



*cutting through complexity*

**Audit Committee Institute**

Sponsored by KPMG

# Enterprise Risk Management - Issues for NEDs/Audit Committee

17 November 2011





**Kevin O'Donovan**

*Chairman, Audit Committee Institute  
Partner Audit, KPMG in Ireland*



**Mike Daughton**  
*Partner Risk and Compliance,  
KPMG in Ireland*

# Introduction



**Risk is a fact of business life.**



**“We had 20 people on the beach looking at grains of sand with microscopes when the tsunami came along and wiped everybody out” - FT 20 April 2008**

**Post financial crisis, Boards are asking themselves how can they manage the full spectrum of risks facing their organisations more effectively.**

# What is Enterprise Risk Management (ERM)?



**Enterprise Risk Management is a framework for identifying, measuring, mitigating, monitoring and managing risks. It recognises that risks are interdependent and places greater emphasis on cooperation between departments to manage the business risks on a portfolio basis.**

# What is Enterprise Risk Management (ERM)?



## And how does it differ from 'traditional' risk management practices?

### Traditional Risk Management

- Risk managers are viewed as 'blockers'.
- Identification and response to risks is siloed, made at BU rather than enterprise level.
- Risk reporting and MI largely internal, and confined to risk management function.
- A 'tick the box' compliance exercise
- Inconsistent application of risk management principles
- Lack of central function headed by a CRO.
- Periodic exercise e.g. annual
- Focus on short term rather than longer term strategic risks which can inform the strategic plan.



### Enterprise Risk Management

- Accountability for risk at Board level.
- Risk managers are viewed as 'enablers' of increased corporate value.
- Holistic approach to identification, assessment and response to risks.
- Measurement and reporting of Key Risk Indicators is aligned to strategic goals.
- Risk management information integrated into business decision making.
- CRO has mandate as a strategic business advisor, role not confined to leading the risk function.
- Risk culture embedded within the organisation.

# Why is ERM important?

## Key external drivers



- EU Directive requirements for increased disclosure on key risks, and the audit committee's duty to monitor the effectiveness of internal control and risk management
- Credit rating agencies now applying Enterprise Risk Management as a section/factor in credit ratings
- Pillar 2 requirements in respect of systems of governance contained in Solvency 2 requirements for insurance/re-insurance entities and Basel 2 for banking institutions
- Corporate governance codes continue to insist that a system of risk management is essential to safeguarding shareholders assets

# Why is ERM important?

## Corporate Governance Codes - illustrations



### Code of Practice for Governance of State Bodies

- Requires a state body approve the risk management framework.
- Key elements of Board oversight should include:
  - consider formation of a Risk Committee or include risk management in the Audit Committee charter;
  - risk management expertise from at least one director;
  - periodic external review of framework effectiveness.

### Corporate Governance Code (and Annual Compliance Statement)

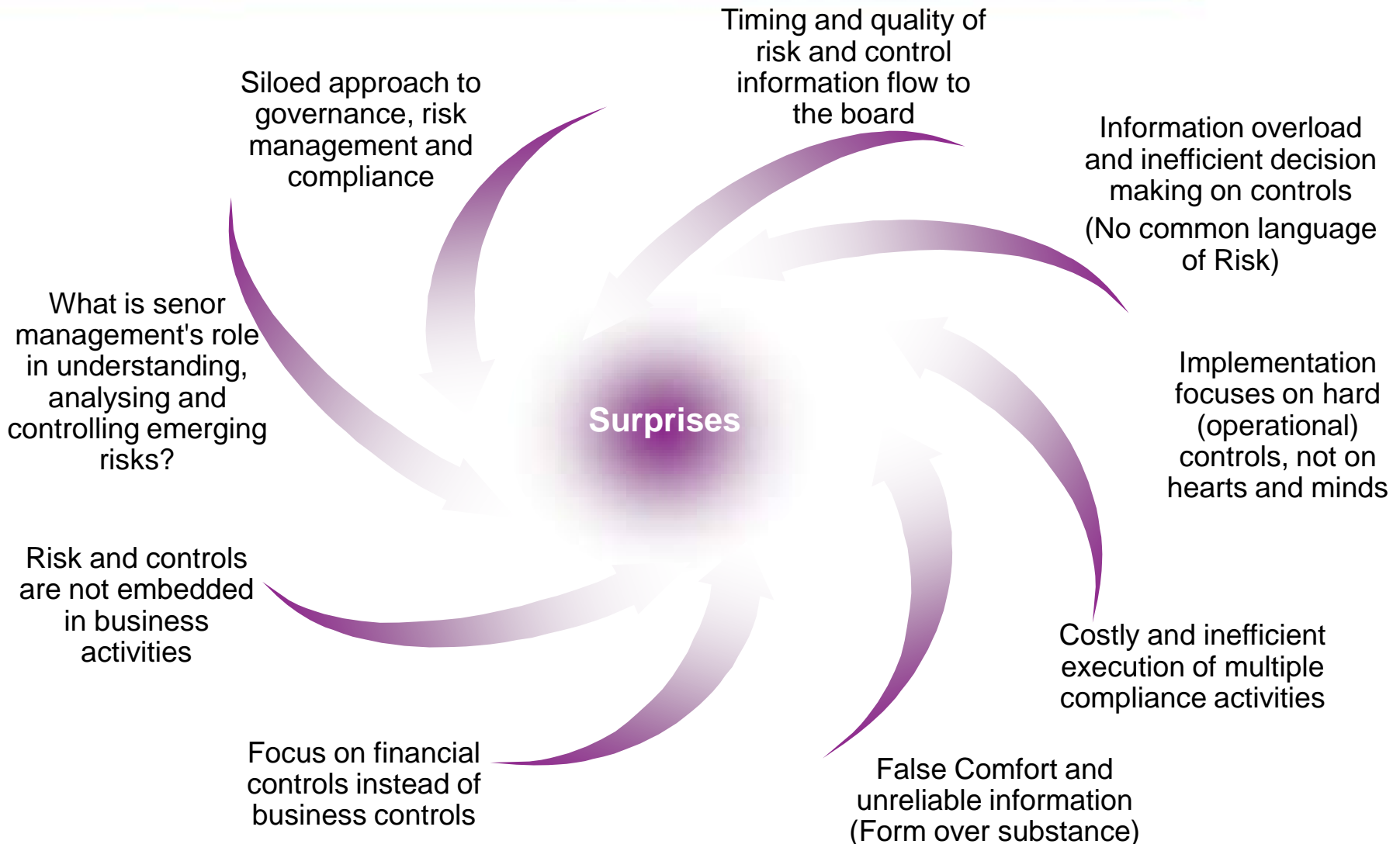
- The Code requires that the Board understands the risks of the business and that Risk Appetite should be clearly defined.
- The Risk Appetite requires qualitative and quantitative metrics to allow a review against strategy.
- Directors must each sign the Annual Compliance Statement and submit to the CBI.

### UK Revised Corporate Governance Code

- The Board is responsible for determining the nature and extent of the significant risks it is willing to take to achieve strategic objectives.
- The Board should, at least annually, conduct a review of the effectiveness of the company's risk management and internal control systems.
- Non Executive Directors should satisfy themselves that the systems of risk management are robust and defensible.

# Why is ERM important?

## Common concerns from Boards...



# The potential benefits of risk management are becoming clear



Improved decision making	Optimisation of costs	Improved performance	Improved management of expectations
<ul style="list-style-type: none"> <li>✓ Prevent surprises through more robust risk identification</li> <li>✓ Increase responsiveness to internal/external change</li> </ul>	<ul style="list-style-type: none"> <li>✓ Allocate resources better</li> <li>✓ Assess risk proactively rather than "after the fact"</li> <li>✓ Aggregate risk transfer and risk acceptance decisions</li> <li>✓ Eliminate redundant/unnecessary controls</li> <li>✓ Reduction in bureaucracy and management time diverted to governance</li> </ul>	<ul style="list-style-type: none"> <li>✓ Integrate with business planning &amp; performance management</li> <li>✓ Risk mitigation actions aligned with business plan objectives</li> <li>✓ Improve communication and knowledge sharing</li> <li>✓ Development of stronger control systems</li> <li>✓ Take risks in line with expertise and core competencies</li> </ul>	<ul style="list-style-type: none"> <li>✓ Improve stakeholder transparency and communication</li> <li>✓ Meet internal business requirements</li> <li>✓ Meet corporate governance better practice guidelines</li> </ul>

**However, for many organisations these benefits are not being realised**

# How do you implement? Suggested approach



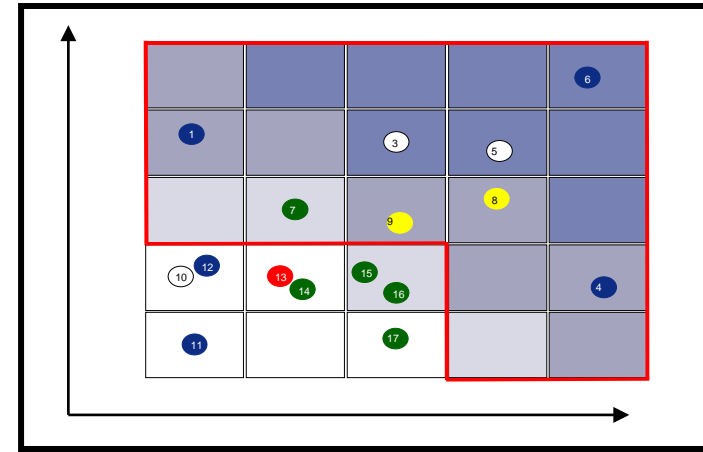
The successful design and implementation of ERM requires both content and process. Each must be supported by a clear philosophy, a practical framework and techniques.



Developing the quality and consistency of risk management information.



Likelihood



Impact



Implementing processes to achieve a sustainable improvement in risk management.



....sounds sensible but needs to be fit for purpose and culturally accepted. Many organisations fail in their implementation of ERM.

Risk Management Framework	
Framework Element	Description
Risk Governance	Establishment of approach for developing, supporting, and embedding the risk strategy and accountabilities
Risk Assessment	Identifying, assessing, and categorizing risks across the enterprise
Risk Quantification & Aggregation	Measurement, analysis, and consolidation of enterprise risks
Risk Monitoring & Reporting	Reporting, monitoring, and assurance activities to provide insights into risk management strengths and weaknesses
Risk & Control Optimization	Using risk and control information to improve performance

# How do you implement?

## Suggested approach – Risk Maturity



		Maturity level		
		Basic	Moderate	Advanced
Framework elements	<b>Risk Governance</b>	A central risk management policy	A risk mgt. structure with clear accountabilities	Risk mgt. is of central value of the organisation
	<b>Risk Assessment</b>	Annual risk assessment	Frequent risk assessment including analysis	Risk & control embedded in business processes
	<b>Risk Quantification</b>	Simple Probability and Impact descriptors	A range of qualitative and quantitative tools and techniques	Risk-based capital allocation capability
	<b>Monitoring &amp; Reporting</b>	Risk registers to support external reporting requirements	Extensive reporting to the board and audit committee	Use of KRIs, early warning mechanisms and risk dashboard
	<b>Risk and Control Optimisation</b>	A tick in the box supported by limited external reporting	Risk information supports the modification of key controls	Risk-adjusted strategy and optimised control investment

### Risk elements definition

- **Risk Governance** – establishment of an approach for developing, supporting and embedding the risk management strategy and accountabilities
- **Risk Assessment** – identifying, assessing, and categorising risks across the business
- **Quantification & Aggregation** – measurement, analysis, and consolidation of key risks
- **Monitoring & Reporting** – reporting, monitoring, and assurance activities to provide genuine insights into risk management approach
- **Risk & Control Optimisation** – using risk and control information to improve performance

# How do you implement?

## Suggested approach – Illustrative Risk register



The risk register acts as a database for risk information. The quality of the content is key, to making risk management a success.

Ref	Source/C at	Risk name	Risk description	Likelihood	Impact	Inherent severity	Existing Controls	Evidence
Risk Ref	What is the source of the risk	Name the risk	Describe the risk	1=Rare, 2=Unlikely, 3=Possible, 4=Probable	1=Minor, 2=Moderate, 3=Major, 4=Severe	Do nothing in this column	What existing processes/ controls are in place to manage the risk	Documented evidence that the control is performed
001				4	4			
002				4	3			
003				3	3			



Evidence	Control effectiveness	Residual risk	Action for further control	Action owner	Due date
Documented evidence that the control is performed	How effective are the controls at mitigating the risk	Do nothing in this column	What further action (if deemed necessary) is planned to treat the risk	Who is responsible for developing and implementing the action plan	When are agreed actions to be delivered by



# How do you implement?

## Implementation challenges



CONTENT	1	The risks contained in the risk register often do not reflect the risks the business is running
	2	The risk assessment process by itself won't help manage risk better – you've got to understand the control environment and behavioural aspects
	3	Companies continue to struggle to embed risk management and still find it difficult to truly describe and understand how they manage their key risks
	4	Reporting of risk information is still largely compliance driven with observations focusing on the priority of risks rather than on control and improvement actions or developments of the risk management process itself
PROCESS	5	Selling the business case is still in the 'too hard' tray – many organisations don't have the dialogue with their key stakeholders or risk management, therefore investment and return are not clear
	6	In many organisations executive management need to take more sponsorship and accountability for risk information
	7	There has been a shift in focus from risk content to a sustainable risk framework. The content however now requires further scrutiny to ensure it is fully understood and that value is derived from it
	8	There are still difficulties with bridging the gap between the theory and day-to-day risk management – "I don't just want to tick boxes"

# How do you implement?

## Implementation challenges



### Positioning

- Restricted role of Risk Manager – difficult to exert restraining influence and cultural change – Not on Senior Management agenda
- ERM perceived as purely a compliance driven exercise

### People and Comms

- Information silos - No integrated risk management function – no holistic view across the company
- Little interaction between risk management and the business managers
- Lack of clarity over risk reporting and true understanding at Board level

### Process

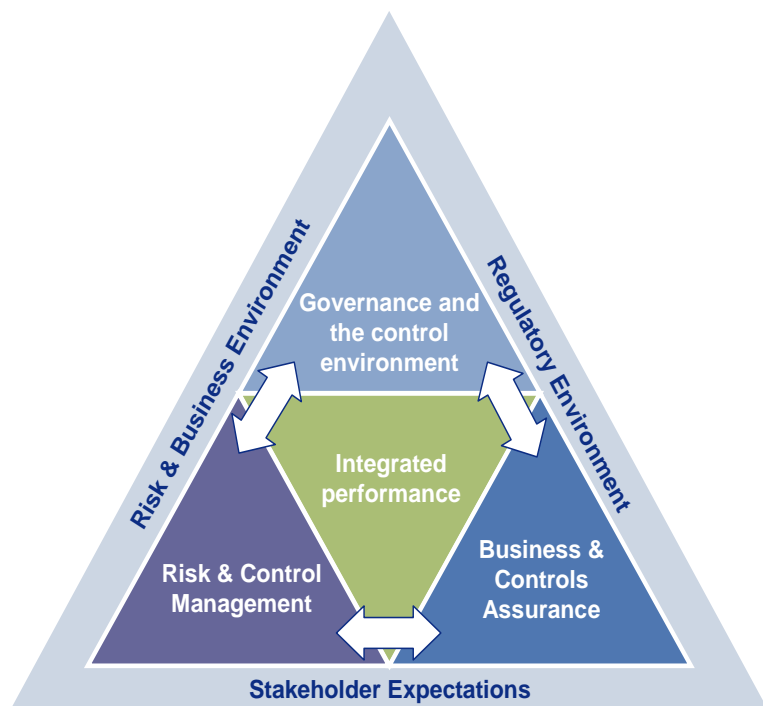
- Failure of the board to set the boundaries for risk taking and monitor performance
- Lack of risk quantification and scenario analysis to assess impacts
- Risk management effort focused on historic risks with little focus on emerging risks
- Scope of risk management is limited

# Where to from now?

## Integrated Assurance – what does it look like?

Those organisations that have successfully implemented solid risk management foundations are now standing back and re-thinking how their activities integrate with the wider system of internal control.

### Integrated Governance, Risk and Assurance model



#### Governance

- Constitution and operations of the Board
- Strategy setting, decision making and change management
- Organisational culture, values and the Code of Conduct
- Corporate structures, reporting lines, accountability and communication
- Management information, monitoring, challenge and reporting
- Stewardship, external disclosure and compliance

#### Risk Management

- Risk strategy and appetite
- Structures, roles and responsibilities
- Identifying and assessing risks and controls
- Review, analysis, risk assurance and reporting
- Using risk and control information to create value e.g. to inform strategic planning

#### Assurance

- Business and management assurance
- Corporate oversight, policy and procedures
- Independent assurance provision

#### Understanding business, risk and regulatory environment and stakeholder expectations

# Conclusion

## Some questions you should be asking and responding to?



- Is the Board well equipped to deliver effective risk oversight?
- How do we link risk to strategy?
- Is Risk Management considered fundamental to the achievement of business objectives?
- Is Risk Management about realising the upside or is it only about minimising the downside that the business could be exposed to?
- What do we need to do to embed risk thinking into decision making?
- Am I receiving the appropriate risk management information?
- Do we really understand the emerging risks we face and how we should be responding?
- What monitoring mechanisms exist and what assurance do I receive on the management of this portfolio of risks?

# Conclusion

## Some key imperatives



- Enhance effectiveness of Board oversight of risks by separating risk process and content
- Integrate Risk Management into decision making by leveraging Key Risk Indicators
- Focus on softer aspects such as risk leadership, risk perception and behaviour, and communication
- Position the role of a CRO as a strategic business advisor
- Integrate the company's Risk Management efforts at an enterprise level



**John Healy**  
*Group Risk Manager, ESB*

# ESB Group – Diverse Risk Profile

International  
Business

Competition, Regulation, Climate Change



Capital Intensive



Commodity Trading

Oil, gas, coal,  
electricity



Environment



Safety



Critical  
Infrastructure



# Rationale for ERM approach in ESB

- Good Risk Management in each BU
  - Business reasons/complexity/challenges
  - Best practice continues to move ahead
  
- Needed a Group perspective of BU risks
  - Better information for more active risk oversight at Board level
  - Improved risk escalation from BU's to Board
  
- ERM encompasses an approach for further development
  - Closer integration with Group Strategies & Group Risk Tolerances
  - Consolidating individual risk plans of each BU

# ERM implementation - first steps



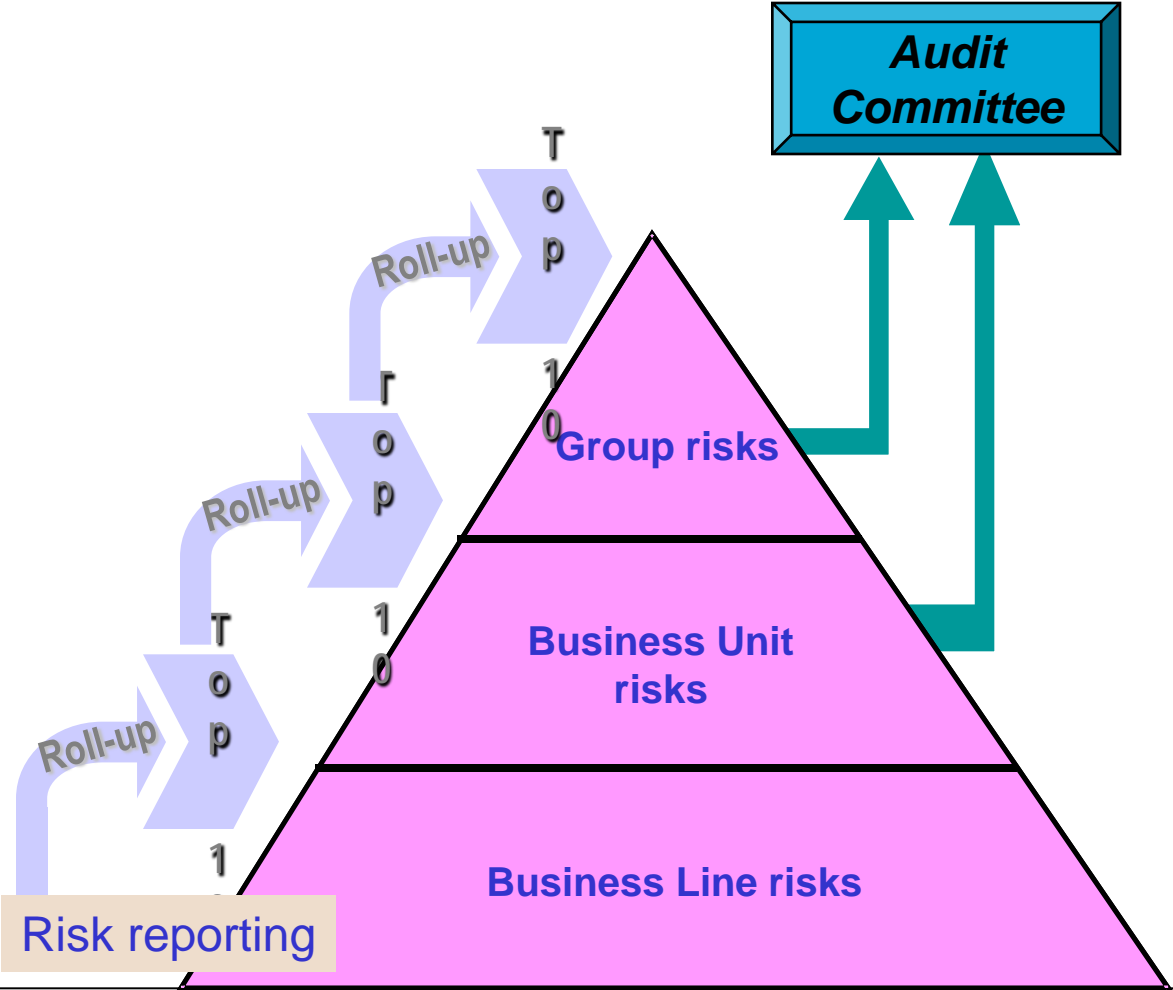
.... not a replacement for managing risk at Business level

# Board Audit & Risk Committee – Risk mgt duties include



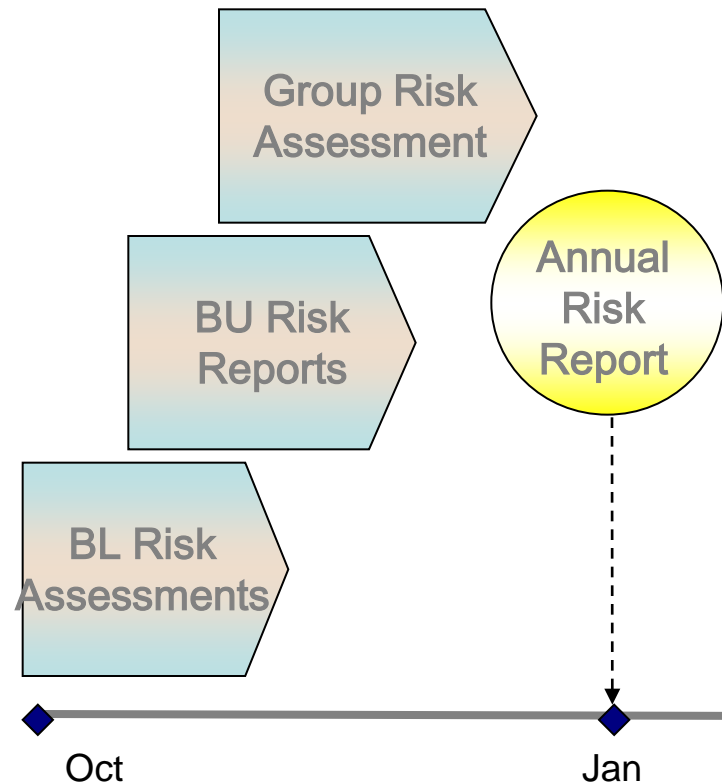
- Recommend for approval to the Board the risk policy
- Monitor the effectiveness of ESB's risk management framework, ensuring its continued functioning and appropriateness.
- Review ESB's key risks & the adequacy of planned mitigation.
- Arrange a regular external review of ESB's risk management process.
- Prepare a risk management report for the annual report & accounts.
- Review Business Continuity Planning & crisis management

# ERM applies at all levels of the Group

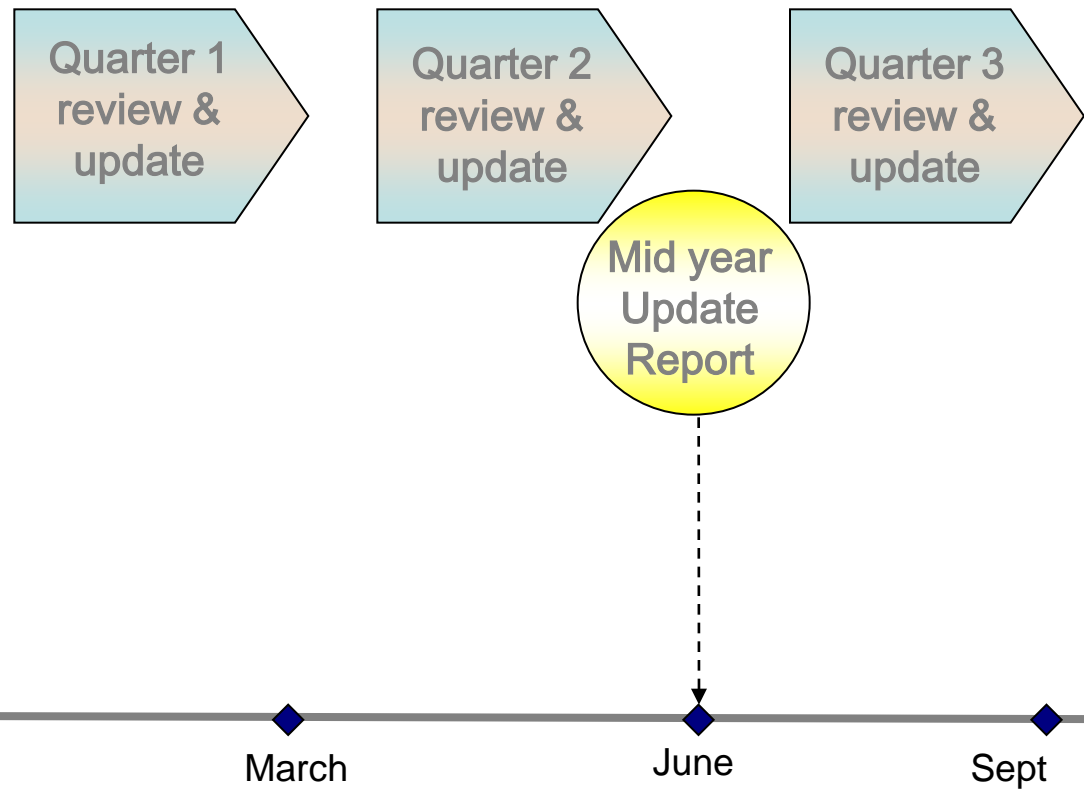


# Identifying & prioritising risk – an ongoing process

## Annual risk assessment



## Quarterly reviews



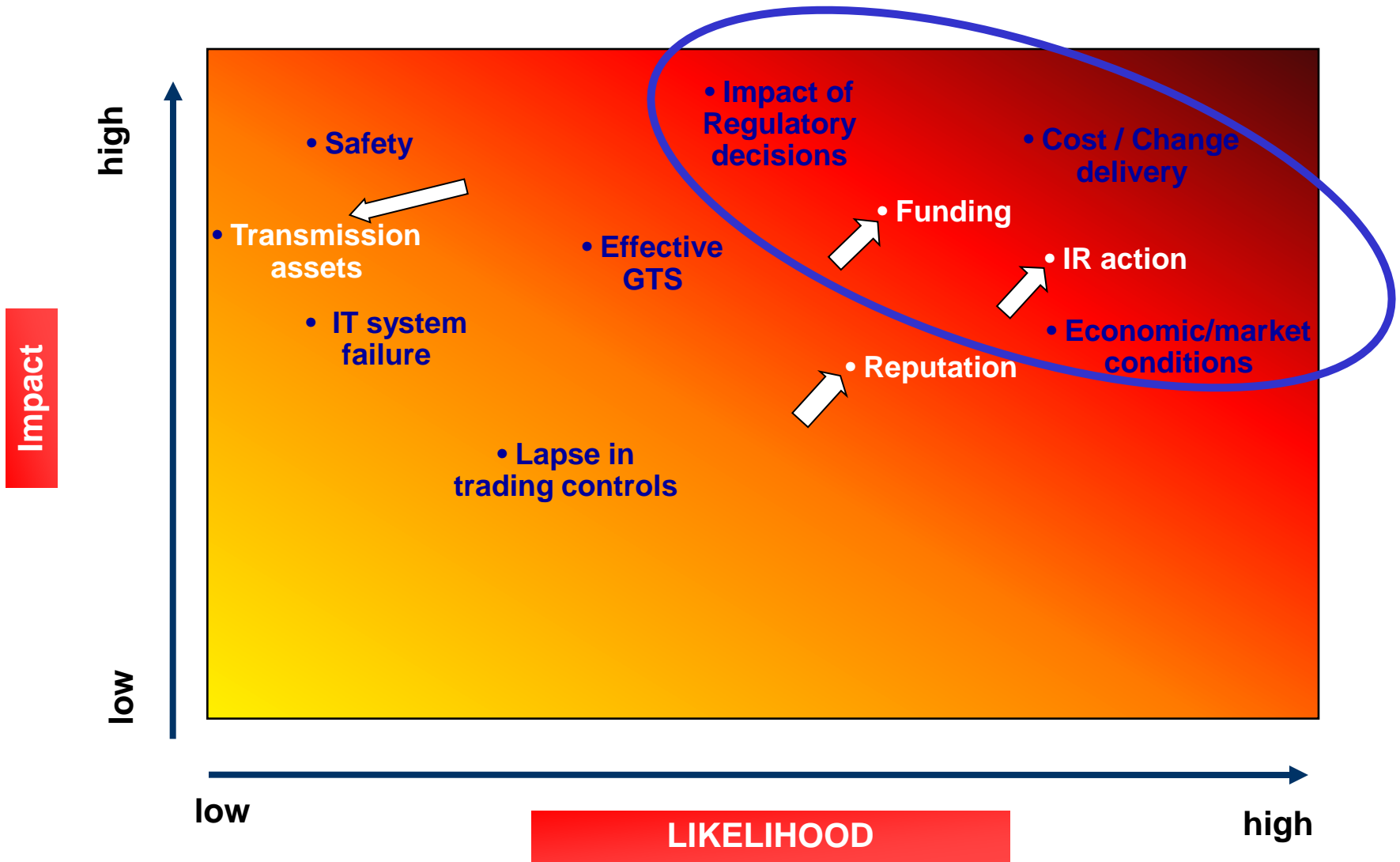


# Risk Update - January 2011

## Table of Contents

<b>1. Executive summary .....</b>	<b>2</b>
1.1 Risk Drivers.....	2
1.2 Top risks for 2011 .....	2
1.3 Planned Mitigation .....	3
1.4 Risk analysis.....	3
<b>2. Details of Group Risks for 2011 .....</b>	<b>4</b>
<b>3. Group Risks (by likelihood, Impact &amp; Immediacy) .....</b>	<b>9</b>
<b>4. BU Risks .....</b>	<b>10</b>
<b>5. Risk Drivers from across the Businesses.....</b>	<b>11</b>
<b>6. Sources of Risks at Group &amp; BU level .....</b>	<b>12</b>
<b>7. The Main HILP Risks.....</b>	<b>13</b>
<b>8. Risk Planning Process for 2011.....</b>	<b>14</b>

# Updates to January 2011 heat map



Rank Q1 Q3		Risk	Action Status/ Progress	Status of Risk	Mitigation impact / effectiveness
1	3	Failure to deliver change & cost savings quickly enough	Year end targets could still be met	↑	Remains key risk with increased mgt focus
2	2	Further deterioration in economic & market conditions	On target	↔	Unchanged since Jan 2011
3	1	Failure to secure funding at appropriate cost	Markets closed for funding	↑	Sovereign rating & Euro Zone uncertainty
4		Impact of regulatory decisions	On target	↔	Continues to be focus of Mgt attention
5		Unfavourable outcome to transmission asset review	Subject to certification	↓	Subject to a certification process by CER
6		Threats to reputation & public standing	On target	↑	Price increases, cost & IR perceptions
7		Ability to deliver effective GTS	Supply integration	↔	CER yet to issue consultation on Supply integration
8		Potential IR/partnership pressures	Negotiations resumed	↑	Increased pressures
9		IT infrastructure failure	On target	↔	Managed well
10		Lapses in energy trading controls & effectiveness	On target	↔	Managed well
11		Safety	On target	↔	Strong safety culture; remains critical issue

# Areas of high impact for ESB

- Fire/explosion
- Safety – public & staff
- Sabotage/terrorism
- IT failure
- Public confidence in ESB billing process
- Transmission/distribution failure
- Environment
- Extreme Weather



# The main HILP risks

	Risk
1	<b>Explosion / fire in plant</b>
2	<b>Major safety incident</b> Involving staff, contractors or Public on construction sites, farm machinery, plant commissioning.
3	<b>Major environmental incident</b> <ul style="list-style-type: none"><li>• Release of oil or chemicals to water</li><li>• Underground leak from oil filled cables</li></ul>
4	<b>Sabotage / Terrorism</b> In generation plant or in network infrastructure (HV lines, HV Tower structure, critical sub stations)
5	<b>Major IT virus attack (malware)</b> <ul style="list-style-type: none"><li>• Infection of Business or SCADA network</li><li>• Significant downtime and data cleanse effort</li></ul>
6	<b>Security incident in overseas location</b> Affecting personnel safety
7	<b>Loss of primary Operations Mgt System</b> Impacting on control of the national distribution grid

	Risk
8	<b>Dam failure/major flooding</b> Dam failure or impact of extreme weather
9	<b>Major data security breach</b> Loss of personal or customer data leading to investigation/sanctions.
10	<b>Major Supply Failure</b> Arising from severe storms or serious network fault e.g. major incident in a critical transformer
11	<b>Major IT/telecoms infrastructure failure</b> Widespread loss of systems & business interruption
12	<b>Integrity of Customer Billing system</b> Loss of public confidence in billing
13	<b>Governance failure/major fraud</b>
14	<b>Major damage to HV lines towers</b>
15	<b>Peat Slide on Wind Farm construction</b>

# Embedding risk is a culture change

*“... integrated business process essential to overall business success”*

- Raising awareness of risk
  - Example & tone set at the top – risks expected to be considered
  - Board demand a rigorous risk management framework
  - Risk policy & practice is set by CE & Board
  
- Decision making is informed by a proper analysis of risk
  - Framework for risk identification, assessment, reporting & escalation
  - Lessons learned from near misses/past experience
  - Ways of thinking about risk
  
- The risk framework is designed to support the culture
  - Mgt are supported in deploying the framework in a manner appropriate to their area

# The overall ERM Framework in ESB

- Maintained & updated by the Group Risk Manager
- Overseen by the Board/Audit Committee
- Implemented by Management at all levels of the Group

....ERM is not a replacement for managing risk at BU level but a key part of the system of assurance and alignment at Group level





**Discussion**

**Questions and Answers**

**Thank You**





*cutting through complexity*

**Audit Committee Institute**

Sponsored by KPMG

# Enterprise Risk Management - Issues for NEDs/Audit Committee

17 November 2011

