An overview of COSO's 2013 *Internal Control-Integrated Framework*

Prepared by:

Sara Lord, *Partner, National Professional Standards Group*, McGladrey LLP
sara.lord@mcgladrey.com

May 2013

Introduction

In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) published *Internal Control-Integrated Framework* (the 1992 Framework), which has become commonly known as the COSO Framework. In May 2013, COSO issued an updated *Internal Control-Integrated Framework* (the 2013 Framework) to reflect changes in the business world over the 20 years since release of the original Framework. While continuing to embrace a principles-based approach, the updated Framework incorporates more guidance illustrating and explaining the concepts in the Framework and is intended to help organizations in their efforts to adapt to today's increasing complexity and pace of change.

The 2013 Framework retains the five components of internal control (i.e., control environment, risk assessment, information and communication, control activities, and monitoring activities); however it adds 17 principles associated with these five components that are necessary for effective internal control. Upon adoption of the 2013 Framework, an entity will need to evaluate the extent to which each of the 17 principles are relevant to its organization and, to the extent a principle is relevant, whether the entity's controls are operating effectively to achieve the principle. This update also introduces 81 points of focus that typically are important characteristics of the 17 principles.

In addition to the 17 principles, the updated Framework contains more guidance on how technology relates to an entity's internal control structure. The 1992 Framework included many concepts directly relevant for technologies of the time. Since then technology has rapidly evolved from not only something embraced by the largest and most advanced companies to a foundation block of nearly all companies. The 2013 Framework includes more focus on technology throughout the components of internal control as well as a broader focus on the impacts of the technology on the internal control structure rather than on the specific types of technology.

Because more companies are outsourcing key portions of their business activities or control systems to third parties, the updated Framework also includes expanded guidance and considerations related to outside resources, such as third-party processors. The updated Framework also expands the reporting aspect of internal control to consider more than just financial reporting, including external reporting of non-financial information and internal reporting.

Finally, the advances in technology and communications have increased the reach of many companies both from a supply and development side and in sales or service delivery. For many entities, local or national boarders no longer serve as significant barriers. Rather, businesses are increasingly conducted on a multi-location or global basis. The 2013 Framework includes additional guidance and consideration for businesses operating in these environments.

It should be noted that the issuance of the 2013 Framework includes a volume of *Illustrative Tools for Assessing Effectiveness of a System of Internal Control,* which include templates to illustrate a possible summary of internal control assessment results under the updated Framework. COSO also simultaneously issued *Internal Control over External Financial Reporting: A Compendium of Approaches and Examples*, which provides illustrations of how various characteristics of principles may be present and functioning within a system of internal control relating to external financial reporting objectives.

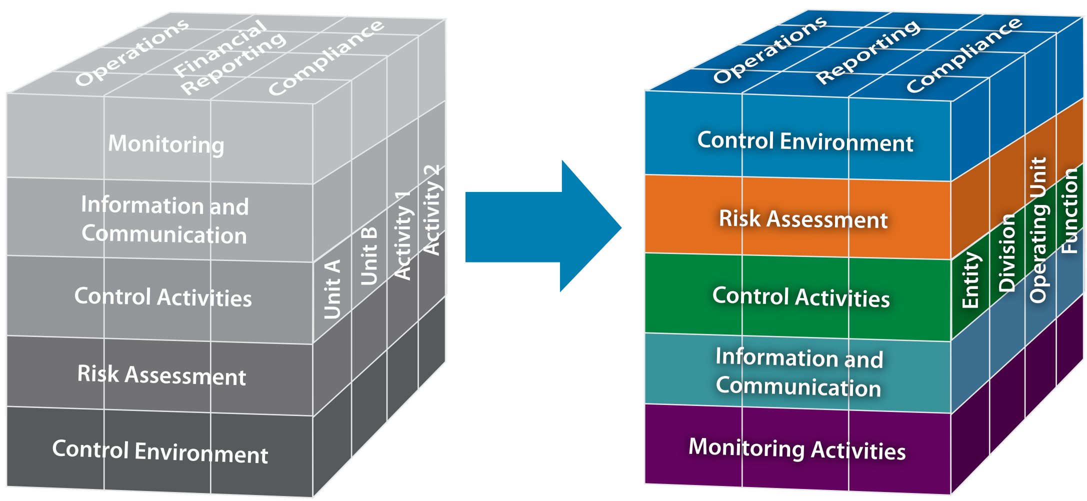
An overview of the 2013 Framework

Foundational similarities and differences

Before discussing the changes in the 2013 Framework, it is important to understand what has not changed. Much of the foundation of the 1992 Framework is retained or only slightly modified in the 2013 Framework. The definition of internal control has not changed. An entity's internal control structure is still based on its identification of objectives and need to structure a sound system to achieve those objectives.

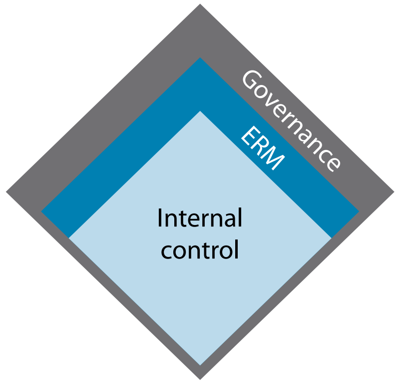
As depicted below, the well-known COSO cube remains with a few specific changes.

1992 COSO Cube **2013 COSO Cube**



The five components of internal control have not changed, as illustrated by the front face of the cube remaining largely the same. The one change to the components is that the category of "Monitoring" has been changed to "Monitoring Activities." This change is intended to broaden the perception of monitoring as a series of activities undertaken individually and as a part of each of the other four components, rather than as one unique process.

Across the top of the cube, "Financial Reporting" has been changed to "Reporting." This change is intended to broaden the application of the Framework not only to external financial reporting as it has often been applied, but also to include internal reporting as well as external reporting of non-financial measures.



Along the right side of the cube, the organization structure has been changed to align with COSO's *Enterprise Risk Management-Integrated Framework* (ERM Framework) and also better illustrate that an effective internal control structure permeates an entire organization at all functional levels both independently and interdependently. It is also important to note that while there was consideration of combining the *Internal Control-Integrated Framework* with the ERM Framework, the two remain separate, but interrelated. Internal control is an integral part of enterprise risk management; however, enterprise risk management encompasses a broader role than internal control in supporting an entity's governance structure.

Introduction of 17 principles

The 2013 Framework introduces 17 principles that are necessary for effective internal control, unless they are not relevant to the entity. Although the Framework presumes that all 17 principles are relevant for each entity, management may determine that a principle is not relevant based on its unique circumstances. If a relevant principle is not present and functioning, a major deficiency exists in the system of internal control. The 17 principles are aligned with each of the five components and are discussed in the component sections below.

Control environment

Five principles related to the control environment are introduced in the 2013 Framework:

1. The organization demonstrates a commitment to integrity and ethical values.
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

These five principles demonstrate how the tone at the top is permeated across business lines and activities. The 2013 Framework provides additional discussion of governance roles in the organization and the notion of risk oversight. Included in the expanded guidance on the control environment are more specific considerations related to outsourced service providers, business partners, and external partners.

Interestingly, for small businesses, principles 2 and 3 are predicated on the entity having an independent board of directors. As noted above, the principles can be evaluated to determine whether they are relevant for the entity. Upon adoption of the 2013 Framework, this is an area many smaller entities may find themselves evaluating for relevance. Although management may determine, based on the ownership structure or users of the financial statements, that an independent board of directors is not relevant to the entity, they may still determine during this evaluation that strategic oversight or processes similar to those performed by a board of directors may be beneficial and relevant for their internal control structure.

Risk assessment

Four principles are introduced related to risk assessment:

6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.
9. The organization identifies and assesses changes that could significantly impact the system of internal control.

A significant addition to the 2013 Framework is the direct consideration in principle 8 of fraud risks for the organization. Although effective internal control is expected to be a means to address fraud risk, the Framework now explicitly addresses the organization's need to consider fraud risks when designing internal control processes to meet its objectives. The failure to adequately assess risks due to fraud for each objective would constitute a major deficiency in the entity's internal control structure.

Finally, principle 9 specifically addresses the organization's need to understand and evaluate how changes in internal and external factors impact its internal control system. This will lead the company to re-evaluate internal control on a timely basis to respond to identified changes.

Control activities

Three principles are introduced related to control activities:

10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
11. The organization selects and develops general control activities over technology to support the achievement of objectives.
12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.

The discussion of technology is significantly expanded in the "control activities" section. This includes discussion of automated control activities and general controls over technology. These concepts are addressed in a broad fashion, not dependent on existing technology, but to provide a foundation to consider the impacts on technology for the organization as technology changes over time.

The guidance in this section also clarifies that the control activities that are part of internal control are the actions established by the policies and procedures, not the policies and procedures themselves. This helps to illustrate that there are multiple factors that must be present in order for a particular control activity to be effective, which include the competence and commitment to quality of the people performing the activities.

Information and communication

Three principles are introduced related to information and communication:

13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

15. The organization communicates with external parties regarding matters affecting the functioning of internal control.

There have been significant changes in both the quantity and availability of information over the last two decades. The changes to the Framework emphasize the importance of a focus on the quality of information and have expanded discussions on reliability of the information produced and used in the internal control system. Additionally, the 2013 Framework focuses on the entity's protection of information. Principle 15 highlights the importance of communications outside of the entity, whether with third-party service providers, owners, or others.

Monitoring activities

Two principles are introduced related to monitoring activities:

16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

As noted above, the title of this component has been changed to broaden the perception of monitoring as a series of activities undertaken individually and as a part of each of the other four components, rather than as one unique process. The 2013 Framework expands the discussions of how technology and third-party service providers impact an entity's monitoring activities. It also introduces two main categories of monitoring activities: ongoing evaluations and separate evaluations.

Introduction of 81 points of focus

In addition to the principles, the 2013 Framework introduces 81 points of focus. The points of focus are typically important characteristics of principles that can be used to facilitate designing, implementing, and conducting internal control. These are items management can consider to determine if the principles are present and functioning. The 2013 Framework is explicit that management is not required to separately evaluate whether each of the points of focus are in place to determine if the principles are present and functioning.

The addition of the principles and points of focus represent a significant amount and volume of the changes to the structure of the Framework and its accompanying guidance. Similar to the relationship between the principles and components, the points of focus are structured to support each principle. While this paper does not delve into a detailed consideration of each of the points of focus, Appendix A includes a chart showing the relationship among the components, principles and points of focus.

Scalability for smaller entities and governments

For many smaller entities, when looking quickly through the points of focus it is evident that many will not be relevant to their operations. Focuses on multiple locations or business units quickly can be dismissed for single-location businesses. Certain reporting objectives, such as external non-financial reporting or compliance reporting, may not be applicable. Understanding the correct focus to view the principles is a first step toward scaling the Framework. Key consideration factors for smaller entities and governments are included in an appendix to the 2013 Framework. Appendix C of this white paper highlights the key consideration factors for these entities.

Effective dates and transition

COSO's goal in updating the original framework has been to reflect changes in the business and operating environments, to formalize more explicitly the principles embedded in the original framework that facilitate development of effective internal control and assessment of its effectiveness, and to increase ease of use when applied to an entity objective. Accordingly, COSO believes users should transition to the 2013 Framework in their applications and related documentation as soon as is feasible under their particular circumstances. However, there are clearly many changes for entities to consider upon adopting the 2013 Framework. See Appendix B for more detailed guidance on the adoption process for entities reporting on their internal control over financial reporting.

Companies should begin the transition process by first taking the time to read and understand the 2013 Framework and related guidance that will be helpful for implementation. Entities then will need to evaluate the 17 principles to determine if they are relevant to their organization and then also determine how they have been implemented. In this process some entities may determine that a relevant principle is not addressed, which could signify a material deficiency in their internal control. They will need to evaluate whether identified deficiencies have implications for the users of their financial information or their auditors, if applicable. In addition to the consideration of the principles, adoption of the 2013 Framework will require both management and the auditor to update the relevant documentation to reflect how the entity's objectives are being met through the components and related principles.

COSO will continue to make available the 1992 Framework during the transition period extending to December 15, 2014, after which time COSO will consider it as having been superseded. COSO believes the key concepts and principles embedded in the original framework are fundamentally sound and broadly accepted in the marketplace, and accordingly, continued use of the original framework during the transition period (May 14, 2013 to December 15, 2014) is appropriate. During that period, the application of the *COSO Internal Control-Integrated Framework* that involves external reporting should clearly disclose whether the original or 2013 version was utilized.

Because entities are not required to use the Framework by any standard setter or regulatory body, each entity will need to individually determine its transition path to the new Framework. It will be important for entities to consider the expectations of the users of the financial statements for the Framework adoption timeframe. Auditors will need to work with clients to understand which framework they are using and how the transition will impact their audit procedures.

The entity's internal control structure is relevant to audit engagements as well as examination or agreed-upon-procedures engagements related to internal control. The impacts of updating the 2013 Framework on the engagement include an updated understanding of the evaluation process and consideration of any deficiencies identified during the transition. Auditors will need to evaluate the 17 principles, including management's assessment of any principles it does not deem relevant to the organization.

Much like the process to update the COSO Framework was a multi-year project, it is likely that the implementation and transition to the 2013 Framework will take time and effort – both on the part of an entity's management and its auditor. The updated guidance and information in the 2013 Framework provide a strong foundation for entities to re-evaluate their internal control systems and ensure they are timely updated for changes in their internal and external risk factors.

Appendix A

Outline of the components, principles and points of focus

Control Environment

Principle 1. The organization demonstrates a commitment to integrity and ethical values.

Points of focus:
- Sets the tone at the top
- Establishes standards of conduct
- Evaluates adherence to standards of conduct
- Addresses deviations in a timely manner

Principle 2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Points of focus:
- Establishes oversight responsibilities
- Applies relevant expertise
- Operates independently
- Provides oversight for the system of internal control

Principle 3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Points of focus:
- Considers all structures of the entity
- Establishes reporting lines
- Defines, assigns, and limits authorities and responsibilities

Principle 4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.

Points of focus:
- Establishes policies and practices
- Evaluates competence and addresses shortcomings
- Attracts, develops, and retains individuals
- Plans and prepares for succession

Principle 5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Points of focus:
- Enforces accountability through structures, authorities, and responsibilities
- Establishes performance measures, incentives, and rewards
- Evaluates performance measures, incentives, and rewards for ongoing relevance
- Considers excessive pressures
- Evaluates performance and rewards or disciplines individuals

Risk Assessment

Principle 6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Points of focus

Operations objectives
- Reflects management's choices
- Considers tolerances for risk
- Includes operations and financial performance goals
- Forms a basis for committing of resources

External financial reporting objectives
- Complies with applicable accounting standards
- Considers materiality
- Reflects entity activities

External non-financial reporting objectives
- Complies with externally established standards and frameworks
- Considers the required level of precision
- Reflects entity activities

Internal reporting objectives
- Reflects management's choices
- Considers the required level of precision
- Reflects entity activities

Compliance objectives
- Reflects external laws and regulations
- Considers tolerances for risk

Principle 7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

Points of focus
- Includes entity, subsidiary, division, operating unit, and functional levels
- Analyzes internal and external factors
- Involves appropriate levels of management
- Estimates significance of risks identified
- Determines how to respond to risks

Principle 8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.

Points of focus
- Considers various types of fraud
- Assesses incentive and pressures
- Assesses opportunities
- Assesses attitudes and rationalizations

Principle 9. The organization identifies and assesses changes that could significantly impact the system of internal control.

Points of focus
- Assesses changes in the external environment
- Assesses changes in the business model
- Assesses changes in leadership

Control Activities

Principle 10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.

Points of focus

- Integrates with risk assessment
- Considers entity-specific factors
- Determines relevant business processes
- Evaluates a mix of control activity types
- Considers at what level activities are applied
- Addresses segregation of duties

Principle 11. The organization selects and develops general control activities over technology to support the achievement of objectives.

Points of focus

- Determines dependency between the use of technology in business processes and technology general controls
- Establishes relevant technology infrastructure control activities
- Establishes relevant security management process control activities
- Establishes relevant technology acquisition, development, and maintenance process control activities

Principle 12. The organization deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Points of focus

- Establishes policies and procedures to support deployment of management's directives
- Establishes responsibility and accountability for executing policies and procedures
- Performs in a timely manner
- Takes corrective action
- Performs using competent personnel
- Reassesses policies and procedures

Information and Communication

Principle 13. The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.

Points of focus

- Identifies information requirements
- Captures internal and external sources of data
- Processes relevant data into information
- Maintains quality throughout processing
- Considers costs and benefits

Principle 14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

Points of focus

- Communicates internal control information
- Communicates with the board of directors
- Provides separate communication lines
- Selects relevant method of communication

Principle 15. The organization communicates with external parties regarding matters affecting the functioning of internal control.

Points of focus

- Communicates to external parties
- Enables inbound communications
- Communicates with the board of directors
- Provides separate communication lines
- Selects relevant method of communication

Monitoring Activities

Principle 16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Points of focus

- Considers a mix of ongoing and separate evaluations
- Considers rate of change
- Establishes baseline understanding
- Uses knowledgeable personnel
- Integrates with business processes
- Adjusts scope and frequency
- Objectively evaluates

Principle 17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Points of focus

- Assesses results
- Communicates deficiencies
- Monitors corrective actions

Appendix B

What should I be doing now to transition to the 2013 Framework?

This appendix provides adoption considerations for organizations that are currently using the 1992 version of COSO to evaluate their internal controls over financial reporting (ICFR) for compliance with the requirements of the Sarbanes-Oxley Act (SOX). As addressed earlier in this white paper, it is important to first realize that 2013 Framework is not fundamentally different from the legacy version you have already adopted, so making the transition to the 2013 Framework may not be as bad as you initially think. However, because the differences between the two versions are not inconsequential, it is important to begin the planning process now.

The 1992 Framework is set to expire for fiscal years ending after December 15, 2014, so for many organizations, 2013 will be the last year it can be used for SOX ICFR assessments. Getting a start now in assessing the relevant differences between the 1992 Framework the 2013 Framework will provide you with an understanding of the time and resources that it will take for your organization to addresses these differences. Also, if any remediation is required to address these differences, starting early will provide your organization an appropriate amount of time to remediate any deficiencies from a design and operating effectiveness perspective.

Having the appropriate individuals involved in your organization's assessment of the impact of transitioning to the 2013 Framework will help ensure that relevant differences are identified and a plan to address these differences is developed. For example, it is reasonable to expect that given the increased emphasis on information technology, third party vendors and fraud in the 2013 Framework, there may be enhancements your organization needs to make regarding the internal controls and/or related documentation in these areas of emphasis. Therefore, you will want to involve the individuals who are familiar with your organization's information technology environment, third party vendor relationships, and anti-fraud programs and controls in the transition assessment.

An initial exercise to perform is mapping the organization's existing internal control structure to the requirements of the 2013 Framework and identifying any potential gaps between the two versions. This will involve mapping your existing ICFR structure to the 17 principles in the 2013 Framework, and then assessing any identified differences. Consideration should be given to whether you believe that any of the 17 principles (as outlined on pages 3 through 5 of this white paper) are not relevant to your organization. If any principles are considered not to be relevant, you should document these considerations. This will be particularly relevant to less complex organizations, possibly including certain non-accelerated filers, as such organizations may determine that certain of the 17 principles are not relevant to their respective organization for the purposes of addressing SOX ICFR.

Once the relevant principles have been identified, the next exercise will be mapping the points of focus for the relevant principles (as introduced on page 5 of this white paper, and detailed in Appendix A) to the organizations existing internal control structure. Consistent with the process used to identify the relevant principles, you should evaluate which of the points of focus are relevant to your organization. However, instead of documenting why individual points of focus are not relevant to each associated principle, in certain circumstances (for example where management believes only one point of focus is required to address a particular principle) management should document its assessment as to why the identified point of focus is adequate to address the associated principle considering the size, scope and complexity of the organization. Your organization may also discover during this process, that although relevant points of focus are partially addressed by the existing internal control structure, enhancements may need to be implemented to adequately address the relevant principles. For example, if your organization places reliance on only one point of focus – as opposed to several – for a particular principle, then that point of focus needs to be particularly strong and well documented in order to demonstrate that the associated principle is appropriately addressed.

For identified gaps in relevant principles and/or associated points of focus, management should develop and document a plan to remediate the difference. This plan should be in sufficient detail to identify what actions should be taken, who is accountable for making these changes, and the expected timeline and resources required to implement the associated changes in the organization's COSO structure. Your timeline should consider the need to establish the operating effectiveness of any remediated control prior to your first fiscal year end after December 15th, 2014 (e.g., three to six months of operations).

Throughout the process of transitioning from your existing internal control structure to the 2013 Framework, consideration should be given to involving your external auditor. As a baseline for involving your external auditor, we recommend:

1. At the outset of your assessment of the 2013 Framework, present to your external auditor your organization's plan to determine the relevant gaps between your existing internal control structure and the 2013 Framework. This allows your external auditor input into your process and potential areas your organization needs to focus upon during your assessment.
2. Upon completion of your principles and points of focus gap analysis, present your results, as well as your detailed plans and timelines to address identified gaps to your external auditor. A key consideration point is to document for your external auditor the organization's thought process supporting the judgments made in determining the relevant principles and the appropriate points of focus. Our experience is that providing this detail will increase the likelihood that your external auditor will have the information needed to provide more practical input on your organizations plans to address the 2013 Framework and ease the transition for the first year of audit of internal control over financial reporting under the 2013 Framework.

Taking a proactive managed approach to assessing your organizations gaps between your existing internal control structure and the 2013 Framework will allow for an effective and timely path to converting to the 2013 Framework. Such an approach should also result in a positive impact to your organization's governance processes, without negatively impacting the productivity of those involved in your organization's internal control over financial reporting.

Appendix C

Specific considerations for smaller entities and governments

The 2013 Framework includes specific additional guidance related to smaller entities and governments. This appendix highlights consideration points related to segregation of duties, management override, board of directors, information technology, and monitoring activities for these entities. Key consideration factors for each area include:

Segregation of duties

- Managers can review reports of detailed transactions on a regular and timely basis
- Managers can select transactions for review to supporting documents
- Managers can take periodic counts of inventory, equipment or other physical assets and compare them with the accounting records
- Managers can review reconciliations of account balances or periodically perform them independently

Management override

- Maintain a corporate culture of integrity and ethical values
- Implement a whistle-blower program
- Engage an effective internal audit program
- Attract and retain qualified board members

Board of directors

- To find qualified board members, companies may expand their search to broader populations with financial and accounting and other valued expertise

Information technology

- The use of commercially developed software packages:
  - Reduces risks from program change control requirements
  - May include the ability to control access to selected employees
  - May perform checks on data processing completeness and accuracy
  - May be able to maintain related documentation

Monitoring activities

- Smaller entities may have less formal monitoring processes, but should still take credit for the monitoring performed
- It is noted in the Framework that smaller entities often need less formal documentation because there are fewer people working closer together. Consequently, management may perform monitoring through direct observation.

800.274.3978
www.mcgladrey.com