

How to Use This Manual

As the numerous laws and regulations continue to evolve and change in order to address the current environment and prevent previous mistakes from re-occurring, it has become more critical than ever to ensure that institutions have in comprehensive policies and procedures in place. As Sheila C. Bair, former Chairman of the Federal Deposit Insurance Corporation, observed in a statement on February 17, 2011, under the Dodd-Frank Act regulators were given the tools that were necessary for increasing large non-bank financial institution supervision, limiting individual financial institutions and transactions risks, and enabling large financial institutions and non-bank financial institutions to have an orderly closing and liquidation if a failure occurred. Additionally, the Dodd-Frank Act developed a comprehensive new regulatory and resolution establishment that was intended to protect the people from the severe economic consequences of financial instability. Because of the recognized need for accurate, clear, and high quality information, and the need for minimizing the threat of unexpected systemic failure, institutions are expected to have controls in place. Sarbanes-Oxley (SOX) Section 404, an internal control system, is required, and simply having accounting policies and procedures does not demonstrate that an internal control system is in place. This requirement is best satisfied when sound, comprehensive accounting procedures document well-defined accounting processes. Regulators and auditors seek proof and supporting documentation to determine compliance with accounting and regulatory requirements.

As such, regulators have increased their scrutiny on an institution's policies and procedures because they are now seen as critical components of an institution's internal control system. Policies and procedures are deemed to be the strategic tools needed to not only meet an institution's goals and objectives, but also to provide an understanding of all their roles and responsibilities, and operation guidelines. A comprehensive action plan for implementing and maintaining policies eliminates common mistakes, and management's internal controls can prevent the institution (or its employees) from making costly mistakes.

As part of the regulators' enhanced scrutiny to ensure compliance is being maintained and all parties are protected, regulators look to see if procedures are in place to ensure consistency in day-to-day operational activities. These procedures provide clarity regarding activities that may be important to the company, as well as dealing with accountability issues (especially those that may have serious consequences). As regulators increased their scrutiny, the consequences and penalties for failing to implement policies and procedures has also increased significantly. As a result, the number of civil monetary penalties, cease-and-desist orders, and other enforcement actions are at their highest level in the last decade. Regulators' tolerance for lack of effective and efficient policies and procedures, as well as internal controls, is very low. Regulators no longer simply issue recommendations in their examinations for improvement in policies and procedures. They have become more stringent in their expectations that comprehensive and efficient policies and procedures are implemented and adhered to, fulfilling all regulatory compliance requirements. With Dodd-Frank and SOX implications, regulators, now more than ever, will develop their overall opinion of an institution starting with their policies and procedures.

Bank Internal Control Manual addresses issues related to implementation and management of internal control systems. In the manual are examples of policy and procedures that provide a range of management resources to help you and your financial institution's management team design, develop, implement, and maintain a proactive risk management supervisory system of internal controls. The manual focuses on different scenarios. For example, your situation may involve implementing an integrated system in your bank, a department, or a subsidiary. Other challenges may exist, such as establishing formal guidelines for an existing internal control system and related processes.

ADDRESSING TODAY'S INTERNAL CONTROL CHALLENGES

The manual focuses on basic challenges for financial institution management today:

- How does a bank management team detail what internal control systems exist?
- If control systems exist, how does an officer or manager determine whether those controls or systems are working?
- How can senior management ensure that internal control systems will be created as needed or specific work flow situations change?
- How do you build flexible controls with appropriate exception tracking systems?

The challenges are further complicated by changing financial institution structures, new regulatory requirements, increased competitive pressures, consolidation of operations, development of new or enhanced products and services, and changing technology. It seems like an impossible task! However, with this manual, there are basic conceptual corporate governance guidelines provided which, through staff accountability and individual understanding of the importance of internal control systems, can capture even the most frequent changes or newest ideas within a viable internal control system. Supervisors and staff can ensure that the written procedure or specific control works. From the top down, however, there must be an overall corporate commitment to a well-run, safe, and sound organization. Cutting costs, reducing staff, and shortcutting controls may save money in the short run, yet leave the institution vulnerable to serious problems in the near future.

The Auditing Standards Board (ASB) definition of internal control is in Statement of Auditing Standard (SAS) No. 78 (AU Section 319), Consideration of Internal Control in a Financial Statement Audit: An Amendment to SAS 55. The definition incorporates the common critical elements of internal control systems in the Committee of Sponsoring Organizations of the Treadway Commission (COSO) report, Internal Control – Integrated Framework, issued in 1992. The COSO framework is the U.S. standard on internal control.

COSO and SAS 78 define internal control “as a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of the following objectives:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations”

The COSO model serves as the basis for the internal control assessment and reporting requirements for depository institutions presented in section 112 of the FDICIA. This model also is broadly applicable to public companies in complying with section 404 of the Sarbanes-Oxley Act. We discuss the section 404 requirements later in this How to Use this Manual’s section.

An effective internal control system better ensures the following important attributes:

- Safe and sound operations
- Integrity of records, financial statements, and managerial reporting
- Compliance with laws and regulations, and supervisory requirements
- Decreased risk of unexpected losses
- Decreased risk of damage to the financial institution’s reputation
- Adherence to internal policies and procedures

- Efficient operations and long-term profitability targets

A system of strong internal control is the backbone of a financial institution's management program. Strong internal controls help a financial institution meet goals and objectives, and maintain successful, healthy operations. Conversely, a lack of reliable records and accurate financial information may cause a financial institution to fail. An effective internal control system integrated into the organization's overall risk management strategy serves the best interest of the shareholders, board of directors, management, and regulators.

Regulators place high importance on internal control systems in light of past corporate scandals and financial institution failures. Some institutions failed primarily because they did not detect insider fraud or abuse due to deficient or nonexistent systems of internal control. The types of control breakdowns typically seen in problem and failed institutions can be grouped into five categories:

1. Lack of adequate management oversight and accountability, and failure to develop a strong control culture within the institution.
2. Inadequate recognition and assessment of the risk of certain banking activities, whether on- or off-balance sheet.
3. The absence or failure of key control structures and activities, such as segregation of duties, approvals, verifications, reconciliations, and review of operating performance.
4. Inadequate communication of information between levels of management within the institution, especially in the upward communication of problems.
5. Inadequate or ineffective audit programs and monitoring activities.

The Federal Deposit Insurance Corporation Improvement Act (FDICIA) of 1991 required the banking agencies to establish certain safety and soundness guidelines. Appendix A of 12 CFR Part 570, Interagency Guidelines Establishing Standards for Safety and Soundness, includes a section on operational and managerial standards. Under these standards, regulatory agencies require management and the board of directors to implement and support effective internal controls appropriate to the size of the financial institution, and the nature, scope, and risk of its activities.

Small Public Companies to Begin Providing Audited Assessment of Internal Controls Over Financial Reporting

The Securities and Exchange Commission announced in October 2009, that the smallest publicly reporting companies will begin complying with the final portion of a key provision of a 2002 corporate governance law that requires companies to report to the public about the effectiveness of their internal control over financial reporting.

Under the provisions of Section 404 of the Sarbanes-Oxley Act, public companies and their independent auditors are each required to report to the public on the effectiveness of a company's internal controls. The smallest public companies with a public float below \$75 million have been given extra time to design, implement and document these internal controls before their auditors are required to attest to the effectiveness of these controls.

This extension of time will expire beginning with the annual reports of companies with fiscal years ending on or after June 15, 2010. This expiration date previously had been for fiscal years ending on or after December 15, 2009. The extension was granted so that the SEC's Office of Economic Analysis could complete a study of whether additional guidance provided to company managers and auditors in 2007 was effective in reducing the costs of compliance. Because the study was published less than three months before the December 15 deadline, the Commission determined that additional time is appropriate and reasonable so that small public companies and their auditors can better plan for the required auditor attestation.

DIRECTOR RESPONSIBILITIES

The board of directors has the primary responsibility of establishing and maintaining an adequate and effective system of internal control. An effective board generally has members who have financial or banking experience and an obligation to stay current with innovations in corporate governance.

The board must report to the FDIC and the OTS on internal control over financial reporting and compliance with certain laws and regulations, as well as file annual audited statements under Section 112 of FDICIA.

The board is also responsible for approving and periodically reviewing the overall business strategy and significant policies of the association, and understanding the major risks the institution takes. The board should set acceptable levels for these risks, and ensure that senior management takes the required steps to identify, measure, and monitor these risks in order to mitigate them to acceptable levels. To remain effective in the dynamic and ever-broadening environment that institutions operate in, the board of directors should periodically review the system of internal control and ensure management regularly assesses and updates it.

The board and senior management must establish a strong culture of compliance at the top of the institution, oversee anti-fraud programs at the institution, and set a proper ethical tone for governing the conduct of business. Staff members at all levels must demonstrate successful completion of an ethics program.

FOCUS ON INTERNAL CONTROLS

The systems of internal controls exist to assure the achievement of intended results, to promote operating efficiency, and to encourage compliance with policies and other established constraints. Management's primary concern must be the continuing effectiveness of the systems of internal controls that influence business results. The important qualities that must be periodically evaluated are adequacy, effectiveness and efficiency.

In evaluating adequacy, management should ascertain whether systems include design features proper to the circumstances and reasonably sufficient to effect control. The evaluation of adequacy begins with the comparison of "what should be" to "what is." Initial implementation of internal controls systems with respect to supporting proposed procedures, should ensure the adequacy of control within the organizational structure.

In evaluating effectiveness, management should ensure compliance with internal control features and the extent to which compliance serves the intended purposes. The question that must be answered is: *Do the controls work?*

In evaluating efficiency, management should assess the practicality of controls in terms of their cost relative to their intended benefit. It is not advisable that management judge internal control efficiency in absolute terms. An evaluation of internal control efficiency is restricted to the controls themselves and does not extend to the measures of operating performance associated with the functioning of such controls. In judging efficiency, management should consider whether the benefits provided by the controls exceed their cost.

The systems of internal controls (including procedures) should address the following:

- Provide reasonable assurance that assets are safeguarded, information (financial and other) is timely and reliable, and errors and irregularities are discovered and promptly corrected.
- Promote operational efficiency.
- Encourage adherence to managerial policies, laws, regulations and sound fiduciary principles.

Members of management who are responsible for policy implementation are also responsible for the design and the maintenance of the systems of control. As a follow-up independent review, internal auditors are responsible for that management function which independently evaluates the adequacy, effectiveness and efficiency of the systems of controls. Internal auditors should make sure that those who rely on their opinions understand that no practical system can guarantee the quality of future performance.

Internal controls should act as a positive force to facilitate successful operations, as well as a negative one that restricts activities. Accordingly, management should evaluate control systems in terms of the incentives they provide, as well as the sanctions. Safeguarding assets relates to physical, legal and all other protective means by which the financial institution assures the full realization of its resources.

All information should be subject to the systems of internal controls. Timely information is a critical monitoring reporting component which anticipates a decision need and is available to the persons who will use it when they need it. Reliable information provides a sound basis for decision because of the authenticity of its source, the manner in which it is recorded and the form and content of its presentation.

The systems of internal controls must detect and correct errors and irregularities when preventive controls fail. Sound systems of control contain safeguards that will counteract failures in other controls. The systems of control should promote operational efficiency. The features of control systems that promote operational efficiency include the processes used to select and train personnel, establish procedures, set performance requirements, measure results and provide incentives.

Managerial policies, laws, regulations and sound fiduciary principles establish boundaries within which the financial institution can conduct its business. The features of the internal control system that encourage compliance with these requirements include the separation of duties, the employment of persons likely to comply, the establishment of authority limits and the communication of expected conduct.

Internal Controls Changes

The Public Company Accounting Oversight Board (PCAOB) streamlined the audit rules that accounting firms must follow when evaluating public company internal controls. The draft statements replace Auditing Standard No. 2 with new standards. The new standards for external firms performing audits of public companies' internal controls over financial reporting, as required by Sarbanes-Oxley Act (SOX) section 404 address cited concerns noted by financial institutions including:

- Extensive reviews often purportedly resulting in overkill audits
- Increased workloads on financial institution staff to cooperate and respond to such reviews
- Unreasonable recommendations for changes in internal controls which often require time to refute
- Significant increases in fees

To address these concerns, the PCAOB recommended the following:

- Reduce testing for companies that have a good control environment.
- Direct auditors to appropriately scope audits for small companies.
- Implement a top-down audit approach, and focus on risk to thereby reduce the amount of testing.
- Improve audit approaches to effectively integrate the financial statement audit with the internal audit control review.
- Require that only material items be tested and reported.
- Permit reliance on effective prior years' controls and controls' reviews, rather than requiring a complete re-audit of those controls.
- Require only one control report, instead of two, from the external auditor.
- Replace the prescriptive requirements for entities with multiple locations, with instead a risk-based approach.

- Required audit firms to consider the work of others that, in turn, may reduce their workload and eliminate the principal evidence requirement now cited in the rules.

The changes that the PCAOB has drafted should have a positive impact on audit reviews. Nevertheless, audit firms will still take a close look at internal procedures and the overall controls environment of a financial institution.

In addressing key elements of SOX, focus on “best practices” that are critical to ensure sufficient controls have been implemented to address risk of noncompliance. These best practices include:

- Development and implementation of clearly articulated roles and responsibilities, and the related assigned accountability.
- Creation of fully integrated financial and internal control processes, utilizing both technology and where applicable, manual controls/procedures to address risk points.
- Integration of adaptability and flexibility elements within control structures, to allow response to organizational and regulatory change.
- Construction of supporting controls and procedures schematics to clearly articulate control points, risk areas, and implemented controls/procedures.
- Utilization of structure education and training to reinforce the organization control environment with periodic refresher/reminder training modules.
- Initiation and ongoing support of effective and efficient evaluation testing, remediating, monitoring, and reporting on control processes.

In May 2007, the PCAOB and SEC approved new guidelines to improve the effectiveness and efficiency of the assessment performed by company management and its auditor of the effectiveness of internal controls over financial reporting covered under SOX. Referred to as Auditing Standard No. 5 (AS5), An Audit of Internal Control Over Financial Reporting That Is Integrated with an Audit of Financial Statements, it superseded Auditing Standard No. 2. The adopted AS5 accomplishes positive changes including:

- Aligns key terms and concepts with terms utilized in SEC rules and guidance.
- Focuses auditors on fulfilling objectives that a properly performed walk-through achieves rather than requiring performance of a walk-through, which under some instances, might lead to a checklist approach.
- Includes discussion of fraud risk and anti-fraud controls within the standard, to emphasize the importance of these controls in assessing risk.
- Emphasizes importance of auditors not to scope the audit to find deficiencies that, individually or collectively aggregated with other exceptions/deficiencies, do not constitute material weaknesses.
- Retains requirements to evaluate all deficiencies that are identified and communicate both material weaknesses and significant deficiencies, in writing, to the audit committee.
- Details how different kinds of entity-level controls have different effects on the selection and testing of controls.
- Empowers auditors to tailor their top-down approach to individual circumstances of each organization by removing the requirement to specifically identify major classes of transactions and significant processes before identifying relevant assertions.

The adoption of AS5 increases the chances that material weaknesses in internal control will be found before they result in material misstatement of a company’s financial statements, and yet at the same time, eliminate

unnecessary procedures. While PCAOB revised AS2 with the release of AS5 to primarily for the benefits of small companies, larger companies also see costs savings up to a 10 percent reduction in their audit bills.

To further assist with the implementation of SOX section 404, new interpretive guidance was provided June 27, 2007, published per 72 FR 25324. The additional information applies to management and auditors. These requirements impact publicly owned banks and other types of financial institutions which are covered under SOX threshold requirements.

The detailed interpretive guidance underscores management's flexibility to undertake an assessment based on its own knowledge of the organization and the company's size, risk profile, and other relative characteristics. The guidance further details specific points to assist smaller publicly held institutions, emphasizing the following points:

- Explanations of the purpose of documentation and how management has flexibility in approaches to documenting support for its assessment
- Guidance to management on how to use different testing approaches from the one utilized by the auditor who performs the section 404 audit and attestation
- Explanation of daily interaction, self-assessment, and other on-going monitoring techniques as support in the evaluation
- Guidance to management on the flexibility to make judgment calls regarding what constitutes adequate evidence in low-risk areas
- Explanation on how to vary evaluation approaches for gathering evidence based on risk assessments

Management evaluations that meet this interpretive guidance are one approach to meet the requirements under SOX. The guidance became effective June 27, 2007.

Enterprise Risk Management

COSO released *Enterprise Risk Management – Integrated Framework* in September 2004. Enterprise risk management expands on internal control to form a more robust framework to effectively identify, assess, and manage risk. Enterprise risk management is interrelated with corporate governance by providing information to the board of directors on the most significant risks and how the association is managing those risks.

Enterprise risk management reflects certain fundamental concepts. It is:

- A process – ongoing and flowing throughout an entity.
- Effected by people at every level of an organization.
- Applied in a strategy setting.
- Applied across the financial institution, at every level and unit, and includes taking an entity-level portfolio view of risks.
- Designed to identify events potentially affecting the institution and manage risk within the board's risk appetite.
- Able to provide management and the board reasonable assurance that the institution is managing its risk.
- Geared to the achievement of objectives in one or more separate but overlapping categories. That is, a particular objective can fall into more than one category – strategic, operations, reporting, and compliance.

The intent of the *Enterprise Risk Management – Integrated Framework* is not to replace the internal control framework, but rather to incorporate the internal control framework within it. Financial institutions may decide to look to this enterprise risk management framework both to satisfy their internal control needs and to move toward a more robust risk management process.

The board and senior management must establish a strong culture of compliance at the top of the association, oversee anti-fraud programs at the association, and set a proper ethical tone for governing the conduct of business. Staff members at all levels must demonstrate successful completion of an ethics program. Enterprise risk management is a critical tool in this process.

An integral part of effective enterprise risk management is an enterprise-wide program that looks at how activities in one area of the association may affect the legal and reputational risks of other business lines and across the association as a whole. Enterprise risk management should consider how compliance with laws, regulations, and internal policies, procedures, and controls should be enhanced or changed. This approach is in marked contrast to the silo approach, which considers the legal and reputational risks of activities or business lines in isolation without considering how those risks interrelate and affect other business lines.

Underlying Value of Solid Controls

Financial and accounting controls, as an example, must be effective. It is critical that a financial institution prepare and present accurate operating results and a risk profile. Unfortunately, weaknesses in these types of controls often contribute to inaccurate or incomplete financial reporting, and subsequently, potential legal fines, significant reputational damage, and loss of business. Strong controls also reflect a primary objective of financial institution regulators. Regulators, in upholding their mission to maintain a safe and sound financial system, assess whether a financial institution has developed and implemented a comprehensive financial control framework.

Top-Level Support¹

Why focus on top-level controls? Everything flows from the top. Controls at the organizational level can have an encompassing influence over controls at the process, transaction, or application level. Controls that apply to all locations and business units help to set consistent standards and expectations across the institution.

Organizational-level controls include governance elements that establish the benchmarks or directives at the highest level of the institution. These basic elements include:

- Policies
- Procedures
- Codes of conduct including details on conflicts of interest
- Assignment of authority and responsibility
- Risk assessment processes
- Identifiable controls that monitor other controls, such as oversight and assessment of the internal audit function, the audit committee, and employee self-assessment and fraud prevention activities, such as whistleblower hotlines, which can have an indirect relationship to financial statement misstatement risk

Many institutions have the opportunity to increase their reliance upon organizational-level controls that can directly mitigate financial statement misstatement risk, such as controls over the period-end financial reporting

1. Adaptation of concepts presented by Deloitte and Touche, LLP, *SOX Optimization: Improving Compliance Efficiency and Effectiveness*, September 2007.

process. Similar controls include monitoring controls such as analytical review and budgeting; and controls governing centralized processing, such as shared service environments.

To ensure top-level controls or organizational controls are fully implemented, identifiable, and consistently communicated, it is important to undertake a procedural approach to reviewing the present control environment, with steps that include the following:

- Understand the overall design and balance of controls and how they align with financial reporting risks.
- As appropriate, flexibility to shift focus toward higher risk areas to enhance compliance quality.
- Support to achieve cost savings by applying more efficient compliance efforts for routine processing-related controls.
- Identification of how organization-level (as opposed to individual process-level) controls can be improved to drive compliance efficiencies and reduce the institution's overall compliance risk profile.

Financial institutions that have instituted successful internal control programs report the following common factors:

- Continuous employee training that integrates institution policies, procedures, and controls
- Review, testing, and enhancement of risk management oversight and related controls
- Automation of controls, processes, and reporting to utilize technology where appropriate
- Documented procedures, including identification of quality assurance checkpoints and internal controls
- Modified policies, procedures, and if applicable forms, to incorporate internal controls
- Increased frequency of testing and auditing internal controls

REGULATORY CONCERNS

The importance of internal control systems and the level of supervision of internal controls have become a regulatory concern. The Federal Financial Institutions Examination Council (FFIEC) has detailed this concern through various issuances of interagency policy statements pertaining to controls and technology. Further, each agency has issued specific internal control system guidance on the need to enhance controls and support proper internal management systems. The Office of the Comptroller of the Currency (OCC) has gone a bit farther by both underscoring these concerns in public speeches and issuing new internal control system examination procedures. Examiners will be taking a much closer look at internal control systems' processes and performing a more detailed review of actual controls. The regulatory emphasis translates to a very real concern for financial institution directors and management.

Statement on Auditing Standards (SAS)

On June 15, 2011, two new issuances which impact the Statement on Auditing Standards (SAS) No. 70 went into effect. These issuances were the Statement on Standards for Attestation Engagements (SSAE) No. 16 (titled *Reporting on Controls at a Service Organization*) and the International Standard on Assurance Engagements (ISAE) No. 3402. U.S. service organizations' reporting guidance is now provided under SSAE No. 16 and not SAS 70. The new SSAE No. 16 was designed to coincide with the compliance requirements of ISAE No 3402. Although most changes from the SAS 70 to the SSAE 16 are minor, some significant changes have been implemented. In regards to service audit reports, a major adjustment of the SSAE 16 includes changing the service auditors' opinion, regarding the system and suitability of design, from a point in time to the report period. Another major adjustment includes the inclusion of a "management assertion" section of the report. The ISAE

No. 3402 provides the ability for service organization control reporting to coincide with the already established global accepted standard and provide its assurance that it meets international standards.

The FFIEC released its Supplement to the 2005 Guidance to *Authentication in an Internet Banking Environment* to reinforce its expectations that organizations implement procedures to ensure customers' identification is authenticated and that the manner in which the organization authenticates identification is appropriate to the organization's risks. The supplement's guidance includes risk assessment updating, layered security system, acknowledgement of separate risk for consumer banking and business banking, mitigation of risk through process changes, evaluation of access to sensitive applications, implementation of risk-based approaches which strengthens controls, and revisiting established procedures to determine if they are still adequate.

As part of KPMG's continued efforts in assisting organizations understand how their organizations compare to others, KPMG released its *2010 Internal Controls Study of Technology Companies*. This study is part of a series of studies conducted by KPMG which looks at process level internal controls in technology companies. Data gathered from KPMG's survey is separated by both company size and its industry. The survey obtains information regarding key controls for processes, automated controls, and manual controls. According to the study's findings, KPMG observed that due to an overall decline in IT General Controls, "the average number of key controls is down by 10% in 2010," while "overall and across processes, automated key control percentages are either flat or down." Other findings showed that while the number of key controls in the software industry increased, the average number of control in the electronics industry declined. The average number of manual controls increased while the average number of automated controls decreased.

CFPB Recodification

With the implementation of the Consumer Financial Protection Bureau (CFPB), there are CFR citations that have changed. A CFPB recodification conversion chart for consumer finance citations can be found before the title page of this manual. As chapters in your manual are updated, they will contain the new citations. We trust that this conversion chart will be a valuable reference.

PREPARING FOR EXAMINATIONS

Your institution may not be at risk today, and it may not even have a specific concern regarding internal control systems. However, various aspects of your next examination will focus your management team's efforts on properly addressing risk management. These examinations will be checking your risk management approach, and examiners will also be correlating risk issues or risk exposures as they are detected throughout the organization. You will reduce your regulatory risk by taking time now to prepare a corporate approach to internal control system processes, reviewing plans for further changes in data flow or system processes which result in internal control changes, and even moving toward a more automated internal control exception tracking system. Analyzing your risk exposure and making enhancements before the start of your next examination will undoubtedly have a positive impact on the examination results.

TOOLS FOR ADDRESSING SOLUTIONS

The manual offers insights and hints not only on evaluating the concepts of risk management and development of internal control systems to address those risks, but also on dealing with other issues such as internal controls design, detailing internal controls, implementing alternatives, assessing risk positions for each type of control risk, developing formal internal control policy and procedures, and implementing systems to ensure ongoing proper control and oversight. By using this manual, management team members will not only become aware of existing internal controls, important internal control system components, and development processes, but also will gain an understanding of the applicable regulatory issues and examination focus points. Risk management processes are a critical management focus point of successfully implementing and maintaining a viable internal control system.

INTERNAL CONTROL CHECKLISTS

The internal control checklists in Volume II are a critical tool to assist in the identification of organizational-level controls and areas where further controls will reduce the institution's overall compliance risk profile. The checklists presented in Volume II are organized by the major operational areas of a bank:

- Executive
- Lending
- Treasury/Finance
- Trust
- International Banking
- Operations
- Data Processing

COMPANION CD ALLOWS YOU TO CUSTOMIZE YOUR CONTROLS

From credit risk to financial software systems, the companion CD for this manual contains sample internal controls for every key area of the institution, checklists, examples of documentation, and clear guidelines that you can use for internal control checklists in your own financial institution.

The CD contains two PDFs — one for each of the two volumes. This makes searching within a volume for specific references or topics an electronic task.

Sample internal control checklists are provided for each key area, so that you can keep your banking functions current with the latest compliance issues. You can easily customize the checklists on CD, using Microsoft Word, so that you keep your banking functions current with the latest compliance issues.

ACKNOWLEDGMENTS

REGCOM would like to thank staff members of various banks, bank holding companies, and banking regulatory agencies. Their insights and comments have helped us develop the background research, writing outline, and tips that are found throughout this manual.