Comprising the professional associations listed above, the Committee of Sponsoring Organizations (COSO) is a voluntary private-sector organization. COSO is dedicated to guiding executive management and governance entities toward the establishment of more effective, efficient, and ethical business operations on a global basis. It sponsors and disseminates frameworks and guidance based on in-depth research, analysis, and best practices.

FAQs for COSO's Enterprise Risk Management — Integrated Framework

A. What is the framework and how do I get it?

1. What is in the framework?
The framework describes the critical principles and components of an effective enterprise risk management process, setting forth how all important risks should be identified, assessed, responded to and controlled. It also provides a common language, so that when executives, directors and others talk about risk management, they are truly communicating.

The framework sets forth how a company applies enterprise risk management in its strategic planning and also describes techniques some companies are using in identifying and managing risk. Importantly, the framework emphasizes how an effective enterprise risk management process identifies not only the downside, but also the upside, or opportunities that can be seized to enhance profitability and return. The framework also describes roles of key players in the enterprise risk management process.

2. Where can I find the framework?
An executive summary of the Framework is posted in .pdf format on www.coso.org. There, you will also be able to place an order for either a hard copy or electronic copy of the two-volume set that includes the executive summary as well as the Enterprise Risk Management – Integrated Framework and associated Application Techniques. The same charge ($75 or $50 for members of COSO organizations) applies to both hard and soft copy

B. Why is this a framework that organizations should support?

1. What limitations of existing enterprise risk management models prompted creation of a new framework?
There have been a wide variety of frameworks utilized across companies and across countries. Some of these focus narrowly on risk management (rather than enterprise risk management). Others focus on specific industries or specific types of risk. In addition, many of these focus on mechanisms for reducing — rather than managing — risk. By contrast, the COSO Enterprise Risk Management – Integrated Framework addresses enterprise risk management applicable to all industries and encompassing all types of risk. Moreover, the framework recognizes that an effective enterprise risk management

process must be applied within the context of strategy setting. This is a fundamental difference from most risk models used to date. It starts with the top of the organization and supports an organization's major mission.

In addition, many of the pre-existing frameworks stood by themselves, and thus tended to be implemented within functions. As a result, many risk management practices have been implemented in silos (i.e., in one part or one function, of the organization). Consequently, risk management may be done very well in one section, but not consider how actions of other parts of the organization affect their risks, or it might not capture the overall significant risks that the organization faces. The Enterprise Risk Management – Integrated Framework presents an enterprise-wide perspective of risk and standardizes terms and concepts to promote effective implementation across the organization.

2. How might the framework assist organizations in structuring their entities to best manage exposure to risk?
By formally organizing risk management responsibilities and activities an organization is much better positioned to achieve its objectives. To achieve its business objectives, management will want to ensure that sound risk management processes are in place and functioning. Board and audit committees have an oversight role to determine that appropriate risk management processes are in place and that these processes are adequate and effective. The COSO Enterprise Risk Management – Integrated Framework provides comprehensive guidance on each of these points and includes numerous examples of approaches used by risk management practitioners in a diverse group of organizations.

3. Is there such a thing as being overly conscientious about risk?
The purpose of an entity is to provide goods and services that people value. The pursuit of that goal is paramount in most organizations. An organization that focuses more on risk management than on pursing its primary goals is likely to under perform.

C. What are some of the key concepts established in this framework?

1. What is the difference between risk appetite and risk tolerance?
Both risk appetite and risk tolerance set boundaries of how much risk an entity is prepared to accept. Risk appetite is a higher level statement that considers broadly the levels of risks that management deems acceptable while risk tolerances are more narrow and set the acceptable level of variation around objectives. For instance, a company that says that it is does not accept risks that could result in a significant loss of its revenue base is expressing appetite. When the same company says that it does not wish to accept risks that would cause revenue from its top-10 customers to decline by more than 10% it is expressing tolerance. Operating within risk tolerances provides management greater assurance that the company remains within its risk appetite, which, in turn, provides a higher degree of comfort that the company will achieve its objectives.

2. How does an organization determine the right amount of risk for the value it is trying to create for stakeholders and how should it communicate its risk policy to stakeholders?

The level of risk that an entity is willing to accept is a management decision – and there is no right answer to this question. One company's management will pursue a higher-risk strategy while another will pursue a lower risk strategy. The shareholder should understand the risk chosen by management and invest in accordance with his/her own tolerances for potential variation in stock performance. Organizations communicate the levels of risk accepted through the MDA, quarterly and annual reports, press releases, investor calls, etc.

3. What is the relationship between effective enterprise risk management and improved financial reporting and transparency?
There are natural linkages between enterprise risk management, improved financial reporting and transparency. The Enterprise Risk Management – Integrated Framework requires that organizations establish a risk appetite, measure actions and decisions against that risk appetite and communicate results. Communication of enterprise risk management to users of financial information clearly enhances transparency.

4. Is this intended for private organizations? Is there any organization this is not intended for?
Enterprise risk management is a process that companies of all sizes and degrees of sophistication should consider. The framework is scalable, enabling companies to be able to match the process to the company's complexity and sophistication. There is an intrinsic expectation that all organizations be they for profit, not-for-profit, government organizations, etc, each work to manage risk. The Enterprise Risk Management – Integrated Framework will facilitate the process.

D. How does this framework relate to COSO's Internal Control Framework?

1. Are you replacing the Internal Control Framework with the Enterprise Risk Management Framework?
The Internal Control – Integrated Framework is conceptually sound and has stood the test of time. The Enterprise Risk Management – Integrated Framework is a broader framework that incorporates the internal control framework within it. In other words, one approach to risk is to develop controls to mitigate the risks. The frameworks are compatible and are based on the same conceptual foundation. We believe the consistent conceptual underpinnings are a major strength of the two models. Appendix C of the Enterprise Risk Management – Integrated Framework provides a detailed discussion of the relationship to Internal Control – Integrated Framework.

2. What is the relationship between technology controls and effective enterprise risk management?
The Enterprise Risk Management – Integrated Framework requires feedback of information from throughout the company. This information must be current and accurate and must be robust enough to support the analysis of different risk responses. Therefore, the technology that provides this data must have the highest levels of integrity and controls. Enterprise risk management cannot be effective if the technology that provides the data used to manage risk is flawed. Controls related to

technology, also referred to as general computer controls, were also discussed in the Internal Control – Integrated Framework.

3. If you have good internal control, isn't that a way of managing risk?
A strong system of internal control supports the achievement of the organization's business objectives and therefore good internal control is a way of managing risk. However, enterprise risk management is much broader than internal control. In addition to supporting management's efforts to achieve business objectives, it aligns risk management with strategy setting and aids a company's ability to assess whether the organization is accepting risk appropriately.

4. What does the new framework offer clients that are focusing on internal control?
Companies that want to move beyond internal control and get more out of their efforts, now have a framework that will help them go to the next level. As the Enterprise Risk Management – Integrated Framework includes the concepts and components initially developed in the Internal Control – Integrated Framework, expanding their practices to incorporate risk management will be more evolutionary and not require that they "throw away" all of the previous efforts. The Enterprise Risk Management – Integrated Framework details, for the first time, the link between value, risk, strategy, objective setting, performance measurement, risk response and control processes.

E. How might organizations view the framework in the context of their Sarbanes-Oxley 404 compliance process?

1. With the significant amount of implementation efforts companies are currently undertaking for Sarbanes-Oxley compliance and adoption of new accounting standards, why should companies be motivated to implement enterprise risk management?
The implementation of COSO's Enterprise Risk Management – Integrated Framework will provide long term benefits to an organization and therefore should be viewed with a longer term implementation perspective. The current emphasis on control in Sarbanes-Oxley is primarily focused on financial reporting. However, there are additional aspects of risk management that go beyond internal controls and are rooted in the strategy setting activities of a company and in the management analysis of risk appetite and risk tolerance necessary to pursue its objectives as a company.

Not all companies are at the same level of expertise or knowledge of risk management techniques and approaches vary widely. Continued adoption of the Enterprise Risk Management Framework by both companies and academics will result in a more consistent approach to risk management as companies strive to create value for stakeholders.

2. What makes this different from the internal control framework? How does it relate to Sarbanes-Oxley reporting?
The Enterprise Risk Management – Integrated Framework is broader than internal control, and actually incorporates the key concepts set out in COSO's earlier Internal

Control – Integrated Framework. While there are several differences, the three points that are probably the most prominent are that risk management considers risks during strategy setting, requires management to form a view of how much risk the organizations is prepared to accept – known as risk appetite – and requires that risk management be done outside of silos through a portfolio view of the organization's risks.

Much of the internal control focus today is on only one aspect of internal control – internal controls over financial reporting for Sarbanes-Oxley 404. This is distinct from reporting on risk management.

F. How do people in an organization intersect with this framework?

1. What is the role of the board in enterprise risk management? How does this framework help them?
The Board provides oversight of enterprise risk management. They will be asked to understand key elements of enterprise risk management, inquire of management about risks, and concur on certain management decisions. However, the board is not in the position of making choices on behalf of management and does not alleviate managements role in enterprise risk management.

2. What is the role of the CFO and others in the financial management organization in enterprise risk management? How will this framework help them?
The CFO and the financial organization play a key role in providing the needed disciplines and procedures to establish risk management as an integral part of the business strategy setting process. The CFO provides the organization with analytical tools to help determine risk appetite and risk tolerance. The CFO is well positioned to look across the businesses and functions within a company to develop and implement the portfolio view of risk. He/she has the experience and knowledge to establish controls necessary to assure that the evaluation of risk is a continuing and integral part of the management process and is consistent with the risk management philosophy agreed to with the board.

3. What is the role of internal auditors in enterprise risk management? How will this framework help them?
Board and audit committees have an oversight role to determine that appropriate risk management processes are in place and that these processes are adequate and effective. Internal auditors can assist both management and the audit committee by examining, evaluating, reporting, and recommending improvements on the adequacy and effectiveness of management’s risk management processes. The COSO Enterprise Risk Management – Integrated Framework provides a benchmark for internal auditors to use in the evaluation of their organization’s risk management efforts.

4. Who are the potential implementers of the framework?
The framework is robust. It works best when an organization develops an integrated process to address risk throughout the organization, and further, that risk approach is led from the top of the organization. The framework can be used in all functional areas,

including information technology, finance, accounting, internal audit and risk specialists within any organization. However, the framework is designed to promote entity-wide capabilities for identifying, documenting, and dealing with risk on a consistent basis. Chapter 10 of the Enterprise Risk Management Framework – Integrated Framework addresses roles and responsibilities in detail.