7 Essential Elements of ERM and the role of Internal Audit

Tony Harb
Director, InConsult

Presented to The Institute of Internal Auditors
NSW Chapter Members Meeting
17th June 2008

NOTE:

As requested by IIA Chapter members, I have included additional notes and examples to this presentation.

Should members require additional information and references, please do not hesitate to contact me by email or at the next Chapter members meeting.

Regards,
Tony Harb

tonyh@inconsult.com.au

What we will cover

With the planned release of the international risk management standard ISO31000 in September 2008, it is timely for auditors to rethink ERM and in particular reassess its impact on the role of internal audit.

Over the last few years, there has been a shift for IA and ERM activities to work closer together to capitalise on strong synergies, yet maintain their respective positions.

AGENDA

- What is ERM and why is it becoming increasingly important
- How do you know it is alive and well
- The key elements of a successful ERM program and how IA can support the key elements of ERM
- Benefits of an effective ERM program to internal audit

What is Enterprise Risk Management?

- A rigorous approach to assessing and addressing the risks from all sources that threaten the achievement of an organization's strategic objectives *(Tillinghast Towers Perrin)*
- The management of corporate or enterprise-wide risks and opportunities in one systematic, structured, and comprehensive framework using both a consistent methodology and terminology *(S&P)*
- 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 *(COSO)*
- A structured, consistent and continuous process across the whole organisation for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives *(IIA)*

People, systems and processes working together across the organisations to systematically think about and manage a wide range of risks that could impede achieving organisational objectives/opportunity.

Why is ERM becoming more important?

- Corporate failures and earning management – ENRON, HIH, Worldcom
- Only some risks are insurable – 25% to 40%
- Limited resources/capital – can't afford to make expensive mistakes
- Less forgiving regulators/stakeholders – NAB, AWB
- Uncertain world and emerging risks – Natural disasters, terrorism, pandemic flu, natural resources, politics
- Recognised management tool
  - Improve understanding of risks associated with opportunity
  - Improve likelihood of achieving objectives
  - Help minimise impact of events we cannot control
  - Support informed decision making – think about risks & opportunities
- Recognised regulatory/good practice tool – APRA, PHIAC, ASX, SOX, S&P, BASELII, ISO9000

Links between ERM and Internal Audit

- IA and ERM both support enterprise governance
- ERM is the management process (1st line of defence), IA is the assurance process (2nd line of defence).
- IA and ERM both support achieving objectives
- IA and ERM are structured processes
- Objectives, risks and controls are central to thinking
- Opportunity to capitalise on synergies, minimise duplication

WARNING:

- ERM is a management process and IA is an independent assurance process
- Ability of IA to rely and work with ERM team will vary depending on the organisations level of risk management maturity

How do you know ERM is alive and well?

- Risk management practices are
  - well defined, clear, well communicated and understood
  - applied at appropriate levels (strategic, operational) to help shape decisions
- Risk management is not one person or one department
  - It is risk owners, risk manager, compliance, audit
- The organisation takes calculated risks to capitalise on opportunities and predict outcomes to a reasonable level of certainty
- The organisation is prepared to deal with various 'threats'
- Less incident frequency and/or incident severity (within risk appetite)
- Important goals and objectives are met

The key elements of successful ERM

Element 1: Management commitment	How can internal audit help?
■ Understand ERM - what, why, benefits, workload and limitations ■ Involved - help shape ERM framework, get their input ■ Encourage leadership - set the tone from the top ■ Strong governance structure and commitment ■ Build a strong culture (everyone owns risks)	■ Promote establishment, maintenance and development of ERM framework ■ Promote & reinforce benefits of risk management to organisation ■ Promote benefits and synergies with internal audit

The key elements of successful ERM

Element 2: Communication and consultation	How can internal audit help?
■ Initial communication - what, why and benefits ■ One-to-one communication - engage and enthuse (WIFM) ■ Ongoing communication/ reports - KPI's, progress, improvements, build confidence, maturity ■ Use appropriate language ■ Risk manager is not always the subject matter expert and they need the risk owner ■ Partnership among senior management, line management, risk management, compliance, internal audit, external audit	■ Include IA responsibilities the ERM framework ■ Communicate and reinforce to all the role of IA in the ERM framework ■ IA involved in issue escalation process ■ IA Charter makes clear reference to ERM framework

The key elements of successful ERM

Element 3: Policies and procedures	How can internal audit help?
■ Clear, concise & easy to understand ■ Risk management policy ■ Risk management strategy ■ Risk management plan ■ Risk management toolkit (procedures, approach, forms, templates) ■ Risk management technology - streamline processes ■ Supporting policies (OH&S, privacy etc) ■ Supporting plans and strategies ■ Supporting procedures (controls)	■ Review RM Strategy, RM policy, RM procedures for appropriateness ■ Align Audit Plan to RM Plan (where possible) ■ Audit of systems and processes to ensure ERM framework is working

The key elements of successful ERM

Element 4 Training and education	How can internal audit help?
■ Investing in people ■ Builds capabilities > empowers > share workload ■ Initial training should be comprehensive ■ Ongoing refresher training ■ On-the-job training - risk workshops ■ Other management skills and technical training is critical	■ Conduct training in areas where IA has strengths (risk identification methods) ■ Review risk profiles & provide feedback to risk owners (on the job training) ■ Audit of training process (ERM and other training)

The key elements of successful ERM

Element 5: Effective and efficient framework	How can internal audit help?
■ Well documented - policy, plan, toolkit ■ Recognised methodology ■ Appropriate technology ■ Roles, responsibilities and accountabilities defined ■ Systematic and co-ordinated approach ■ Risk appetite defined and reflected in common risk criteria ■ Enterprise-wide context (per COSO strategic, operational, financial and regulatory)	■ Align key activities (risk profiles) to minimise duplication. ■ Well aligned activities create interdependencies between the IA and ERM - good cross-check and reduces the excuses for not doing things on time ■ Independent review of RM framework

The key elements of successful ERM

Element 6: RM is applied in practice	How can internal audit help?
■ Regular risk assessment process ■ Risks identified, understood, quantified and prioritised ■ Risk reporting and linked to performance management system ■ Accountability of actions ■ Integrated into strategic plans, control framework and reporting systems ■ RM practices can be audited and verified	■ Facilitate risk workshops ■ Support (partner) and coach management ■ Review management of key risks ■ Ensure risks correctly evaluated

The key elements of successful ERM

Element 7: Ongoing monitoring and review	How can internal audit help?
■ All components of ERM framework ■ Periodic risk profile review including actual incidents and emerging risks (climate change, mobile phones, fuel prices, GM foods etc) ■ Regular process and not just a one-time event ■ Commitment to continuous improvement ■ Formal scheduling and reminder systems ■ Effective internal audit, self assessments & compliance processes	■ Assurance of ERM systems and processes ■ Assurance of reporting and monitoring of risks ■ Independent testing of internal controls (2nd line of defence)

Benefits of effective ERM to Internal Audit

- Strong control environment (first line of defence)
  - A 'risk aware' culture (commitment from management)
  - Risk ownership and accountability
  - Structured risk management approach
- Synergies between ERM and auditing activities
  - Risk assessment and control evaluation is at the core
  - Utilise managements risk assessments/risk register to improve quality of risk and control information
  - Choice of controls to test or not to test (key controls, 'catastrophe' risks - high impact/low likelihood, 'problem' risks - low impact/high likelihood
  - Joint risk and audit unit, Joint Risk & Audit Committee
- Improve audit efficiency - leveraging from ERM program, ERM technology
- Add-value - coaching, facilitating and training risk owners

Question Time

Tony Harb
Director, InConsult

tonyh@inconsult.com.au