



SOCIETY OF ACTUARIES

**ERM Symposium  
April 2009**

**B2-A Global Perspective on Risk Management  
Structure and Governance for the Insurance  
Sector**

**Sylvie Hulin  
Denis Tauscheck**

**Moderator  
Thomas Fineis**



**Deloitte.**

---

# A Global Perspective on Risk Management Structure and Governance for Insurance

Thomas Fineis

DC Director

Deloitte Consulting LLP

April 30, 2009

Sylvie Hulin

Senior Manager

Deloitte Consulting LLP

Denis Tauscheck

Chief Actuary

Aviva North America

# Agenda

---

Laying a Strong Foundation

---

The Current State Globally

---

External Guidance

---

Leading Principles for ERM Structure and Governance

---

Roles and Responsibilities

---

Governance at Aviva

---

Next Steps

# Introduction

---

- The market has witnessed huge losses at global financial giants and the biggest collapse of established financial institutions since the Great Depression. These events have affected virtually all FSI sectors, including insurance companies.
- It is clear the not all organizations in the financial sector have a fully-developed or well-integrated function.
- Companies should take a fresh look at their risk management programs and focus on developing capabilities that place risk management as an integral part of both strategy setting and day-to-day business.

## Laying a Strong Foundation

---

- Enterprise Risk Management (ERM) is an integrated risk management framework that places consideration of risk as a focal point of business activities.
- Program that enables a company to make intelligent risk-based decisions and manage its expected returns by selecting the risks it is willing to assume.
- A successful ERM program must be consistent with the company's culture and also be responsive to local regulatory and rating agency guidance.

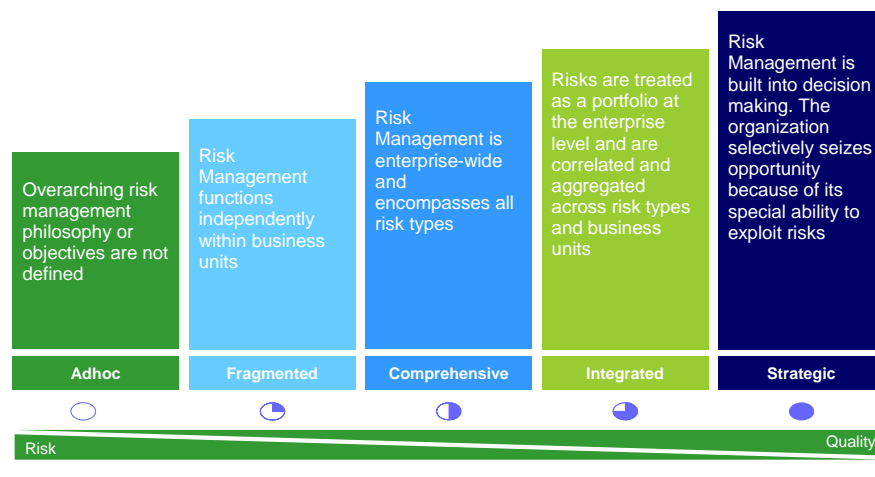


The Current State Globally

## Risk Management Capability Maturity Model

- The Risk Management Capability Maturity Model provides a useful framework to set the groundwork for a discussion of ERM practices globally.
- The model is a tool to help identify and classify the current state of risk management capabilities with five distinct levels of ERM capability:
  - Adhoc
  - Fragmented
  - Comprehensive
  - Integrated
  - Strategic
- Many companies are currently situated somewhere between the Fragmented and Integrated stages on the Capability Maturity Model.

## Risk Management Process Capability Maturity Model†



†Adapted from the Capability Maturity Model framework developed by Carnegie Mellon University, 1993.

## European Union

---

- The development of ERM in the EU has been driven by the promulgation of Basel II (for banks) and the proposal of Solvency II (for insurers), which has placed significant regulatory focus on ERM.
- In the UK, the Financial Services Authority's Prudential Sourcebook and Individual Capital Assessment (ICA) requirements have forced insurers to think more critically about the measurement of risk.
- Various regulatory developments within the EU focus on the capital impacts of risk, though not all offer specific guidance with respect to the non-quantitative aspects of ERM.



## United States

---

- Rating agencies like A.M. Best and Standard & Poor's, and external organizations such as COSO<sup>1</sup>, are now driving the development of ERM practices.
- The National Association of Insurance Commissioners (NAIC) risk-based capital guidelines for life and property casualty insurers require insurers to maintain a minimal level of capital adequacy, and the Sarbanes-Oxley Act has mandated the need for financial risk controls.
- Rating agencies play a significant role in the movement of insurers beyond these basic regulatory requirements to think more holistically about ERM.



## Australia

---

- The adoption of Basel II for authorized deposit-taking institutions and certain regulations promulgated by the Australian Prudential Regulation Authority (APRA) have drawn attention to risk management standards and practices across the financial services industry.
- Standards and requirements for the insurance industry are still in development and lag behind some other areas of the world.
- There also exists the Australian/New Zealand Standard – Risk Management. Here, Australia and New Zealand formed a joint technical committee of representatives from numerous organizations to publish two documents on risk management in 2004.



## Asia

---

- ERM practices in Asia are in the early stages of the Maturity Model. Many of the region's leading practices have been influenced by the ERM programs of parent companies located elsewhere.
- Some companies have explored asset-liability management or embedded value calculations as an initial step in their ERM programs.
- Regulators have been the primary driver of ERM in Asia, with many countries adopting IFRS regulations requiring insurers to disclose risks in their financial statements. Some countries are also discussing Solvency II-type regulations, although these have not been adopted yet.





# External Guidance

## IAIS (International)

---

The International Association of Insurance Supervisors outlines 19 requirements for ERM categorized by: **1) Governance and an ERM framework**, and **2) Own Risk and Solvency Assessment (ORSA)**.<sup>†</sup> The requirements for governance are:

1. As part of its overall governance structure, an insurer should establish, and operate within, a sound **ERM framework** which is appropriate to the nature, scale, and complexity of its business and risks.
2. The ERM framework should be **integrated** with the insurer's business operations and culture, and address all reasonably foreseeable and relevant material risks faced by the insurer in accordance with a properly constructed risk management policy.
3. The establishment and operation of the ERM framework should be led and overseen by the insurer's **board and senior management**.
4. For it to be adequate for capital management and solvency purposes, the framework should include provision for the **quantification of risk** for a sufficiently wide range of outcomes using appropriate techniques.
5. Measurement of risk should be supported by **accurate documentation** providing appropriately detailed descriptions and explanations of risks.

<sup>†</sup> International Association of Insurance Supervisors, "Guidance Paper on Enterprise Risk Management for Capital Adequacy and Solvency Purposes," October 2007; [http://www.iaisweb.org/\\_temp/14\\_Guidance\\_paper\\_No\\_2\\_2\\_5\\_on\\_ERM\\_for\\_capital\\_adequacy\\_and\\_solvency\\_purposes.pdf](http://www.iaisweb.org/_temp/14_Guidance_paper_No_2_2_5_on_ERM_for_capital_adequacy_and_solvency_purposes.pdf)  
Copyright © 2009 Deloitte Development LLC. All rights reserved.

## Solvency II (European Union) †

---

Solvency II is structured around three pillars of risk management: quantitative requirements; **governance and supervisory requirements**; and disclosure and transparency rules. The second pillar moves beyond pure quantitative measures of risk to address issues of corporate governance.

- The governance system includes compliance with the requirements on fit and proper, risk management, the own risk and solvency assessment (ORSA), internal control, internal audit, the actuarial function and outsourcing.
- Undertakings are required to have written policies in place which clearly set out how they deal with internal control, internal audit, risk management and, where relevant, with outsourcing.
- Administrative or management body must be actively involved in the governance system and approve written policies and revise them at least annually or before any significant change is implemented in the system.

† Commission of the European Communities, "Directive of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance" (Solvency II), February 2008: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0119:REV1:EN:PDF>  
Copyright © 2009 Deloitte Development LLC. All rights reserved.

## MCCSR Advisory Committee (Canada)

---

The Minimum Continuing Capital and Surplus Requirements (MCCSR) Advisory committee is chaired by representatives of the Office of the Superintendent of Financial Institutions (OSFI) and the Canadian Institute of Actuaries (CIA). In November 2007, the Advisory Committee released a paper on its vision for a new principles-based solvency framework.†

- The framework proposes regulatory requirements across three areas: financial requirements, governance, and market conduct.
- The framework notes the important role of effective governance in managing risks that cannot be suitably addressed through financial requirements.
- The guidance does not provide much detail as to what constitutes appropriate governance.
- The discussion of ERM roles and responsibilities focuses primarily on the models and processes used to assess capital adequacy.

† MCCSR Advisory Committee, "Canadian Vision for Life Insurer Solvency Assessment," November 2007: <http://www.lautorite.qc.ca/userfiles/File/projets-speciaux/solvabilite/solvency-committee-3.pdf>  
Copyright © 2009 Deloitte Development LLC. All rights reserved.

## APRA (Australia) †

### The Role of the Board

- Ultimately responsible for the Risk Management (RM) framework of the company.
- Must approve a written Risk Management Strategy (RMS) and must be notified of any deviation.

### Risk Management Framework

- The totality of systems, structures, policies, processes and people within the company that identify, assess, mitigate and monitor all internal and external sources of risk.

### Risk Management Strategy

- RMS is a high level document describing the company's approach to RM.
- Must detail extent and conditions under which company will accept risk.

### Review of RM Framework

- The RM framework is subject to effective and comprehensive review by operationally independent, appropriately trained and competent persons.

### Risk Management Declaration

- The Board must provide APRA with a declaration on RM, relating to each financial year of the company, signed by two directors.

† APRA Prudential Standard LPS 220 for Life Insurers, March 2007: [http://www.apra.gov.au/Life/upload/LPS\\_220-1.pdf](http://www.apra.gov.au/Life/upload/LPS_220-1.pdf)

† APRA Prudential Standard GPS 220 for General Insurers, February 2006: <http://www.apra.gov.au/General/upload/Final-GPS-220-July-2008.pdf>

Copyright © 2009 Deloitte Development LLC. All rights reserved.

## Standard & Poor's †

The foundation of S&P's strategic risk management framework focuses on **culture**, controls, emerging risk management, risk and economic capital models, and strategic risk management. The governance component assesses an institution's risk culture, strategy, appetite, and awareness based on the following criteria:

- Does the risk management function have sufficient stature within the firm?
- How well does the firm establish and articulate its risk appetite? Is it consistent with the articulated business strategy, and what is the role of risk management in this process?
- Is the reach of the risk management function sufficiently wide across the group? Are the established policies of the business lines consistent with the group's stated risk appetite and business strategy?
- How well informed is senior management on risk issues? Is there effective internal reporting of risk issues? How good is external disclosure?

† Standard and Poor's, "Criteria: Summary Of Standard & Poor's Enterprise Risk Management Evaluation Process For Insurers," November 26, 2007: <http://www2.standardandpoors.com/portal/site/sp/en/eu/page/article/2,1,5,0,1148449517749.html>

† Standard and Poor's, "Enterprise Risk Management For Financial Institutions: Rating Criteria And Best Practices," December 2007: <http://www2.standardandpoors.com/sp/pdf/events/ERMArticle107.pdf>

Copyright © 2009 Deloitte Development LLC. All rights reserved.

## A.M. Best †

### Set the Tone at the Top

- Senior management establishes an environment and corporate framework that embeds risk awareness throughout the organization.
- Board/senior management receive and critique frequent reports on risk metrics and updates on key risk-management activities.

### Establish/Communicate RM Objectives

- Board/senior management define risk profile supporting overall goals.
- Senior management communicates risk profiles to business unit management and requires implementation of appropriate RM practices.

### Define Roles and Responsibilities

- Appropriate segregation of duties between those monitoring/measuring risk and those making risk decisions.
- Establish a separate department to take a holistic view of the company led by a member of senior management – chief risk officer (CRO).

### Strategic Decision-Making Process

- Business strategy and capital allocation are based upon risk-adjusted returns and other risk metrics consistent with the corporate risk profile.
- Financial planning and budgeting process measures impact of projected financial results on corporate risk profile.

† A.M. Best, "Risk Management and the Rating Process for Insurance Companies," January 25, 2008:  
<http://www.ambest.com/ratings/methodology/riskmanagement.pdf>  
 Copyright © 2009 Deloitte Development LLC. All rights reserved.

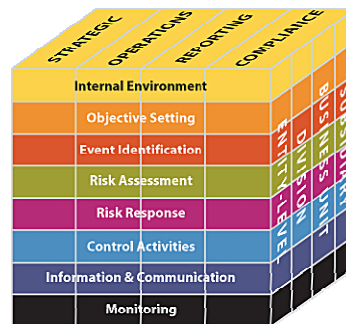
18

## COSO

- COSO released an integrated framework for ERM in September 2004† which helps a company to assess its overall ERM capabilities.

### COSO Roles and Responsibilities


- The **Board** should discuss with senior management the state of ERM and ensure that it is apprised of the most significant risks
- The **CEO** must assess the organizations ERM capabilities by engaging key staff
- The **CRO** has key responsibilities for the implementation of the ERM framework
- **Internal Audit** plays an important role in monitoring ERM and reporting to the Board but is not responsible for implementation.



**COSO's framework is a valuable tool in assessing a company's internal controls as it relates to ERM.**

† Commission of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management – Integrated Framework, September 2004:  
[http://www.coso.org/documents/COSO\\_ERM\\_ExecutiveSummary.pdf](http://www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf)  
 Copyright © 2009 Deloitte Development LLC. All rights reserved.

19



# Leading Principles for ERM Structure and Governance

## Leading Principles

---

- A set of best practices can be distilled from the guidance and experiences of insurance companies worldwide in four key areas:
  - Culture
  - Communication
  - Integration into the business
  - Roles and Responsibilities

## Culture

---

- 1) An insurer's ERM program must be appropriate to the organization's culture. A program for a decentralized organization with significant autonomy in each business unit should be very different from a program for a company where decision making is centralized.
- 2) Enterprise leadership must create an ERM culture by setting a clear mandate for ERM within the organization. The CEO must clearly convey the company's commitment to effective ERM.
- 3) Risk awareness and policies should be embedded in all layers of the organization, rather than being viewed as an issue only for those in the ERM function.

## Communication

---

- 1) The board and senior management should clearly define and communicate a corporate risk profile that is integrated with the company's strategy.
- 2) There must be clear communication from senior management risk owners and business unit management regarding risk policies and expectations for compliance.
- 3) A process for monitoring and reporting risks, including escalation and communication of risks, must be clearly defined. In particular, the board should be kept periodically informed of major developments concerning the company's risks by means of formally established sessions and other access to senior risk management personnel.

## Integration into the Business

---

- 1) The ERM program must be appropriate for the size, complexity, and business strategy of the company.
- 2) ERM must be fully integrated into the decision-making process. Business performance decisions should be based on appropriate risk-adjusted metrics.
- 3) Compensation for risk personnel should be linked to performance on key risk management goals, and compensation for all personnel should be linked to risk-adjusted metrics. Incentive compensation should be reviewed to ensure that it drives the desired behavior with respect to risk.

## Roles and Responsibilities

---

- 1) Clear roles and responsibilities must be prescribed for the board, board committees, senior management, those with jobs within the ERM function and other risk-related personnel. Oversight of, and guidance related to, the risk management function must be provided by the board, and risk-related board committees should be clearly aligned with key risks.
- 2) Risk ownership must be clearly defined and aligned with roles and responsibilities throughout the organization consistent with where risks are taken. However, this role/function must take responsibility for ensuring that all risks are owned and addressed somewhere in the organization and that risks are aggregated appropriately to an enterprise level.
- 3) Risk roles and that associated accountabilities must be structured to ensure independence between management and risk measurement.



# Roles and Responsibilities

## Roles and Responsibilities

### The Board – Its Role in Risk Management

---

Boards are under pressure – regulatory, legal, fiduciary, stakeholder – to oversee risk management activities, but many wonder where to start.

- First, delineate responsibility. Options include:
  - Keep at full board level → broad airing of issues, but unwieldy
  - Delegate to Audit Committee → overworked dealing with financial risk, now you add operational and strategic
  - Create dedicated Risk Management Committee → provides coordinating and harmonizing function for all the board's committees (audit, compensation, succession, etc)
- The loop is closed when the full board addresses risk issues with management on a regular basis
- Boards are slowly realizing risk management is as important to value creation as it is to value protection. All growth strategies require an element of risk.

## Roles and Responsibilities

### The Board – Its Role in Risk Management – Cont'd

---

- The topic of risk should be a regular discussion topic at full board meetings
  
- Silos of risk are good for specialization, but the Board must see the "big picture". Here are some things that can be done:
  - Invite risk managers to share their varying perspectives on risk
  - Don't limit risk discussion to the traditional. Introduce risks associated with new value creation strategies
  - Evaluate the risk governance structure of the board and its committees
  - Evaluate risk in a disciplined framework, not ad-hoc
  - Work in synch with management
  - Periodically assess the effectiveness of the full risk management program

## Roles and Responsibilities

### The Audit Committee – Its Role in Risk Management

---

- NYSE listing standards mandate that the Audit Committee is responsible for financial risk oversight.
  
- The Audit Committee may or may not take on non-financial risk oversight, depending on structure. Either way:
  - Must be very involved in risk oversight function and risk governance structure
  - Monitor management's risk appetite against approved guidelines
  - Engage in open communication with management as to significant financial risks, including improbable ones
  - Understand how the company uses models, the assumptions made, and the limitations of those models – i.e., ensure management understands the transaction and is not overly reliant on model output
  - Be attuned to "tone at the top" and what it implies for risk taking
  
- Inevitably, more activities will end up on the door of the audit committee; the chair must evaluate what areas, what level of work, and what level of responsibility are appropriate

## Roles and Responsibilities

### The Audit Committee – Its Role in Risk Management – Cont'd

---

#### Current areas of risk focus given the economy:

- Liquidity, access to funding, counterparty risk, debt covenants
  - Stress testing various scenarios related to debt covenants
  - Monitoring financial positions of counterparties
  - Renewal of credit lines and other financial arrangements
- Evaluating incentive compensation plans for effectiveness
  - Does it promote the kind of behavior that is desired
  - Does it help retain your best performers and attract new talent
- Review of critical accounting policies in current environment
  - Goodwill and intangible asset impairments
  - Valuation allowances
  - Fair value accounting and impact on volatility
  - Cost and effectiveness of hedging transactions

## Roles and Responsibilities

### The Audit Committee – Its Role in Risk Management – Cont'd

---

#### Developing Trends and Expectations of Audit Committee:

- Concerned with understanding all forms of risk better
- Communicate information succinctly with more precision and less volume
- Desire an overall risk function within the entity that operates across the organization (i.e., financial, regulatory, operations)
- Not willing to "outsource" risk oversight function to Internal Audit, SOX 404 group, or other group
- As with the full Board, the Audit Committee realizes the stakes are greater than ever

## Roles and Responsibilities

### Internal Audit – Its Role in Risk Management

---

Internal Audit provides assurance that internal controls are in place, are sufficient to mitigate the risk, and working; and that governance processes are adequate.

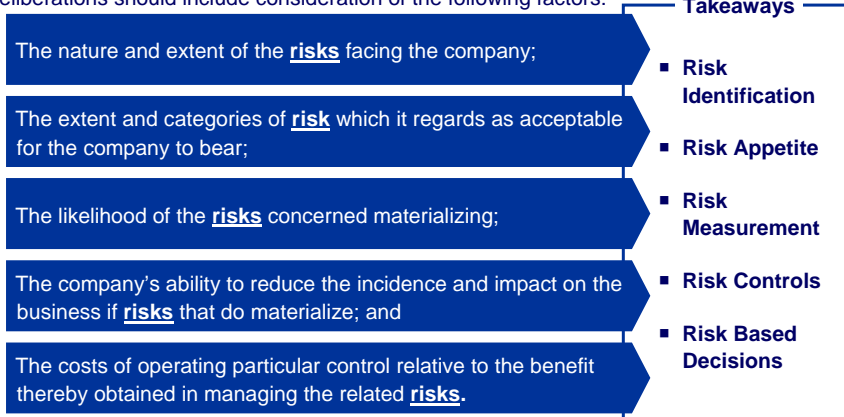
- The Audit Committee (AC) and Internal Audit (IA) are interdependent
  - Internal Audit provides objective opinions, information, support and education to the Audit Committee on risks and internal controls – i.e., IA is "eyes" and "ears" for AC and helps to bridge the span between senior management and the Board
  - The Audit Committee provides validation and oversight to Internal Audit
  - The chairs of each committee should have frequent contact, ideally more frequently than regularly scheduled Audit Committee meetings
  
- Internal Audit aids the Audit Committee in corporate governance with activities to evaluate risk related to:
  - Legal and regulatory compliance
  - Conflicts of interest, unethical behavior, fraudulent activities
  - Internal investigations – e.g., whistleblower hotlines



Governance at Aviva

# Turnbull Guidance

The Aviva PLC Board of Directors is required to implement a risk management and control framework as outlined by the FSA within the Turnbull Guidance. In determining its policies with regard to internal control and assessing a sound system of internal control, the board's deliberations should include consideration of the following factors:



The FSA has extended their control framework to incorporate ERM

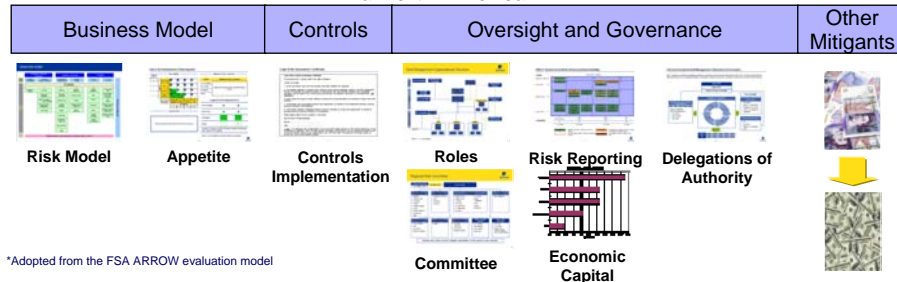


# Aviva PLC Enterprise Risk Management Framework

## Necessary ERM Components\*

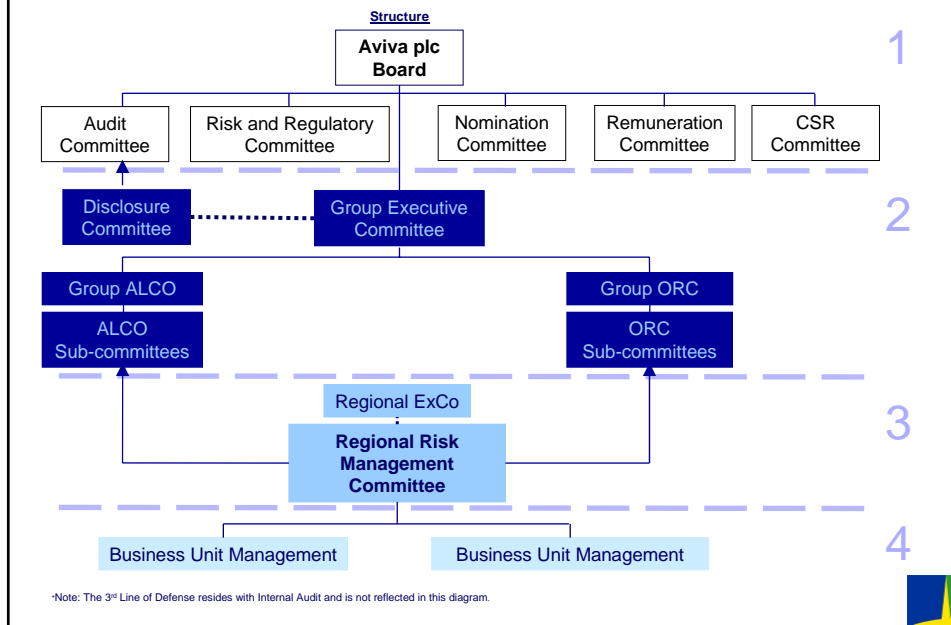
Business Model		Controls	Oversight and Governance			Other Mitigants
Environment Risk	Customers, Products, and Markets	Customers, Products, and Market Controls	Control Functions	Risk Reporting	Management, Governance & Culture	Excess Capital & Liquidity
	Business Process	Financial & Operating Controls				
	Financial & Insurance Risks	Insurance Risk Controls				

## Aviva North America ERM



\*Adopted from the FSA ARROW evaluation model

## Aviva Risk Governance and Oversight Framework



## Governance – Three Lines of Defense

- **1<sup>st</sup> Line of Defense** – Business Unit and Regional Policy Owners responsible mitigating individual risks.
- **2<sup>nd</sup> Line of Defense** – Responsible for an evaluation of the effectiveness of the entire risk management framework.
- **3<sup>rd</sup> Line of Defense** – Responsible for evaluating the effectiveness and accuracy of individual controls through testing.
- **Governance** – Policy owners and risk management work together in committees to make important decisions and understand their risk impact.

The Aviva risk management program depends on Policy owners, Risk Management, and Group audit forming three lines of defense and working together through governance committees.

# Target Operating Model

## Data

- Policy owners and risk communities have access to a data platform containing information on both functional performance and risk across all policies.

## Roles

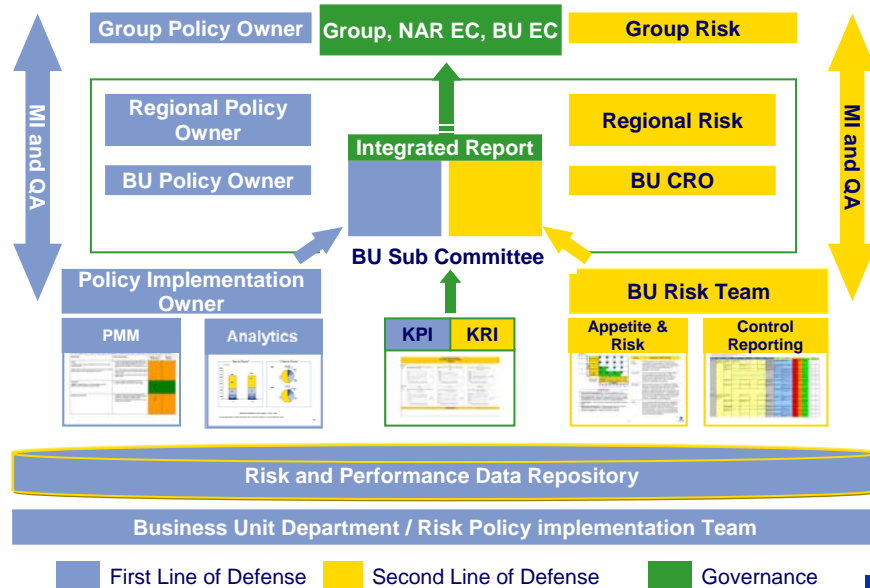
- Business Units and Regional representation responsible for gathering information.
- Management has the ability to challenge those running business and managing risk.

## Committees

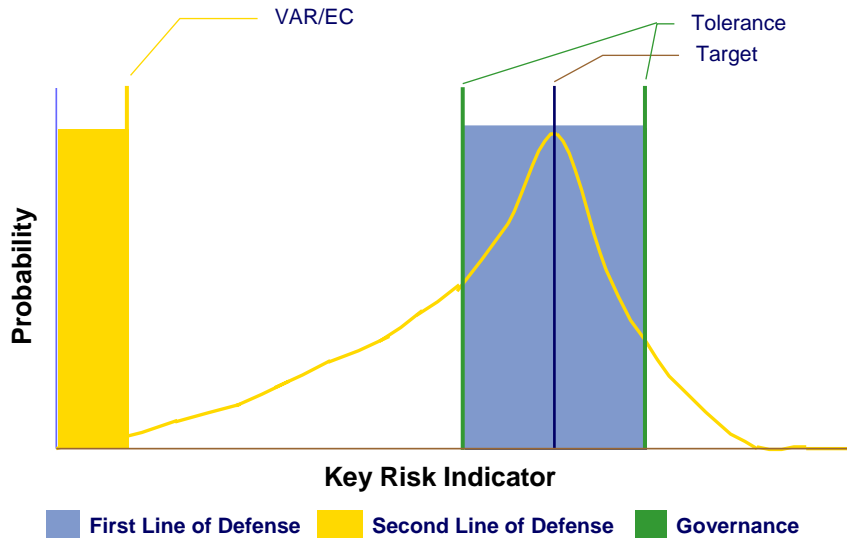
- The risk and performance data is coupled and challenged during committee meetings which use the information to make decisions.
- BU risk committees report to the local risk committee which in turn reports to the executive committees.



# Risk Policy Information Flow



## Analytical Review of policy owner's role



## Distribution of Responsibilities

We have distributed responsibilities for all of our **Risk Procedures** to the different **groups of people** across the **Business Unit and the Region**

Risk Identification Risk Appetite Risk Reporting Controls Corporate Planning Key Risk Indicators Performance Management	Policy Owner	Business Unit
		Region
	Risk Department	Business Unit
		Region
	Committee	Business Unit
		Region

## Distribution of Responsibilities

Risk Appetite	Policy Owner	• <b>BU:</b> Recommends risk tolerance statement and supports assessment with facts
		• <b>Region:</b> Provides oversight on action plans
	Risk Department	• <b>BU:</b> Aggregates risk tolerance to form <b>business unit</b> risk appetite statement
		• <b>Region:</b> Aggregates risk tolerance to form <b>regional risk</b> appetite statement
	Committee	• <b>BU:</b> Approves <b>business unit</b> risk appetite
		• <b>Region:</b> Approves <b>regional</b> risk appetite



Next Steps

## Next Steps

---

### **Implementation or improvement of an ERM program requires key steps to be followed to create a strong foundation.**

- The tone at the top must be established by a strong corporate governance structure that defines board and senior management involvement in the risk management process.
- Clearly stated risk policies must be documented to establish top-down and bottom-up roles and responsibilities around managing risk.
- Information on existing risk programs must be gathered and evaluated to determine how many of the company's current risk practices can be leveraged to create or improve on ERM.
- Creation of a Chief Risk Officer to lead the risk management function and help embed a richer risk culture in the organization.

Due to the complexity and length of time required, companies should start the process now of laying a solid foundation upon which to develop a successful ERM program.

This presentation contains general information only and is based on the experiences and research of Deloitte practitioners. Deloitte is not, by means of this presentation, rendering business, financial, investment, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, "Deloitte" means Deloitte Consulting LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

# Deloitte.

Copyright © 2009 Deloitte Development LLC. All rights reserved.

Member of  
Deloitte Touche Tohmatsu



Actuaries  
Risk is Opportunity®

