



Measuring and enhancing ERM maturity

IRM Global Risk Management
Professional Development Forum

Owen Purcell & Leif Tveide

23 March 2011

Introduction



Owen Purcell

Partner – Risk
UK&I Advisory, Ernst & Young



Leif Tveide

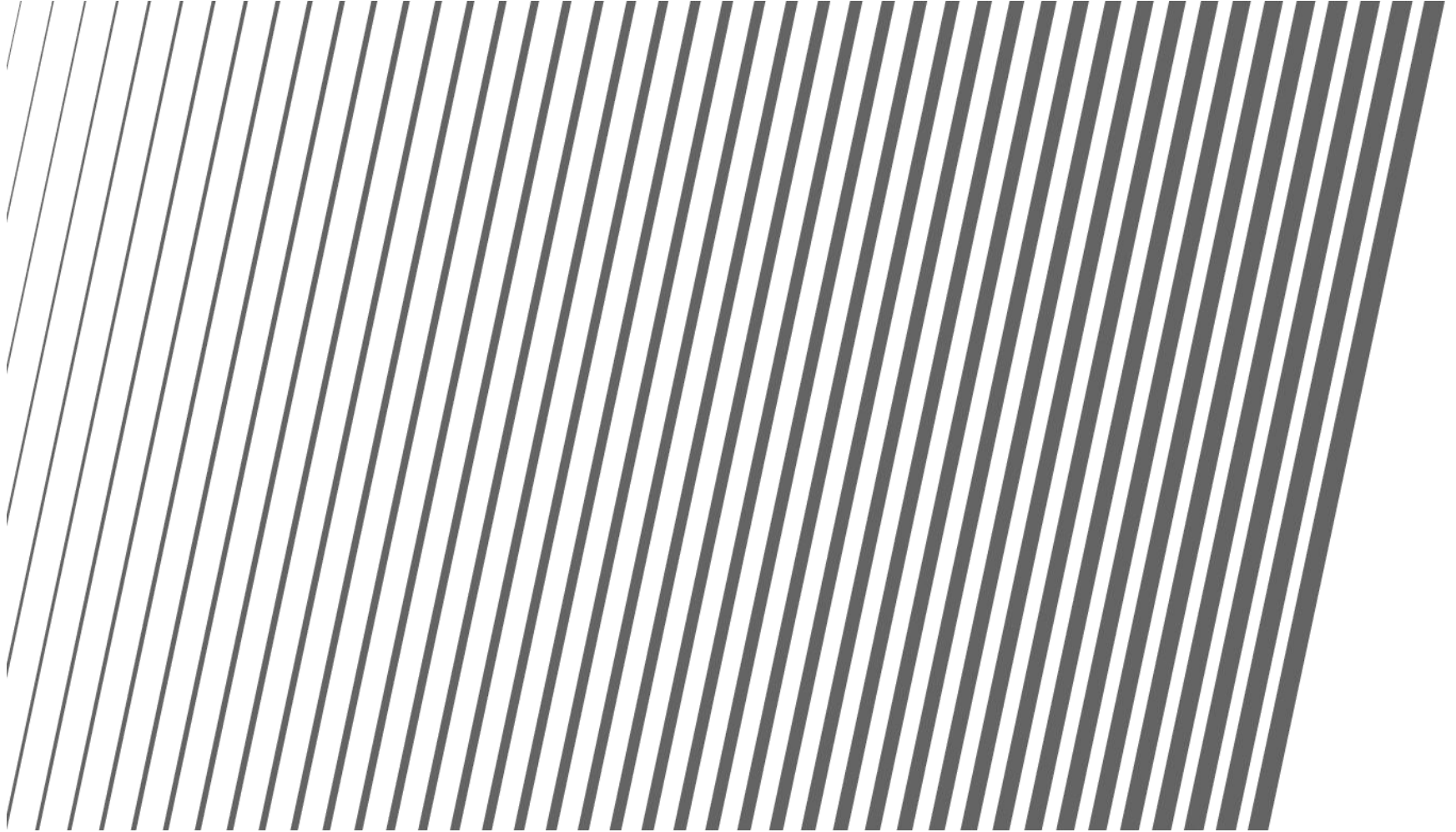
Senior Manager – Risk
UK&I Advisory, Ernst & Young

Our agenda for today

1. What is keeping ERM on the corporate agenda?
2. How to measure and further enhance ERM maturity?
3. A practical example from the UK energy sector
4. Questions & Answers



1. What is keeping ERM on the corporate agenda?



Following the economic crisis, organisations are facing increasing pressures to improve ERM practices

Business pull

- ▶ Desire to learn the lessons from the crash, avoid similar in the future
- ▶ Need to protect business reputation in turbulent times as shareholders, credit agencies and customers are more cautious, expecting to see robust risk management and ready to punish failure swiftly
- ▶ Opportunities for growth returning, but a changed world and so need for better risk taking and management
- ▶ Clear concern from management that GRC functions need enhancing

Regulatory push

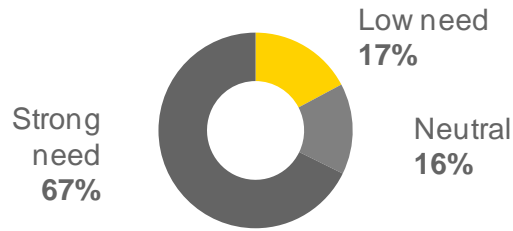
- ▶ Regulators' response requires a more explicit Risk Management process and structure (e.g., Walker Report, UK Corporate Governance Code, FSA regulations, 8th EU Directive, Basel III)

An organisation's approach to dealing with changes in regulatory requirements determines the potential value that can be derived from risk management and controls

Business pull – the majority of respondents see a strong need to enhance GRC* functions

*GRC includes governance, risk and compliance activities, e.g., Risk Management, Internal Control, Compliance, Internal Audit, etc.

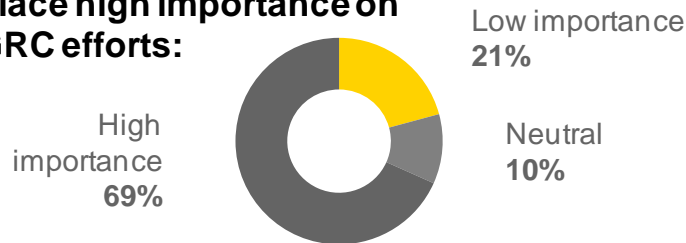
Companies feel there is a strong need to enhance their GRC functions:



There is strong external pressure on organisations to increase their GRC Capability. They see GRC as having:



Shareholders and investors place high importance on GRC efforts:



Business pull: In general, two out of three respondents and four out of five stakeholders see a fundamental need to enhance the GRC functions of companies because of external pressure increases

“Expectations on governance, risk and compliance from the management, operational leader and external stakeholder perspective”, an Ernst & Young survey of 567 companies in Europe, the Middle East, India and Asia, 2010

Regulatory push – the evolving regulatory landscape for Financial Services increases focus on ERM



Regulatory push – the UK Corporate Governance Code 2010 drives focus on ERM in non-FS organisations

More explicit focus on risk and risk management:

The revised Code is **more explicit** about risk and articulates increased requirements for the assessment, management and monitoring of risks, including **responsibilities for the board** to:

- ▶ Identify and assess all risks that are 'significant', including the **strategic risks**
- ▶ Define the organisation's **risk appetite/tolerance**, described as *"the nature and extent of the significant risks it is willing to take in achieving its strategic objectives"*.

It reaffirms, as per the previous Code, the requirements for the board to:

- ▶ Maintain a sound **risk management system**.
- ▶ Conduct an **annual review** of the effectiveness of the organisation's risk management system as well as the internal control system.

The Combined Code 2008

C.2 Internal Control¹²

Main Principle

The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets.

Code Provision

C.2.1 The board should, at least annually, conduct a review of the effectiveness of the group's system of internal controls and should report to shareholders that they have done so¹³. The review should cover all material controls, including financial, operational and compliance controls and risk management systems.

The UK Corporate Governance Code 2010

C.2 Risk Management and Internal Control¹⁴

Main Principle

The board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The board should maintain sound risk management and internal control systems.

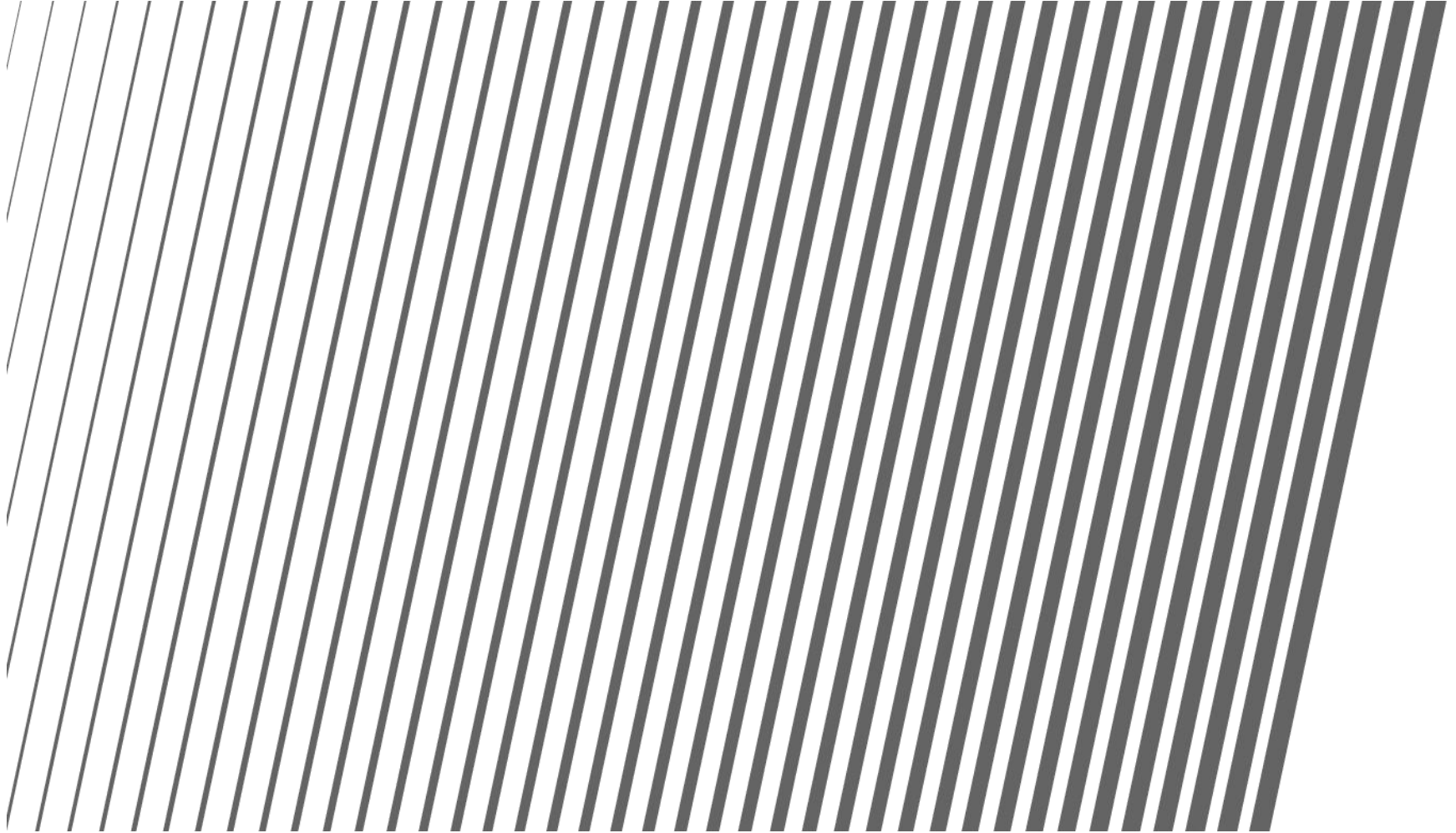
Code Provision

C.2.1 The board should, at least annually, conduct a review of the effectiveness of the company's risk management and internal control systems and should report to shareholders that they have done so¹⁵. The review should cover all material controls, including financial, operational and compliance controls.

Leading practices are emerging in the wake of the current economic crisis....

- ▶ **Changing attitudes:** Risk is now everybody's responsibility and plays a major role in decision-making across the organisation
- ▶ **Comprehensive:** Organisations are taking a more holistic view ("end-to-end integrated view") to better understand risk interdependencies and aggregate impacts
- ▶ **Proactive:** Companies are becoming more forward-looking and predictive, incorporating stress-testing and scenario analysis
- ▶ **Risk appetite and tolerance:** Leading organisations are defining risk tolerances and building a consistent organisational risk management culture
- ▶ **Transparency:** Sharing of data, open decision-making and enhanced reporting to executive management has become increasingly important
- ▶ **Board communications:** A majority of organisations indicate they are changing the frequency and substance of their Board-level risk discussions
- ▶ **Risk committees:** Companies have added committees focused on enterprise risk and/or crisis management
- ▶ **Specialty skills:** Leading companies are enhancing their risk management control functions, adding new people and leveraging specialty skills to address business risk on a comprehensive basis
- ▶ **Monitoring:** Ongoing monitoring and the escalation of risk has become more robust with greater clarity or information and enhanced consistency across risk functions
- ▶ **Governance:** Overall, leading organisations are driving "Risk Governance" from a holistic business perspective

2. How to measure and further enhance ERM maturity?



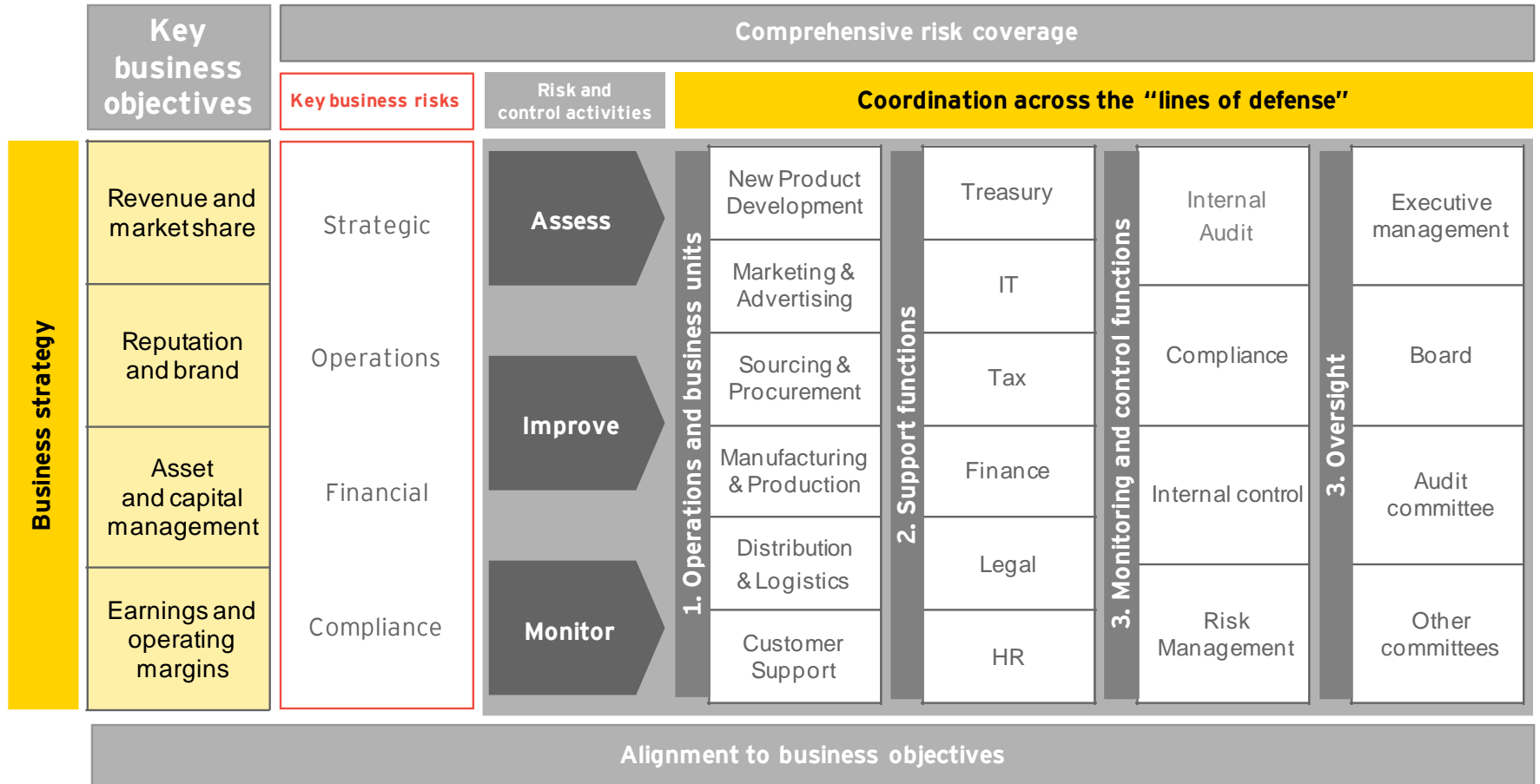
What is ERM?

“... a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

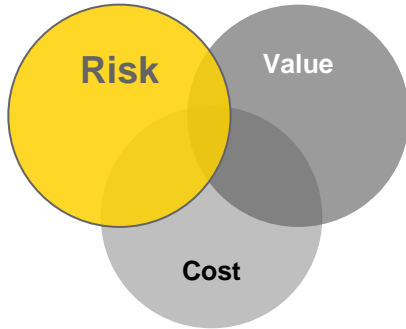
Source: COSO Enterprise Risk Management – Integrated Framework, 2004, COSO.

What does it mean in practice?

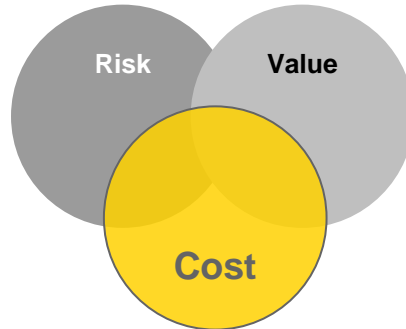
An enterprise approach to risk and performance



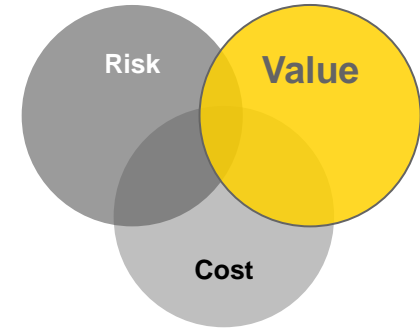
The objective for ERM is increasingly to achieve the 'right' balance between risk, cost and value



- ▶ Do we know our key risks?
- ▶ Do we have effective risk reporting for executive management and the Board?
- ▶ Are we accepting the right level of risk?
- ▶ Do we know if our risks are being properly managed?
- ▶ Do we have a comprehensive risk framework in place?
- ▶ Do we understand the risks that our company faces?



- ▶ Are we focused on the risks that matter?
- ▶ Do we have duplicative or overlapping risk functions?
- ▶ Are we leveraging automated controls versus manual controls?
- ▶ Do we have the right mix of skills at the right cost?
- ▶ Have we optimized the use of technology to manage risk?
- ▶ Can we use alternative sourcing strategies to reduce costs?



- ▶ Are the risks we take aligned to our business strategies and objectives?
- ▶ Are we getting the right return on our risk investment?
- ▶ Are we getting process improvement ideas?
- ▶ Are we taking the right risks to achieve competitive advantage?
- ▶ Is risk management slowing me down or helping me go faster?

Measuring ERM maturity – Standard & Poor’s ERM scoring definitions

Excellent

Companies that can demonstrate all characteristics of those scored “strong”, have well developed capabilities and can also demonstrate risk / reward optimization

Strong

Companies that can demonstrate an enterprise-wide view of risks and can demonstrate capabilities to consistently identify, measure and manage risk exposures and losses in-line with predetermined risk tolerance guidelines

Adequate

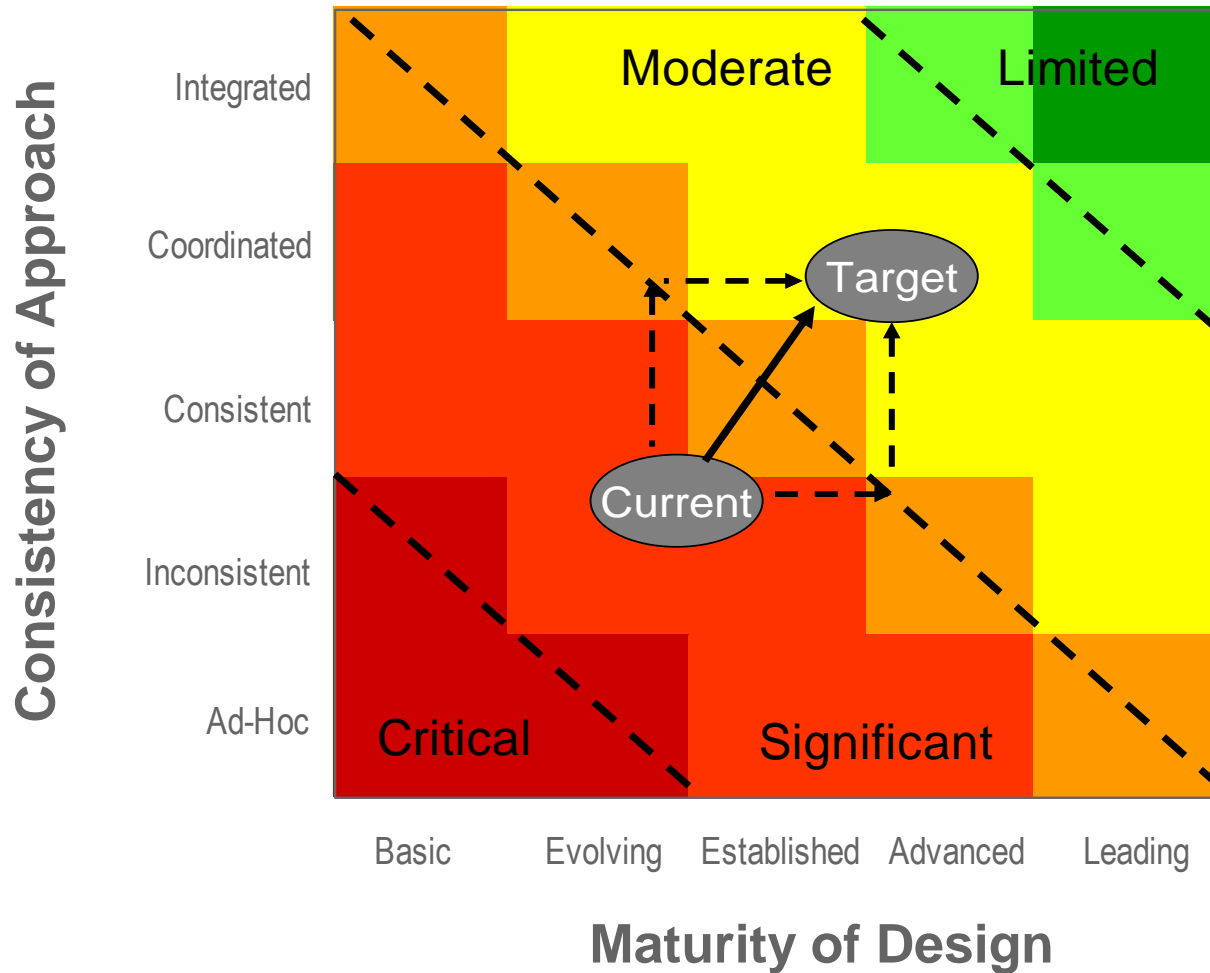
Companies with baseline capabilities to consistently identify, measure and comprehensively manage risk exposures, yet continue to manage risk in separate silos

Weak

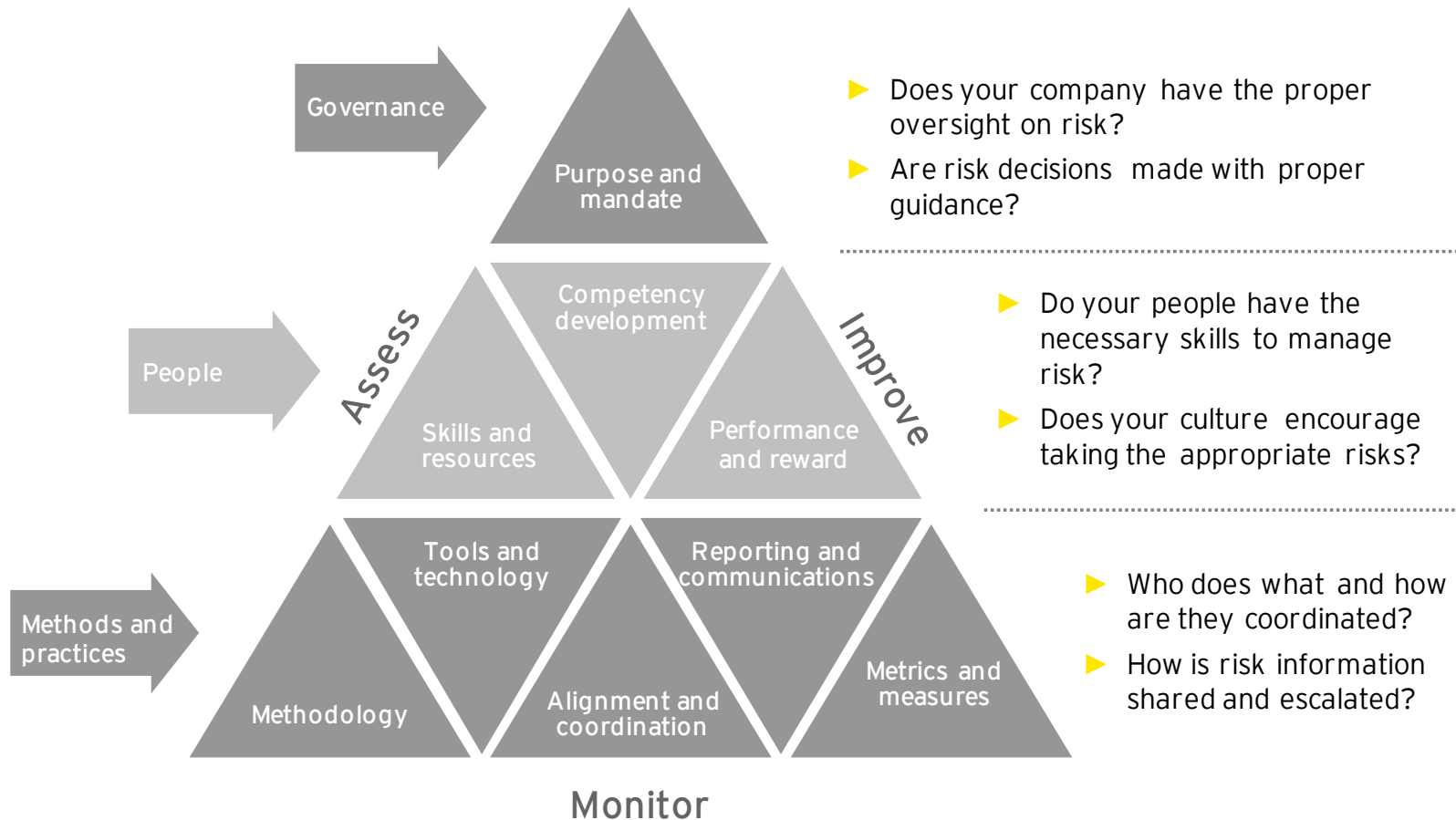
Companies with limited capabilities to consistently identify, measure and comprehensively manage risk exposures and thus, limit losses

Source: *Standard & Poor’s To Apply Enterprise Risk Analysis To Corporate Ratings*, 7 May 2008

Measuring ERM maturity – maturity of framework design versus consistency of application



Components of ERM maturity – example 1



Components of ERM maturity – example 2

Governance

- ▶ Tone at the top
- ▶ Strategies and objectives
- ▶ Policy and procedures
- ▶ Organizational structure
- ▶ Compliance

People

- ▶ Culture and performance
- ▶ Alignment and coordination
- ▶ Competence and capabilities
- ▶ Roles and responsibilities
- ▶ Communication

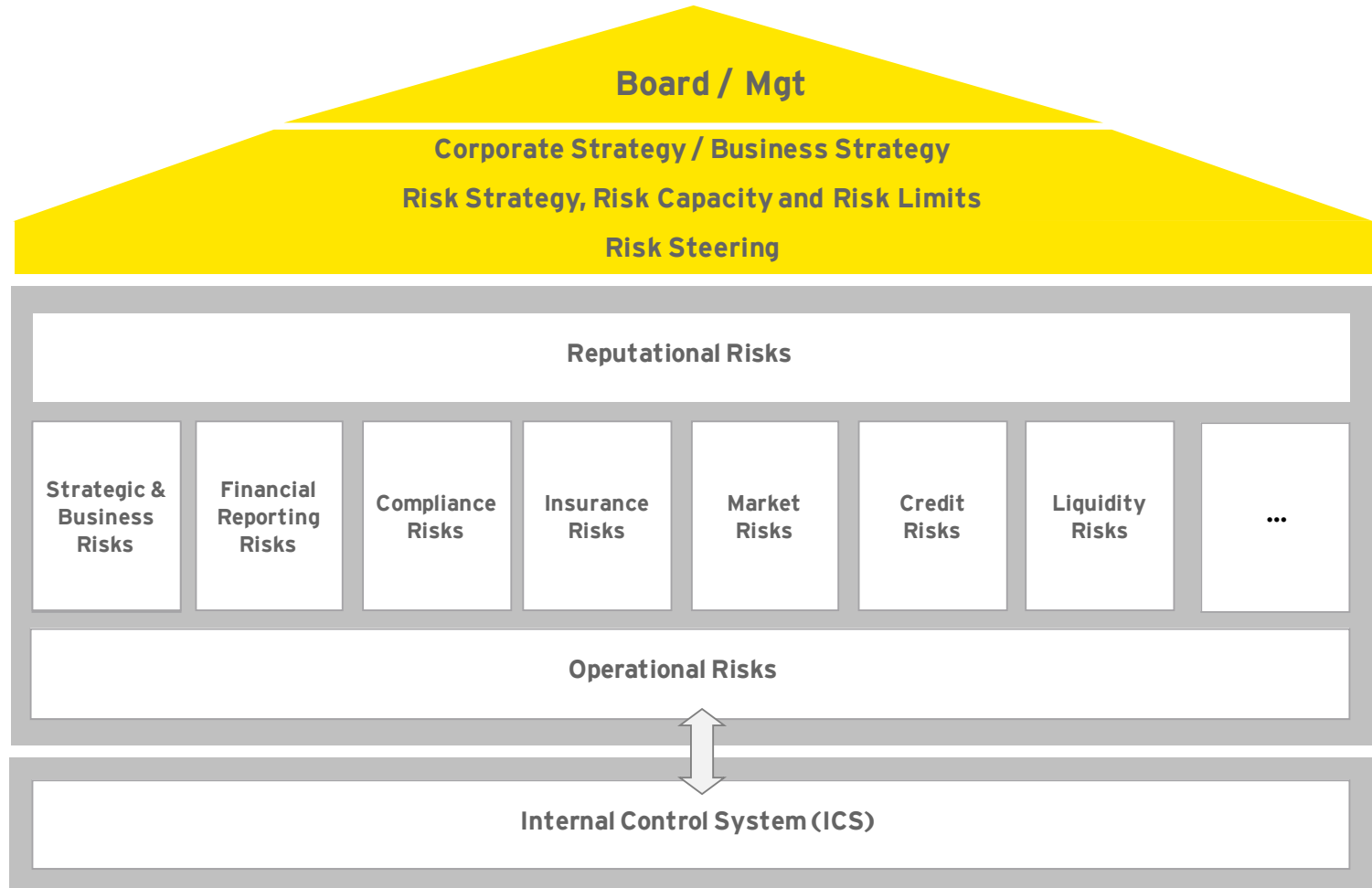
Methods & Practices

- ▶ Risk identification and assessment
- ▶ Control design and effectiveness
- ▶ Process improvement and efficiency
- ▶ Monitoring and reporting
- ▶ Technology

Components of ERM maturity – example 3



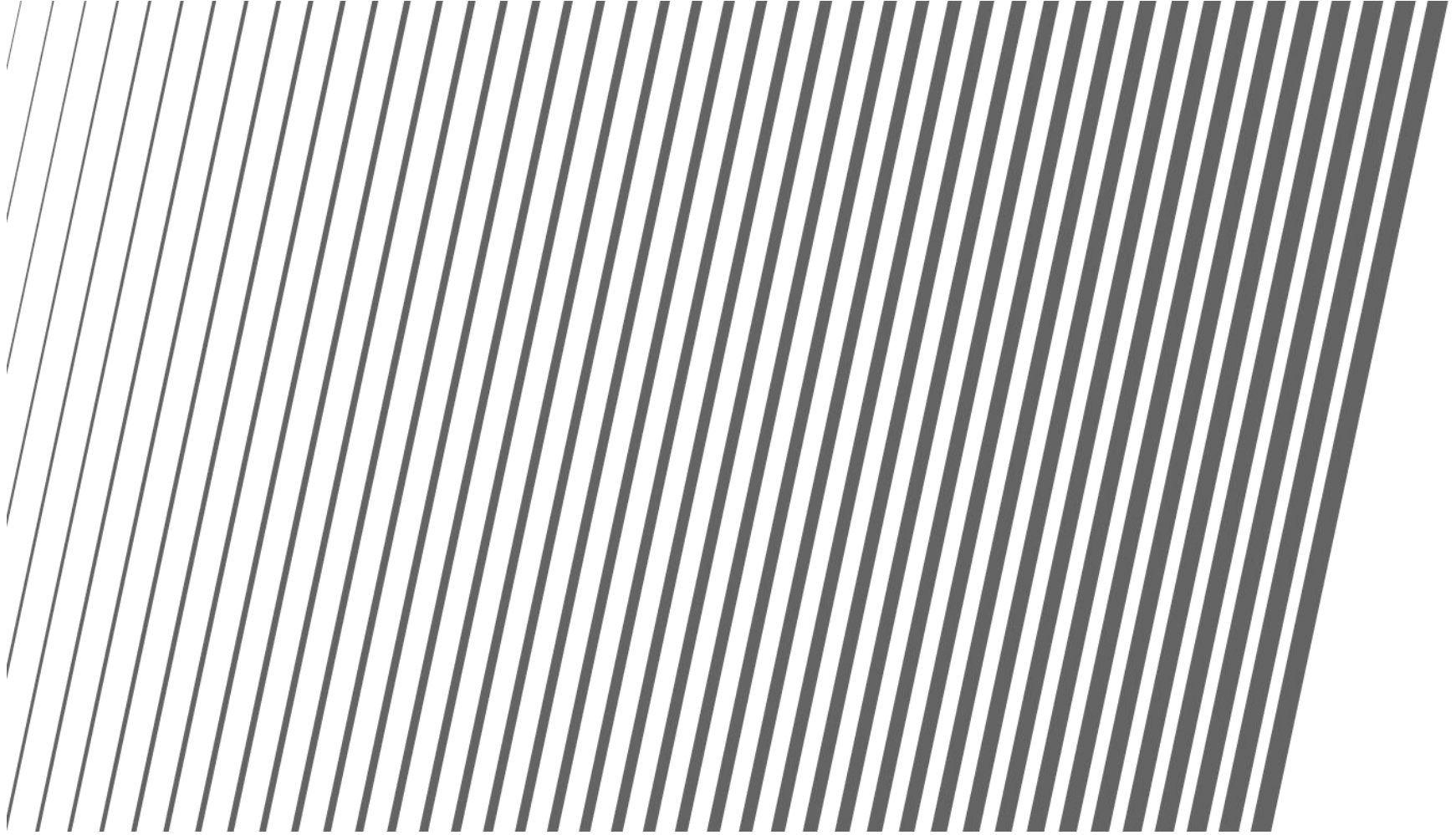
Components of ERM maturity – example 4



The future of ERM framework diagnostic



3. A practical example from the UK energy sector



Background

- ▶ A subsidiary of a large integrated energy company was transforming its business model to provision of insurance-based services
- ▶ As a result of becoming FSA regulated, the company is subjected to stricter requirements with respect to governance, risk management and internal control
- ▶ A review was anticipated in 2011 by the FSA which would focus on these frameworks when assessing the adequacy of the company's enterprise risk and control practices
- ▶ Prior to this project the organisation had five control frameworks: regulatory, financial, operational, risk management and IT – operating discretely, at different maturity
- ▶ Large elements of these frameworks required further development and were not on par with the rest of the group or recognised 'better' practice
- ▶ The organisation acted to address the above by setting up a project and forming a cross-functional team with external support from Ernst & Young

Project objective – establish a structured and sustainable Enterprise Risk & Control Framework which covers risk management, financial, regulatory, operational and IT

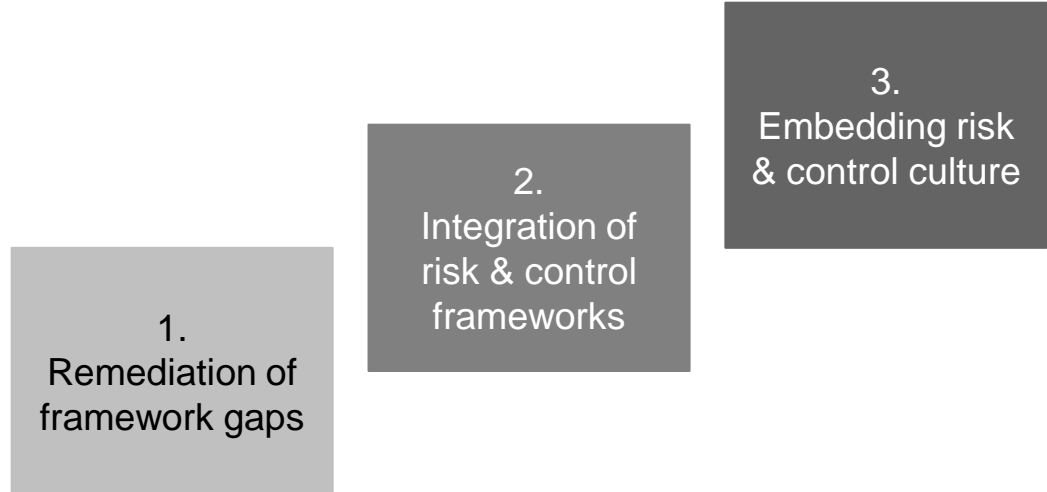
Approach

1. Diagnostic

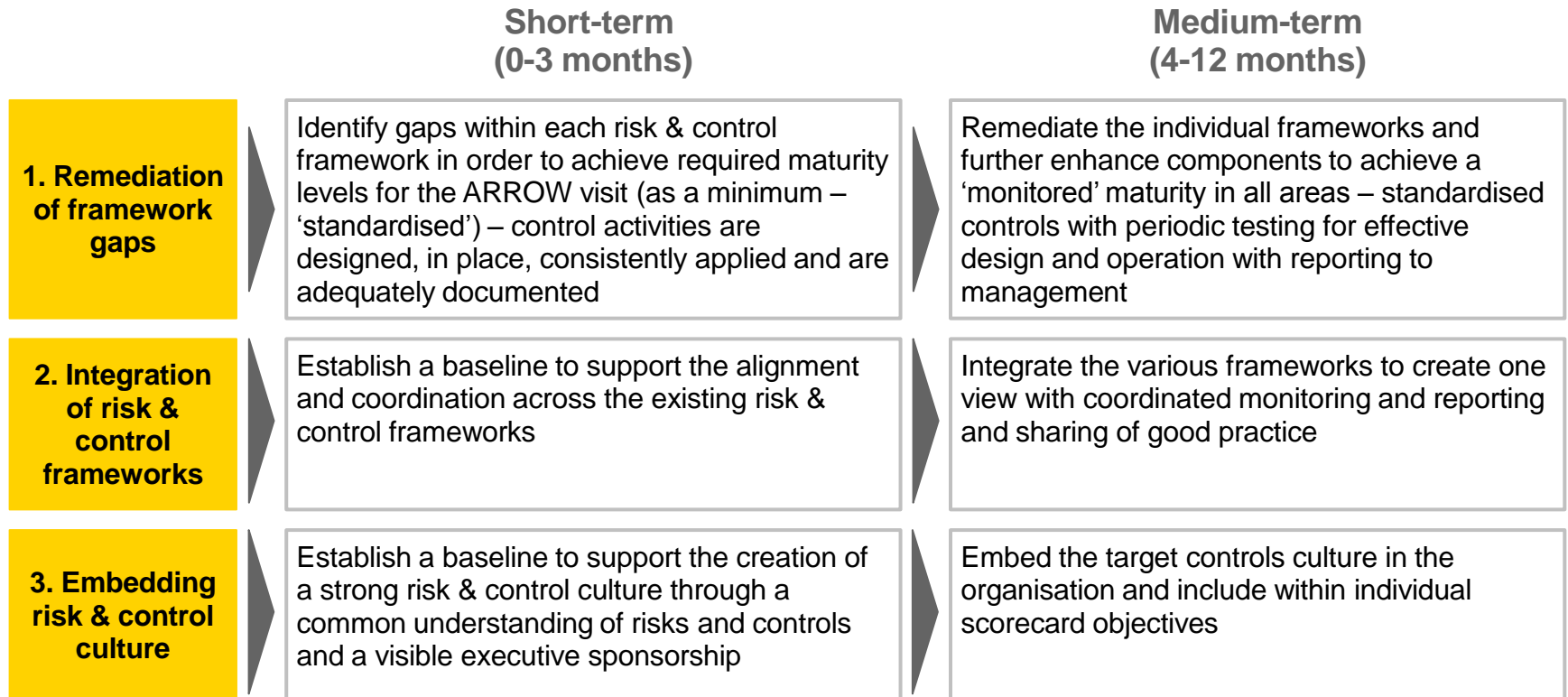
- ▶ Review of risk & control framework documentation
- ▶ Stakeholder interviews and walkthroughs of detailed controls
- ▶ Benchmarking against FSA requirements and 'better' practice
- ▶ Development of a roadmap to improve the company's enterprise risk & control practices

2. Remediation (short and medium term)

Improvements were identified and grouped in three areas which formed the basis for the '**Improvement Roadmap**'



Improvement 'roadmap'



The short-term and long-term actions were designed to support the achievement of an integrated ERM&C framework supported by an embedded risk & control culture

Implementing the improvements

- ▶ A **PMO** was established to direct and monitor the implementation of the agreed improvement actions
- ▶ Appropriate project governance was established to enable and monitor implementation through a **Steering Group** and a **Working Group**
- ▶ **Weekly progress/status updates** were provided to the Steering Group and the Working Group through management dashboards
- ▶ **QA sessions** were scheduled after the completion of short-term actions to challenge the action owners and ensure completeness

The agreed improvement actions were signed off formally by the respective owners to ensure appropriate accountability for implementation of the actions

Benefits and next steps

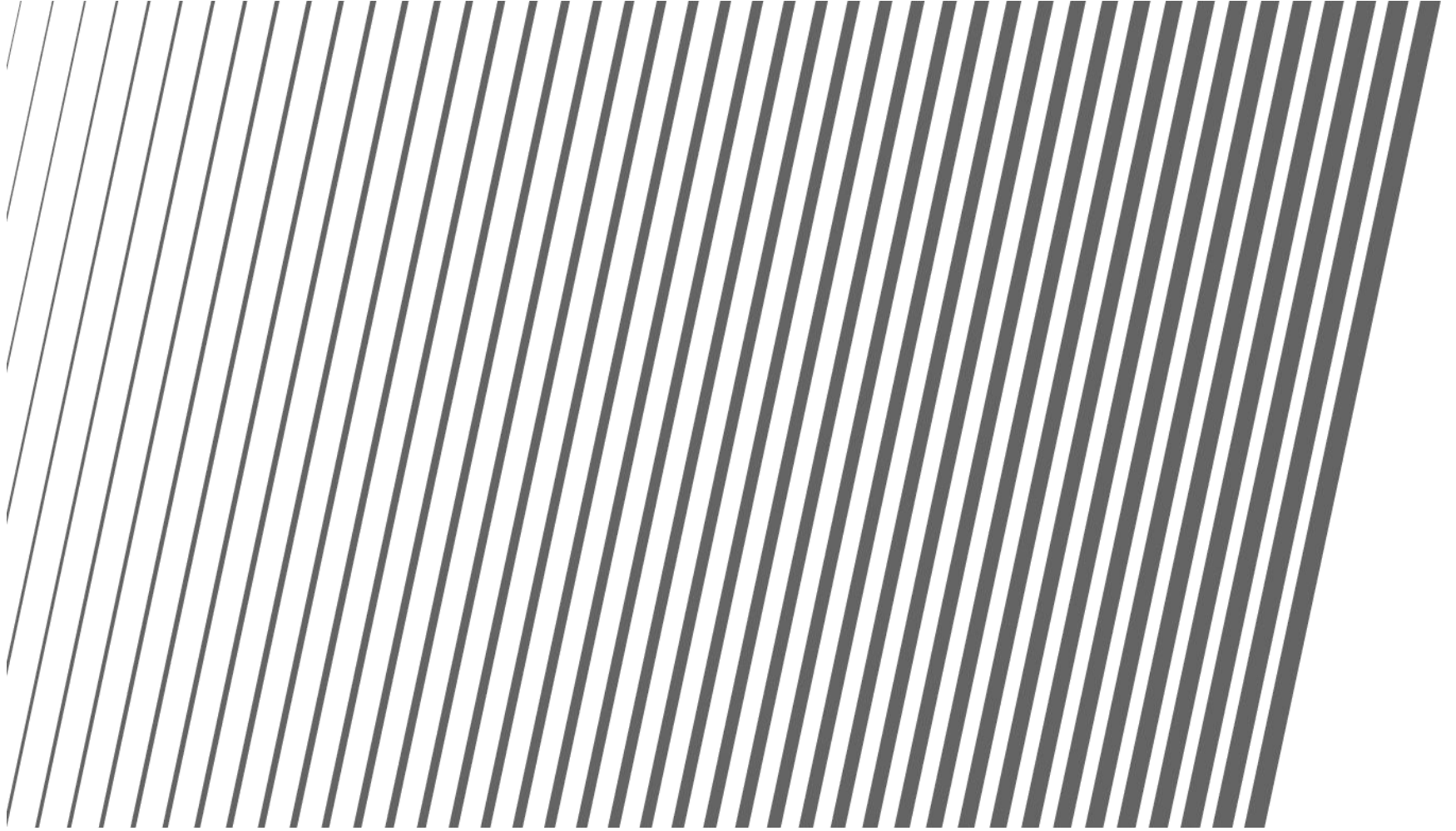
Benefits realised to date

- ▶ Compliance with key FSA obligations
- ▶ Enhanced risk management, control processes and documentation
- ▶ Consistent methodologies, templates and tools across the frameworks
- ▶ Stronger accountability for risk & controls amongst senior stakeholders
- ▶ Improved risk & control awareness and competence amongst stakeholders
- ▶ Improved governance through revised committee composition
- ▶ Better appreciation of risk appetite and calibrated risk assessment approach

Next steps

- ▶ Further integration across the risk & control frameworks through the use of a common IT system
- ▶ Further integration between risk & control frameworks and major programmes
- ▶ Implementation of KRI reporting
- ▶ Validation of control effectiveness
- ▶ Further optimisation of controls through standardisation and automation
- ▶ Benefits realisation – demonstrating tangible P&L improvements

4. Questions & Answers



For further information



Owen Purcell

Partner – Risk
UK&I Advisory, Ernst & Young

Tel: 020 7951 0059

Email: opurcell@uk.ey.com



Leif Tveide

Senior Manager – Risk
UK&I Advisory, Ernst & Young

Tel: 020 7951 6887

Email: ltveide@uk.ey.com



Thank you