Assessing the Adequacy of Risk Management Using ISO 31000

Tea Enting-Beijering

INTOSAI Internal Control Subcommittee Meeting

April 26-27 2012, Warsaw, Poland

IPPF Practice Guide

- Practice Guide on *Assessing the Adequacy of Risk Management Using ISO 31000*
  - Issued December 2010
  - Authored by members of The IIA Professional Issues Committee (PIC)
  - The IIA is framework neutral, not endorsing any particular framework (ISO 31000, COSO ERM, etc.)

Demand for Risk Management

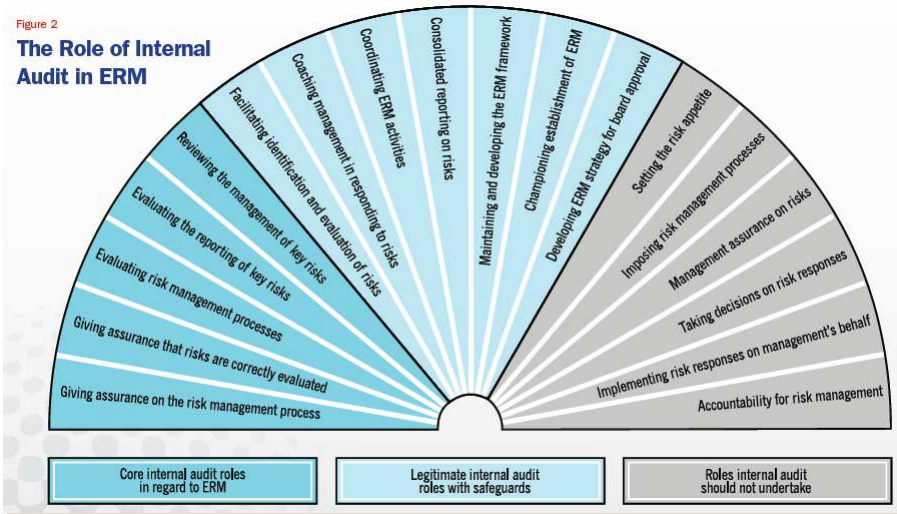
- Volatile economy resulting in increased pressure to manage numerous risks
- Requirement by senior management, the board, stakeholders, and regulators
- IIA Standard 2120 states that "the internal audit activity must evaluate the effectiveness and contribute to the improvement of risk management processes"

Demand for Risk Management

- Internal audit is being asked to provide risk management consulting where there is no formal risk management function
- Internal audit should strongly consider risk management assurance activities in the audit plan

Figure 2

The Role of Internal Audit in ERM



Providing Assurance on Risk Management Processes

- Core internal audit roles:
  - Giving **assurance** on the risk management program
  - Giving **assurance** that risks are correctly evaluated
  - **Evaluating** risk management processes
  - **Evaluating** the reporting of key risks
  - **Reviewing** the management of key risks

Providing Assurance on Risk Management Processes

- Roles internal audit should not undertake:
  - **Setting** the risk appetite
  - **Imposing** risk management processes
  - **Management assurance** on risks
  - Taking **decisions** on risk exposures
  - **Implementing** risk responses on management's behalf
  - **Accountability** for risk management

Providing Assurance on Risk Management Processes

- Roles that could compromise assurance testing in the near future:
  - **Maintaining and developing** the risk management framework
  - **Developing** a risk management **strategy** for board approval
  - **Coordinating** ERM activities approval

PROFESSIONAL GUIDANCE Setting the Standard
www.theiia/guidance/ippf.org

Providing Assurance on Risk Management Processes

- Roles internal audit can perform as a consultant(with safeguards):
  - Consolidated **reporting** on risks
  - **Championing** establishment of the risk management framework
  - **Facilitating** identification and evaluation of risks
  - **Coaching** management in responding to risks

Providing Assurance Using ISO 31000

- Three forms of assurance:
  - Process Elements Approach
  - Key Principles Approach
  - Maturity Model Approach

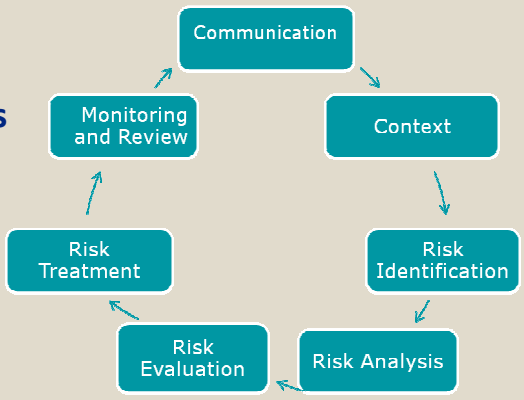
Note: These approaches are quoted from HB158:2010 Delivering assurance based on IS 31000:2009 Risk management – Principles and guidelines, A joint publication of Standards Australia, IIA-Australia, and the IIA Research Foundation.

Providing Assurance Using ISO 31000

- Process Elements Approach
  - Determines whether each element of the risk management process is in place
  - Evidence must be obtained to determine if each element is in practice
  - Seven elements exist

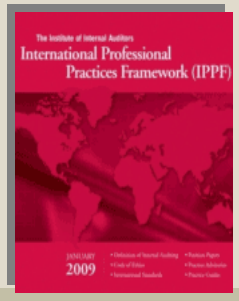
Providing Assurance Using ISO 31000

Process Elements



Providing Assurance Using ISO 31000

- Key Principles Approach
  - Based on a minimum set of principles
  - Evidence must be obtained to determine if each principle is true
  - Eight key principles exist



Providing Assurance Using ISO 31000

- Eight Key Principles
  - Risk management creates and protects value
  - Risk management is an integral part of organizational processes
  - Risk management is part of decision-making
  - Risk management explicitly addresses uncertainty

Providing Assurance Using ISO 31000

- Eight Key Principles
  - Risk management is systematic, structured, and timely
  - Risk management is based on the best available information
  - Risk management is tailored
  - Risk management takes human and cultural factors into account

Providing Assurance Using ISO 31000

- Maturity Model Approach
  - Assumes that the quality of a risk management program improves over time
  - Assumes that several components of a risk management system exist
  - Links risk management performance to a separate performance measurement and management system
  - Measures of performance are shared with senior management and the board

Providing Assurance Using ISO 31000

- Maturity Model Components
  - A protocol of performance standards
  - A guide showing how the standards and sub-requirements can be completed
  - A means of measuring actual performance against each standard and sub-requirement
  - A means of recording and reporting performance and improvements
  - Periodic independent verification of management's assessment

Providing Assurance Using ISO 31000

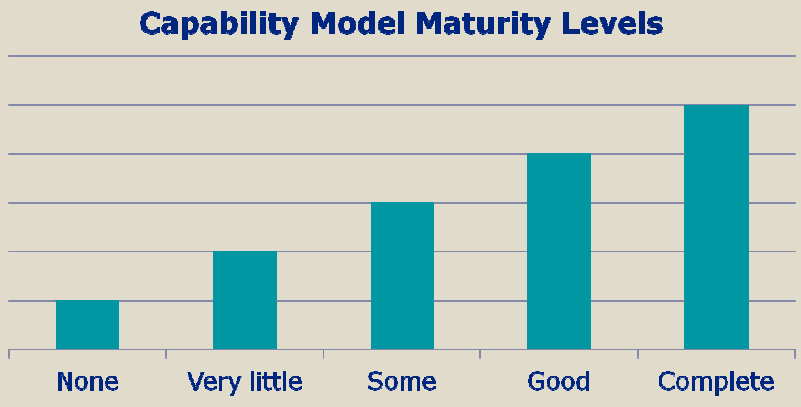
- Maturity Model Evaluation
  - Determination of whether maturity model component exist
  - Are components effective and relevant for the organization
  - Do components add value

The Institute of Internal Auditors | PROFESSIONAL GUIDANCE Setting the Standard
www.theiia/guidance/ippf.org

Providing Assurance Using ISO 31000

- Maturity Model Measurement
  - A method of measuring maturity
  - Actual performance against each component must be measured
  - Example – Capability Maturity Model developed by *Carnegie Mellon University*

Providing Assurance Using ISO 31000



The Institute of Internal Auditors | PROFESSIONAL GUIDANCE *Setting the Standard*

www.theiia/guidance/ippf.org