



Institute  
and Faculty  
of Actuaries

## The Three Lines of Defence – Where does the CRO's role start and end?

Ciara Regan and Angela McNally

15 November 2013



### Agenda

- **Introductory Remarks**
- **Background and Context**
- **Outlining the 3 LOD model and impact of Solvency II**
- **Challenges with the 3 LOD model and specific challenges for the CRO**
- **Risk culture and the CRO role**
- **Adding value – the role of the CRO**
- **Conclusion**



Institute  
and Faculty  
of Actuaries

15 November 2013

2



Institute  
and Faculty  
of Actuaries

# Introductory Remarks

15 November 2013



## Introductory Remarks

- **Significant changes** have occurred in the whole area of risk governance over the past 10 years
- Insurance has always **been ahead of the curve** relative to other industries
- Risk management existed e.g. **Appointed Actuary** responsibilities but **not** in a **formalised** sense
- Increased recognition of the **importance of risk management** and governance
- **CRO** role, in particular, has been created and/or **elevated** to C-suite
- The relative "newness" of the CRO role and the evolving nature of risk governance has meant that entities' **focus on ensuring clearly defined roles and responsibilities** for various function holders has **not been a priority**
- However, risk governance operating models are now **reaching a stage of maturity** where this is now becoming a priority



Institute  
and Faculty  
of Actuaries

15 November 2013

4

## Introductory Remarks

*"its not enough that various risk and control functions exist – **challenge is to assign specific roles** and to co-ordinate effectively and efficiently among these groups so that there are **neither 'gaps' in controls or unnecessary duplications** in coverage."*



Board and senior management are the primary stakeholders served by the three "lines" of defence. They have responsibility for the governance structures and processes required to achieve an entity's strategic objectives and the **"three" lines of defence is best implemented with support and guidance of governing bodies.**

Source: The three lines of defence in effective risk management and control (IIA – January 2013)

15 November 2013

*"not uncommon to find diverse teams of internal auditors, ERM specialists and other risk and control professionals working together to help their organisations manage risk. Each of these specialities has a unique perspective and specific skills...but **because duties related to risk management and control are increasingly being split across multiple departments and divisions, duties must be coordinated carefully to assure that risk and control processes operate as intended.**"*



Institute  
and Faculty  
of Actuaries

5



Institute  
and Faculty  
of Actuaries

## Background and Context



15 November 2013

## Key Regulatory Drivers of Risk Governance : Historic

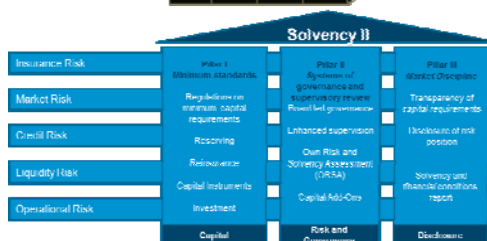
- **Generic guidelines:**

- COSO
- Sarbanes-Oxley
- Combined Code
- ISO 31000



- **ERM in Financial Services:**

- Basel III (Banking)
- Solvency II (Insurance)



- **Other:**

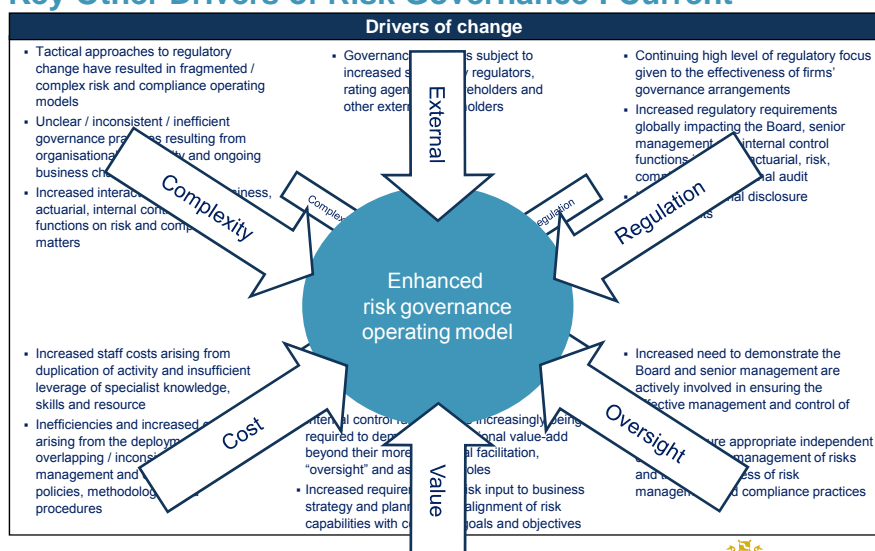
- Walker report



15 November 2013

7

## Key Other Drivers of Risk Governance : Current



15 November 2013

8

## Changing Risk Governance Expectations

### *FSB Thematic Review on Risk Governance (Feb 2013)*

- A more **holistic approach** to risk governance is required
- **Sound risk governance practices recommended** in relation to the **Board** are:
  - Ensuring the independence of the board and the **suitability of it's composition**
  - Consider the **relevant types of skills** the board should possess and the **time** commitment expected
  - Conduct periodic reviews of the **training and skills** needed by Board members
  - Assess if the **level, type and frequency of risk information** provided to the Board enables an **effective discharge of responsibilities**
  - **Communication procedures** should exist between the Risk Committee and the rest of the Board and across Board committees, most importantly audit and finance committees. Cross membership of audit and risk committees is a positive
  - The Board or audit committee should obtain **independent assurance of the design and effectiveness of the risk governance framework on an annual basis**



15 November 2013

9

## Changing Risk Governance Expectations

### *FSB Thematic Review on Risk Governance (Feb 2013)*

- Specific **recommendations in relation to the role of the CRO** include:
- Specific **recommendations in relation to the role of the CRO** include:
- Other recommendations:
  - Actively work to develop the '**risk culture**' of the organisation and **link risk management to performance management objectives**
    - FSB producing report on how to formally assess risk culture
  - Ensure there is an appropriate attitude towards ownership of risk across the firm with the **business lines firmly responsible / accountable for risks** created by their activities
  - Ensure there is an appropriate attitude towards ownership of risk across the firm with the **business lines firmly responsible / accountable for risks** created by their activities



15 November 2013

10

## Changing Risk Governance Expectations

### PRA and FCA regulatory approaches to governance

#### What the PRA is looking for

- Ensure individuals appointed to senior management positions are **competent** to fill such roles
- The **Board** should set **strategy and policies clearly**
- **Clear accountability and delegation** of responsibilities
- **A culture** that supports prudent management
- **Remuneration and incentive structures** should reward careful and prudent management
- The Board should **hold management to account**
- The PRA expects all boards of legal entities within groups to have regard to the PRA's objectives
- **Open dialogue** with the regulator

#### What the FCA is looking for

- Does the firm have the **interests of its customers** and the **integrity** of the market at the heart of how the business is run?
- *"Senior management teams set the culture of their firms, so we test that the strategy and tone set at the top align with good customer outcomes"*

Extract from speech by FCA, on 02/07/2013

Governance is one of the most common areas for PRA and FCA-mandated reviews



Institute and Faculty of Actuaries

15 November 2013

11

## Risk Governance Practices

### Findings from the most recent Deloitte Risk Practices survey

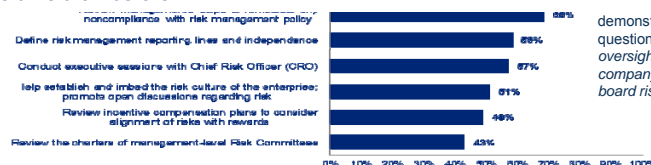
#### Role of the board of directors

- **Regulators** are paying **increased attention to the role of the board of directors** in risk governance, i.e. providing direction to and approval of the institution's risk appetite and risk policy, and overseeing their implementation by management

#### Role of the board of directors

94% of the institutions surveyed said their board of directors devoted **more time to the oversight of risk** compared to five years ago, with 67% saying it committed considerably more time than before

- **Regulators** are paying **increased attention to the role of the board of directors** in risk governance, i.e. providing direction to and approval of the institution's risk appetite and risk policy, and overseeing their implementation by management
- 94% of the institutions surveyed said their board of directors devoted **more time to the oversight of risk** compared to five years ago, with 67% saying it committed considerably more time than before



demonstrates the responses to the question – which of the above risk oversight activities does your company's board of directors or board risk committee(s) perform?

Source: Deloitte global risk management survey, 2013 (86 financial institutions around the globe)



Institute and Faculty of Actuaries

15 November 2013

12

## Risk Governance Practices

### Findings from the most recent Deloitte Risk Practices survey

#### Board risk committees

- Most institutions (62%) **assign primary responsibility to risk oversight to one or more board committees** that oversee risk management, including risk policies and the organisation's risk appetite
- Most common approach adopted by 43% of institutions surveyed is to place the responsibility for risk

#### Incorporating risk management into incentive plans

- Lately, more attention has been paid to the **relationship between compensation plans and risk management** in an effort to help increase alignment between incentive compensation and the institution's risk appetite. As a result, it has become a leading practice to incorporate risk management considerations into performance goals and compensation decisions
- In 2012, 45% of institutions indicated that reviewing the compensation plan to assess its impact on risk appetite was a responsibility of the CRO and the independent risk management function, up from 34% in 2010. More common at large institutions (52%) than at small institutions (29%)
- Lately, more attention has been paid to the **relationship between compensation plans and risk management** in an effort to help increase alignment between incentive compensation and the institution's risk appetite. As a result, it has become a leading practice to incorporate risk management considerations into performance goals and compensation decisions
- In 2012, 45% of institutions indicated that reviewing the compensation plan to assess its impact on risk appetite was a responsibility of the CRO and the independent risk management function, up from 34% in 2010. More common at large institutions (52%) than at small institutions (29%)



Institute  
and Faculty  
of Actuaries

15 November 2013

13

## Risk Governance Practices

### Findings from the most recent Deloitte Risk Practices survey

#### Key role of the CRO

#### Key role of the CRO

- CROs have a **key role** in the organisation with overall responsibility for oversight of risk management – and attention to risk considerations and implement consistent risk management across the organisation
- Most institutions cited a wide range of responsibilities for their CRO and independent risk management group. More than 80% of institutions said these responsibilities included escalating risk issues to the CEO and/or the board of directors, identifying risk concentrations, and identifying new and emerging risks. At many institutions, the CRO and risk management function also have **more strategic responsibilities**, indicating their higher profile in the organisation: assisting in developing the firm-wide risk appetite statement (87%), participating in executive sessions with the board of directors and/or board risk committee (79%), **providing input into business strategy development** and the periodic assessment of the plan (79%), and approving new business or products (63%)
- In the survey, **88% of institutions** reported using a **three lines of defence governance model**, including 97% of large institutions
- Institutions said the biggest challenge they faced in using this governance model was **defining and maintaining the distinction in roles between line 1, the business, and line 2, risk management (45%)**
- Institutions said the biggest challenge they faced in using this governance model was **defining and maintaining the distinction in roles between line 1, the business, and line 2, risk management (45%)**



Institute  
and Faculty  
of Actuaries

15 November 2013

14

## Conclusions and Challenges

- Regulatory change has been at an **unprecedented level** and has driven the introduction of **risk governance operating models** and greatly **enhanced the role of the CRO**
- **The 3 Lines of Defence** model has become the **de facto standard** in risk governance
- Many entities are also **seeking to drive greater efficiencies and 'value add'** from their risk governance model
- These changes present a number of challenges:
  - **Governance:** How do we optimise the overall governance framework to:
    - Ensure the CRO has an important and strategic role
    - Avoid gaps and overlaps in roles and responsibilities
  - **Operating Model:** How do we ensure an operating model is established that helps to be a value creator for the organisation?
  - **People:** How do we optimise the use of resource and leverage the use of specialist skills to improve risk management?
  - **Culture:** How can we embed an appropriate risk culture throughout the organisation?



15 November 2013

15



Institute  
and Faculty  
of Actuaries

## Three lines of defence: Outline & Impact of Solvency II



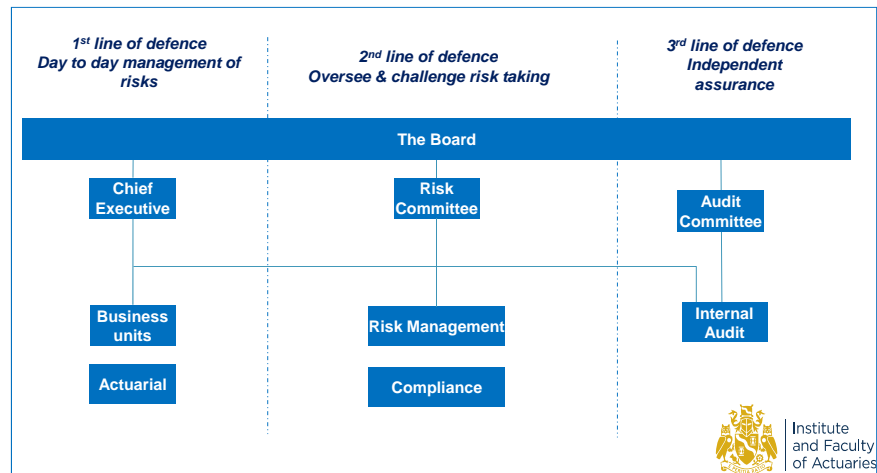
15 November 2013



## Risk governance operating model design : 3LOD

### Key principles

Many financial institutions have adopted the 3LOD principles in relation to the design of their risk governance operating models. Whilst the Solvency II requirements are consistent with these principles some modifications are likely to be required.



15 November 2013

17

## First Line of Defence & Interaction with CRO

### 1st Line: Responsible for owning and managing the risks of the business

#### Key Responsibilities of 1st line

• **Board**, supported by the Risk Committee, sets the firm's **risk appetite** and strategies and **Interaction with CRO, who is responsible for:**

- **Oversight and challenge** of 1st line
- Developing, **training** and maintaining skills required among the **1st line staff** to define, assess and manage their day-to-day risks **effectively and consistently**
- **Communicating to 1st line** the **alignment of the company strategy** with risk management activities
- Ensuring awareness by 1st line (person, section, department) of their role within the company, risks they are facing and how those feed into the overall strategic objectives i.e. risk culture
- **Collecting feedback from the 1st line** and integrating it into the next risk management cycle
- **Communicating to 1st line** the **alignment of the company strategy** with risk management activities
- Ensuring awareness by 1st line (person, section, department) of their role within the company, risks they are facing and how those feed into the overall strategic objectives i.e. risk culture
- **Collecting feedback from the 1st line** and integrating it into the next risk management cycle



15 November 2013

18

## Second Line of Defence

### 2<sup>nd</sup> Line: Responsible for providing expert advice, oversight and challenge

- Responsible for **oversight and challenge of the 1<sup>st</sup> line** in its day to day management, control, monitoring / reporting of risks and **independent of management / personnel responsible for originating risk exposures** :
  - Advises on best **risk management framework** and facilitates its implementation by 1<sup>st</sup> line
  - Ensures 1<sup>st</sup> line risk management **tools and controls** are properly designed and implemented
  - **Assists risk owners** in identifying risks, defining risk exposures, managing risk and risk reporting
  - Constructively **challenges** the actions and decisions of the 1<sup>st</sup> line and assists the 1<sup>st</sup> line in considering risk when making key decisions
  - **Identifies** known and emerging risk issues or shifts in the entity's risk appetite
- Development and delivery of risk education / training across the firm i.e. **risk culture**
- **Close working relationship with 3rd line**
- Development and delivery of risk education / training across the firm i.e. **risk culture**
- **Close working relationship with 3rd line**



Institute  
and Faculty  
of Actuaries

15 November 2013

19

## Third Line of Defence & Interaction with CRO

### 3<sup>rd</sup> Line: Responsible for providing independent assurance on the effectiveness of the overall system of internal control, including risk management and compliance

#### Key Responsibilities of 3<sup>rd</sup> line

- **Audit Committee** supported by the **Internal Audit Function** provides **independent**

#### Interaction with CRO, who is responsible for:

- Ensuring Internal Audit has access to all relevant risk related information
- Co-operating with Internal Audit on aligning the Internal Audit and Risk Management plans with the entity's strategy
- Mutual communication of identified issues, risks, observation and trends in order to ensure that no risks are missed out
- Internal Audit is **independent of both the business and control functions** and reports directly to the Chief Executive (typically) and Audit Committee
- Recommend **improvements** to the design and operation of the ERM and/or internal controls framework
- Mutual communication of identified issues, risks, observation and trends in order to ensure that no risks are missed out

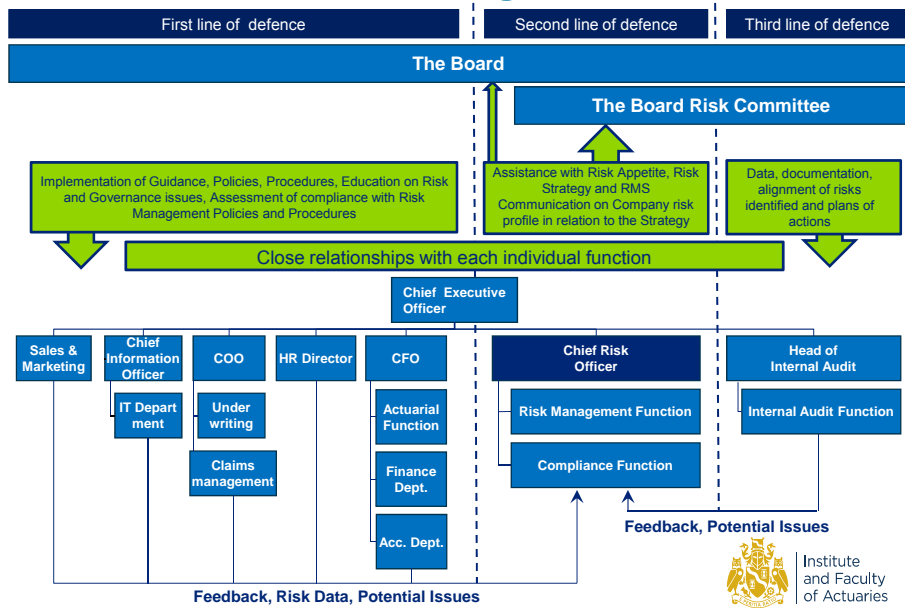


Institute  
and Faculty  
of Actuaries

15 November 2013

20

## Interaction of CRO within the organisation



15 November 2013

21

## Three lines of defence model

### Thick versus Thin operating models



		Model 1: Thick			Model 2: Thin		
Model		1 <sup>st</sup> Line	2 <sup>nd</sup> Line	3 <sup>rd</sup> Line	1 <sup>st</sup> Line	2 <sup>nd</sup> Line	3 <sup>rd</sup> Line
Pros and Cons	Model	1 <sup>st</sup> Line	2 <sup>nd</sup> Line	3 <sup>rd</sup> Line	1 <sup>st</sup> Line	2 <sup>nd</sup> Line	3 <sup>rd</sup> Line
	Pros	Clear segregation of duties. Supports consistency and integration of approaches Facilitates the development of specialist risk functions within the 2nd line.			Supports clear accountability. Enhanced alignment of cost and revenue to risk creation.		
	Cons	Absence of deep business knowledge may result in generic / sub optimal risk management approaches. Greater challenge to segregate conflicting responsibilities within the 2nd line. Potential for disproportionate increase in costs for the 2nd line.			Greater challenge to segregate conflicting responsibilities within the 1st line. Greater potential for inconsistent approaches and reporting. Potential for the 2nd line to be perceived as an 'administrative function' and hence not value adding.		
Pros and Cons	Cons	2nd line. Absence of deep business knowledge may result in generic / sub optimal risk management approaches. Greater challenge to segregate conflicting responsibilities within the 2nd line. Potential for disproportionate increase in costs for the 2nd line.			Greater challenge to segregate conflicting responsibilities within the 1st line. Greater potential for inconsistent approaches and reporting. Potential for the 2nd line to be perceived as an 'administrative function' and hence not value adding.		

15 November 2013

22

## How has Solvency II impacted the 3LOD model?

### Risk (2<sup>nd</sup> line) and Actuarial (1<sup>st</sup> line) functions

Risk function role includes:	Actuarial function role includes:
<ul style="list-style-type: none"> <li>Defining and documenting the risk management strategy, including objectives, key principles, risk appetite and assignment of responsibilities.</li> <li>Assisting the effective operation of an overall risk management system</li> </ul>	<ul style="list-style-type: none"> <li>Coordinating the calculation of technical provisions</li> <li>Ensuring the appropriateness of the methodologies and underlying models used and assumptions made in the calculation of technical provisions</li> </ul>
Risk function role includes:	Actuarial function role includes:
<ul style="list-style-type: none"> <li><b>Designing, documenting, testing, validating and implementing the internal model</b></li> <li><b>Integrating the internal model into the internal risk management system</b></li> <li><b>Analysing and reporting on internal model performance, suggesting areas needing improvement</b></li> </ul>	<ul style="list-style-type: none"> <li><b>Contributing to the implementation of an effective risk management system, including the risk modelling underling the calculation of capital requirements and the 'Own Risk Solvency Assessment'</b></li> </ul>
<ul style="list-style-type: none"> <li>Analysing and reporting on internal model performance, suggesting areas needing improvement</li> </ul>	Assessment



Institute  
and Faculty  
of Actuaries

15 November 2013

23

## How has Solvency II impacted the 3LOD model?

### Compliance (2<sup>nd</sup> line) and Internal Audit (3<sup>rd</sup> line) functions

Compliance function role includes:	Internal Audit function role includes:
<ul style="list-style-type: none"> <li>Ensuring all actions of the firm comply with applicable laws and regulatory requirements</li> <li>Identifying, assessing, monitoring and reporting the firm's compliance risk exposures</li> <li>Assessing the possible impact of significant changes in the legal environment that well as compliance risks ar</li> <li>Monitoring projected revisi introduce new regulation a and asses their potential in</li> <li>Assessing the appropriater procedures and guidelines deficiencies and making su</li> <li>Promptly escalating major Board</li> </ul>	<ul style="list-style-type: none"> <li><b>Evaluating the adequacy and effectiveness of the internal controls and all other elements of the system of governance, as well as compliance with internal strategies, policies, processes and reporting procedures</b></li> </ul>
	<p><b>Internal Audit function role includes:</b></p> <ul style="list-style-type: none"> <li><b>Evaluating the adequacy and effectiveness of the internal controls and all other elements of the system of governance, as well as compliance with internal strategies, policies, processes and reporting procedures</b></li> </ul> <p>ommendations arising from the any deficiencies with regard</p> <p>itability of the internal control</p> <p>mal policies, procedures and</p> <p>p procedures for the closure</p> <p>ting out the work to be undertaken in the upcoming business year(s) for approval by the Board</p> <ul style="list-style-type: none"> <li>Reporting to management and the Board on the performance of Internal Audit function</li> </ul>



Institute  
and Faculty  
of Actuaries

15 November 2013

24

## 3LOD & the Solvency II Governance Model

*Whilst the key principles of the 3 Lines of Defence model have been widely adopted, firms have tailored their approaches, resulting in differing allocations of responsibilities. As there is no single solution to the allocation of risk management responsibilities across a group or a single entity and a range of potential options exist.*

### Key considerations include:

- The overall **operating philosophy** of the group or entity (e.g. thick versus thin approach)
- The availability of **specialist resource** and / or the need to optimise the use of specialist resource e.g. actuarial
- The **maturity** of the various risk management practices
- The need for specific and **sophisticated risk management approaches** that are more closely aligned to the nature and complexity of a given business
- The **level of independence required** in relation to the assignment of potentially conflicting roles e.g. the design and development of risk models versus their validation

**Solvency II compliant governance frameworks** also need to address a number of other key matters including:

- The Board, senior management and other staff have the **requisite skills and experience** to discharge their (new) responsibilities effectively; and
- **Ensuring changes** required to the governance arrangements are appropriately **embedded** and can be **evidenced** in operation as part of the firm's internal model application process



15 November 2013

25



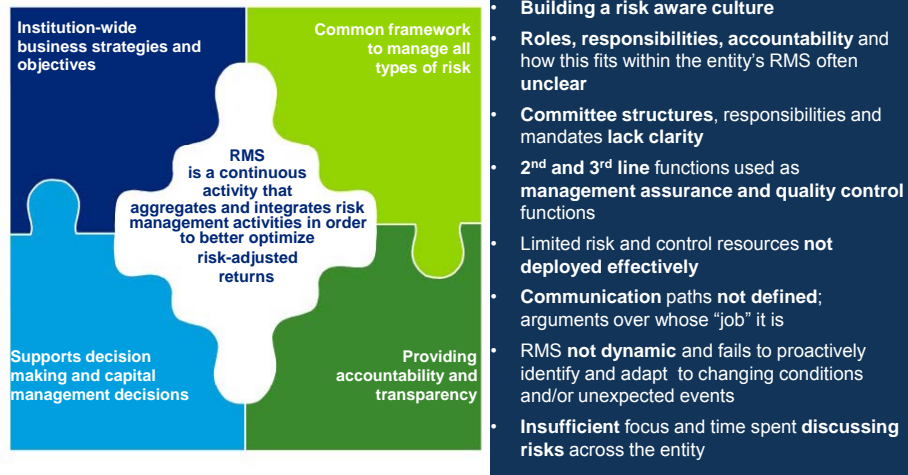
Institute  
and Faculty  
of Actuaries

## Challenges: Three lines of defence model & Role of CRO



15 November 2013

## Risk Governance: Key Challenges



Institute  
and Faculty  
of Actuaries

15 November 2013

27

## CRO & Other Roles: Key Challenges

- Overall, **clarity on the roles and responsibilities** of
  - each line of defence; and
  - each function within individual lines**is crucial**
- **Specific challenges for CROs** in terms of their roles and responsibilities include:
  - Dual Role or "Dual-hatting" CROs
  - Conflicts of interest
  - The Actuary as CRO



Institute  
and Faculty  
of Actuaries

15 November 2013

28

## Clarity of Roles – General

- For the 3 lines of defence model to work effectively, **each individual business unit / function must understand their role and responsibilities**
- **Collaboration between the lines** is required but lack of a clear mandate can mean some risks 'fall through the gaps' or there is unnecessary overlap between functions
- Where 1<sup>st</sup> line functions perform some oversight functions (e.g. the Actuarial Function), you **must clearly distinguish between 1<sup>st</sup> line activities and 1<sup>st</sup> line resources doing 2<sup>nd</sup> line activities**:
  - **Independence** must be clearly demonstrated and documented
  - The **biggest challenge** institutions face in using the 3 LOD model is *defining and maintaining the distinction between roles in the first and second line (Deloitte Risk Practices Survey 2012)*
- **Role definition** can be assisted by:
  - Having a **clear policy** for each function / role setting out roles and responsibilities
  - **Accountability for risk management** being included in **1<sup>st</sup> line performance** appraisal
  - Ensure that **no responsibilities** are **delegated to Internal Audit** that could **compromise** their **independent** oversight function



15 November 2013

29

## Clarity of Roles – Risk Function & CRO

- It is particularly important for there to be clarity on the **role of the Risk Management Function**
- Risk management must be seen as an **imperative for the whole firm** and not just the responsibility of the Risk Management Function
- **1<sup>st</sup> line must take ownership for risk management** – this cannot be seen as a 2<sup>nd</sup> line activity
- Risk management must be seen as **more than just about regulatory compliance**
- An appropriate **risk culture** must be modelled by all key executives and the Board
- The CRO must also ensure:
  - They have the **required profile** throughout the business and are viewed as a **peer with the rest of the 'C suite'**
  - **Direct reporting line to the CEO is preferred**
  - Reporting to the **Board Risk Committee**



15 November 2013

30

## Clarity of Roles – Actuarial Function

- Where do **specialist functions** like Actuarial sit – in the **1<sup>st</sup> or 2<sup>nd</sup> line**?
- If the Actuarial Function straddles the 1<sup>st</sup> and 2<sup>nd</sup> line in terms of the activities it carries out, then **responsibilities and reporting lines must be very clear**
- Where the actuarial function is 1<sup>st</sup> line, the Risk Management Function must have the **necessary expertise** to adequately oversee them
  - Must be able to demonstrate objective review and **skilled challenge** of key decisions
- For actuaries in the **1<sup>st</sup> line** doing **2<sup>nd</sup> line activities**, **accountability** rests with the **CRO**
- Actuarial may provide **management information and processes** to support the 1<sup>st</sup> line in **evaluating risk**, while also providing oversight and challenge to business units (e.g. providing opinions on the underwriting policy)
  - Must **collaborate and communicate with the 2<sup>nd</sup> line** to ensure no overlaps



15 November 2013

31

## Clarity of Roles – Ownership of the Internal Model

- **Ownership of the Internal Model** presents particular difficulties under the 3 lines of defence model. Under Solvency II:
  - **Risk Function** must ensure the effective design, implementation, testing, validation and documentation of the Internal Model
  - **Actuarial Function** also has specific responsibilities:
    - *Ensuring the appropriateness of the methodologies, models and assumptions*
    - *Data sufficiency and quality*
    - *Opinion on underwriting and reinsurance*
- If both **Risk and Actuarial are involved in developing the model**, **who will validate it?**
  - **Separate** people in the Risk Function
  - **Internal Audit?**
    - *Could create a conflict when it comes to reviewing controls later*
  - **External validation**



15 November 2013

32



## Role Interaction between CRO & Chief Actuary

Duties	CRO	Chief Actuary
Risk Management	Oversight of firm wide risk management systems and control	<ul style="list-style-type: none"> <li>Contributes to the effective implementation of the risk management system</li> <li>Opines on underwriting and reinsurance policy</li> <li>Ensures the appropriateness of the methodologies, models and assumptions used in the calculation of technical provisions</li> </ul>
Internal Model	Ensures the effective design, implementation, testing validation and documentation of the Internal Model	Ensures the appropriateness of the methodologies, models and assumptions used in the Internal Model
Risk MI	Ensures adequacy of risk MI and analysis	Production of actuarial aspects of risk reporting and MI
Risk Appetite vs. Risk Profile	Monitors and reports on risk appetite vs. risk profile	Assists in monitoring risk appetite vs. risk profile by: <ul style="list-style-type: none"> <li>Advising management on the risks the firm runs and the required capital</li> <li>Monitoring and reporting on those risks</li> <li>Escalating if there are any material concerns or if risk appetite / limits are likely to be breached</li> </ul>
Business Strategy	Challenges the business strategy	Assists in the production and challenge of the business strategy



Institute  
and Faculty  
of Actuaries

15 November 2013

33

## Dual Role CROs – Chief Actuary & CRO

- Clearly there is **potential overlap between the two roles**; this can create efficiencies but also may lead to conflicts of interest where roles are not well defined
  - Example: Actuarial function must express an opinion on the Reinsurance Policy but this may be set by the Risk Management Function*
- Appointed Actuary & CRO**; in some cases, actuarial function **does not report** to the Appointed Actuary (Ireland); **entity size** not always a factor
- Firms must be able to demonstrate that **any conflicts of interest** arising are **formally acknowledged, managed and mitigated** and that individual has **capacity and skills** to "dual-hat"
- Actuarial function may also perform other roles outside those outlined in Solvency II (**e.g. pricing**) which can create further conflicts
- Even within the 2<sup>nd</sup> line, independence within the structure is important**, for example, if an internal model is used different people should be responsible for:
  - Designing and implementing the model*
  - Testing and validating the model.*



Institute  
and Faculty  
of Actuaries

15 November 2013

34

## Dual Role CROs – Compliance & Other

### CRO and Head of Compliance Function

- **Natural fit** between these roles?
  - CRO may be Head of Compliance or the Head of Compliance may report to the CRO
  - May avoid duplication of operational controls
  - **Integrated approach can lead to better risk management**
- **Danger** that the CRO is **seen** as being **narrowly responsible for regulatory compliance** diminishing overall effectiveness unless separate compliance and risk teams report into CRO

### CRO and Other Roles

- Key question: **Is performance based on measures that could conflict with the risk and control duties of the CRO?**
- If so, **how is this conflict addressed** and the **integrity** of the 3 lines of defence maintained
  - CRO and Head of Pricing?



15 November 2013

35

## Conflict of Interest Checklist

Question	Check
What could go wrong?	✓
How much would such an event cost to rectify?	✓
Are there vested interests materially conflicting with responsibilities?	✓
Is there a misalignment between performance measurement / remuneration and responsibilities?	✓
Are the personnel responsible subject to professionalism requirements e.g. code of conduct?	✓
Are there executive / Board oversight committees in place?	✓
Is periodic external review in place?	✓
Could the entity define the conflict of interest if issues arise?	✓
Would the structure withstand regulator or media scrutiny?	✓
What would be the cost of full segregation of duties?	✓

Source: Society of Actuaries in Ireland



15 November 2013

36

## The Actuary as CRO

- Actuaries (or the actuarial function) have in reality been the financial risk function in (re)insurance companies for many years
- **Are actuaries the natural CROs for (re)insurers?**
- A wide understanding of the business and a range of risks is required.

### Advantages

- Strong understanding of **financial risk**
- Technical understanding of **insurance risk**
- Technical understanding of the **Internal Model**
- Strong understanding of the business typically
- **Actuarial training** gives a broad view of the risks insurers face and a **framework for analysing those risks**
- Experience of communicating complex concepts to non-experts.



15 November 2013

37

## The Actuary as CRO

### Challenges

- May **overly focus on what they know (i.e. financial risk)** at that expense of other risks (e.g. operational)
- CRO role is as much **qualitative as quantitative**
  - Must appreciate the limits of quantitative models (focus of CRO is on tail risk)
- Management of risk is about **processes and controls**
- **Management skills** – managing risks / areas in which you are not an expert
- **Excellent communication and relationship management** skills – wider range of stakeholders
  - High level of visibility required.



15 November 2013

38

## CRO Role – Your “ideal” CRO

### Key Attributes

- Understands the (re)insurer's **business strategy and plans**
- Understands **how the business operates**
- Understands the **role of each function within the business** and how each **function interacts**
- Must have a **similar level of cross-functional knowledge as the CEO** – this is different to all other functions / roles
- Must be **strong at communicating** and **building relationships**, whilst maintaining independence
- Must be **credible** to all parties to enable working across cross-functional lines
- Must be **technically competent**



15 November 2013

39



Institute  
and Faculty  
of Actuaries

## Risk Culture: Importance & role of CRO



15 November 2013

## Characteristics / Benefits of Risk Intelligent Culture

“For me, it is a red flag when I see communication lines being controlled in an organisation”

(Source: HP Executive, *The Intoxication of Power – Leadership and Hubris*, Cambridge Judge Business School and DePaulus Trust Conference 19 September 2013)

### Characteristics



### Benefits

More effective management of risk

Improved risk based decision making throughout the organisation

Increased confidence of external stakeholders, including investors, analysts, rating agencies, the government and regulators

Enhanced credit ratings

Compliance with regulatory requirements



Institute  
and Faculty  
of Actuaries

15 November 2013

41

## How CRO can influence Risk Culture?

Understand  
current risk  
culture

Define “target risk  
culture”

Develop a change  
management plan

Implement the  
plan and assess  
results

- Identify and address gaps in competences
- Provide input into the recruitment and on-boarding
- Facilitate sharing of Risk Knowledge
- Deliver consistent risk-based thought leadership

- Appropriate risk taking rewarded
- Performance management linked to risk taking
- Risk Owners are aware of their roles and responsibilities
- Financial incentives in terms of Risk Capital Allocation



- Ensure that people understand how Risk Management ties in with company strategy and objectives
- Project consistent “tone at the top”
- Clarity of direction and structure

- Consistent approach to communication
- Encourage and lead by example in collaboration between functions and departments
- Positive response to constructive criticism
- Clear management expectations



Institute  
and Faculty  
of Actuaries

15 November 2013

42

## Evolution of Risk Culture

A focused assessment is needed to fully understand an organisation's operating culture with respect to risk and to track progress in evolving the values, beliefs and expected behaviours regarding risk



November 15, 2013

Barnett Waddingham 43

## Risk Culture and Practices Maturity Model

### Maturity levels

**“Unaware”** It is a characteristic of the processes/practices at this level that they are either non existent, not implemented and/or not commonly/clearly defined. There is also a lack of formality regarding risk processes and the enterprise is not conscious or understanding of their importance

### Maturity levels

**“Unaware”** It is a characteristic of the processes/practices at this level that they are either non existent, not implemented and/or not commonly/clearly defined. There is also a lack of formality regarding risk processes and the enterprise is not conscious or understanding of their importance

**Optimised** It is a characteristic of the processes/practices at this level that they be well entrenched in business as usual, and that the focus be on continually improving them. The processes/practices are at the optimum level and enterprise is able to sustain and/or strengthen them

**Optimised** It is a characteristic of the processes/practices at this level that they be well entrenched in business as usual, and that the focus be on continually improving them. The processes/practices are at the optimum level and enterprise is able to sustain and/or strengthen them



15 November 2013

44



Institute  
and Faculty  
of Actuaries

# Risk Governance: Adding value – the role of the CRO

15 November 2013

## Adding value – the role of the CRO

- Solvency II has shifted the focus and **risk is now centre stage in the strategic management of the organisation**
- Goal for the CRO should be for **risk to be seen as a source of competitive advantage**
  - Will help to ensure risk has a high profile and 1<sup>st</sup> line business units are bought in
- To achieve this the CRO must have an **active role in strategic decision making**, they must provide a forward looking risk perspective **working in collaboration with their 'C suite' peers**
- A good Risk Management Function should complement the activities of the 1<sup>st</sup> line, it should be seen **not (just) as an enforcer but as a trusted advisor and enabler of best practice**
- Risk management should be a **'centre of excellence'** advising line management on the most appropriate risk framework and tools.
- CRO should be an **enabler** of change in the **risk culture**



Institute  
and Faculty  
of Actuaries

15 November 2013

46

## Adding value – the role of the CRO

- There are a number of **key relationships that a CRO must cultivate** in order to be effective. These include those with:
  - Actuarial Function
  - Finance Function (and CFO)
  - Compliance (if a separate function)
  - Internal Audit
  - CEO
  - Board (Risk Committee)
- **Strong relationships** between all parties with risk management responsibilities (everyone!) **improves the effectiveness** of the risk management system and reduces cost
- In many cases, **several functions will be involved in 'risk management'** of a particular business process.



15 November 2013

47

## Adding value – the role of the CRO

### Example: Underwriting

- **Risk Management Function:** analyses the impact of underwriting on the company's overall risk situation
- **Actuarial Function:** considers the interdependencies between the underwriting acceptance policy and reinsurance
- **Internal Audit Function:** considers the effectiveness of internal control system around the underwriting process
- Regular exchange of information is required to ensure **consistent communication**
- Where all of the functions work together, this can induce a **positive feedback loop** improving overall risk management.



15 November 2013

48





Institute  
and Faculty  
of Actuaries

# Getting Risk Governance Right: Conclusion



15 November 2013

## Risk governance systems are strongest when...

- **Clearly defined** lines of defence (LOD) and risk governance framework
- Each LOD is **supported by appropriate policies and role definitions**
- **Proper coordination** between LOD ensures efficiency and effectiveness
- LOD **not combined** in such a manner to compromise their effectiveness i.e. *"conflicts of interest"* are managed
- Strong risk awareness culture, philosophy and **"tone at top"** – risks managed through changing situations
- Clear view that its **risk is managed by the first line**
- Strong internal **cross functional relationships**
- CRO role is important, **proactive** (e.g. involved in strategic planning) and **reports to CEO**
- **Alignment** of risk appetite, limits, understanding, behaviours and incentives
- **Informative, responsive, timely and frequent** risk measurement, management and reporting



Institute  
and Faculty  
of Actuaries

15 November 2013

50



Institute  
and Faculty  
of Actuaries

# Questions ?



15 November 2013