Society of Actuaries in Ireland

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

08.05.14

Angela McNally, Sinéad Kiernan and Anlo Taylor

Agenda

- **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**

Background

Introductory Remarks

- **Significant changes** have occurred in the whole area of risk governance over the past 10 years, driven by regulation

- 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**

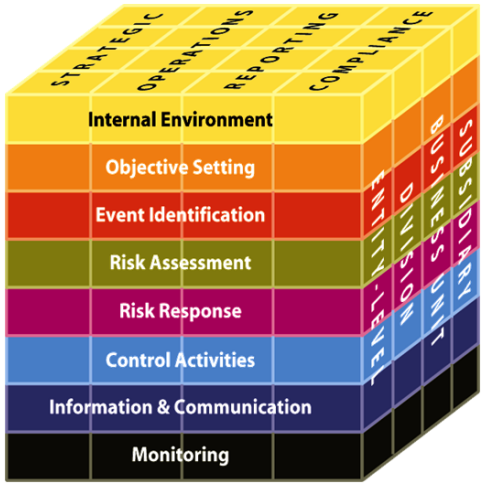
- However, risk governance operating models are now **reaching a stage of maturity** where this is now becoming a priority

- *"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."*

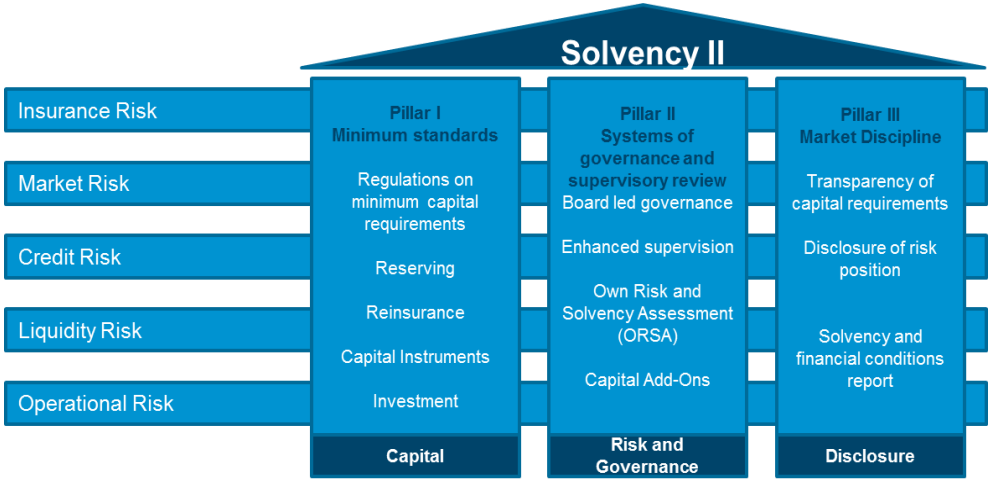
Source: The three lines of defence in effective risk management and control (IIA – January 2013)

Key Regulatory Drivers of Risk Governance : Historic

- **Generic guidelines:**
  - COSO
  - ISO 31000



- **Financial Services Regulation :**
  - Irish Corporate Governance Code
  - UK Corporate Governance Code
  - Basel III (Banking)
  - Solvency II (Insurance)

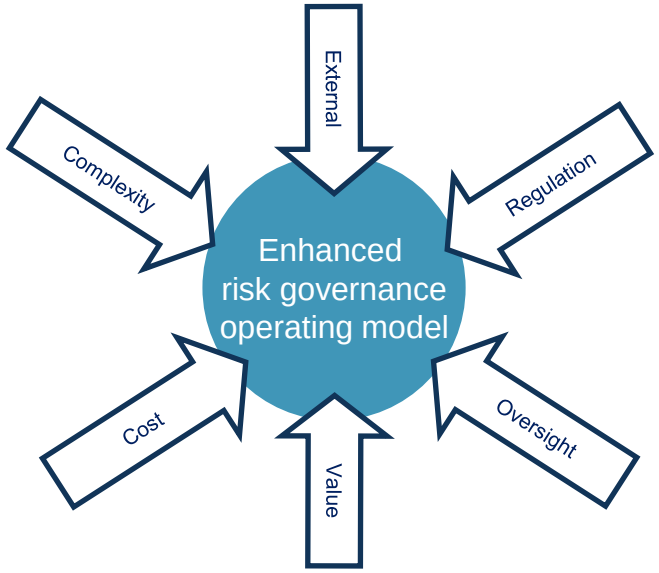


- **Other:**
  - Walker report
  - Sarbanes-Oxley

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 its composition**
  - 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



  - The Board or audit committee should obtain **independent assurance of the design and effectiveness of the risk governance framework on an annual basis**

Changing Risk Governance Expectations

FSB Thematic Review on Risk Governance (Feb 2013)

- Specific **recommendations in relation to the role of the CRO** include:
  - Ensuring the CRO role has an **appropriate level of authority and independence**
  - **Risk committee** should **review performance** and objectives of the CRO
  - CRO should have **unfettered access to the Board and Risk Committee** including meeting periodically with INEDs and NEDs
  - CRO should have **direct reporting line to CEO** and have a **distinct role** from other executive functions and business line responsibilities (**no dual-hatting**)
  - CRO **involved in decisions** and activities from a risk perspective that may **impact the firms risk profile** including strategic planning and M&A
- Other recommendations:
  - Actively work to develop the **'risk culture' of the organisation** and **link risk management to performance management objectives**
  - 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

CRO & Corporate Governance Code (2013)

CRO role:

- The CRO role will be **mandatory** but, it may be filled by another PCF for non-High Impact firms or by the Chief Actuary for a High Impact firm.
- The CRO will have sufficient **seniority** and **independence** to challenge decisions that affect risk profile.
- The Code suggests that the CRO has a role in promoting a strong **risk culture**.
- Responsible for facilitating the setting of the **risk appetite** by the board.
- The CRO provides **risk information** to board and report to the board risk committee. Responsible for maintaining processes to **monitor and report risks**.
- The CRO's primary responsibility is to the board.

Risk Governance Practices

Findings from the most recent Deloitte Risk Practices survey

Key role of the CRO

- **88% of institutions** reported **using a three lines of defence governance model.**
- The biggest challenge in using this governance model was **defining and maintaining the distinction in roles between line 1, the business, and line 2, risk management (45%).**
- **CRO can play a key role** as a senior executive with overall responsibility for oversight of risk management.
- **CRO reports to the CEO** at 71% of the institutions surveyed, while reporting to the board of directors or a board committee at 43%.
- Having the **CRO report to the board of directors** as well as to management is considered a best practice. However, 50% said CRO did not report to the board.
- Most institutions cited a **wide range of responsibilities** for their CRO which included escalating risks, identifying risk concentrations and identifying new and emerging risks.
- The CRO and risk management function also have **more strategic responsibilities**. For example, assisting the risk appetite statement, participating in executive sessions, providing input into business strategy and approving new business or products.

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.
- Optimising the effectiveness of this model presents some challenges in defining the CRO role:
  - Avoid **gaps and overlaps** in roles and responsibilities
  - Ensure the CRO has an **important and strategic** role
  - How do we **add value** through the CRO role?
  - How can the CRO foster an **appropriate risk culture?**

Three lines of defence:
Outline & Impact of Solvency II

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.

Three lines of defence model

Thick versus Thin operating models

Characteristics	1st Line	2nd Line	3rd Line
Risk appetite & strategy & Risk management policy	• Executes • **Monitors execution**	• Defines and develops policies • Oversees approval • **Monitors execution** • **Monitors**	• Testing embedding • Testing adherence
Risk management methodologies	• **Develops detailed methodologies** • Executes methodology (implements controls) • **Manages risk IT systems**	• Designs • Identifies • Oversees approval • Monitors execution • Shares good practice • **Manages risk IT systems** • **Develops detailed methodologies** • **Monitors**	• Tests controls (design & operating effectiveness) • Tests execution
Risk management reporting	• Executes • **Develops** • **Monitors data** • **Monitors profile**	• Designs • Oversees approval • Executes • Monitors • **Develops**	• Tests framework implementation
Risk capital calculation & allocations	• **Builds calculation & allocation tool** • **Executes**	• Designs • Oversees approval • Monitors • **Builds calculation & allocation tool** • **Executes**	• Tests • Model validation

General to both models **Thin Model** **Thick Model**

Three lines of defence model

Thick versus Thin operating models

Thick Model	Thin Model
Pros ▪ Clear segregation of duties. ▪ Supports consistency and integration of approaches. ▪ Facilitates the development of specialist risk functions within the 2nd line.	**Pros** ▪ 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 cost for the 2nd line.	**Cons** ▪ 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. ▪ Risk of Silo Approach.

3LOD 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

How has Solvency II impacted the 3LOD model?

Risk (2nd line) and Actuarial (1st line) functions

Risk function role includes:	Actuarial function role includes:
▪ Defining and documenting the risk management strategy ▪ Assisting the effective operation of an overall risk management system ▪ Monitoring the risk management system ▪ Maintaining a firm-wide and aggregated view of the risk profile ▪ Reporting on risk exposures and risk management matters Internal Model ▪ **Designing, documenting, testing, validating and implementing the internal model** ▪ **Integrating the internal model into the internal risk management system** ▪ **Analysing and reporting on internal model performance, suggesting areas needing improvement**	Technical provisions ▪ Coordinating the calculation ▪ Ensuring the appropriateness of the methodologies and assumptions ▪ Assessing the sufficiency and quality of data ▪ Comparing best estimates against experience ▪ Overseeing the calculation of technical provisions and reporting to the Board on their reliability and adequacy Other ▪ Opining and reporting on the overall underwriting policy and adequacy of reinsurance arrangements ▪ **Contributing to the implementation of an effective risk management system, including the risk modelling underlying the calculation of capital requirements and the 'Own Risk Solvency Assessment'**

How has Solvency II impacted the 3LOD model?

Compliance (2nd line) and Internal Audit (3rd line) functions

Compliance function role includes:	Internal Audit function role includes:
▪ Ensuring the firm complies with laws and regulations ▪ Managing the firm's compliance risk exposures ▪ Monitoring and assessing the impact of potential new regulations ▪ Assessing the appropriateness of the compliance procedures and guidelines ▪ Promptly escalating major compliance problems to the Board	▪ **Evaluating the adequacy and effectiveness of the internal controls and of the system of governance, as well as compliance with policies, processes and reporting procedures** ▪ Reporting findings and recommendations arsing from the work undertaken ▪ Ensuring adequate follow up procedures for the closure of any remedial actions ▪ Preparing an annual audit plan for approval by the Board ▪ Reporting to management and the Board on the performance of Internal Audit function

The 3rd Line of Defence

Third Line of Defense = Internal Audit

Definitions

Third Line of Defence ≠ Functions that provide independent assurance

Internal auditors provide the Board and senior management with comprehensive assurance based on the **highest level of independence and objectivity within the organization.**

Provides assurance on the effectiveness of governance, risk management, and internal controls, including the manner in which the **first and second lines of defence** achieve risk management and control objectives.

Definition of Internal Auditing

(Per Institute of Internal Auditors('IIA'))

Internal auditing is an **independent, objective** assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to **evaluate and improve** the effectiveness of **risk management, control, and governance processes**.

Third Line of Defense

Scope of Assurance

Range of objectives	All elements of risk management & internal control framework	The overall entity
✓ Efficiency and effectiveness of operations ✓ Safeguarding of assets ✓ Reliability and integrity of reporting processes ✓ Compliance with laws, regulations, policies, procedures, and contracts	✓ Internal control environment ✓ All elements of an risk management framework i.e., risk identification, risk assessment, and response ✓ Information and communication ✓ Monitoring	✓ Divisions, subsidiaries, operating units ✓ Functions, including supporting functions ✓ Business processes

Reported to Board & senior management

Coordinating the 3 Lines of Defense

Role	1st Line	2nd Line	3rd Line
	Own & manage risk = Operating management	**Control & Compliance** • Maintaining & monitoring risk management system • Implementing risk management framework & policies • Limited independence • Reporting line to Management & Risk Committee	**Risk Assurance** • Internal audit • Greatest independence • Reports to Audit Committee

Under IIA Standards, required to "share information & coordinate activities with other **internal & external providers of assurance & consulting services** to ensure proper coverage & minimize duplication of efforts."

RECOMMENDED PRACTICES (IIA – Jan 2013): :

- Risk and control processes **structured** along 3 LOD model.
- Each line of defence supported by appropriate **policies & role definitions**.
- Proper coordination among separate LODs to foster efficiency & effectiveness.
- Risk and control functions operating at the different lines should appropriately **share knowledge** and information to assist all functions in better accomplishing their roles in an efficient manner.
- Lines of defence **not be combined/coordinated** in manner that compromises their effectiveness.

Interaction between 2nd & 3rd Lines of Defense

Balance	CRO	Internal Audit
	CRO can never provide 'independence' of IA	IA can never support business to the same extent as CRO can IA carries out assessment of Risk Management

Risk Management output
- Risk Register (with documented controls)
- Periodic Risk Reports
- Incident reports

Internal Audit input
- Annual Audit Plan & periodic updates:
  - Audit universe
  - Residual risk ratings – design & operating effectiveness
- Out of course assurance & consulting engagements
- Engagement risk assessment & scope definition

IA output
- Assurance engagement reports
- Consulting engagement reports

Risk Management input
- Periodic review and update of Risk Registers & risk ratings
- Bottom up and Top Down risk assessments

Corporate Governance Code
- Audit Committee & Risk Committee shall have at least 1 shared member
- No Single individual may hold position of Chairman of Audit Committee and Risk Committee simultaneously

What regulations & standards impact Internal Audit functions

Regulation/ Standard	Impact
IIA Standards	'Self regulation'
IIA recommendations for Financial Services Internal Audit	• Enhance independence & impact of IA • Broaden scope of IA
SII requirements & CBI guidelines	Legalise IA requirement – 'key function'
Fit & Proper requirements	PCF role
Corporate Governance Code	Legalise IA requirement – 'key control function'
Reserving Requirements for Non-Life Insurers and Non-Life & Life Reinsurers (CP73)	IA assessment of reserving process

2014 Hot topics for Internal Audit in Insurance

Business leadership

- ✓ **Governance**: Shift from testing compliance with codes and regulations, to assessing the IMPACT of governance activities in practice
- ✓ **Culture**: Organisations will need to move towards clearly stated values, with reinforcing incentive cultures

Risk Management

- ✓ **Risk Appetite**: Assess whether risk appetite framework properly established, embedded & enforced
- ✓ **Third Party Risk Management**: Assess effectiveness of approach to third-party risk management and assurance frameworks over outsourced activities
- ✓ **Model Risk Management**: IA should have framework for providing assurance over modelling governance & management, including having access to the quantitative skills for assessing models themselves.

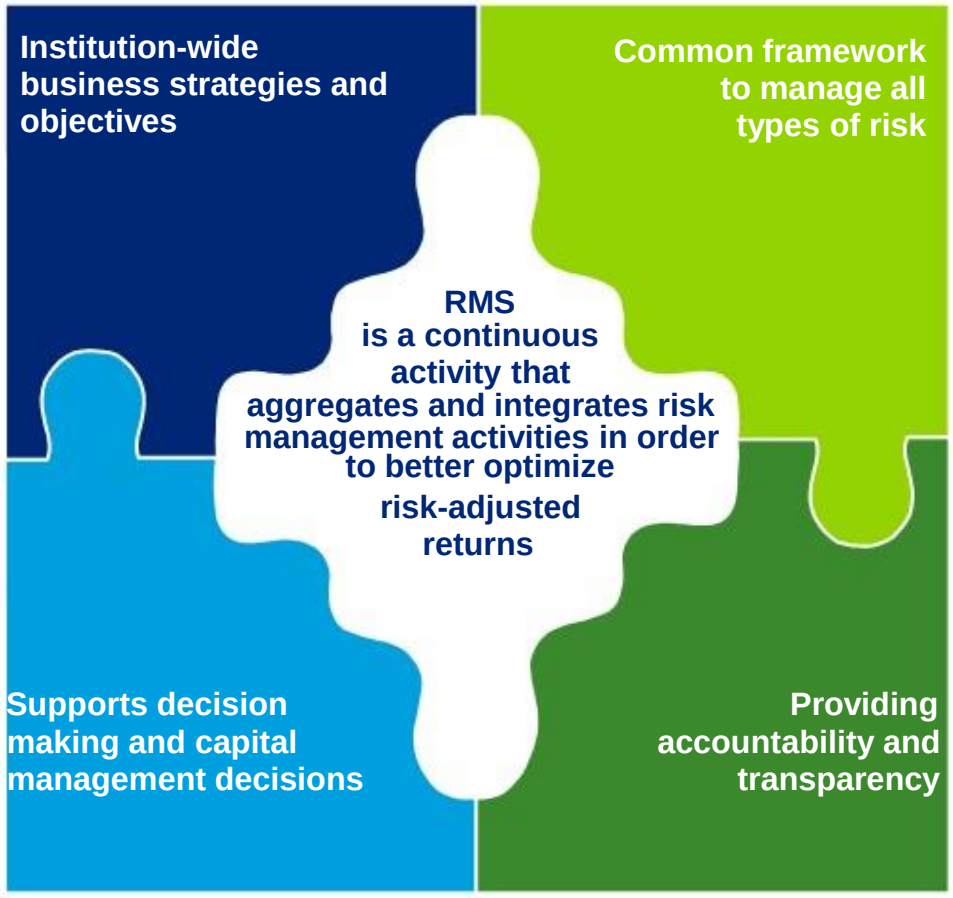
Regulatory matters

IT

- ✓ **Data Governance & Quality**

Challenges:
Three lines of defence model & Role of CRO

Risk Governance: Key Challenges



- **Building a risk aware culture**
- **Roles, responsibilities, accountability** and how this fits within the entity's RMS often **unclear**
- **Communication** paths **not defined**; arguments over whose "job" it is
- **Committee structures**, responsibilities and mandates **lack clarity**
- **2nd and 3rd line** functions used as **management assurance and quality control** functions
- Limited risk and control resources **not deployed effectively**
- RMS **not dynamic** and fails to proactively identify and adapt to changing conditions and/or unexpected events
- **Insufficient** focus and time spent **discussing risks** across the entity (The "Siloed approach")

Clarity of Roles

- **Each function must understand its 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
- Organisations **must clearly distinguish between 1st and 2nd line activities carried out by 1st line resources:**
  - **Independence** must be clearly demonstrated and documented
  - The **biggest challenge** institutions face in used 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 **1st line performance** appraisal
  - Ensure that **no responsibilities** are **delegated to Internal Audit** that could **compromise** their **independent** assurance function
- It is particularly important for there to be clarity on the **role of the Risk Management Function**
  - Risk management must be the **responsibility of the whole firm** and not just the Risk Management Function
  - **1st line must take ownership for risk management** – this cannot be seen as a 2nd line activity
  - Risk management must be seen as **more than just about regulatory compliance and role profiles must reflect this**

Clarity of Roles – Actuarial Function

- Where do **actuarial roles** sit – in the **1st or 2nd line**?
- If work in the actuarial department straddles the 1st and 2nd line activities, then **responsibilities and reporting lines must be very clear**
- Typically, the actuarial function is a 1st line function
- Where there are actuaries working in the 2nd 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 **1st line** doing **2nd line activities, accountability** rests with the **CRO**

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
    - The risk management function owns the internal model
  - **Actuarial Function** shall “contribute to the effective implementation of the risk management system”
    - May assist the risk function in its internal model tasks

- 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**

Role Interaction between CRO & Actuarial Function (SII)

Duties	CRO	Head of Actuarial Function
Risk Management	Oversight of firm wide risk management systems	• Contributes to the effective implementation of the risk management system • Opines on underwriting and reinsurance policy • Ensures the appropriateness of the methodologies, models and assumptions used in the calculation of technical provisions
Internal Model	Ensures the effective design, implementation, testing validation and documentation of the Internal Model	• Assist with modelling the risks underlying the SCR calculation • May contribute to building 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: • Advising management on the risks the firm runs and the required capital • Monitoring and reporting on those risks • Escalating if there are any material concerns or if risk appetite / limits are likely to be breached
Business Strategy	Challenges the business strategy	May assist in the production and challenge of the business strategy

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
- In life companies, the actuarial function **does not always report** to the Appointed Actuary; **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”
- Chief Actuary may also perform other roles outside those outlined in Solvency II **(e.g. pricing)** which can create further conflicts.

Dual Role CROs – Compliance & Other

CRO and Head of Compliance

- **Natural fit** between these roles?
  - CRO may be Head of Compliance or the Head of Compliance may report to the CRO, the CEO or another member of senior management
  - 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

- **Is performance based on measures that could conflict with the risk and control duties of the CRO?**
  - How is the CRO **rewarded?**
  - How is any **conflict addressed?**
  - How is the **integrity** of the 3 lines of defence maintained

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

CRO Role – The “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.**

Risk Culture & Governance:
Adding value

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 Deadalus Trust Conference 19 September 2013)

Characteristics

- **C** – Commonality of purpose, values and ethics
- **U** – Universal adoption and application
- **L** – Learning organisation
- **T** – Timely, transparent and honest communications
- **U** – Understanding the value of effective risk management
- **R** – Responsibility – individual and collective
- **E** – Expectation of challenge

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

CRO influence and evolution of Risk Culture

Understand current risk culture	Define "target risk culture"	Develop a change management plan	Implement the plan and assess results
Reluctance to learn from past mistakes	Following the herd	Risk Competence	Proactive Sharing of best practices	Consulting with others when in doubt
Shooting the messenger	Yielding to inappropriate pressure from others	Motivation	Admitting to making mistakes	Taking personal accountability for managing risks and opportunity
Inadequate challenge of inappropriate risk taking	Rewarding inappropriate risk taking	Attitude to Risk	Open and honest dialogue regarding risks and opportunities	Constructive response to challenge
Reticence to escalate risks appropriately	Cutting corners	Organisation	Following management policies and procedures	Involving risk professionals in key decisions

Adding value – the role of the CRO

- Solvency II and the Corporate Governance Code have shifted the focus and **risk is now centre stage in the strategic management of the organisation**
- Goal should be for risk management to b**e a source of competitive advantage**
- The CRO must have an **active role in strategic decision making**, provide a forward looking risk perspective working in collaboration with senior management and the CEO
- A good Risk Management Function should complement the activities of the 1st 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**
- **Strong relationships** between all parties with risk management responsibilities improves the effectiveness of the risk management system and reduces cost

Getting Risk Governance Right:
Conclusion

Defining the CRO Role so that Risk governance systems are strong

- **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

Questions ?