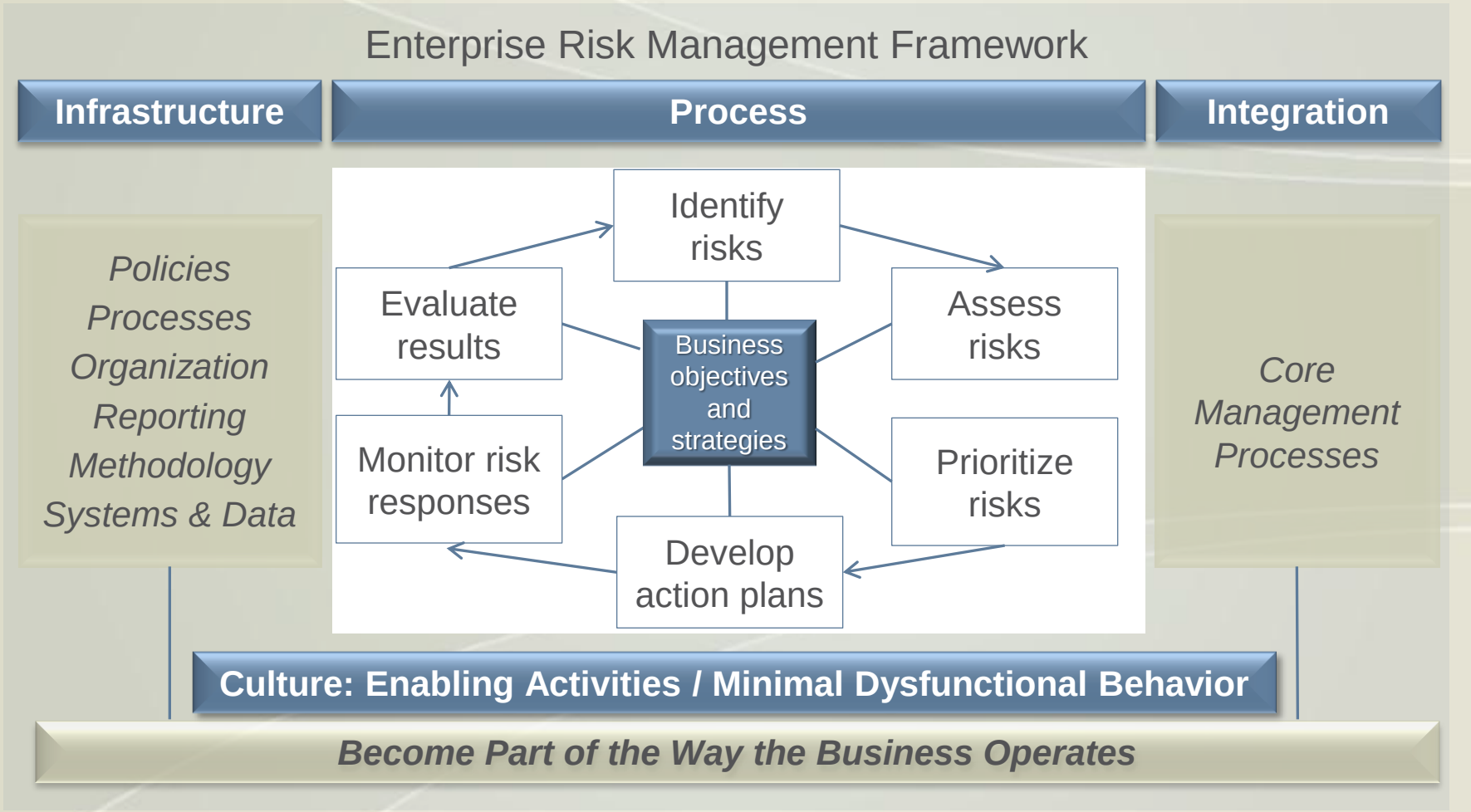
AUDITING ENTERPRISE RISK MANAGEMENT

ERM: A Simple Definition

ERM establishes the oversight, control and discipline to drive ***continuous improvement*** of an entity's risk management capabilities in a constantly changing operating environment.

Integration with What Matters is Key



Polling Question #1

Enterprise Risk Management is currently being implemented in my company:

(a) Yes

(b) No

Common Barriers to Effective ERM Functions

Governance / Cultural	Process	Tools / Methodologies
• Articulating ERM's value • Lack of executive sponsorship for ERM • Assigning ERM ownership • Creating a risk aware culture throughout the organization	• Establishing a common risk language • Identifying and assessing risk • Setting risk appetite and tolerances • Bottom-up focus rather than top-down • Inability to break out of a silo mentality	• Lack of succinct and tailored risk reporting • Simulations and stress tests • Data and information systems • Inability to quantify certain risk types

* *Sources: "The practical challenges of enterprise risk management", Keeping Good Companies – Protiviti , 2007; "Common ERM Challenges". Risk Management Magazine, 2011"; industry experience*

Does This Feel Familiar?

Foundational Elements to Avoid Pitfalls

- People and Buy-in
  - Critical to have Board and Executive Sponsorship
  - Appoint a risk leader (e.g., CRO)
- Focus on Material Business Risks
  - Attention should be on risks that would prevent achievement of strategic objectives
- Align Risk and Business Planning
  - Risk management should be a core components of strategic planning process and not viewed as stand-alone activities

* *Source: "The practical challenges of enterprise risk management", Keeping Good Companies – Protiviti , 2007.*

Foundational Elements to Avoid Pitfalls

- Integrate ERM Across Business
  - Involving risk management in planning process can help breakdown silos
- Risk Reporting
  - Useful and succinct information on material risks to facilitate decision-making
- Involvement of Internal Audit
  - Act as eyes and ears of the Board and provide an independent assessment on effectiveness of risk management control systems

* *Source: "The practical challenges of enterprise risk management", Keeping Good Companies – Protiviti , 2007.*

Polling Question #2

Enterprise Risk Management is challenged because:

(a) Executive management buy-in doesn't exist

(b) Reporting is challenged by data availability and multiple information systems

(c) Failure to integrate ERM process into strategy setting and performance management

(d) Not clear of the value being provided

(f) Failure to link risk assessments into business plans

(g) All of the above

(h) None of the above

INTERNAL AUDIT'S ROLE

Mandate to Get To Strong

Increased expectations regarding Enterprise Wide Risk Management, including Internal Audit

- Origins – How the concept of Getting To Strong evolved
- Background – What does Getting To Strong really mean?
- Expectations

Internal Audit – Satisfactory to Strong

Challenges Facing Internal Audit Functions

- Increasing complexity and velocity of risk facing the bank.
  - Complexity of new markets (*e.g.,* derivatives market, mortgage market).
  - Change in new products and processes (*e.g.,* fraud prevention, trading platforms).
  - Expansion of risk management at the enterprise and line of business ("LOB") levels.
- Compliance with additional laws and regulations in the industry (*e.g.,* Basel, Dodd-Frank, etc).
- Managing timely remediation of internal control deficiencies and audit recommendations in continuously changing environment.

Defining a "Strong' Audit Function: Core Elements

Core Elements of a Strong Audit Function

Accountability / Effective Challenge

- Audit reports include comments on the efficacy of LOB self-assessments, emerging issues and appropriateness of risk levels relative to control environment and risk appetite
- Effectively challenge LOB leaders
- Consider holding audit results against compensations decisions

Stature / Independence

- Integrating IA into corporate risk management, policy development, new product and service deployments, strategy changes, etc.

Core Elements of a Strong Audit Function

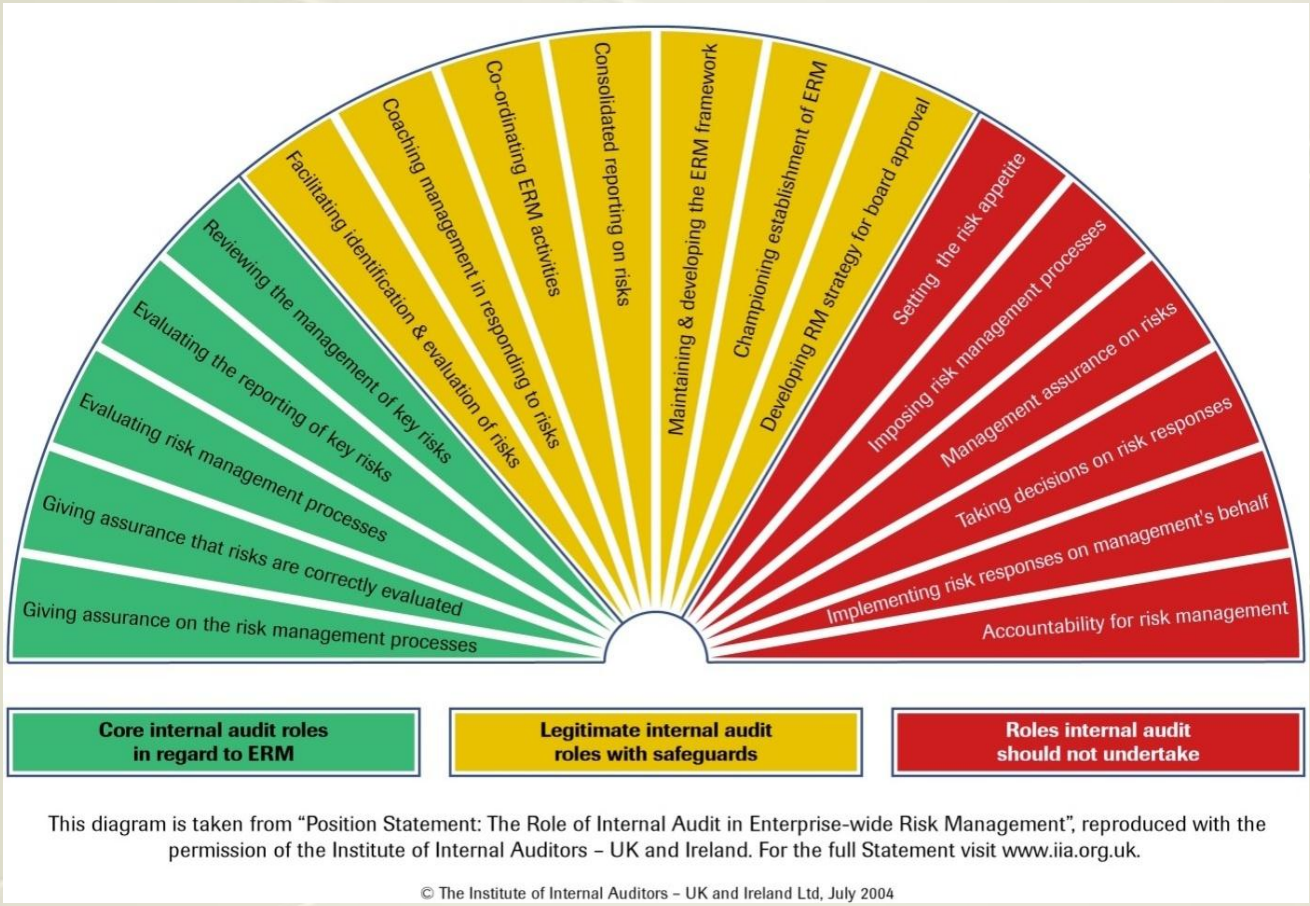
Competence / Talent

- Specific knowledge of audit and risk management practices, commensurate with the complexity and risk profile
- Ability to make tough calls on top-of-house issues

Scope and Frequency

- Audit plan and scope of audits consider reputation and strategic risks
- Audits include assessment of the “sensibility” of risk levels and trends

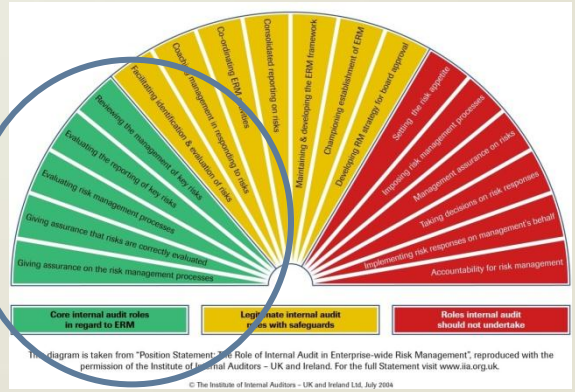
The Appropriate Role for Internal Audit



This diagram is taken from "Position Statement: The Role of Internal Audit in Enterprise-wide Risk Management", reproduced with the permission of the Institute of Internal Auditors – UK and Ireland. For the full Statement visit www.iia.org.uk.

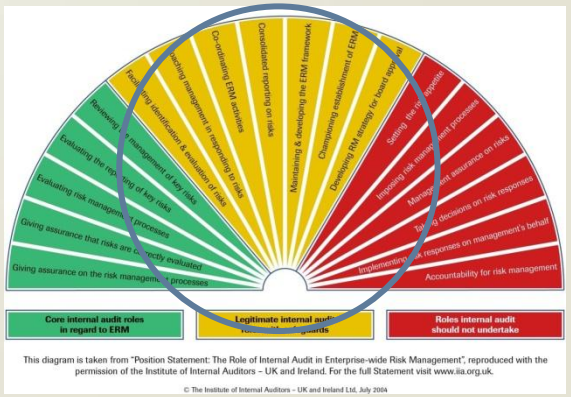
Core IA Roles Relative to ERM

- Review management of key risks
- Evaluate reporting of key risks
- Evaluate risk management processes
- Provide assurance that risks are evaluated correctly
- Provide assurance on the risk management processes



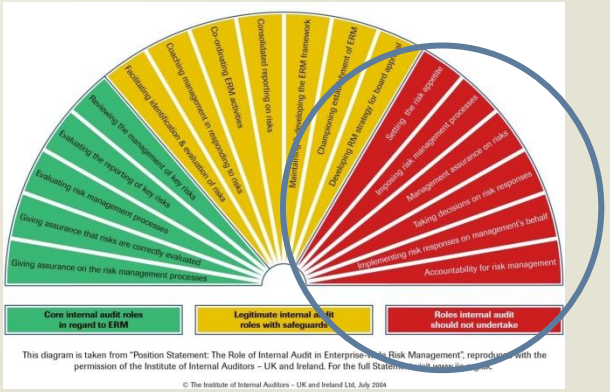
Legitimate IA Roles with Safeguards

- Developing ERM strategy for board approval
- Championing establishment of ERM
- Maintaining / Developing the ERM framework
- Consolidated reporting on risks
- Coordinating ERM activities
- Coaching management in responding to risks
- Facilitating identification and evaluation of risks



Roles IA Should Not Undertake

- Setting the risk appetite
- Improving risk management processes
- Management assurance on risks
- Making decisions on risk responses
- Implementing risk responses on management's behalf
- Accountability for risk management



Auditing ERM Process is a Challenge

- What is the standard? Who decides the standard?
- What does “effectiveness” mean?
- How do you evaluate “effectiveness?”
- At this time, are we more concerned with signs of “ineffectiveness?”

Ideas for Auditing the ERM Process

(1) Use a framework as a standard

- Choose a suitable framework
  - COSO ERM Integrated Framework
  - ISO 31000
  - Standards Australia
  - S&P ERM Framework
- Use your framework of choice as a tool for planning, execution and reporting
- Define “effectiveness” standard, i.e., the means by which to evaluate risk responses
- While frameworks aren’t perfect, they’re better than starting with a blank sheet of paper

Ideas for Auditing the ERM Process

(2) Become an active ERM champion

- Play the roles of a champion:
  - Facilitate
  - Coordinate
  - Educate
  - Aggregate
  - Integrate
- Be involved with company risk committees and councils
- Expand skillsets of IA function

Ideas for Auditing the ERM Process

(3) Expand your audit universe

- Identify auditable components for inclusion in the audit universe
  - Governance
  - Risk management
- Obtain input from senior management and the Board as to the components
- Consider the components provided by your chosen framework
- Focus more broadly on enterprise risk
- Pay attention to the evolving risk oversight process of the Board

Ideas for Auditing the ERM Process

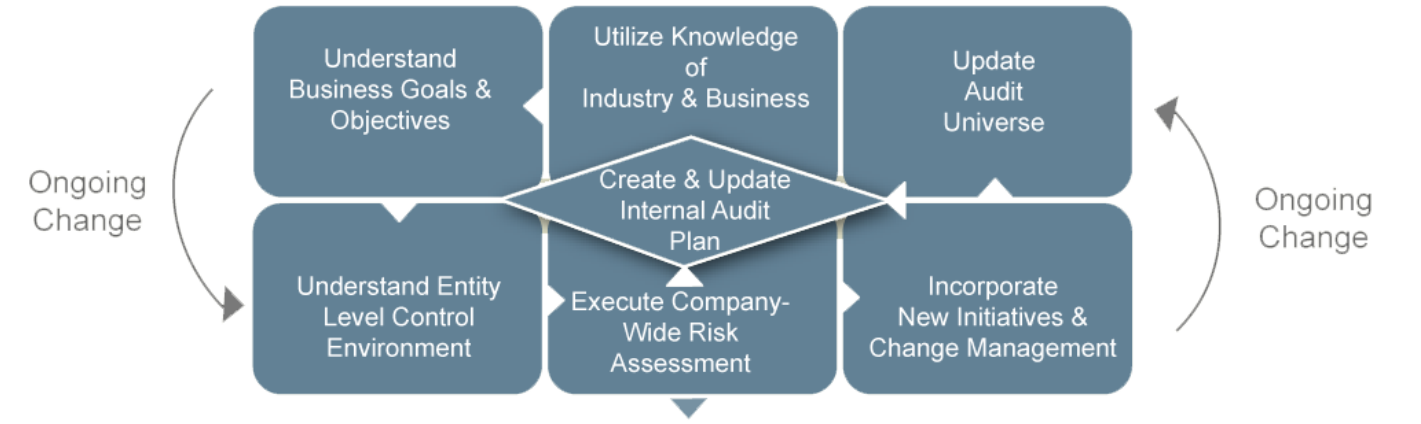
(4) Focus on enterprise risks

- Link IA reporting to the enterprise's critical risks
- Acknowledge the key risks the IA plan doesn't cover
- Compare risks identified by IA to the risks reported through the ERM process
- Ensure adequate focus on operational risks
- Be alert for emerging risks, including the potential for "black swans" and "transforming events"

Ideas for Auditing the ERM Process

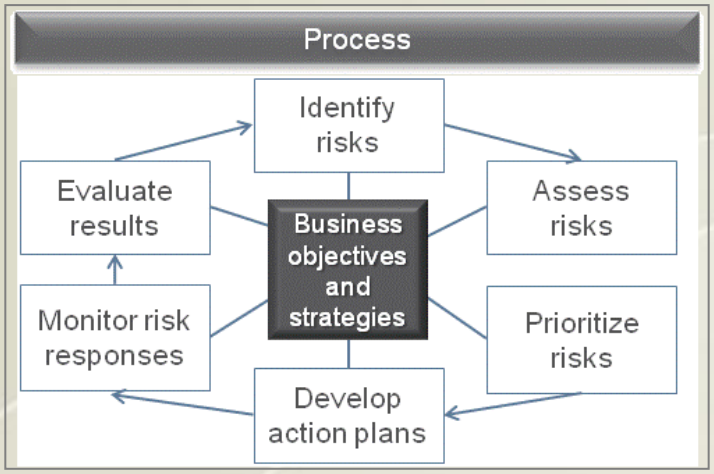
(5) Keep your risk assessment evergreen

- Understand business goals / objectives as a context
- Know the industry and business
- Stay abreast of changes in external and internal environment



Ideas for Auditing the ERM Process

(6) Consider components of the ERM process in developing the audit plan



- Is there evidence that the process activities, including the supporting tools, are in place and used effectively?
- Are the process activities integrated with core management processes?
- Key questions to consider:
  - How effective is the risk identification and prioritization process?
  - Are robust action plans formulated to address the critical risks?

Ideas for Auditing the ERM Process

(7) Look for integration opportunities

- Strategy setting
- Annual business planning
- Performance management
- Budgeting
- Capital expenditure funding
- M&A targeting, due diligence and integration

Ideas for Auditing the ERM Process

(8) Pay attention to key indicators

- Are risk-management efforts mired down into minutiae?
- Are there gaps and overlaps in accountability?
- Are the warning signs escalated by risk management ignored?
- Is there a lack of a “tone at the top” conducive to effective risk management?
- Is the compensation structure incenting unacceptable risk taking?

Ideas for Auditing the ERM Process

(8) Pay attention to key indicators (Cont'd)

- Is anyone making higher than expected returns and no one understands why?
- Is the Board engaged with key decisions timely?
- Is risk management an appendage from performance management?
- Is risk an afterthought to strategy-setting?
- lacking sufficient authority or time?

Ideas for Auditing the ERM Process

(9) Increase relevance of the audit plan

- Evaluate completeness of ERM risk assessment
- Link audit plan to the entity's risk responses
- Update audit plan for major changes in the external and internal environment
- Increase value of face time with senior management and the Board

Ideas for Auditing the ERM Process

(10) Watch for deficiencies in infrastructure

- Report on “current state” maturity of ERM capabilities
- Work with risk owners to ascertain a desired future state
- Identify and prioritize gaps
- Recommend improvements

Polling Question #3

In my company, we use the following risk management framework:

(a) COSO Internal Control Integrated Framework

(b) COSO ERM Integrated Framework

(c) ISO 31000 Framework

(d) Standards Australia Framework

(e) S&P ERM Framework

(f) Another framework

(g) We don't use a framework at the current time

AUDITING ENTERPRISE RISK MANAGEMENT