolve as an approach for companies to manage risks on a holistic, organization-wide basis. Audit functions employing a risk-based audit approach are probably already focusing on the same key risks that management focuses on as part of the ERM process. However, there are other characteristics of ERM that a risk-based audit approach does not comprehensively address. Therefore, a fourth generation of auditing, risk management-based auditing, is necessary to optimize audits in an ERM environment.

Risk management-based auditing embodies many of the characteristics of risk-based auditing, with an expanded focus on key business objectives, management's tolerance of risk, key risk measurements or performance indicators, and risk management capabilities. Additionally, risk-based auditing primarily focuses on mitigating risks to an acceptable level, whereas risk management-based auditing considers optimizing key risks where necessary to achieve business objectives. In fact, risk management-based auditing is a key part of a successful ERM program.

Risk management-based audits have the following characteristics:

- *Objective* Determine the primary business objectives, risks, measurements, and tolerances, and evaluate how effectively the risk management activities are supporting the objectives by managing the risks to an acceptable level (i.e., management's tolerance).
- *Approach* Focus on the following:
  - — Understanding management's strategic, operational, and value objectives;
  - — Identifying and evaluating the key business risks that are barriers to achieving those objectives;
  - — Understanding management's tolerance relative to risk occurrence;

Chapter 1, enterprise risk management is a process . . . to provide reasonable assurance regarding the achievement of entity objectives. The board provides the direction and oversight to management regarding the guidelines or boundaries in which management is expected to operate in order to achieve the business objectives. Therefore, enterprise risk management is somewhat aimless without a sound governance structure to provide those boundaries. That is, without the direction from the top of an organization, as would exist with a good governance structure, it would be difficult to manage risks that align with and benefit the key stakeholders of an organization.

Question: Can an organization have good corporate governance without implementing ERM?

Answer: Yes. Governance principles require a governing body to provide direction, authority, and oversight to an organization. A board can exercise its governance responsibilities without the existence of a defined or robust ERM program. However, one of the board's responsibilities is to oversee the business to evaluate whether management is operating within the boundaries established by the board. This oversight requires some structure for communications between management and the board. More specifically, there must be parameters that articulate what information is appropriate to provide the board; too much or too little information may make it more difficult for the board to evaluate how effectively management is carrying out the direction and whether management is operating within the established boundaries. Although these communications can certainly be structured in a manner that supports effective corporate governance, organizations will find that utilizing ERM concepts makes this process more efficient and effective. Therefore, although full ERM implementation is not necessary to obtain good corporate governance, applying ERM principles will enhance the effectiveness of corporate governance.

Question: Can an organization have an effective ERM program without good corporate governance?

Answer: Using the COSO ERM Framework as an illustration of ERM, one notices that the first two components of ERM are the internal environment and objective setting, both of which have elements that are heavily dependent on board input and oversight. That is, if these two components provide the foundation for effective ERM, corporate governance provides key building blocks of that foundation. An organization cannot have an effective ERM program without an effective internal environment (e.g., tone at the top, integrity and ethical values, commitment to competence) and an effective objective setting that aligns with the organization's mission. Therefore, inadequate corporate governance will undermine the implementation of an effective ERM program. Enterprise risk management is somewhat aimless without a sound governance structure to provide those boundaries.

Question: How important is it for an organization to formally structure three lines of defense? How important is it to implement a combined assurance model to reduce "assurance fatigue?"

Answer: All organizations have different lines of assurance, whether they realize it or not. The definitions of the three lines contained in Chapter 1, "Overview of Enterprise Risk Management," should apply in any organization. It is not necessary to formally depict such a model in an organization, nor is it necessary to classify all control activities as one of the three lines. However, recognizing the type of assurance that different activities provide is important. The different lines provide varying levels of assurance, with the third line bringing the most confidence. A growing number of organizations are finding that a combined assurance model is the only way to determine whether they are obtaining the right level of assurance. Such a model helps to assure there are no gaps in assurance, and also helps identify the more common occurrence of overlaps in assurance, which typically result in spending more on assurance than is necessary.

Question: Must an organization apply a recognized framework to implement ERM?

Answer: As with most projects and initiatives, there can be different ways of achieving success. In the long run, ERM is more of an operating mindset than a formal process or project; nevertheless, certain fundamental principles must be applied to make ERM sustainable. Frameworks outline those principles and provide a road map for full implementation of ERM. Without such frameworks, the likelihood of success is greatly diminished. Just as companies typically do not embark on a significant systems implementation without a sound systems development methodology, it is not prudent to begin the ERM journey without a sound framework as the guide. Full ERM implementation achieved without a recognized framework as a basis will likely take longer, cost more, and be less sustainable.

Many organizations with more advanced ERM programs have found that, as their ERM programs continue to evolve, the existing frameworks may not be adequate. This is not surprising considering that the frameworks are based on fundamental principles and do not outline the more advanced ERM techniques. Organizations should look to these frameworks as a starting point for effective and efficient ERM implementation and be flexible and dynamic enough to customize and expand the chosen framework to meet their particular needs as their ERM programs evolve.

Question: Two frameworks were discussed in this book; the COSO ERM Framework and ISO 31000. Which is better?

Answer: As one might expect, the answer to this question depends on the circumstances. COSO ERM is widely embraced in the United States, while ISO 31000 is quickly becoming a global standard that's embraced throughout much of the rest of the world. For organizations just beginning or in the early stages of the ERM journey, the author believes ISO 31000 is probably a better place to start. The primary reason is that it is a broader standard that includes principles, a

framework, and a risk management process. It is likely that those with less experience will find ISO 31000 more intuitive and easy to grasp, while also providing the essential first steps toward embarking on the ERM journey. In addition, there are a growing number of tools and aids aligned with ISO 31000, so its use is becoming better defined. COSO ERM, on the other hand, tends to be more detailed and prescriptive, making it a useful tool as organizations become more advanced with ERM (particularly since COSO ERM includes a separate volume with examples of application techniques). The selection of a framework will be influenced by the organization's culture, ERM capabilities, and access to examples from other successful organizations.

Question: Why, typically, do organizations decide to implement ERM?

Answer: There are probably as many answers to this question as there are organizations; however, the primary reason tends to be one of the following:

- The organization experienced a negative risk outcome and must find a way to better avoid, anticipate, or mitigate similar future risk outcomes. That is, it is reacting to an event, the recurrence of which would not be tolerated by the board, management, or stakeholders.
- An organization recognizes that it has opportunities in its industry to create value by managing risks or exploiting opportunities better than its competition. It takes a proactive approach because it believes that ERM concepts will help it leverage its internal knowledge to create such value.
- Organizations that have been subject to the Sarbanes-Oxley Act or other governance-type regulations in other countries recognize that they have already made a significant investment in ERM-type activities, and the additional investment to reap the benefits of full ERM are incrementally manageable. Therefore, they view ERM as a continuance of initiatives that are already in place.
- Board members have seen the benefits of ERM at other companies with whom they have worked, either as an employee or board member, and recommend it to management. This reason is becoming increasingly more common as the board's responsibilities for risk oversight are reinforced.

Question: In light of the 2008 crisis among financial institutions and organizations in other industries, many of which were believed to have had advanced risk management practices, does ERM really work?

Answer: There are many lessons learned from this crisis, two of which are particularly relevant to ERM. First of all, some of the new financial instruments created (e.g., collateralized securities) were probably overly complex. They were designed to take advantage of financial accounting and reporting standards and the underlying economics of the instruments tended to obscure the embedded risks. As a result, some purchasers (and perhaps the rating agencies) may not have fully understood what they were buying. Second, one must remember that both governance and ERM are dependent on people making sound judgments and decisions. The risk management activities deployed by many of these institutions were sound and, in fact, did identify some of the scenarios that ended up occurring, such as the subprime mortgage problems. However, management at the institutions that failed probably did not believe those scenarios were likely enough to prompt actions to manage the risks. Thus, governance and risk management techniques can certainly be strengthened in many organizations, and their existence helps organizations improve their chances of being successful and being able to weather the challenges that arise in cyclical markets.

Question: Considering the growing attention to GRC programs, does this mean compliance programs typically operate outside of ERM?

Answer: While a key focus on GRC is to integrate governance, risk management, and compliance activities, that does not mean that they are necessarily separate and discreet. Thinking back to the COSO ERM framework, one of the four objective types is compliance. Following that framework down through the different components of ERM, one can understand how compliance risks, strategies, controls, information, and monitoring activities would be developed. These activities make up a compliance program. Despite its separate recognition in the GRC acronym, compliance is really a subset of ERM. More importantly, organizations pursuing GRC initiatives are finding that there are synergies between the three components, most noticeably between risk management and compliance. By integrating all three, organizations are able to more efficiently and effectively manage the risks facing the organization while also providing reasonable assurance that they remain in compliance with laws, regulations, contracts, policies, etc.

Question: There seems to be a proliferation of GRC technology solutions in the market. Is it necessary to purchase one of these packages?

Answer: Like so many aspects of business, at some point the amount of data collected and used becomes unmanageable without the help of an enabling technology. Such technology solutions can help ensure decision makers have access to the proper data, and messages and alerts are sent to the right people when an action or a decision is needed. GRC products continue to evolve and are becoming more customized to the needs of a holistic GRC environment. However, some organizations may find that existing software and tools will effectively serve their automation needs. The author believes outside tools should be evaluated to avoid "recreating the wheel;" however, organizations may learn from such evaluations that their internal technology resources can be customized and leveraged for less money, which may also help avoid the change management challenges of moving to a new package.

Question: From a payback, or return on investment, perspective, are the costs of implementing a robust ERM program justified?

Answer: Determining a return on investment is challenging when evaluating an ERM program. Most aspects of ERM focus on preventing something bad from happening, thus successful ERM is typified by relative few bad things happening. However, it's tough to determine return on investment if the impact of what didn't happen is one of the variables. Therefore, the focus of an ERM program is to balance the costs and efforts against the potential impact of various risk scenarios. Typically, preventing just one catastrophic risk event, or being

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.

PROCESS RISK ASSESSMENT

As discussed in Chapter 8, process risk assessment is composed of two primary steps: (1) risk identification and definition and (2) risk assessment.

Risk Identification and Definition

The audit team began by researching quality assurance risks, and brainstorming barriers to success. The following key barriers were identified for each objective:

Zero Defects

- Personnel on the production line are not properly trained to prevent and detect defects in products being assembled.
- The technology used in the quality control process does not consistently operate effectively.
- Outsourcing vendors who build assembled components do not have the quality control necessary to ensure that the assembled components are free of defects prior to supplying them to the company.
- Parts and supplies purchased for the production process have inherent flaws that are not detected when the goods are received.
- Quality Assurance personnel are not adequately trained or they do not have the skills and tools to perform their quality control duties effectively.
- There are an inadequate number of Quality Assurance employees to check all finished products on a timely basis.
- Production or Quality Assurance personnel intentionally build in or ignore defects, either for personal gain or because of malicious intent.

- Policies and procedures do not effectively guide Quality Assurance personnel regarding how to accurately and efficiently execute quality control activities.
- Performance incentives do not effectively motivate employees to execute their tasks in the desired manner.

Quality Mind-Set

- Quality Assurance personnel are not adequately trained or do not have the skills and tools needed to effectively educate, train, and advise employees on quality concepts.
- Employees do not understand how high-quality products give AfterMath a competitive advantage.
- Employees have neither the desire nor incentive to learn quality concepts, due to the lack of support by management.
- Performance incentives do not effectively motivate Quality Assurance employees to educate, train, and advise employees on quality concepts.

Based on this list of potential barriers to success, the audit team identified the following as the primary risks relating to this area (note that risks specifically related to the production process are not considered a part of this audit):

- **Cultural Risk** Failure to educate employees on the value and means to ensure quality in processes, and to create a quality-focused culture, may cause employees to act in a manner that is inconsistent with management's criteria (i.e., does not promote quality in all activities).
- **Human Resources Risk** Failure to attract, train, develop, deploy, and empower competent Quality Assurance personnel may inhibit AfterMath's ability to execute, manage, and monitor key quality control activities.
- **Integrity Risk** Dishonest or misdirected employees may carry out activities that are not in accordance with management's criteria or expectations.
- **Performance Incentive Risk** Lack of appropriate performance incentives may result in behavior that is misaligned with management's objectives.
- **Performance Measurement Risk** Lack of defined metrics and the inability to gather relevant information for measurement purposes may impair management's ability to monitor individual, team, and overall business performance.
- **Policies and Procedures Risk** Policies and procedures that are ineffective, insufficient, unclear, or outdated may result in poorly executed quality control activities, and, as a result, defects in shipped products.
- **Quality Control Risk** Failure to consistently and effectively execute quality control procedures may result in defects in shipped products.
- **Technology Risk** Inadequate or inconsistent technology to support quality control testing may result in defects being undetected.

- **Third-Party Risk** Failure to manage outsourcing vendors and suppliers, and appropriately inspect incoming assembled components and supplies, may result in unexpected defects in the company's finished products.

After identifying and defining the risks, the final step in this area is to show the linkage between objectives and risks. This helps demonstrate the completeness of the risks identified and can be used as guidance when analyzing the design of current controls to ensure aspects related to all relevant objectives are considered. The matrix discussed in Chapter 5, "Risk Assessment: Business Level," is used to document this linkage.

Illustration 24-1: Link between Objectives and Risks

Risks \ Objectives	Zero Defects	Quality Mindset
Cultural Risk	X	X
Human Resources Risk	X	X
Integrity Risk	X	X
Performance Incentive Risk	X	X
Performance Measurement Risk	X	X
Policies and Procedures Risk	X	X
Quality Control Risk	X	
Technology Risk	X	
Third Party Risk	X	

Risk Assessment

Confident that all key quality assurance risks have been identified and appropriately defined, the next step is to assess the significance and likelihood of the identified risks. The audit team determined the significance and likelihood of each risk, based on their discussions with management and their own judgments. (Refer to Exhibit 24-1 where the significance and likelihood of each risk are identified and discussed.)

Based on the risk assessment, the audit team prepared the following nine-box risk matrix to illustrate the judgments regarding significance and likelihood.