The Hong Kong stock exchange concluded the consultation paper on risk management and internal control and amended the Corporate Governance Code, which becomes effective for accounting periods beginning on or after 1 January 2016. HKEx emphasized that internal control is an integrated part of risk management and the internal audit function plays an important role in ensuring the effectiveness of a listed company’s risk management and internal control systems. Although risk management is not a new idea to professional accountants, what exactly should internal auditors do to address these changes and create values for its organization?

Enterprise risk management
Organizations face uncertainties, which emanate from the inability to determine the likelihood of an event and the associated impacts. Uncertainties, which can be further classified as risk and opportunity, may erode or enhance value. Enterprise risk management allows management to effectively deal with uncertainties and eventually enhance the organizations’ capacity to build value. ERM is defined as follows by the Committee of Sponsoring Organizations of the Treadway Commission: “ERM is 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 risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

The role of internal auditors in enterprise risk management
Roy Lo looks at how internal auditing can create value for organizations amid changing reporting requirements.

According the ERM Framework issued by COSO, ERM assists an organization to align risk appetite and strategy, and to enhance risk-response decisions. It also helps to reduce operational surprises and losses, providing integrated responses to multiple risks. Eventually, it may allow management to seize opportunities and improve deployment of capital.

Responsibilities of the board and management
Responsibilities of the board and management on ERM are clearly stated in the international frameworks (such as the ERM Framework) and the Corporate Governance Code.

Generally, the board should oversee the ERM by:
• Knowing the extent of ERM within the organization;
• Reviewing the risk portfolio of the organization and considering it against the risk appetite;
• Understanding the changes and significant risks the organization is facing; and
• Considering whether the risk responses are appropriate or not.

Management, on the other hand, is directly responsible for the ERM. They are responsible for the design, implementation and monitoring of it. There is no rigid definition of management, but it normally includes the chief executive officer (who has ultimate ownership responsibility for the ERM), chief financial officer (who has responsibility in handling financial reporting risks and compliance risks) and chief operating officer (who is responsible for handling operation risks).

Role of an internal auditor
Due to the new demands from the board and management, the role of an internal auditor shifts from a control-focus advisor, to a consultant who creates value by supporting the organization’s objectives, monitoring enterprise risks and ensuring the effectiveness of the internal control framework. Internal auditors should consider whether the upcoming activities will affect their independence and objectivity or not.

Core internal audit roles in regard to ERM
The Institute of Internal Auditors states that “Internal auditing has a core role with regard to ERM, which is to provide objective assurance to the board on the effectiveness of risk management.” The IIA Position Paper: The Role of Internal Auditing in Enterprise-wide Risk Management suggests that internal auditors can provide the following assurance activities:
• Giving an assurance on the risk management processes;
• Giving an assurance that risks are correctly evaluated;
• Evaluating risk management processes;
• Evaluating the reporting of key risks; and
• Reviewing the management of key risks.

Determining whether the ERM is effective is a judgment resulting from the internal
auditor’s assessment showing that:
• Organizational objectives support and align with the organization’s mission;
• Significant risks are identified and assessed;
• Appropriate risk responses are selected that align risks with organization’s risk appetite; and
• Relevant risk information is captured and communicated in a timely manner across the organization, enabling staff, management and the board to carry out their responsibilities.

Apart from assurances provided by the internal auditor, the board should obtain assurances from other sources such as management, external auditor and legal advisors. Under the Corporate Governance Code, the management should provide a confirmation to the board on the effectiveness of risk management and internal control systems.

Other consulting activities
In the early stages of introducing ERM to an organization, internal auditors may act as a project manager to provide consulting services for improving the governance and risk management process. When risk management embeds in normal operations, internal auditing roles should shift back to assurance roles. The IIA’s position paper suggests that the following consulting roles, with appropriate safeguards, can be taken up by internal auditors:
• Developing risk management strategy for board approval;
• Championing establishment of ERM;
• Maintaining and developing the ERM framework;
• Consolidating the reporting on risks;
• Coordinating ERM activities;
• Coaching management in response to risks; and
• Facilitating identification and evaluation of risks.

Appropriate safeguards include but are not limited to:
• Management remains responsible for risk management system;
• Internal auditor’s responsibilities, plan of work and the responsible teams should be properly documented;
• Internal auditing should not manage risks on behalf of management, it should instead provide advice and guidance to management on its decision making;
• Internal auditing cannot give assurance on any part of the ERM framework in which it is responsible for.

Last but not least, the position paper suggests that internal auditors should not undertake the role of:
• Setting the risk appetite;
• Imposing risk management process;
• Management’s assurance on risks;
• Making decisions on risk responses;
• Implementing risk responses on management’s behalf; and
• Accountability of risk management.

Conclusion
Internal auditors can assist an organization to achieve its objectives by not only utilizing its “process or control-based” knowledge, but also “risk-based” knowledge. In addition, by facilitating the management on risk assessment, consolidating key risks faced by the organization, evaluating ERM and enhancing the internal control systems, internal auditing can create value for the organization.

Roy Lo is Managing Partner at ShineWing (HK) CPA