Office of Inspector General

September 3, 2004
Report No. 04-032

Strategies for Enhancing Corporate Governance

AUDIT REPORT

TABLE OF CONTENTS

TABLES:

FDIC

Federal Deposit Insurance Corporation
801 17th Street NW, Washington, DC 20434-0002

Office of Audits
Office of Inspector General

DATE: September 3, 2004

MEMORANDUM TO: Steven O. App
Chief Financial Officer

[Electronically produced version;
original signed by Russell A. Rau]

FROM: Russell A. Rau
Assistant Inspector General for Audits

SUBJECT: *Strategies for Enhancing Corporate Governance*
(Report No. 04-032)

This report presents strategies for enhancing corporate governance. The objective of this audit was to synthesize information and provide a prospective focus that may be used in evaluating approaches for enhancing some key elements of the corporate governance framework – the audit committee, risk management, and internal control over financial reporting.

BACKGROUND

Accountability breakdowns at several U.S. corporations have led to scandals, financial statement restatements, and even bankruptcy. These breakdowns affected thousands of shareholders and employees and contributed to diminishing investor confidence. In response to these events, legislative and regulatory reforms were initiated to restore the public's trust. For example, the Sarbanes-Oxley Act of 2002[1] provided a reform framework for more effective corporate governance and regulation of the accounting profession that performs audits of financial statements and related internal controls.

These reforms are challenging the way organizations have conducted business. Organizations are being challenged with achieving new accountability standards while meeting their performance objectives. Audit committees representing the Board of Directors and shareholders are expected to be more involved in understanding the entity's business and monitoring complex accounting and financial reporting issues. In addition, the audit committee should be aware of financial risks and how management is addressing those risks.

A practice that has emerged to assist organizations in managing risk is enterprise risk management (ERM). ERM enables management to evaluate risk from a corporate-wide perspective and is sometimes referred to as strategic, business, or integrated risk management.

[1] Pub. L. No. 107-204, codified principally to titles 15 and 18, United States Code (U.S.C.).

Also, as a result of the Sarbanes-Oxley Act, management now must evaluate its internal control structure over financial reporting and report on its effectiveness. In addition, auditors must attest to management's assertion regarding the effectiveness of those controls. Certain financial institutions have been required to meet similar but not identical requirements enacted by the Federal Deposit Insurance Corporation Improvement Act of 1991.[2]

The Federal Deposit Insurance Corporation (FDIC) currently has structures in place or in development that address these emerging business practices. This report provides information on audit committee best practices, ERM, and internal control over financial reporting that can be useful in further enhancing the FDIC's governance structure. The FDIC Office of Inspector General (OIG) actively supports a sound governance structure.

GOVERNANCE DEFINED

Governance can be defined as the processes for managing an organization's affairs or for ensuring accountability. Governance can include various activities such as setting business strategies and objectives, determining risk appetite, establishing culture and values, developing internal policies, and monitoring performance.[3]

A board of directors and internal and external auditors play a key role in corporate governance. The board reviews the development and execution of business strategies. Auditors may identify risks and controls and confirm adherence to policies. According to Ernst & Young,[4] some key components of effective corporate governance include the following:

- An instrumental executive management team.
- An effective, independent board.
- A sound culture that allows the principles of good governance to thrive.
- A proactive audit committee.
- A compensation committee aligning executive compensation to shareholder value.
- A nominating committee ensuring effective governance of the board.
- A sound internal control framework.
- A relevant code of ethical behavior.
- Clear, enforced policies and procedures.
- Effective management of risk.
- An objective, well-resourced internal audit function.
- Independent, effective external audit.
- Transparent disclosure, effective communication, and systems that ensure effective measurement and accountability.

[2] Pub. L. No. 102-242.
[3] *Integrity-Driven Performance, A New Strategy for Success Through Integrated Governance, Risk and Compliance Management*, PricewaterhouseCoopers, 2004.
[4] *What is Corporate Governance*? Corporate Governance Series, © Ernst & Young, March 2004.

Also, in the aftermath of major corporate failures such as Enron, the National Association of Corporate Directors[5] developed recommendations for practices in corporate governance. Those recommendations, provided below, include some of the same components as described above.

Table 1: National Association of Corporate Directors' Core Recommendations for Governance Practices

Board of Directors should:

- Be composed of a substantial majority of independent directors.
- Consider designating an independent director as chairman or lead director.
- Regularly evaluate the performance of the Chief Executive Officer (CEO), other senior managers, the board as a whole, and individual directors.
- Annually review the adequacy of their company's compliance and reporting systems.
- Adopt a policy of holding periodic sessions of only independent directors, providing board and committee members the opportunity to react to management proposals and/or actions in an environment free from formal or informal constraints.
- Be engaged with management on company strategies.
- Have an orientation program for new directors, and ensure that directors are current on company issues.

Key committees of the Board of Directors should:

- Be composed entirely of independent directors, and be free to hire independent advisors as necessary.
- Have a board-approved written charter detailing the board's duties.

Audit committees should meet independently with both the internal and independent auditors.

Source: *Recommendations from the National Association of Corporate Directors Concerning Reforms in the Aftermath of the Enron Bankruptcy*, National Association of Corporate Directors.

Although the FDIC is an independent agency of the federal government, many of the key components of effective corporate governance may be used in the Corporation's governance structure. For example, a proactive audit committee, sound internal control, an ethics program, effective risk management, and independent and objective auditors are elements that are part of the existing structure.

[5] A national nonprofit organization established to serve the corporate governance needs of individual corporate directors and boards.

CORPORATE GOVERNANCE COMPONENTS AT THE FDIC

The FDIC has similar corporate governance components as those discussed earlier. For example, the FDIC has a Board of Directors (Board), which has an Audit Committee; a newly established Office of Enterprise Risk Management (OERM); executive management; and independent auditors -- the FDIC OIG and the Government Accountability Office (GAO).[6] The Board consists of five directors, three of which are appointed by the President and confirmed by the Senate. The other directors include the Comptroller of the Currency and the Director of the Office of Thrift Supervision (OTS).

The Board's Audit Committee monitors the FDIC's financial reporting responsibilities and internal control programs. The committee also regularly meets with and discusses issues with the OIG. The following officials compose the Audit Committee:

- Vice Chairman of the Board of Directors;
- Director, OTS; and
- Deputy to the Chairman and Chief Financial Officer.

OERM administers the FDIC's Internal Control Program (ICP), which monitors risks. The audit committee may direct OERM and appropriate divisions and offices to clarify or follow up on specific issues and conduct special projects. Additionally, OERM conducts the FDIC's program to fulfill the Chief Financial Officers Act of 1990[7] annual reporting requirements, including reporting on the ICP.

The OIG is another key element in the FDIC's governance structure. The OIG, as an independent unit, reports to the Congress and Board Chair. The OIG conducts audits and investigations of the FDIC's programs and operations. Also, through semiannual reports to the Congress and other products, the OIG provides insights into the key FDIC management and performance challenges.

Another independent audit unit is the GAO, which reports to the Congress and primarily audits the financial statements of the funds administered by the FDIC. Additionally, the GAO attests to the effectiveness of the Corporation's internal control over financial reporting and compliance and may audit other areas of interest to Congress.

Each of these components contributes to the governance structure of the FDIC. As concerns for governance reforms have affected companies worldwide, it may be an opportune time to examine some of the strategies developed to enhance existing structures and build proactive risk reduction measures into business practices.

[6] The name of the GAO was changed, effective July 7, 2004, as a result of recent legislation.
[7] Pub. L. No. 101-576, codified principally to title 31, U.S.C.

STRATEGIES FOR ENHANCING THE CORPORATE GOVERNANCE FRAMEWORK

Audit Committee Overview

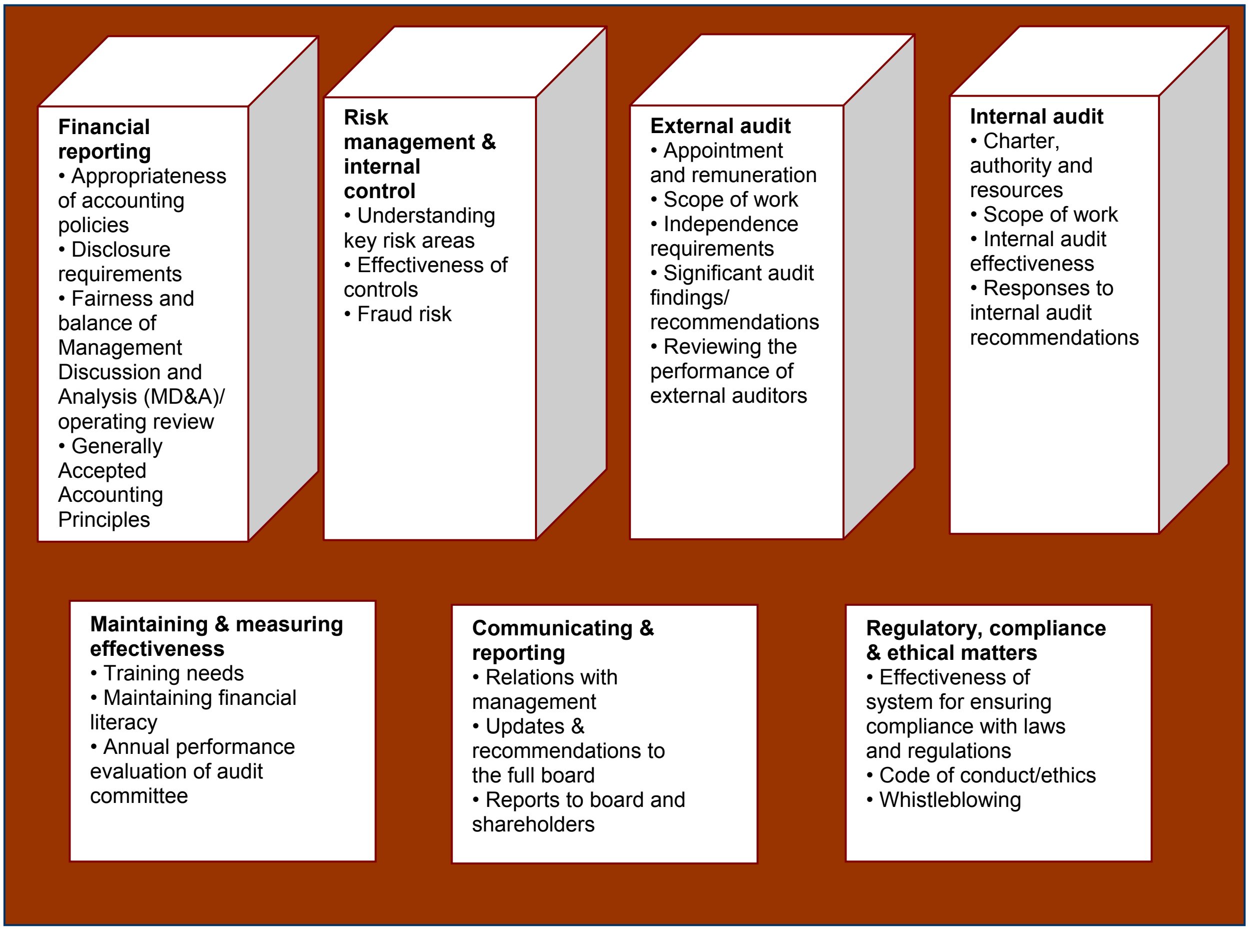
According to the 1999 Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees,[8] the role of an audit committee is one of oversight and monitoring. In its report entitled, *Report and Recommendations of the Blue Ribbon Committee on Improving the Effectiveness of Corporate Audit Committees*, the Committee stated:

> … in carrying out this job it acts in reliance on senior financial management and the outside auditors. A proper and well-functioning system exists, therefore, when the three main groups responsible for financial reporting -- the full board including the audit committee, financial management including the internal auditors, and the outside auditors -- form a "three-legged stool" that supports responsible financial disclosure and active and participatory oversight. However, in the view of the Committee, the audit committee must be "first among equals" in this process, since the audit committee is an extension of the full board and hence the ultimate monitor of the process.

The Sarbanes-Oxley Act placed renewed emphasis on the role of the audit committee. The Act requires audit committees to be independent and to assume certain oversight responsibilities. To meet these requirements and enhance their effectiveness, organizations have developed various practices. Based on a PricewaterhouseCoopers worldwide study of best practices, the main areas of audit committee responsibility include oversight of financial reporting, management of risks and internal control, and the work of external and internal auditors. Also, audit committees need to evaluate their own performance, establish effective working relationships with management, and monitor compliance with regulations and ethical issues. These areas of responsibility are illustrated in more detail in Table 2 on the next page.

[8] The panel was established in September 1998 by the New York Stock Exchange and National Association of Securities Dealers, Inc., to make recommendations on strengthening the role of audit committees in overseeing the corporate financial reporting process.

Table 2: Main Areas of Audit Committee Responsibility



Financial reporting
- Appropriateness of accounting policies
- Disclosure requirements
- Fairness and balance of Management Discussion and Analysis (MD&A)/ operating review
- Generally Accepted Accounting Principles

Risk management & internal control
- Understanding key risk areas
- Effectiveness of controls
- Fraud risk

External audit
- Appointment and remuneration
- Scope of work
- Independence requirements
- Significant audit findings/ recommendations
- Reviewing the performance of external auditors

Internal audit
- Charter, authority and resources
- Scope of work
- Internal audit effectiveness
- Responses to internal audit recommendations

Maintaining & measuring effectiveness
- Training needs
- Maintaining financial literacy
- Annual performance evaluation of audit committee

Communicating & reporting
- Relations with management
- Updates & recommendations to the full board
- Reports to board and shareholders

Regulatory, compliance & ethical matters
- Effectiveness of system for ensuring compliance with laws and regulations
- Code of conduct/ethics
- Whistleblowing

Source: *Audit Committees: Good Practices for Meeting Market Expectations*, © PricewaterhouseCoopers, July 2003.

Audit Committee Best Practices

Some examples of audit committee best practices to consider are provided in Table 3. These practices were adapted from *Audit Committees: Good Practices for Meeting Market Expectations,* © PricewaterhouseCoopers, dated July 2003.

Table 3: Audit Committee Best Practices

Authority
Obtained board authority to perform activities within its terms of reference.
Has access to members of management, employees, and relevant information, unless such access is restricted by law.
Has authority to establish procedures to deal with concerns of employees and complaints received regarding accounting, internal control, and auditing matters.
Membership
The board periodically reviews the mix of experience and skills of committee members to maintain an appropriate balance.
Committee members are appointed by the board or a nominating committee of the board.
The size of the committee is appropriate to the organization.
The experience and qualifications of committee members are compatible with the duties of the committee, including the ability to understand financial statements. At least one of the members has accounting or related financial expertise.
Meetings
The committee meets regularly, with special meetings called as circumstances warrant. (At least 3 or 4 meetings each year are desirable.)
Meeting agendas and supporting papers are prepared and distributed sufficiently far enough in advance to enable committee members to prepare for meetings.
The chairman or another member of the committee attends the board meeting at which the financial statements are approved.
Members of the committee attend every meeting.
Minutes of meetings are circulated on a timely basis to members of the board and audit committee (and auditors where appropriate).

The committee meets with in-house legal counsel on a regular basis.
New committee members are provided with sufficient background information and training to meet their responsibilities effectively.
The committee has adequate resources to discharge its responsibilities.
The Committee's Internal Control Responsibilities
Evaluates the "control culture" established by management.
Understands the control systems implemented by management for approval of transactions, recording of data, and compliance of the financial statements with relevant standards and requirements.
Considers whether internal control recommendations made by auditors have been implemented by management.
Considers how management has reviewed the adequacy of controls surrounding electronic data processing and computer security.
The Committee's Financial Reporting Responsibilities
Reviews the areas of greatest financial risk and management's actions to address those areas.
Reviews significant accounting and reporting issues and understands their likely impact on the financial statements.
Oversees the periodic financial reporting process and reviews the interim financial statements, annual financial statements, and preliminary announcements prior to their release.
Meets with management and external auditors to review the financial statements and results of the audit.
Ensures that significant adjustments, unadjusted differences, disagreements with management, and critical accounting policies have been discussed with the external auditor.
Considers whether the narrative information included in the other sections of the annual report is understandable and consistent with the information in the financial statements.
Reads the representation letters given by management to the external auditors and considers any specific representations therein.

The Committee’s Compliance With Laws and Regulations Responsibilities
Reviews management’s procedures for monitoring the company’s compliance with laws and regulations.
Reviews updates from management and legal counsel regarding compliance matters that may affect the financial statements.
The Committee’s Responsibilities Regarding Auditors
Discusses the auditors’ proposed audit scope and approach.
Discusses any audit problems, including restrictions on the scope of the audit or denials of access to requested information.
Reviews reports made by the auditors to management, and ensures that management responds to these findings.
Meets privately with auditors on a regular basis.
Discusses the extent to which auditing and accounting firms are used, and understands the rationale for their use.
The Committee’s Reporting Responsibilities
Reports committee activities to the board regularly.
Ensures that reports on committee activities required by law have been prepared.
The Committee’s Performance Evaluation Responsibilities
Periodically assesses the performance of individual members and of the committee as a whole.
Assesses the achievement of the duties specified in the charter and reports to the board.
The Committee’s Charter
Reviews the committee charter annually, and discusses any proposed changes with the board.
Ensures the charter is approved/reapproved by the board.

We have organized these practices into an audit committee self-assessment tool in Appendix II. The tool can be modified to reflect the specific operations of the FDIC.

Overview of Enterprise Risk Management

As discussed earlier, risk management and internal control are in the areas of audit committee responsibility. A practice that has emerged to identify and manage risk from a corporate-wide perspective is ERM. Based on the 2002 benchmarking survey[9] of ERM in the insurance industry, insurance companies were implementing ERM for the reasons noted in Table 4.

Table 4: Insurance Companies That Implemented ERM

Reason for Implementation	Percent of Companies That Responded*
Good business practice	88
Provides coherent conceptual framework to coordinate risk management activity	52
Provides competitive advantage	46
Corporate governance guidelines	42

Source: Tillinghast-Towers Perrin.
*Eighty-two companies responded.

Essentially, ERM differs from the traditional approach to risk management as illustrated in Table 5 on the next page.

[9] The Tillinghast-Towers Perrin survey of insurance companies discussed in its report entitled, *Enterprise Risk Management in the Insurance Industry 2002 Benchmarking Survey Report*.

Table 5: Traditional Risk Management in Comparison to ERM

Traditional Risk Management	ERM
Risk as individual hazards	Risk in the context of business strategy
Risk identification and assessment	Risk portfolio development
Focus on discrete risks	Focus on critical risks
Risk mitigation	Risk optimization
Risk limits	Risk strategy
Risk with no owners	Defined risk responsibilities
Haphazard risk quantification	Monitoring and measuring of risks
"Risk is not my responsibility"	"Risk is everyone's responsibility"

Source: Excerpt from "Enterprise Risk Management: What CPAs [Certified Public Accountants] Need to Know About this Company-Wide Approach," © *Journal of Accountancy*, June 2004.

Determining an ERM Framework

Organizations with experience in ERM note that implementation is not without its challenges. For example, some of the common challenges for insurance companies include a lack of tools for assessing, measuring, mitigating, and financing operational risks; organizational turf; processes; and time.[10]

To implement an ERM program, an organization needs to decide on a framework. There are no "right answers" for establishing a framework; however, organizations can develop four key questions to help in establishing an ERM framework appropriate for the specific situations and culture of the organization. These four key questions[11] are as follows.

Question 1: What are the objectives for ERM? Organizations can have several objectives, but the priority they assign to each objective is important. Some objectives include:

- Compliance - reacting to external guidance
- Defense - anticipating problems
- Coordination/integration – breaking down internal "silos" by coordinating risk management activities for the sake of efficiency

[10] *RiskValueInsights: Creating Value Through Enterprise Risk Management – A Practical Approach for the Insurance Industry*, Tillinghast-Towers Perrin.
[11] *Implementing Enterprise Risk Management: Getting the Fundamentals Right*, Jerry Miccolis, Brinton Eaton Associates, Inc., © International Risk Management Institute, June 2003.

- Exploiting opportunities and creating value – appreciating risk interaction across the enterprise

Question 2: What will be the scope of the ERM program? The following are examples of the types of risks that may be included in an ERM program:

- Financial – interest rate, investment, credit, liquidity
- Operational – technology, political, regulatory
- Hazard – legal liability, property damage, natural catastrophe
- Strategic – poor planning and poor execution

Also, management may desire that ERM influence processes such as:

- Strategic planning
- Capital management
- Asset allocation
- Performance measurement
- Financial modeling

The scope of the risks and management processes need to be aligned and are likely to help the organization achieve the ERM objectives determined in response to Question 1.

Question 3: What kind of organizational structure, based on ERM, will work for the organization? To answer this question, consider the following:

- The organizational components that will be involved in managing ERM and the functions that will be integrated into the ERM program. Some organizations use existing functions, while others create new functions such as a chief risk officer (CRO) or ERM policy committee.

- The anticipated responsibilities of the ERM. Will the function serve as a coordinating body for the individual risk management activities or as an advisory body?

- The management level to which the ERM function will report. A CRO may report to either the Chief Executive Officer (CEO) or Chief Financial Officer (CFO), while an ERM committee may report to the CEO.

- The most important capabilities and competencies for the ERM function. The ERM function's capabilities and competencies could include risk assessment, modeling, financial engineering, communication, organizational management, and project management.

Table 6 shows examples of the risk infrastructure used by some major corporations.

Table 6: Examples of Risk Infrastructures

Company	**Risk Infrastructure**
J.P. Morgan Chase	Highly organized committee structure to communicate and drive risk management considerations into operating decisions.
E.I. du Pont de Nemours and Company	Risk management committee assists the CEO in setting risk management policies and guidelines. Committee maintains close contact with business units.
Microsoft Corporation	Driven by technology via Intranet and ongoing personal communication of risk management group with operating management.
United Grain Growers Limited [Merged with Agricore Cooperative Ltd. on November 1, 2001]	Risk management committee recommends policy and process: reports to audit committee on risk management performance.
Unocal Corporation	Efforts of internal audit department and health, environmental, and safety department to promote enterprise-wide risk management throughout operating management.

Source: *Making Enterprise Risk Management Pay Off, How Leading Companies Implement Risk Management*, Thomas L. Barton, William G. Shenkir, and Paul L. Walker, © Prentice Hall, 2002.

Question 4: What tools will the organization need to implement the ERM program? Some possible tools include:

- Risk audit guides – for risk mapping of individual risks, risk assessment workshops, and risk assessment interviews with management and staff.
- Stochastic risk models – to simulate a specific system by developing cause-effect relationships between all the variables of that system.
- Risk monitoring reports – for managers, boards, and external stakeholders.

When determining the type of tools to select, organizations should consider tools that fit the risks and processes within the scope of the ERM program.

Lessons Learned From Others in Developing an ERM Framework

Although no single ERM model fits all organizations, a study of how large companies were implementing ERM identified some "lessons learned" that could be used in the process of customizing an ERM framework. The study, sponsored by the Financial Executives Research Foundation, reviewed five major companies, including J.P. Morgan Chase and Microsoft Corporation, identified the following 18 lessons learned.[12]

Lesson 1

Organizations may have difficulty identifying a "cookbook recipe" for implementing ERM because developing an appropriate approach depends on the culture of the company and the agents leading the effort. Decision-makers need to make sure that risk management is a critical part of their job, and they need to be aware of the risks facing other units and the organization as whole.

Lesson 2

Managing risk effectively requires implementing a formal initiative to identify all significant risks. Some possible risk identification methods include scenario analysis, self-assessments, brainstorming sessions, and team meetings.

Lesson 3

Risk identification should be dynamic and continuous because the business environment continually changes. The risk identification process involves identifying all risks and sorting them by importance.

Lesson 4

Determining the importance, severity, or dollar amount of risks is important to the risk ranking process. A risk ranking component helps management understand the perceived importance of a risk, and by sorting the risks according to importance, management can develop a risk management strategy and allocate resources efficiently.

Lesson 5

"Risks should be ranked on some scale of frequency or probability." One company lists risks and rates them on probability, while another company assigns a frequency to each risk. Tools such as risk lists help management develop a view of all the risks and those that are most significant.

[12] *Making Enterprise Risk Management Pay Off, How Leading Companies Implement Risk Management*, Thomas L. Barton, William G. Shenkir, and Paul L. Walker, © Prentice Hall, 2002.

Lesson 6

Financial risks should be measured with the most sophisticated and relevant tools available. Risk measurement helps ensure that the organization is not spending resources on the least risky areas. Organizations face a challenge in this area because not all risks are measurable. For example, operational risk management is in the early stages, so there may not be a lot of historical information to use as a baseline. Sharing best practices is a possible approach.

Lesson 7

"Develop sophisticated tools and measures that meet the organization's needs and that management can easily understand." The most developed area of risk measurement is the financial risk area. Various tools such as value at risk (VAR) are available to assist in measuring financial risk. VAR measures the worst expected loss over a given time period and was originally developed for use in financial institutions. Other methods include earnings at risk (EAR) and stress testing. EAR measures the impact of risks on earnings, and stress testing involves reviewing the impact of worst-case scenarios.

Lesson 8

Understand the organization's risk appetite. Risk appetite concerns the amount of risk that the company is willing to accept. Knowing the amount of risk the company is willing to accept and having a measure of how that risk affects areas such as earnings permit managers to understand the relationship between risk and achieving expectations.

Lesson 9

Thoroughly measure nonfinancial risks. As noted earlier, measuring operational risks is new and is not as advanced as measuring financial risks. Recognizing that operational risks are important, some companies are engaged in sharing best practices in this area and developing metrics. Also, techniques used in measuring financial risks may be adopted for operational risk measurement. Risk profiles and worst-case scenario possibilities are examples of techniques that may be adapted to operational risk measurement.

Lesson 10

"Companies are choosing different combinations of acceptance, transfer, and mitigation[13] to manage risk." The organization's willingness to accept risks may influence the approach to managing risks. For example, an organization can accept a risk if management determines that the organization can bear the consequences or the risk has been mitigated or has been transferred to a level that the company is willing to accept.

[13] An organization may build controls to mitigate a risk.

Lesson 11

Reevaluate decisions regarding control, acceptance, and transfer of risk on a continuous basis. Building control is a form of mitigating risks. Companies that identify risks evaluate the controls to mitigate higher priority risks and implement continuous monitoring to detect potential problems.

Lesson 12

Identify original solutions and transfer risk where economic opportunities exist. Companies may use a combination of acceptance, transfer, and mitigation strategies. Also, companies may link risk management to employee incentives. This approach reinforces the importance of managing risk.

Lesson 13

View risk management from an enterprise-wide perspective. An enterprise-wide view permits the entity to identify inconsistencies in the level of risks management was taking and determine whether a small group of risks have a major influence. In addition, opportunities for savings may be identified.

Some steps for integrating risk management into the organization's processes are identified in Table 7.

Table 7: Steps for Integrating ERM

Step	**Action**	**Methods**
1	Determine all significant risks.	List risks, assess risks, map risks
2	Measure risk, and integrate best practices and tools	VAR, EAR, and stress testing
3	Conduct research throughout the organization	Search for • Inconsistencies • Natural offsets • Transfer/financing opportunities

Source: *Making Enterprise Risk Management Pay Off, How Leading Companies Implement Risk Management*, Thomas L. Barton, William G. Shenkir, and Paul L. Walker, © Prentice Hall 2002.

Lesson 14

Permit consultants to only supplement senior management involvement in the risk management effort. Consultants are used to provide information on how other companies manage specific risks and to provide data on incidents.

Lesson 15

ERM can offer more effective risk management than traditional approaches. Upon developing the proper strategy, ERM enables organizations to control their risks with greater efficiency than traditional approaches involving organizational "turf" issues.

Lesson 16

"Making risk consideration a part of the decision-making process is an essential element to enterprise-wide risk management." Companies link risk management and business strategy and use the Intranet to integrate risk management and everyday business management.

Lesson 17

Risk management infrastructures are important for ensuring that decision-makers consider risks. One approach is to use a committee structure to integrate risk management into operations. Other examples were discussed in Table 6.

Lesson 18

The commitment of champions at the senior management level is a prerequisite for implementing ERM. ERM succeeds when senior management commits to the program. Senior management commitment is critical because the integration process requires a balancing of various interests and skills.

A Model ERM Framework

To provide some insights into a viable ERM framework, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued a draft ERM framework. The COSO defines ERM as:

> … a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

In effect, ERM reflects certain fundamental concepts. Specifically, ERM:

- Is a process.
- Is effected by people.
- Is applied in a strategy setting.
- Is applied across the enterprise.
- Is designed to identify potential events and manage risk within a risk appetite.
- Provides reasonable assurance.
- Is geared to achieving objectives.

A discussion on each of these concepts is provided in Appendix III.

Components of the COSO ERM Framework

According to the COSO framework, ERM consists of eight interrelated components: internal environment, objective setting, event identification, risk assessment, risk response, control activities, information and communication, and monitoring. These components are derived from the way management runs a business and are integrated with the management process. The COSO draft ERM framework identifies the components as follows.

Internal Environment

The internal environment is the foundation for all other components and influences how a strategy and objectives are established. The board of directors is a critical component of the internal environment and influences other elements such as the entity's ethical values, competence and development of personnel, and management's operating style. Also, as part of the internal environment, management establishes a risk management philosophy and integrates risk management with related initiatives.

Objective Setting

Management establishes strategic objectives within the context of an established mission or vision and establishes related objectives. ERM provides assurance that management has a process to set objectives consistent with the entity's risk appetite and align the objectives with the entity's mission/vision.

Event Identification

Event identification involves considering external and internal factors that affect the occurrence of an event. External factors may include economic, business, natural environment, or political factors. Internal factors include issues such as infrastructure, personnel, process, and technology. Potential events may be grouped into categories to assist management in understanding their interrelationship. Risk is the possibility that an event will occur and adversely affect the achievement of objectives.

Risk Assessment

Risk assessment involves considering how potential events may impact the achievement of objectives, and the risk assessment methodology may involve a combination of qualitative and quantitative techniques. Some examples include benchmarking and conducting interviews and workshops. Determining the proper technique depends on factors such as the need for precision and the culture of the business unit.

Risk Response

ERM requires management to select a response that is expected to reduce risk to the entity's risk tolerance level. Risk responses include risk avoidance, reduction, sharing, and acceptance. The COSO draft ERM framework explains these terms as follows:

> Avoidance responses take action to exit the activities that give rise to the risks. Reduction responses reduce the risk likelihood, impact, or both. Sharing responses reduce risk likelihood or impact by transferring or otherwise sharing a portion of the risk. Acceptance responses take no action to affect likelihood or impact. As part of enterprise risk management, for each significant risk, an entity considers potential responses from a range of response categories. This gives sufficient depth to response selection and also challenges the "status quo."

Control Activities

Control activities occur throughout the organization and are the policies and procedures that assist management in ensuring that risk responses are properly executed. The policies establish what should be done, and the procedures effect the policy.

Information and Communication

Information from internal and external sources involves collecting information and communicating that data to personnel in a manner that enables them to conduct their responsibilities. Communication is effective when it flows down, across, and up the organization. Communication can also occur with external parties such as customers and suppliers.

Monitoring

Monitoring involves evaluating whether the ERM components are present and functioning. Monitoring also involves assessing the quality of components' performance over time. Management can implement a monitoring program through ongoing activities or separate evaluations. Both methods help ensure that ERM is applied at all levels and across the organization.

Assessing the Current State of Internal Control

Another area receiving increased attention as a result of the Sarbanes-Oxley Act is internal control over financial reporting. An emerging practice that is being used to evaluate the current state of an organization's internal control over financial reporting is the internal control maturity framework.

The primary objective of the internal control maturity framework is to determine whether existing or proposed controls for activities and processes adequately manage related risks and are documented to facilitate review. The hierarchy for categorizing the maturity levels of controls is provided in *The Sarbanes-Oxley Act of 2002, Strategies for Meeting New Internal Control Reporting Challenges: A White Paper,* PricewaterhouseCoopers, and is presented as follows.

<u>Level 1: Unreliable</u>

- Unpredictable environment in which controls are not designed or in place.

<u>Level 2: Informal</u>

- Controls are designed and in place but are not adequately documented.
- Controls are mostly dependent on people.
- No formal training program is in place.
- No formal training or communication of controls.

<u>Level 3: Standardized</u>

- Controls are designed and in place.
- Controls have been documented and communicated to employees.
- Deviations from controls may not be detected.

<u>Level 4: Monitored</u>

- Standardized controls with periodic testing for effective design and operation with reporting to management.
- Automation and tools may be used in a limited way to support controls.

Level 5: Optimized

- An integrated internal control framework has been established with real-time monitoring by management with continuous improvement (Enterprise-Wide Risk Management).
- Automation and tools are used to support controls and allow the organization to make rapid changes to the controls if needed.

The maturity framework can assist CFOs in evaluating whether the level of maturity for a given control area is satisfactory or whether additional action is needed.

SUMMARY

In light of the recent scandals that have caused the failure of several major corporations, reforms have been initiated by the Congress and regulatory organizations. Also, new strategies have been developed to respond to these reforms and the public demand for improved corporate governance and accountability. Federal agencies have the opportunity to develop sound corporate governance structures and lead by example. The FDIC is in a particularly unique position because it already has key governance components. The Corporation has an audit committee, ERM program, and independent auditors. The information in this report is intended to assist the Corporation in reviewing current practices and programs and determining the need for enhancements.

CORPORATION COMMENTS

A written response was not required for the report. OERM advised the OIG that it had no official comments.

APPENDIX I

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of our research was to provide information that may be used in evaluating approaches for enhancing some key elements of the corporate governance framework – the audit committee, risk management, and internal control over financial reporting. To achieve our objective, we searched the following for best practices and information related to our topic: the Internet, prior GAO reports, trade journals and magazines, private sector studies, pronouncements from authoritative sources, and other resources issued within the last 2 years with a particular focus on information pertaining to financial organizations. Also, we researched recent case studies and information on the challenges other organizations faced and the lessons they learned when implementing an ERM program. Our work was conducted from June to July 2004 in accordance with generally accepted government auditing standards.

APPENDIX II

AUDIT COMMITTEE SELF-EVALUATION TOOL

Adapted from *Audit Committees: Good Practices for Meeting Market Expectations*,
©PricewaterhouseCoopers, July 2003

Section No. of Charter	Audit Committee Practice	Practice Being Followed (Yes/No/N/A)	Action Item	
	Authority			
	Obtained board authority to perform activities within the audit committee's terms of reference.			
	Has access to members of management, employees, and relevant information, unless such access is restricted by law.			
	Has authority to establish procedures to deal with concerns of employees and complaints regarding accounting, internal control, and auditing matters.			
	Membership			
	The board periodically reviews the mix of experience and skills of committee members to maintain an appropriate balance.			
	Committee members are appointed by the board or a nominating committee of the board.			
	The size of the committee is appropriate to the organization.			
	The experience and qualifications of committee members are compatible with the duties of the committee, including the ability to understand financial statements. At least one of the members has accounting or related financial expertise.			
	Meetings			
	The committee meets regularly, with special meetings called as circumstances warrant. (At least three or four meetings each year are desirable.)			
	Meeting agendas and supporting papers are prepared and distributed sufficiently far enough in advance to enable committee members to prepare for meetings.			
	Minutes of meetings are circulated on a timely basis to members of the board and audit committee (and auditors where appropriate).			
	The chairman or another member of the committee attends the board meeting at which the financial statements are approved.			

APPENDIX II

Section No. of Charter	Audit Committee Practice	Practice Being Followed (Yes/No/N/A)	Action Item	
	Members of the committee attend every meeting.			
	The committee meets with in-house legal counsel on a regular basis.			
	New committee members are provided with sufficient background, information, and training to meet their responsibilities effectively.			
	The committee has adequate resources to discharge its responsibilities.			
	Internal Control			
	Evaluates the "control culture" established by management.			
	Understands the control systems implemented by management for approval of transactions, recording of data, and compliance of the financial statements with relevant standards and requirements.			
	Considers whether internal control recommendations made by auditors have been implemented by management.			
	Considers how management has reviewed the adequacy of controls surrounding electronic data processing and computer security.			
	Financial Reporting			
	Reviews the areas of greatest financial risk and management's actions to address those areas.			
	Reviews significant accounting and reporting issues and understands their likely impact on the financial statements.			
	Oversees the periodic financial reporting process and reviews the interim financial statements, annual financial statements, and preliminary announcements prior to their release.			
	Meets with management and external auditors to review the financial statements and results of the audit.			
	Ensures that significant adjustments, unadjusted differences, disagreements with management, and critical accounting policies have been discussed with external auditor.			
	Considers whether the narrative information included in the other sections of the annual report is			

APPENDIX II

Section No. of Charter	Audit Committee Practice	Practice Being Followed (Yes/No/N/A)	Action Item	
	understandable and consistent with the information in the financial statements.			
	Reads the representation letters given by management to the external auditors and considers any specific representations therein.			
	Compliance with Laws and Regulations			
	Reviews management's procedures for monitoring the organization's compliance with laws and regulations.			
	Reviews updates from management and legal counsel regarding compliance matters that may affect the financial statements.			
	Responsibilities Regarding Auditors			
	Discusses the auditors' proposed audit scope and approach.			
	Discusses any audit problems, including restrictions on the scope of the audit or denials of access to requested information.			
	Reviews reports made by the auditors to management, and ensures that management responds to these findings.			
	Meets privately with auditors on a regular basis.			
	Discusses the extent to which audit and accounting firms are used and understands the rationale for using them.			
	The Committee's Reporting Responsibilities			
	Reports committee activities to the board regularly.			
	Ensures that any reports required by law concerning committee activities have been prepared.			
	Evaluating Performance			
	Periodically assesses the performance of individual members and the committee as a whole.			
	Assesses the achievement of the duties specified in the charter and reports to the board.			
	Charter			
	Reviews the committee charter annually, and discusses any proposed changes with the board.			

APPENDIX II

Section No. of Charter	Audit Committee Practice	Practice Being Followed (Yes/No/N/A)	Action Item	
	Ensures the charter is approved/reapproved by the board.			

APPENDIX III

EXCERPT FROM COSO EXPOSURE DRAFT: *ENTERPRISE RISK MANAGEMENT FRAMEWORK*

A Process

Enterprise risk management is not one event or circumstance, but a series of actions that permeate an entity's activities. These actions are pervasive and inherent in the way management runs the business.

Enterprise risk management is different from the perspective of some observers who view it as something added on to an entity's activities, or as a necessary burden. That is not to say effective enterprise risk management does not require incremental effort. For instance, risk assessment may require incremental effort to develop needed models and make necessary analysis and calculations. However, these and other enterprise risk management mechanisms are intertwined with an entity's operating activities and exist for fundamental business reasons. Enterprise risk management is most effective when these mechanisms are built into the entity's infrastructure and are part of the essence of the enterprise. By building in enterprise risk management, an entity can directly affect its ability to implement its strategy and achieve its vision or mission.

Building in enterprise risk management also has important implications for cost containment, especially in the highly competitive marketplaces many companies face. Adding new procedures separate from existing ones adds costs. By focusing on existing operations and their contribution to effective enterprise risk management, and integrating risk management into basic operating activities, an enterprise can avoid unnecessary procedures and costs. And a practice of building enterprise risk management into the fabric of operations helps identify new opportunities for management to seize in growing the business.

Effected by People

Enterprise risk management is effected by a board of directors, management and other personnel. It is accomplished by the people of an organization, by what they do and say. People establish the entity's mission/vision, strategy and objectives and put enterprise risk management mechanisms in place.

Similarly, enterprise risk management affects people's actions. Enterprise risk management recognizes that people do not always understand, communicate or perform consistently. Each individual brings to the workplace a unique background and technical ability, and has different needs and priorities.

These realities affect, and are affected by, enterprise risk management. Each person has a unique point of reference which influences how they identify, assess and respond to risk. Enterprise risk management provides the mechanisms needed to help people understand risk in the context of the entity’s objectives. People must know their responsibilities and limits of authority. Accordingly, a clear and close linkage needs to exist between people's duties and the way in which they are carried out, as well as with the entity's strategy and objectives.

An organization's people include the board of directors, as well as management and other personnel. Although directors primarily provide oversight, they also provide direction and approve strategy and certain transactions and policies. As such, boards of directors are an important element of enterprise risk management.

Applied in Setting Strategy

An entity sets out its mission or vision and establishes strategic objectives, which are the high-level goals that align with and support its vision or mission. An entity establishes a strategy for achieving its strategic objectives. It also sets related objectives it wants to achieve, flowing from the strategy, cascading to business units, divisions and processes. In setting strategy, management considers risks relative to alternative strategies.

Applied Across the Enterprise

To successfully apply enterprise risk management, an entity must consider its entire scope of activities. Enterprise risk management considers activities at all levels of the organization, from enterprise-level activities such as strategic planning and resource allocation, to business unit activities such as marketing and human resources, to business processes such as production and new customer credit review. Enterprise risk management also applies to special projects and new initiatives that might not yet have a designated place in the entity's hierarchy or organization chart.

Enterprise risk management requires an entity to take a *portfolio view* of risk. This might involve each manager responsible for a business unit, function, process or other activity developing an assessment of risk for the unit. The assessment may be quantitative or qualitative. With a composite view at each succeeding level of the organization, senior management is positioned to make a determination whether the entity's overall risk profile is commensurate with its risk appetite.

Management considers interrelated risks from an entity-level portfolio perspective. Interrelated risks need to be identified and acted upon to bring the entirety of risk within the entity's risk appetite. Risks for individual units of the entity may be within the units' risk tolerances, but taken together may exceed the risk appetite of the entity as a whole. The overall risk appetite is reflected downstream in an entity through risk tolerances established for specific objectives.

Risk Appetite

Risk appetite is the amount of risk an entity is willing to accept in pursuit of value. Entities often consider risk appetite qualitatively, with such categories as high, moderate or low, or they may take a quantitative approach, reflecting and balancing goals for growth, return and risk.

Risk appetite is directly related to an entity’s strategy. It is considered in strategy setting, where the desired return from a strategy should be aligned with the entity’s risk appetite. Different strategies will expose the entity to different risks. Enterprise risk management, applied in a strategy setting, helps management select a strategy consistent with the entity’s risk appetite.

The entity’s risk appetite guides resource allocation. Management allocates resources across business units with consideration of the entity’s risk appetite and individual business unit’s strategy for generating a desired return on invested resources. Management considers its risk appetite as it aligns its organization, people and processes, and designs infrastructure necessary to effectively respond to and monitor risks.

Risk tolerances are the acceptable level of variation relative to the achievement of objectives. In setting specific risk tolerances, management considers the relative importance of the related objectives and aligns risk tolerances with its risk appetite. Operating within risk tolerances provides management greater assurance that the entity will remain within its risk appetite and, in turn, provides a higher degree of comfort that the entity will achieve its objectives.

Provides Reasonable Assurance

Well-designed and operated enterprise risk management can provide management and the board of directors reasonable assurance regarding achievement of an entity's objectives. As a result of enterprise risk management determined to be effective, in each of the categories of entity objectives, the board of directors and management gain reasonable assurance that:

- They understand the extent to which the entity’s strategic objectives are being achieved,
- They understand the extent to which the entity's operations objectives are being achieved,
- The entity’s reporting is reliable, and
- Applicable laws and regulations are being complied with.

Reasonable assurance reflects the notion that uncertainty and risk relate to the future, which no one can predict with certainty. Limitations also result from the realities that human judgment in decision making can be faulty, decisions on risk responses and establishing controls need to consider the relative costs and benefits, breakdowns can occur because of human failures such as simple errors or mistakes, controls can be circumvented by collusion of two or more people, and management has the ability to override enterprise risk management decisions. These limitations preclude a board and management from having absolute assurance that objectives will be achieved.

Achievement of Objectives

Effective enterprise risk management can be expected to provide reasonable assurance of achieving objectives relating to the reliability of reporting and to compliance with laws and regulations. Achievement of those categories of objectives is within the entity’s control and depends on how well the entity’s related activities are performed.

However, achievement of strategic and operations objectives is not always within the entity's control. For these objectives, enterprise risk management can provide reasonable assurance only that management and the board, in its oversight role, are made aware, in a timely manner, of the extent to which the entity is moving toward achievement of the objectives.