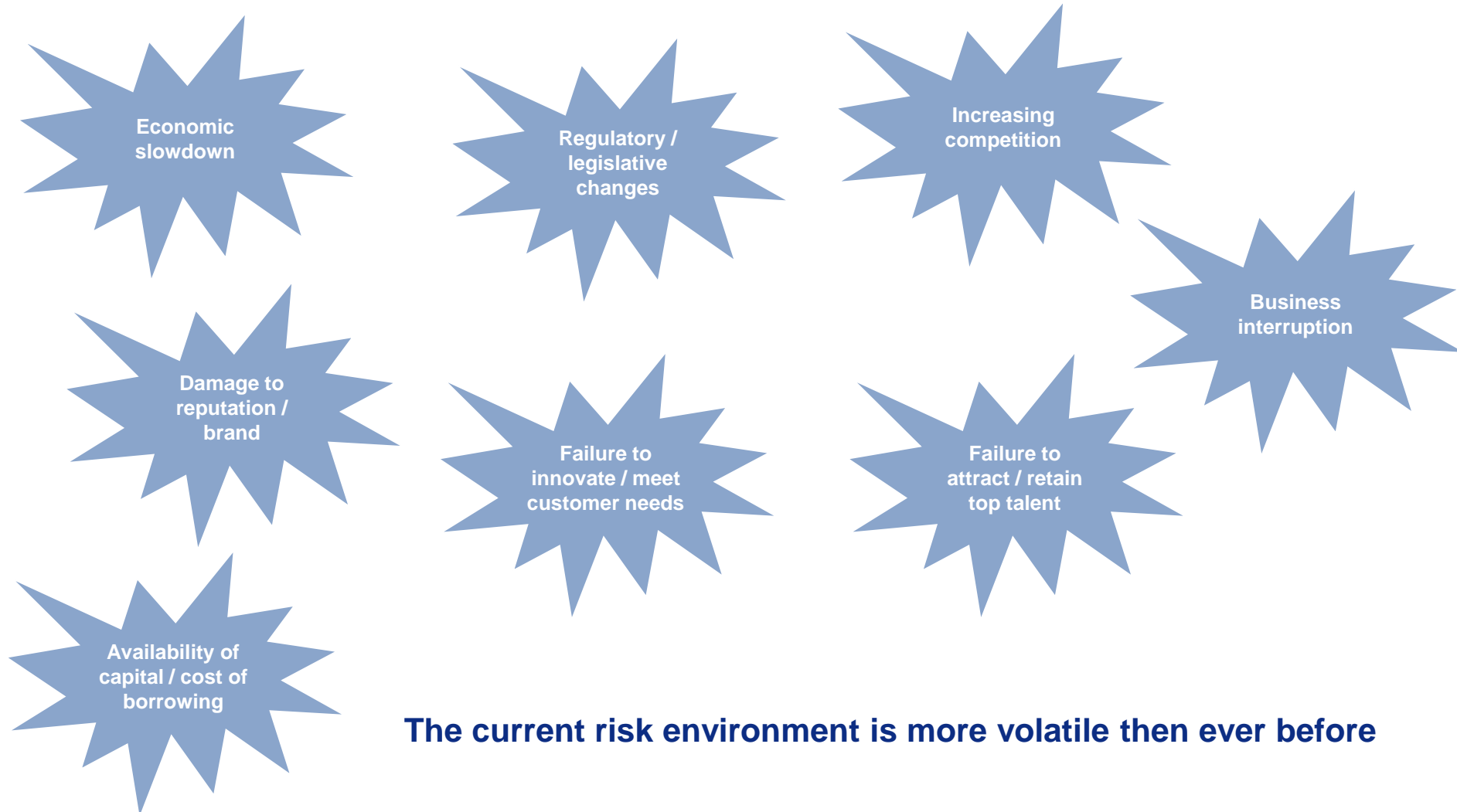


What makes a successful risk function?

Chris Thomas

The risk landscape is changing



The current risk environment is more volatile then ever before

Increased risk management focus

- Investors and key stakeholders
- Critical partners, vendors and suppliers
- Ratings agencies and some market intermediaries
- Standards organisations and professional associations
- Regulatory bodies

Many boards are looking to understand what this means in practice

Stepping up to the challenge

Practical questions to consider:

- Have we defined what “good risk management looks like”?
- What role should the full board play in risk management?
- What are the company’s top risks and how big are they?
- What is management doing about the top risks?
- What discussions about risk have taken place at the board level or among top management when strategic decisions are made and where is this documented?
- How well did we manage a recent risk event?
- How do we measure the effectiveness of the current risk management system?

So what does good risk management look like?

Under-performing	Components of leading practice	Excelling
Unclear control environment and silo oversight	Effective governance and oversight	Transparent control environment, policy framework and challenge
Risk process disconnected to strategy setting	Risk input to strategic direction and business planning	Embedded in key decision making processes
Stand alone risk assessment	Risk integrated with performance management	Embedded in key decision making processes
Ad hoc risk assessment at project outset	Risk and change	Aggregated view of programme and project risks
Costly silos	Integrated assurance	Single view, risk-based
Pockets of expertise	Maintaining capability and risk awareness	Induction and ongoing training and awareness programmes
Not considered	Extended enterprise (partners, suppliers, customers etc.)	Influence on and oversight over third parties

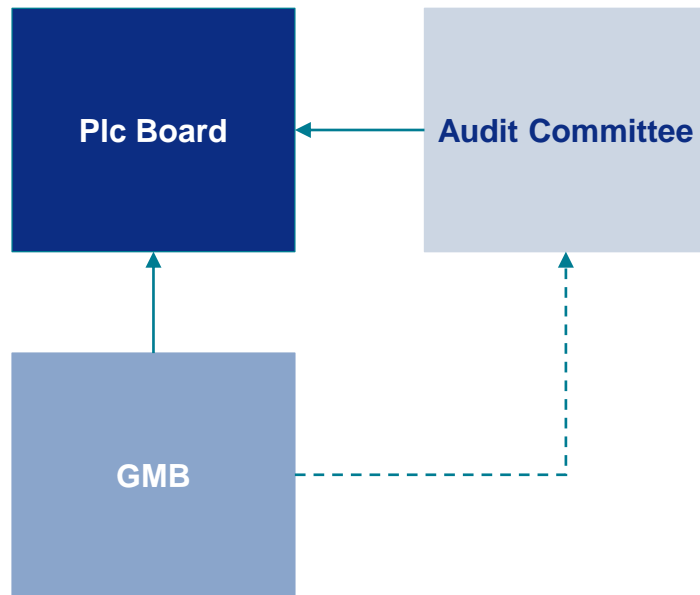
Risk oversight is key

- Too much focus on getting the “process” right
- Boards need to focus more on “content” and “outcomes” – have we identified the right risks and are risk mitigation actions appropriate?
- Leading practice recommendations:
 - Add risk as a standing item to the board agenda
 - Select two or three top risks for discussion at each board meeting such that the board is able to gain coverage of all key risks during the course of the year
- A clear risk management organisation and reporting structure is essential in ensuring appropriate accountability, oversight and challenge

Key to this structure is the use of a risk committee...

Option 1 – traditional model

- The traditional model adopted by UK Plc is shown below although in our experience more mature organisations have moved on from this model

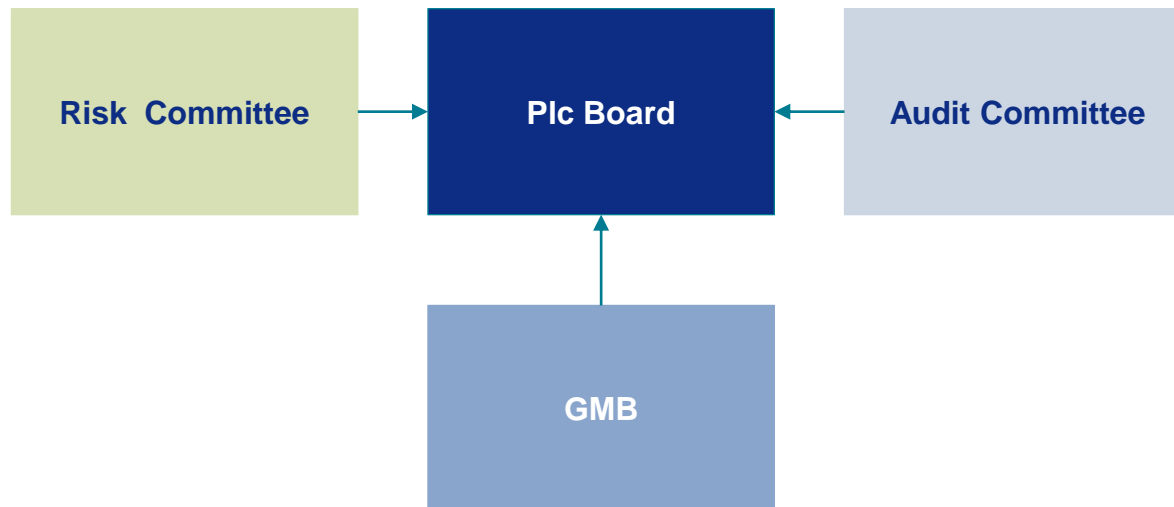


Characteristics :

- The Board delegates the risk discussion to the Audit Committee
- Independent Non Executive Chairman
- Executive management involvement in risk debate via invitation only

Option 2 – board risk committee

- The model below shows a formally constituted Board Risk Committee
- This model is typically found in the financial services sector as well as industries that have critical safety or technical risks

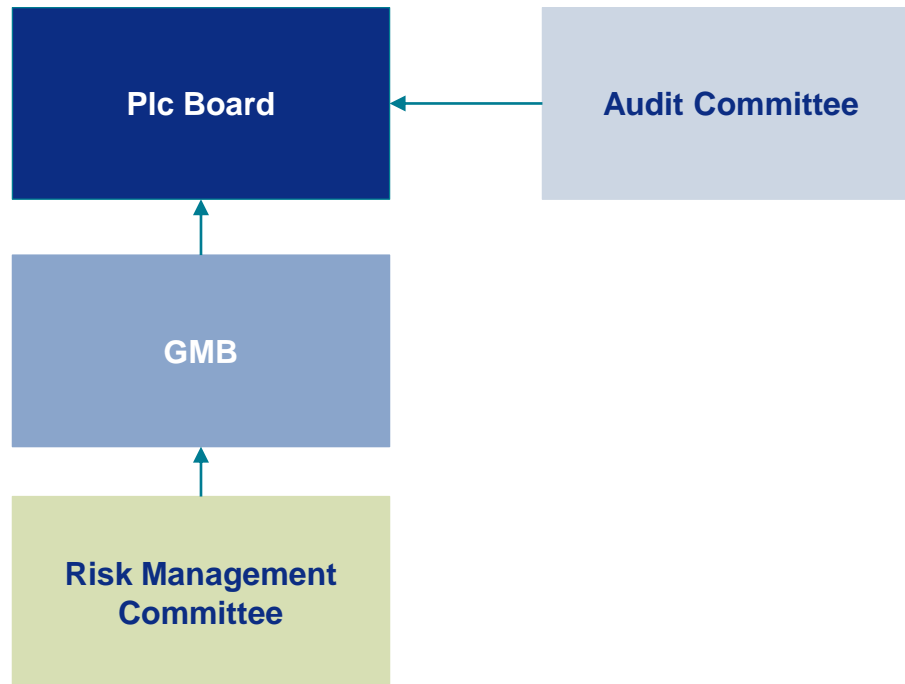


Characteristics :

- A formal Board sub committee for risk management
- Non Executive Chairman
- Executive management involvement on risk committee through invitation only
- Audit Committee focus remains on reviewing the effectiveness of the Company's internal control and risk management systems

Option 3 – emerging model

- The below model is emerging as a popular method of engaging Executive management in the risk debate
- This model is typically found in the commercial sector



Characteristics :

- An Executive risk committee reporting through the GMB to the Board
- Collective Executive management engagement and oversight through the risk committee with healthy debate and challenge over the content of the risk reporting
- Audit Committee focus remains on reviewing the effectiveness of a company's internal control and risk management systems

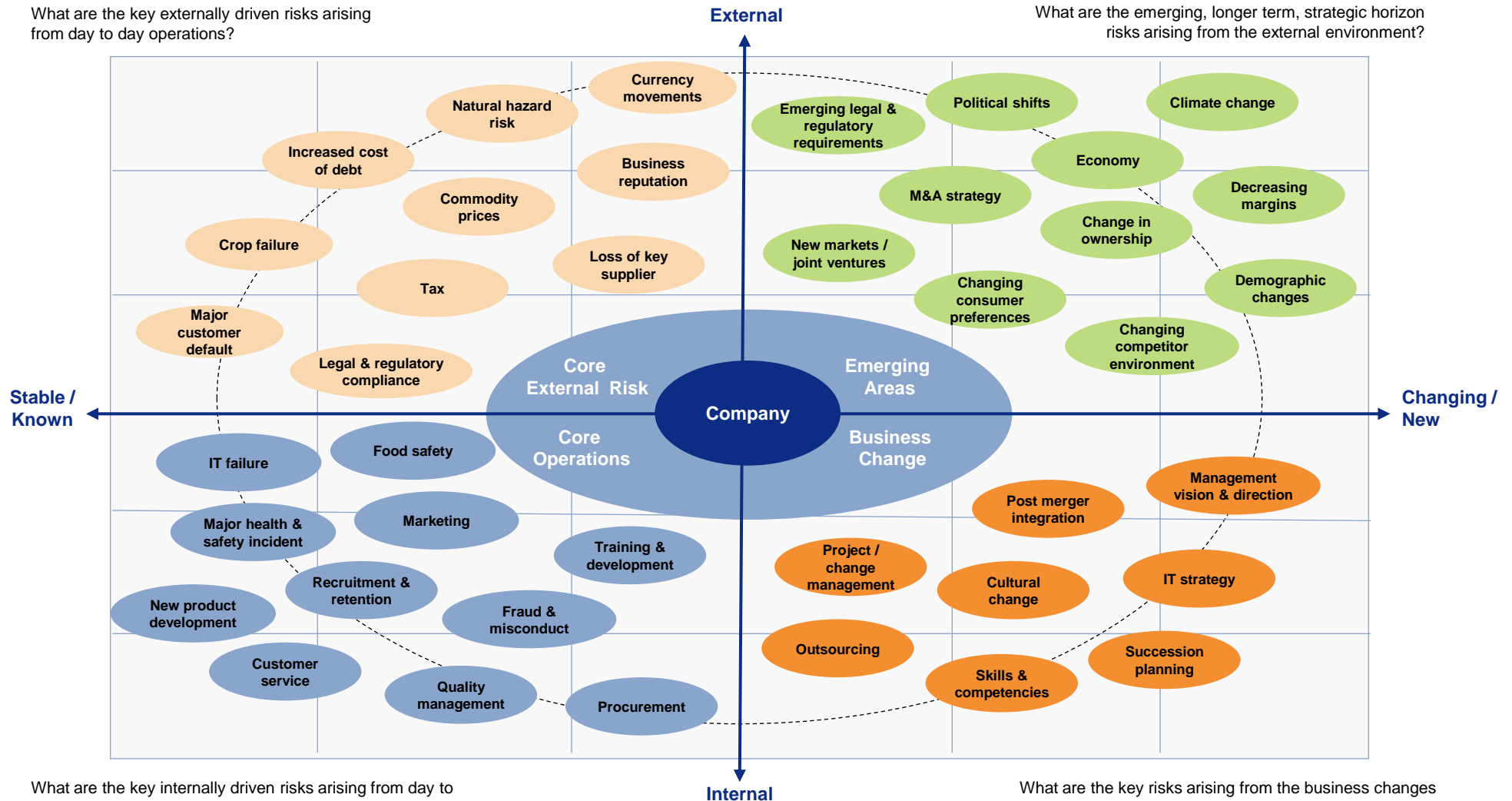
Risk identification and assessment

- Sources for identifying risks tend to be internal and focus on day-to-day operations rather than longer term strategic risks
- Limited analysis of the causes and consequences of risks
- Limited analysis of controls, compliance and assurance activities and whether these are operating effectively
- Leading practice recommendations:
 - Define the risk universe for your entity
 - Integrate risk management into the strategic planning cycle
 - Conduct deep dive analysis for top risks
 - Develop a combined assurance map for top risks

Risk universe: applying a different lens

What are the key externally driven risks arising from day to day operations?

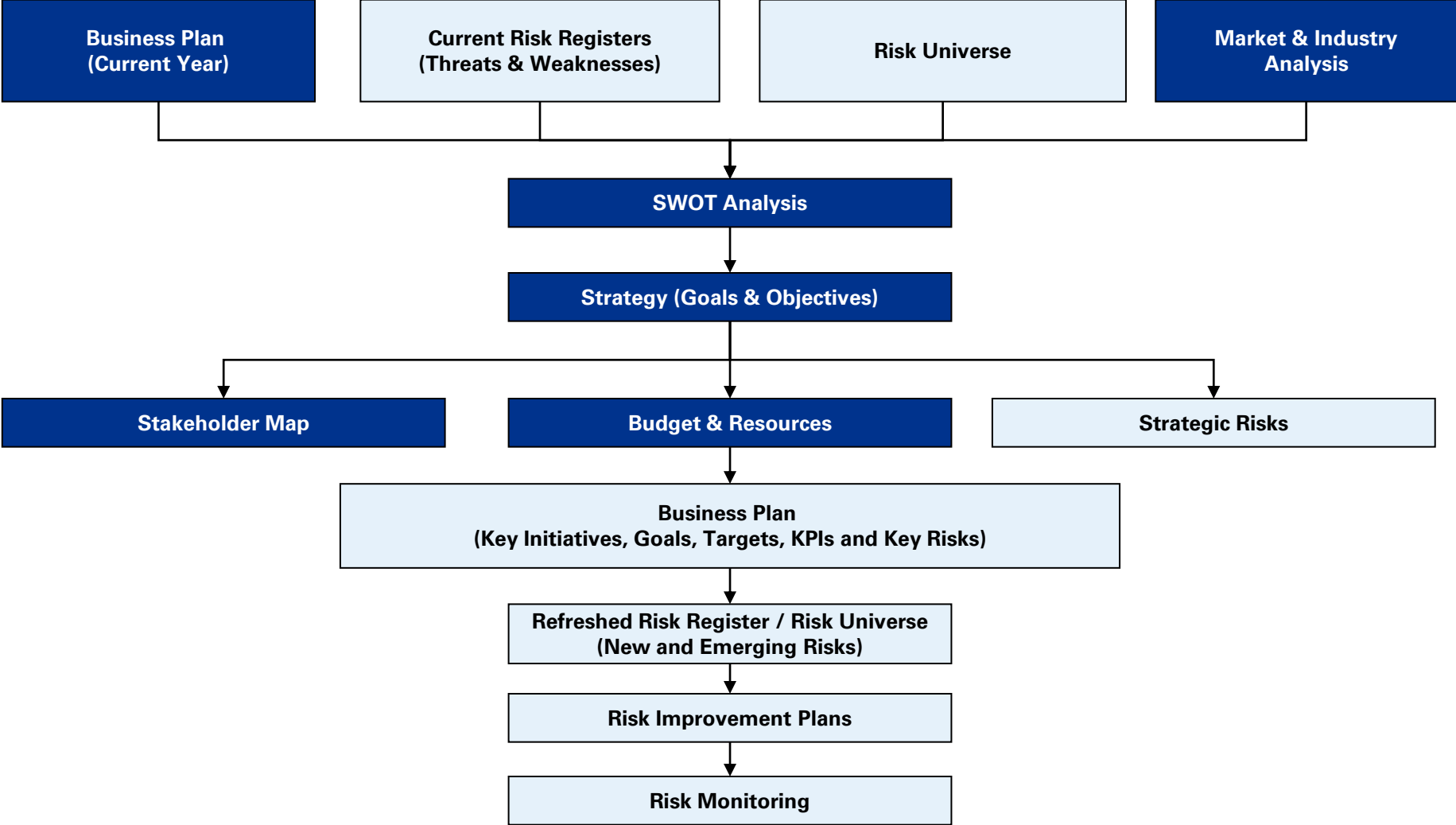
What are the emerging, longer term, strategic horizon risks arising from the external environment?



What are the key internally driven risks arising from day to day operations, primarily within management control?

What are the key risks arising from the business changes required to implement the business strategy?

Link to strategic planning



Improving risk insight: deep dive analysis

Review Area	Deep Dive Questions
Inherent Risk Rating	<ul style="list-style-type: none"> • Is there a clear understanding of the causes and consequences of the risk? • Does the inherent risk rating align with past history of the risk within the business? • Have instances of this risk materialising within the operating environment occurred and its impact been considered? • Has the level of dependence to business strategy or operations been fully captured? • Have risk interdependencies across the business been evaluated?
Control Effectiveness and Residual Risk Rating	<ul style="list-style-type: none"> • Is there a clear understanding of the control, compliance and assurance activities that mitigate this risk? • Have instances occurred where the risk has materialised? If so, was this due to control failure, absence or ignorance? • Have assurance reports been completed for this risk or supporting controls? If so, what was the rating and is this consistent with the control effectiveness rating in the risk register? • Have any management reviews been performed? If so, what were the outcomes and are these consistent with the control effectiveness rating in the risk register? • Has the level of skill and competence of staff operating these controls been considered? • Has the level of resources and budgets had an impact on the level of controls? • What is the control culture of the business and has this been included in this evaluation?
Risk Improvement Plan	<ul style="list-style-type: none"> • Do the action plan items clearly link to the risk to be mitigated? • Does the action plan align to the business plan and strategy? • Has the likelihood and impact of successful implementation been evaluated? • Have resource and budget constraints been considered as part of the action plan?
Target Risk Rating	<ul style="list-style-type: none"> • Is the target risk rating aligned to business strategy and risk management policy? • Is target risk rating achievable considering the operating environment both internally and within the market? • Is the target risk rating achievable considering the budget and resource constraints of the business?

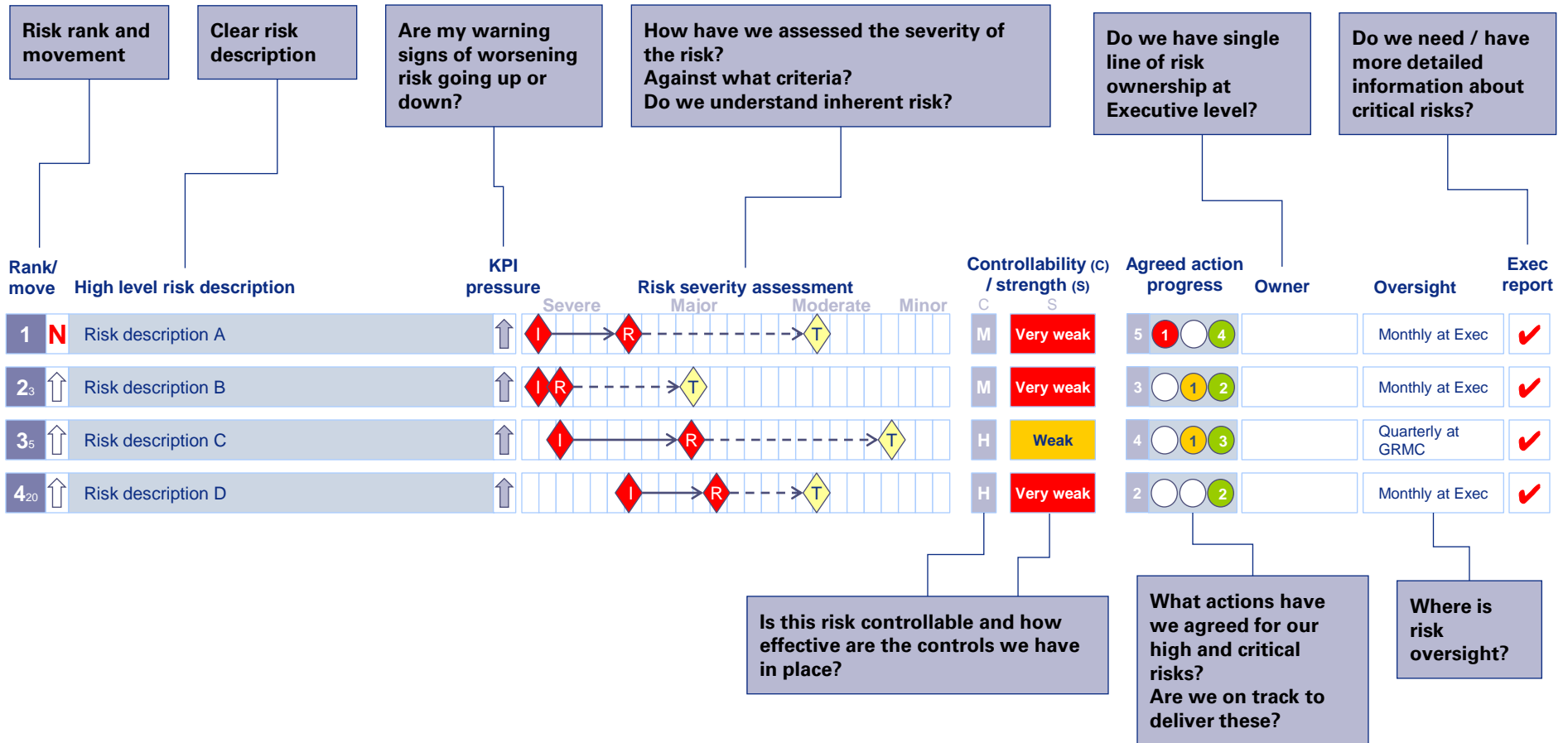
Combined assurance map

Risks	Three Lines of Defence										
	Line Management				Oversight Functions				Independent Assurance		
	Reviews	Sign-offs	Self-Assess	KPIs	Finance	H&S	HR	IT	External Auditors	Internal Audit	Specialists
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											

Risk monitoring and reporting

- Quality of risk management information is one of the biggest challenges to boards in providing effective risk oversight
- Top down versus bottom up reporting
- How do we know if we are taking on too much or too little risk?
- Leading practice recommendations:
 - Develop a risk dashboard reporting format
 - Develop a set of common Key Risk Indicators (KRIs)
 - Define risk appetite

What might the Executive dashboard look like?

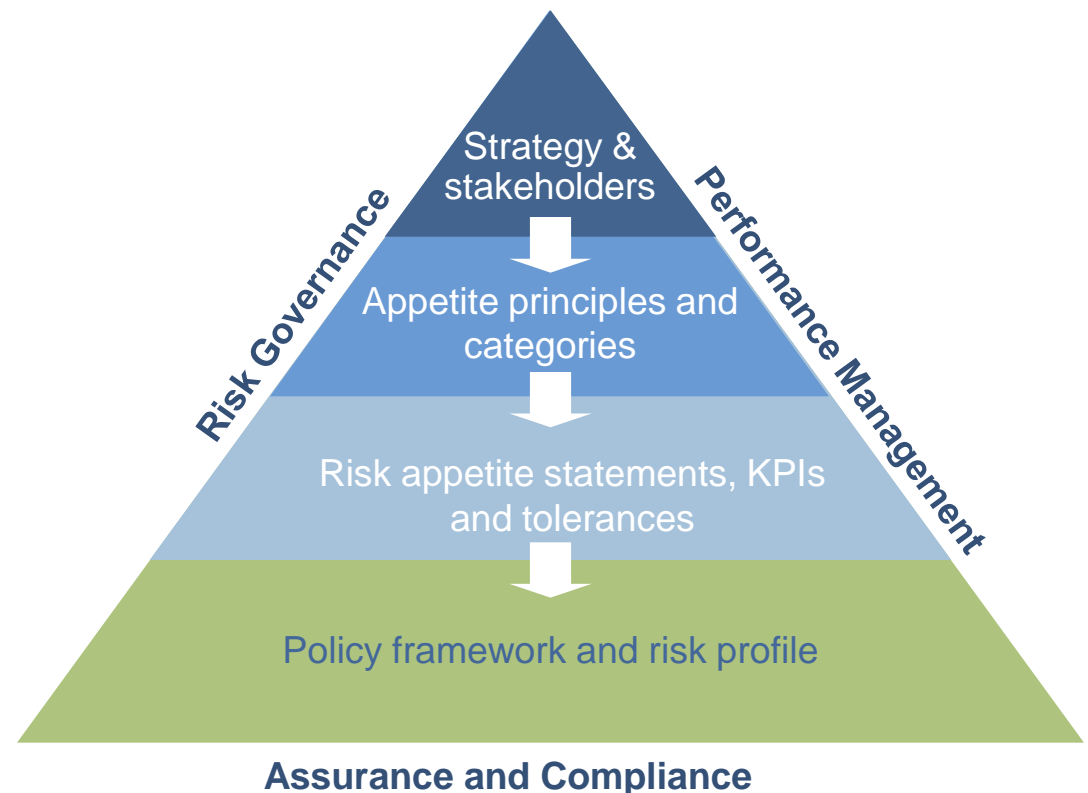


Risk appetite: the missing link

Risk Appetite is the amount of risk an organisation is willing to take in pursuit of its business objectives. It is at the heart of how a company does business and how it is perceived by its stakeholders and provides context and influence over the organisations system of internal control

The benefits of understanding and applying risk appetite correctly:

- Inform decision making, aligning risk and reward considerations
- Create consistent behaviours
- Help to define the appropriate control and policy framework
- Reduce personal biases and attitudes towards risk
- Focus on measures and limits, numeracy and analytics



Risk appetite: employees

Risk appetite for Employees	Key Risk Indicator	Current Status / Measurement
<ul style="list-style-type: none"> Company XYZ will accept deviation of 10% from staff engagement target measure Company XYZ is willing to absorb short term periods of increased staff turnover up to 5%. Company XYZ has no appetite for three consecutive periods of increased turnover without a formal remediation plan Company XYZ has no appetite for loss of key executives without a formal succession plan being in place Company XYZ has no risk appetite for: <ul style="list-style-type: none"> Any policies, practices or behaviours that discriminate on the basis of sex, race, disability, sexual orientation, creed, colour, trade union status or age Management actions or inaction in conflict with Company XYZ's core values 	Staff Engagement	
	Staff Turnover	
	Succession Plans for Key Personnel	
	Respect at Work	

Thank you

Chris Thomas, Financial Services Risk Management

Mobile: 07833 737 672

E-Mail: Chris.Thomas@KPMG.co.uk