Top Ten ‘Next’ Practices for Enterprise Risk Management

2010 AICPA Survey Results

Presented by the AICPA’s Business, Industry & Government Team
# Table of Contents

- The Case for ERM ................................................................. 2
- Methodology ........................................................................ 6
- Resources ........................................................................... 7
- AICPA Products .................................................................. 7
- AICPA Briefs ...................................................................... 8
- AICPA Management Accounting Guidelines (MAGs) ............... 9
- COSO Resources .................................................................. 10
In late 2010, the American Institute of CPAs (AICPA) conducted a survey of the Top Ten “Next” Practices for Enterprise Risk Management (ERM). The survey results represent the CPA’s unique perspective regarding the ERM practices they believe will significantly influence the management and value of the business in the coming year. This survey report and resource guide was prepared under the direction of the AICPA Risk Management and Internal Control Advisory Panel.

“Best’ practices asks what is working, while ‘next’ practices asks what could work more powerfully.”

— C.K. Prahalad, Professor of Corporate Strategy, the University of Michigan
The Case for ERM

According to a joint research report, Enterprise risk oversight: A global analysis, published by the AICPA and the Chartered Institute of Management Accountants (CIMA), ERM practices are “immature” in most organizations. At one end of the ERM development spectrum, organizations manage the risks within functional silos with very little communication of overall risks to the organization and its strategy. At the other end of the spectrum, ERM is integrated into the management process and is an ongoing process. The report indicates that executives want to have a better handle on risk management within their organizations, but are stymied by the process of implementing an ERM program.

Given the rate of change in today’s environment, organizations need to use ERM to guide the decision-making process and challenge the assumptions that are being made internally based upon external forces and market data. Emerging risks or unknown, unknowable risks can catch a company by surprise. In addition, organizations must find practices that will hasten their ERM maturity so they can answer questions such as “why didn’t we see this coming earlier?” and take advantage of opportunities in the marketplace and/or reduce losses.

CPAs have a significant opportunity to contribute to the development of ERM programs in their organizations, and can use insights gleaned from their colleagues’ responses to the AICPA’s Top Ten “Next” Practices for Enterprise Risk Management as a benchmark for their own organizations’ progress in implementing ERM.

The 2010 survey results can help CPAs adopt innovative methods and processes to manage risk, educate management and staff about the importance of integrating ERM practices into day-to-day activities, bring change and provide opportunities for value creation within their organizations.

Top Ten ’Next’ Practices at a glance

1. Establish the right monitoring processes to make sure risk mitigation activities operate as designed.
2. Regularly track and monitor the risks facing the organization both internally and externally.
3. Communicate regularly, thoroughly, top to bottom, bottom to top and across the organization.
4. Encourage open discussions of “what keeps people awake at night.”
5. Ensure board of director and executive level support for ERM is communicated throughout the organization.
6. Use key risk indicators that are leading indicators.
7. Establish a risk management policy.
8. Understand and assess risk as it relates to the organization’s objectives.
9. Incorporate ERM into the strategic planning process.
10. Use ERM to guide the behavior and thought process of decision-makers.
The Top Ten ‘Next’ Practices

The Top Ten “Next” Practices are based upon survey results from AICPA members in business and industry (for more information about the survey methodology, see page 6). We asked members to rank — in order of their importance to their companies — items on a list of ERM “next” practices. Here, we have listed the “next” practices in the order in which respondents ranked them.

1 Establish the right monitoring processes to make sure risk mitigation activities operate as designed.
According to the Committee of Sponsoring Organization’s (COSO) Enterprise Risk Management — Integrated Framework, management can choose ongoing activities to monitor risk, conduct separate evaluations or take on a combination of both processes in order to determine the effectiveness of risk mitigation activities. Respondents indicated that this is the No. 1 ERM trend for the coming year, showing they recognize that putting the right process into place can help make ERM activities a part of the fabric of everyday tasks throughout the organization.

2 Regularly track and monitor the risks facing the organization both internally and externally.
In order to assess, plan for and adjust to all risks, respondents are seeing the need for their organizations to consider both internal and external forces as they implement the tracking and monitoring system that works best for them. For example, an organization may become focused on the external circumstances that may present challenges or opportunities for growth, but what about internal forces? For example, a rebounding economy may spark a boon for business, but it also may lead to staff turnover.

3 Communicate regularly, thoroughly, top to bottom, bottom to top and across the organization.
Keeping clear and frequent communication ensures that the key risks identified and monitored across all internal teams are relevant and that any emerging risks are identified, assessed and responded to appropriately. Survey respondents understand that, in order for their organizations to achieve their objectives, all functional areas from all lines of business need to be involved in the communication process. In addition, senior management must keep the board up-to-date on risks facing the organization, so the board may be effective in carrying out its oversight responsibilities.

4 Encourage open discussions of “what keeps people awake at night.”
Part of the communication process is listening to and understanding the input of staff and management regarding risk. Organizations with a communicative and transparent culture allow — or even require — staff members, who are closer to organizational operations and may provide insight on risks threatening the organization, to contribute to the risk dialog. CPAs can play a role in these discussions by encouraging openness from multiple levels and acknowledging that, without candid conversations about risk, the organization could jeopardize meeting its objectives.

COSO’s definition of ERM is “a process affected 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 risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”
Ensure board of director and executive level support for ERM is communicated throughout the organization.

ERM is not a compliance program; it’s a method for managing business and must be integrated into an organization’s culture in order for it to be most effective. The support of ERM by the board of directors and senior management is critical to ensure adequate resources and attention are focused on risk management. The board of directors and senior management set the “tone from the top” and must communicate the importance of risk awareness across the organization. Having identified this emerging next practice for the coming year, CPAs may point senior leadership to various AICPA resources to help them in the communications process. See the resources section (page 7) of this report for more information.

Use key risk indicators that are leading indicators.

Establishing key risk indicators (KRIs) to identify risks that threaten achievement of an organization’s business strategy and objectives requires all stakeholders to have an in-depth understanding of organizational strategy and objectives. The next practice of utilizing KRIs is not to be confused with using key performance indicators (KPIs). KRIs, such as the analysis of customers’ financial results, signaling potential and late payments, are metrics used to provide an early signal of increasing risk exposure or about emerging events that may lead to risks or opportunities. KPIs provide information on historical performance of the organization (for example, write-offs of the year’s accounts receivable).

Establish a risk management policy.

As indicated in the Enterprise risk oversight: A global analysis survey report, organizations are at various stages of implementing ERM, so it comes as no surprise that creating a risk management policy would make the list of ERM next practices. A written risk policy serves as the basis for procedures for implementing ERM and communicating the organization’s risk appetite and tolerance. It also serves to define roles and responsibilities for risk assessment processes.
8 Understand and assess risk as it relates to the organization’s objectives.
One of the many benefits of an ERM culture is that it creates a common risk language. All staff members are aligned with ensuring the achievement of organizational goals and objectives and understand how the organization’s risk appetite and tolerance fit into meeting those goals and objectives. Survey respondents see the important role CPAs can play in participating in this next practice in the coming year. CPAs can assist in instituting risk language within the organization by highlighting the link between meeting organizational goals and objectives, and assessing risk.

9 Incorporate ERM into the strategic planning process.
When risk management is embedded into the strategy development and execution process, it should be seamless, so the organization can take advantage of opportunities and take risks within their risk appetite and tolerance. As with next practice No. 8, CPAs play an important role in helping to ensure that ERM processes and practices are woven into the strategic planning process. They become champions of ERM’s strategic relevance at their organizations and help senior management and staff understand the need to integrate risk into strategic planning.

10 Use ERM to guide the behavior and thought process of decision-makers.
The organization’s risk management policy and culture need to be aligned, and its culture needs to support the ERM process. When ERM is embedded into the culture, all employees use it in decision-making; ERM drives awareness and action through a new lens in achieving the organization’s goals and objectives.
The Top Ten “Next” Practices for Enterprise Risk Management survey was conducted through an online survey instrument sent electronically to the AICPA’s business and industry members who served in chief financial officer or equivalent senior executive positions between Nov. 22, 2010, and Dec. 19, 2010. In total, we received 274 responses.

### Methodology

**Respondent Organizations Annual Revenue**

<table>
<thead>
<tr>
<th>Annual Revenue</th>
<th>% of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Under $10 Million</td>
<td>21.0</td>
</tr>
<tr>
<td>$10 Million to $49 Million</td>
<td>26.0</td>
</tr>
<tr>
<td>$50 Million to $249 Million</td>
<td>20.0</td>
</tr>
<tr>
<td>$250 Million to $1 Billion</td>
<td>14.0</td>
</tr>
<tr>
<td>Over $1 Billion</td>
<td>19.0</td>
</tr>
</tbody>
</table>

**Respondent Industry Representation**

<table>
<thead>
<tr>
<th>Industry</th>
<th>% of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial/Banking/Accounting/Insurance</td>
<td>25.0</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>15.0</td>
</tr>
<tr>
<td>Health care/Medicine/Pharmaceutical</td>
<td>10.0</td>
</tr>
<tr>
<td>Real Estate</td>
<td>6.0</td>
</tr>
<tr>
<td>Retail/Wholesale/Distribution</td>
<td>6.0</td>
</tr>
<tr>
<td>Energy/Utilities/Electricity/Gas/Water</td>
<td>5.0</td>
</tr>
<tr>
<td>Engineering/Construction/Architecture</td>
<td>5.0</td>
</tr>
<tr>
<td>Consulting/Auditing</td>
<td>3.0</td>
</tr>
<tr>
<td>Hospitality/Entertainment/Travel</td>
<td>3.0</td>
</tr>
<tr>
<td>Education</td>
<td>2.0</td>
</tr>
<tr>
<td>High-technology/Computer hardware/software</td>
<td>2.0</td>
</tr>
<tr>
<td>Information Technology/Computer services</td>
<td>2.0</td>
</tr>
<tr>
<td>Media/Publishing</td>
<td>2.0</td>
</tr>
<tr>
<td>Telecommunications</td>
<td>2.0</td>
</tr>
<tr>
<td>Transportation/Automotive</td>
<td>1.0</td>
</tr>
<tr>
<td>Other</td>
<td>11.0</td>
</tr>
</tbody>
</table>
The AICPA and CIMA joint research report *Enterprise risk oversight: A global analysis* demonstrates that respondents’ organizations are in various stages of implementing ERM. In the Top Ten “Next” Practices for Enterprise Risk Management survey, we asked respondents: “What enterprise risk practices, if any, are proving most challenging for your company to implement?” Several themes emerged:

- Gaining support from senior executive and/or board
- Investing in ERM process not seen as priority or valuable
- Communicating risks between functional silos/business units and at an enterprise level
- Defining and establishing risk tolerance and appetite
- Monitoring/tracking risks (internal and external) and mitigation plans

These responses point to the increasing need to educate stakeholders about the need for ERM implementation. The AICPA has numerous resources to help members learn more about ERM and share with their senior management and staff. In addition, COSO has several important resources for CPAs.

**Resources**

- **Case Studies on ERM Implementations: Practical Illustrations for Launching Effective Enterprise Risk Oversight**
  This collection of case studies includes the real-world scenario of a company just starting an ERM program. It follows the organization through its implementation process and touches on working with the board, senior management and the management team as the organization works to identify and rate significant risk categories. Other case studies describe cases that will further enhance your understanding of ERM implementation.

  For the CPA or CFO who is familiar with the COSO Integrated Framework, Risk Assessment for Mid-Sized Companies transforms those standards into actionable ERM processes.

- **Smart Risk Management: A Guide to Identifying and Reducing Everyday Business Risks**
  Any decision-maker who recognizes that too much effort in controlling risks hurts innovation and not enough control is wasteful and expensive, will want to read this publication.

**AICPA Products**

The AICPA wants to help CPAs play a bigger role in driving ERM implementation within their organizations and has several publications and conferences that can help CPAs learn more about how their peers handle implementation, how organizations can benefit from the enterprise-wide approach to risk and how regular monitoring of risks helps organizations prepare for challenges and take advantage of opportunities.

**You can find the AICPA’s ERM resources online at aicpa.org/ERM**
AICPA Briefs

The AICPA publishes Business, Government Accountability and Audit Committee Briefs, periodic articles with practical guidance for CPAs on a number of topics. Briefs are easily accessible at AICPA.org.

**Board and Audit Committee Involvement in Risk Management Oversight**
This brief describes the role of the board and audit committees in ERM to develop a stronger top-down, holistic view of enterprise-wide risks.

**Adding Value, Not Bureaucracy: Linking Governance, Enterprise Risk Management and Internal Controls**
This brief provides a foundation for the connection between governance, ERM and internal control.

**Effective Enterprise Risk Management Starts With a Conversation**
Read “lessons learned,” success stories and guidance from organizations on the front lines of ERM implementation.

**S&P’s ERM Reviews for Non-Financial Issuers — Where Do We Stand?**
Read a summary of the Standard & Poor’s progress report, issued July 22, 2009, which discloses findings to date and specific ERM analyses within its corporate credit ratings reports.

**The Link Between Decision-Making and ERM: A Case Study**
This business brief focuses on integrating ERM within organizational strategy and incorporating it into an organization’s core activities.

**Enterprise Risk Management: Meeting Today’s Challenges**
Read an excerpt from the Report on The Current State of Enterprise Risk Oversight, research conducted on behalf of the AICPA by faculty who lead the ERM Initiative in the Poole College of Management at North Carolina State University. It provides a framework for developing the right risk culture and summarizes drivers of risks.

**The Basics of Fraud Risk Management**
Read an excerpt from the Chartered Institute of Management Accountants (CIMA) publication: Fraud Risk Management: A Guide to Good Practice © CIMA 2008. This brief provides a definition of fraud and an anti-fraud strategy containing four main components: prevention, detection, deterrence and response.

**The Perils and Promises of Integrated Enterprise Risk and Performance Management**
This brief is for businesses interested in ERM and enterprise performance management. It discusses the opportunities and consequences related to implementing an enterprise risk and performance management framework.

**Enterprise Risk Management: Is It Relevant to Government?**
This brief provides an overview of ERM and its importance to government entities.

**Increasing Risk Awareness for Mission Critical Objectives of Not-for-Profit Organizations**
Much of the current risk dialogue has been discussed in the for-profit realm, however ERM is relevant to not-for-profits as well, especially in light of the impact the tough economy is having on donations, endowments and grants. This brief covers the relevance of risk oversight to not-for-profits, developing an enterprise risk awareness view and focusing on emerging strategic risks.
AICPA Management Accounting Guidelines (MAGs)

The AICPA's Management Accounting Guidelines (MAGs) publications provide practical guidance to CEOs; CFOs; senior management teams; boards of directors; members of audit committees; and accounting, internal audit and finance professionals on a number of issues, including risk assessment, analysis, control and reporting. MAGs are available on AICPA.org and require member login to access.

Scenario Planning: Plotting a Course Through an Uncertain World
Scenario planning is a management tool designed to allow organizations to evaluate strategies, tactics and plans based on a range of possible future environments.

Financial Risk Management for Management Accountants
This MAG summarizes the basic principles of financial risk management and focuses on the interlinked issues of risk assessment and possible control tools.

Managing Opportunities and Risks
There are a multitude of opportunities created by organizational risks. This MAG provides insight into the positive aspects of risk and champions the risk management process as a way to exploit opportunities and drive new organizational innovation.

Integrating Social and Political Risk into Business Decision-Making
A follow-up to the Identifying, Measuring, and Managing Organizational Risk for Improved Performance MAG, this publication provides the tools, techniques and specificity needed to aid managers to more effectively integrate social and political risks into their decision-making processes.

The Reporting of Organizational Risks for Internal and External Decision-Making
Internal and external decision-makers need a clear understanding of the risks and fair disclosure within an organization. This MAG provides guidance for the reporting of these risks.

Identifying, Measuring and Managing Organizational Risks for Improved Performance
A Risk Management Payoff Model includes a selection of performance measures to properly identify, measure, manage and report risks. The model demonstrates that improved risk measurement and management helps the organization prevent loss, achieve performance and profitability targets and increase shareholder value.
COSO Resources

The Committee of Sponsoring Organizations (COSO) is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on ERM, internal control and fraud deterrence. COSO’s supporting organizations are the Institute of Internal Auditors (IIA), the American Accounting Association (AAA), the AICPA, Financial Executives International (FEI) and the The Association for Accountants and Financial Professionals in Business (IMA®). You can find out more about COSO by visiting coso.org.

Effective Enterprise Risk Oversight: The Role of the Board of Directors
This thought paper is aimed at helping boards of directors strengthen their oversight of enterprise risk and emphasizes the critical role boards of directors play in overseeing ERM.

Strengthening Enterprise Risk Management for Strategic Advantage
Senior management can work with its board of directors to enhance the board’s risk oversight capabilities and the organization’s strategic value. This publication highlights senior management’s role and details on how it can work with the board and others in the organization to strengthen risk management in all types of organizations.

Embracing Enterprise Risk Management: Practical Approaches for Getting Started
Find out how an organization can begin implementing and executing an ERM process. Read about perceived barriers to effective ERM and how to work through those barriers.

Developing Key Risk Indicators to Strengthen Enterprise Risk Management
This thought paper discusses the importance of developing key risk indicators to be used to monitor emerging risks that might affect the strategic success of the enterprise.