airmic
www.airmic.com

Connecting the Risk Function and Internal Audit

Marsh Ltd

David Stark and David Gwilt

Introductions

- **David Stark** – Consulting Director and Practice Leader of Enterprise Risk Services, Marsh Advisory UK&I
- **David Gwilt** - Risk Partner, Marsh Advisory UK&I

Learning objectives

Provide information on the following:

1. Corporate governance context
2. Key risk principles
3. FTSE100 analysis
4. Exploration of the common themes
5. Practical internal audit considerations
6. Conclusions

1. Corporate governance context

Background
Guidance has been provided to the UK's listed companies since the early 1990's

Definition

- The Financial Reporting Council (FRC) **defines** corporate governance as: *"…the system by which companies are directed and controlled*."[1]
- The UK has a well established history of guidance and stipulations for listed companies which have been formalised and revised since the **Cadbury Committee**'s work on the UK Corporate Governance Code in **1992**.
- Other notable guidance includes the **Sarbanes-Oxley (SOX) Act**[2] introduced in the early 2000's, applicable to US listed companies.

Requirements

- Listed companies are required to abide by the governance requirements applicable to the stock exchange on which they are listed. Companies listed on **London Stock Exchange** (LSE) **Main Market** (premium listings) are required to apply the UK Corporate Governance Code. **Key requirements**:
  - 'Comply or Explain' to the application of the Principles and Provisions
  - CEO and Chair person roles to be separate
  - Boards should have at least 3 Non-Executive Directors (NEDs)
  - The board should have an Audit Committee composed of NEDs [Provision 24]
- Companies listed on the Alternative Investment Market (AIM) can chose to apply either the UK Corporate Governance Code or the **Quoted Companies Alliance (QCA) Corporate Governance Code**.
- Guidance to private companies is provided in the FRC's '**The Wates Corporate Governance Principles for Large Private Companies**'[3], issued in response to a UK Government Report[4] stating the need for improved transparency and accountability.

Recent company failures and crises have heightened public awareness and the need for effective governance.

1. Abstracted from paragraph 2.5 of the Combined Code, 1992. Key UK legislation includes the Companies Act 2006.
2. The Sarbanes-Oxley (SOX) Act was introduced as a US Federal Law in 2002 and states governance requirements for all US public companies. SOX was legislated due to corporate and accounting scandals, primarily Enron and Worldcom.
3. Published in December 2018. Large private companies will apply these principles to their reporting in 2020.
4. Corporate Governance Report published in April 2017 by the House of Commons' Business, Energy and Industrial Strategy Committee .

Background
Guidance has been provided to the UK's listed companies since the early 1990's

UK Govt – Restoring Trust in Audit and Corporate Governance

- Consultation paper issued in March 2021 and recently closed.
- Various objectives including "…improve company reporting on the key issues of risk, assurance and internal controls."
- New authority to be created - Audit, Reporting and Governance Authority (ARGA), replacing the Financial Reporting Council (FRC).
- Company directors will have new reporting and attestation requirements for internal controls and resilience planning.
  - **Annual Resilience Statement**, setting out how directors are assessing the company's prospects and addressing challenges to its business model over the short, medium and long-term, including risks posed by climate change;
- Expected to apply to reporting periods starting in 2023.

Source: BEIS; Restoring trust in audit and corporate governance; Consultation on the government's proposals; March 2021.

UK Corporate Governance Code
Effective Enterprise Risk Management implementation is key to success

UK Corporate Governance Code Structure

- The UK Corporate Governance Code[1] is divided into 5 sections: (1) Board leadership and company purpose; (2) Division of responsibilities; (3) Composition, succession and evaluation; **(4) Audit, risk and internal control**; (5) Remuneration.

3	**Principles** for Audit, Risk & Internal Control (ref. M. N. O.)
8	**Provisions** for Audit, Risk & Internal Control (ref. 24. - 31.)
1	**Guide** on Risk Management, Internal Controls and Related and Financial Business Reporting[2]

Enterprise Risk Management (ERM) definition

- COSO[3] defines **ERM** as "The **culture, capabilities** and **practices, integrated** with **strategy and execution**, that organisations rely on **to manage risk in creating, preserving and realizing value**".
- Identifying, analysing, controlling, monitoring and reporting risk across an organisation is key to the success of its corporate governance.

UK Corporate Governance – applicable Principles for risk management

- In addition to Principal M for Audit, the following Principles apply under 'Section 4 – Audit, Risk and Internal Control':
  - N "The board should present a **fair, balanced and understandable assessment** of the company's **position and prospects**."
  - O "The board should **establish procedures** to **manage risk**, **oversee the internal control framework**, and determine the **nature and extent of the principal risks** the company is **willing to take** in order to achieve its long-term strategic objectives."
- Guidance on **principal risks** is as follows: "Principal risks should include, but are not necessarily limited to, those that could result in events or circumstances that might threaten the company's business model, future performance, solvency or liquidity and reputation. In deciding which risks are principal risks companies should consider the potential impact and probability of the related events or circumstances, and the timescale over which they may occur."

1. The UK Corporate Governance Code, July 2018.
2. Guidance on Risk Management, Internal Control and Related Financial and Business Reporting, September 2014. Note: As of early 2020, the FRC has announced that further changes will be made to this document in light of the collapse of Carillion.
3. COSO Enterprise Risk Management – Aligning Risk with Strategy and Performance (June 2016) guidance.

UK Corporate Governance Timeline
Overview of key events

1990's

1992
Cadbury Committee[1] create the first version of the UK Corporate Governance Code, titled "*Financial Aspects of Corporate Governance".*

1995
Confederation of British Industry (CBI) release the **Greenbury Report**.
Focus on remuneration.

1998
Hampel Committee issues report which reviewed Cadbury and Greenbury recommendations and provided guiding principles. Led to the publication of **The Combined Code on Corporate Governance** in June 1998

1999
Turnbull Report issued on "Internal Control: Guidance for Directors on the Combined Code".
Focus on controls and **risk management.**

2000's

2003
Higgs Report [2]on "Review of the role and effectiveness of non-executive directors". Focus on NEDs and Audit Committee. **Revised Combined Code** published in June 2003.

2005
Turnbull Guidance[3] reviewed, updated and published.
Focus on disclosure.

2006
Revised version of Combined Code following **consultation**.

2008
Revised version of Combined Code following **new EU requirements** for audit committees and corporate governance statements.

2010's

2010
Revised version of Combined Code to give **clearer guidance** and **improved risk management reporting** provisions.

2011
Sharman Inquiry to identify lessons on going concern and liquidity risk.

2012
Revised version of Combined Code.
Focus on audit reporting, annual reports &board diversity.

2014
Revised **UK Corporate Governance Code**.
Focus on investor info., business long term health and strategy, and publication of **Guidance on Risk Mgmt, Int. Control & Related Financial/Business Reporting.**

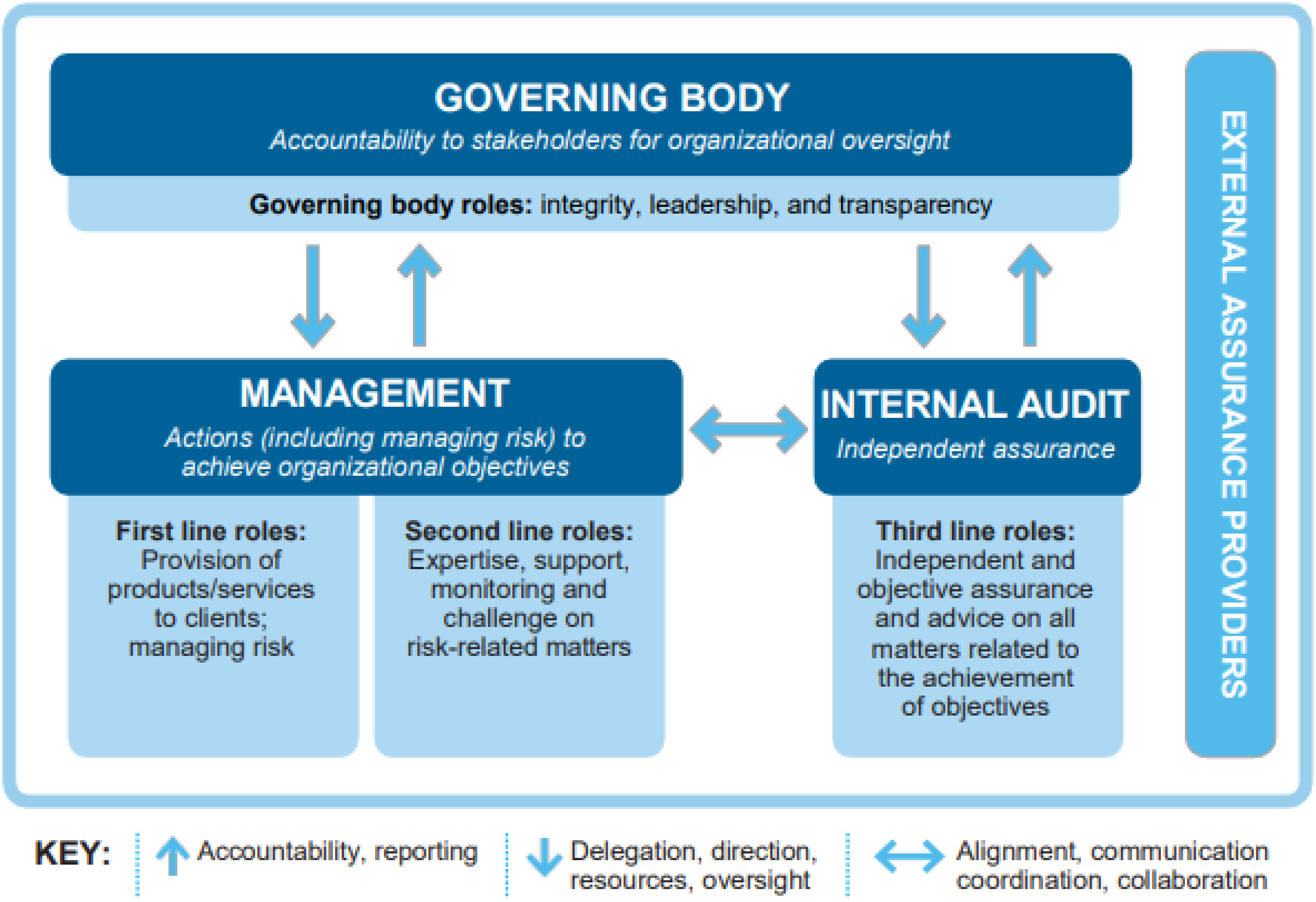
2015
Insurance Act introduced

2016
Revised version following **new EU Audit Regulation and Directive.**

2018
Revised **UK Corporate Governance Code** following a comprehensive review. **Guidance on Board Effectiveness** also published.

1. The Committee on the Financial Aspects of Corporate Governance was created in 1991 by the Financial Reporting Council, the Stock Exchange and the accountancy profession, chaired by Sir Adrian Cadbury.
2. UK Government appoints Sir Derek Higgs to review the role of independent directors and audit committees.
3. Superseded by the 'Guidance on Risk Management, Internal Control and Related Financial and Business Reporting' in September 2014.

The Institute of Internal Auditors (IIA) Three Lines Model



Source: *The Institute of Internal Auditors: The IIA's Three Lines Model: An update of the Three Lines of Defense*

Notable business failures and corporate crises[1]
Leading to the evolution of Corporate Governance for large listed companies

1990's	Pan Am, Source Perrier, Eli Lilly, Ratners, BCCI, Noordbanken, Barings Bank, Commercial Union, Heineken, Mirror Group Newspapers (Maxwell), Commodore, Firestone.
2000's	Equitable Life, Independent Insurance, Railtrack, Worldcom, Swissair, Enron, Arthur Anderson, Tyco, MG Rover Group, Bear Stearns, Northern Rock, Lehman Brothers, AIG, Washington Mutual, Royal Bank of Scotland, ABN-Amro, Bernard Madoff Investment Securities, Cadbury Schweppes, Nortel, Anglo Irish Bank, Société Générale, Blockbuster, Woolworths, General Motors.
2010's	BP, Borders, Honda, Nissan, Olympus, Toyota, Kodak, UBS, Sony, JP Morgan, Telia Company, Target, eBay, Home Depot, Petrobras, General Motors, TalkTalk, Toshiba, Volkswagen, Samsung Electronics, Wells Fargo, Equifax, BT Group, Facebook, British Home Stores, Carillion, Toys R Us, Thomas Cook.

Abstract from the FRC's 'Guidance on Risk Management, Internal Control and Related Financial and Business Reporting':

Section 1 – Introduction	MA research reference
Economic developments and **some high profile failures of risk management** in **recent years** have reminded boards of **the need to ensure that the company's approach to risk has been properly considered** in setting the company's strategy and **managing its risks**. **There may be significant consequences if the company does not do so effectively**.	2018 research on the impact of corporate crises on share price

Source: The Impact of Catastrophes on Shareholder Value, Knight and Pretty; *Publically available information such as business news websites, and AIRMIC Roads to Ruin research.*

1. The above list is not exhaustive and represents a summary list of companies liquidated / bankrupt or that have suffered from significant crises events which has undermined shareholder value. All of the above companies have been widely reported in the media and some have been the subject of academic or industry body research.
2. Abstracted from FRC's 'Guidance on Risk Management, Internal Control and Related Financial and Business Reporting', September 2014.

2. Key risk principles

UK Corporate Governance Code[1]
Key Provisions[2] within Section 4

#	Risk Area	Guidance	Principal / Provision No.
1	Robust Risk Assessment	**Assessment of the company's principal and emerging risks**. Confirm its completion in its annual report. Include description of its principal risks and an explanation of **how these are managed or mitigated** (establish procedures to manage risk).	Provision: 28
2	Emerging risks	Carry out **robust assessment of its emerging risks** and confirm its completion in its annual report. Include what **procedures** are in place **to identify emerging risks** and explain how these are being managed and mitigated.	Provision: 28
3	Monitor and review	Board should **monitor** the company's **risk management and internal controls system**. Carry out a review of their effectiveness and report on that review in their annual report. Monitoring and review should cover all material controls, including financial, operational and compliance controls.	Provision: 25, 29
4	Going concern basis of accounting	The board should state whether it considers it appropriate to adopt the going concern basis of accounting in preparing in its annual financial statement; **identify any material uncertainties** to the company's ability to continue to do so.	Provision: 30
5	Viability	Consider company's **current position and principle risks**. Company should report how it has assessed its prospects, **over what period** it has done so and **why it considers that period**. State company's ability to operate and meet its liabilities as they fall due over their period of assessment. Attention should be paid to any qualifications or assumptions as necessary.	Provision: 31
6	Risk Appetite	The board should determine the nature and **extent of the principal risks the company is willing to take**.	Principal: O

Annual Report

- Risk information is included in the Strategic Report section of a company's Annual Report.
- Information typically provided on the company's approach to risk management, the principal risks and uncertainties and the viability statement.
- Risk governance information is provided in the Governance section.

The revised Corporate Governance Code is applicable to accounting periods commencing 1 January 2019.

1. The revised UK Corporate Governance Code was published in July 2018 and applies to accounting periods beginning on or after 1 January 2019.
2. The UK Corporate Governance Code, July 2018, Section 4 – Audit, Risk and Internal Control.

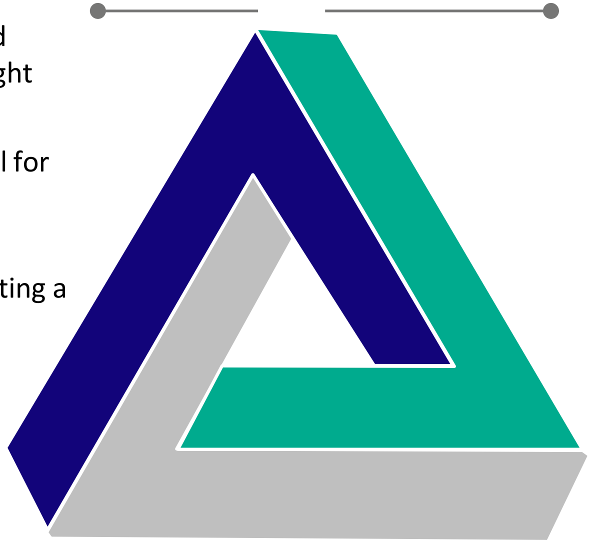
ISO 31000:2018 Risk management

Principles and Guidelines provides a common approach to managing any type of risk

- Three fundamental elements of ISO 31000:2018 – Framework, Principles and Process – are described below

Framework

- Risk governance objective is to create and protect value through integration, oversight and assurance
- Leadership and commitment are essential for the successful implementation of risk framework
- Risk governance defines the steps of creating a risk framework is structure:
  1. Design
  2. Implementation
  3. Evaluation
  4. Improvement
  5. Integration



Principles

- Effective risk framework is characterised by the following:
  - Integrated
  - Structured and comprehensive
  - Customised
  - Inclusive
  - Dynamic
  - Based on reliable information
  - Embedded with human and cultural factors
  - Improved continuously

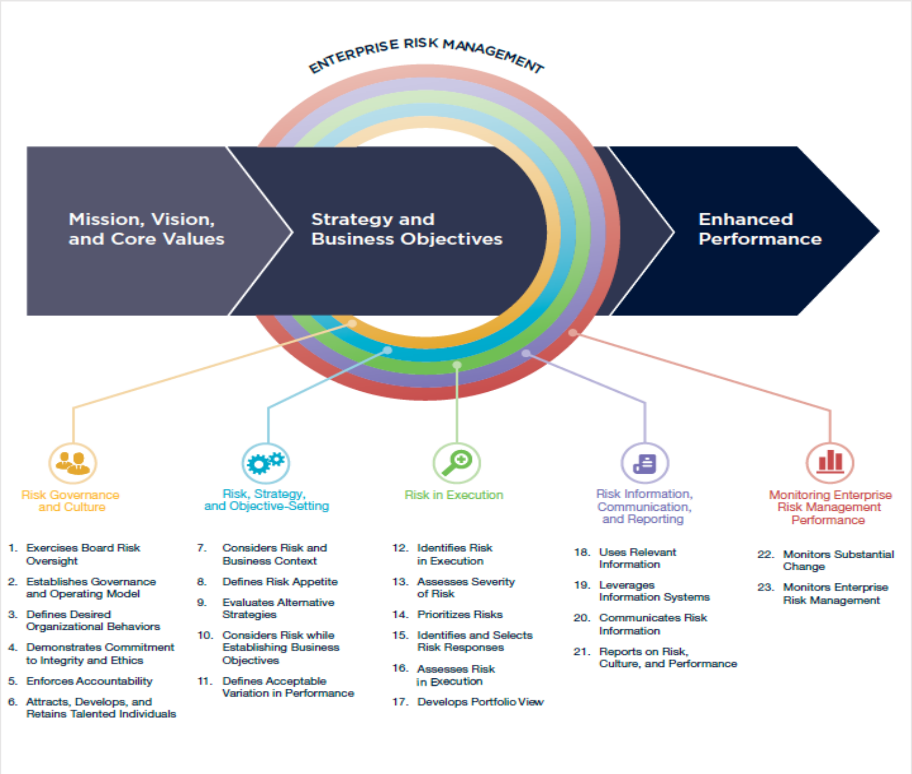
Process

- Risk management process consists of the following elements:
  1) Communication and consultation
  2) Establishing the context
  3) Risk assessment
  4) Risk treatment
  5) Monitoring and review

Source: *ISO31000*

COSO[1] framework

Integration of ERM into all aspects of organisational operations, and emphasises the link between risk, value and performance



1 – Committee of Sponsoring Organizations of the Treadway Commission

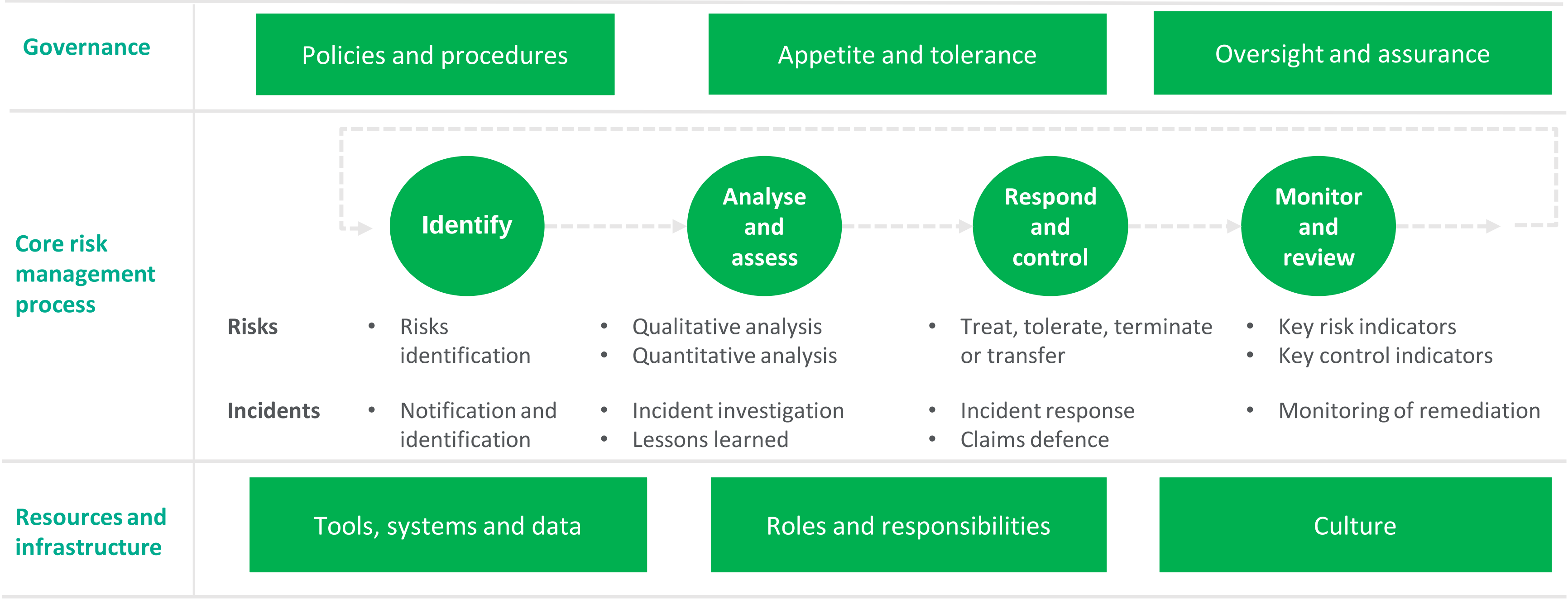
Source: *Aligning Risk with Strategy and Performance, © [2016] Committee of Sponsoring Organizations of the Treadway Commission (COSO).*

Marsh Advisory's ERM Framework

Consists of three major components: Governance, Core risk management process, and Resources and infrastructure

- The ERM framework sets out a consistent approach to the management of risk within the organisation which is integrated with business processes as well as providing independent oversight to assure performance. The latter demonstrates the approach to stakeholders (internal or external) to instil confidence on the organisation's approach to risk management
- An organisation's stakeholder reporting (e.g. the risk section of the Annual Report) should be based upon the information within the Framework, whilst not disclosing full details as this will be commercially sensitive.

Marsh Advisory Consulting Solutions generic ERM Framework



1 – Enterprise Risk Management – Aligning Risk with Strategy and Performance (June 2016)

Source: *Marsh Ltd*

Effectiveness of controls

Determines control adequacy and to identify where additional control improvement actions may be required

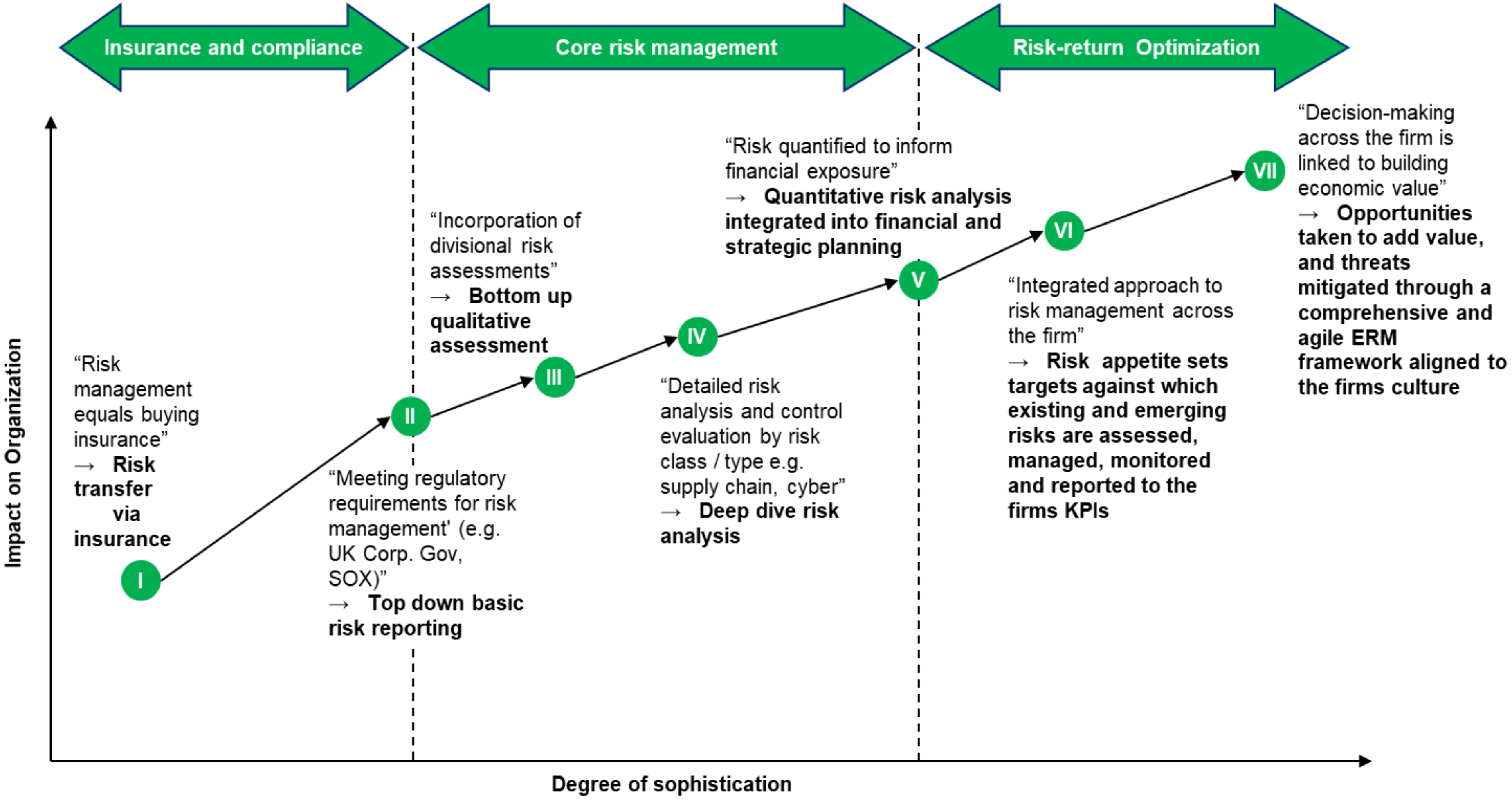
- Example criteria for control effectiveness are outlined below

<table>
<tr><th>Stage</th><th>Criteria</th><th>1 – None/ ineffective</th><th>2 – Partially effective</th><th>3 – Fully effective</th></tr>
<tr><td rowspan="4">Design</td><td>Control design</td><td rowspan="7">• Insufficient or non-existent controls currently in place
• Procedures and / or resources not in place or being developed through change projects
• Insufficient staff resources (capacity and competency)
• Limited attempt made to implement preventative measures</td><td rowspan="7">• Reasonable compliance with statutory requirements
• Reasonable standards established with staff (capacity and competency), processes and assets established
• Some preventative measures in place
• Controls can be improved to improve proactivity and continuous improvement</td><td rowspan="7">• Full compliance with statutory requirements
• Comprehensive procedures in place with required staff (capacity and competency), processes and assets
• Continuous improvement in place
• No other controls considered necessary, ongoing monitoring only</td></tr>
<tr><td>Accountability and ownership</td></tr>
<tr><td>Assurance and testing</td></tr>
<tr><td>Training</td></tr>
<tr><td rowspan="3">Operation</td><td>Implementation</td></tr>
<tr><td>Monitoring, maintenance and reporting</td></tr>
<tr><td>Supervision</td></tr>
</table>

Source: *Marsh Ltd*

Evolution of Enterprise Risk Management

An effective ERM program moves beyond compliance focus and drives toward risk-return optimisation



Note: Stages I to VII illustrate a continuous movement towards higher degree of risk management sophistication without downturns

Source: *Marsh Ltd*

3. FTSE100 Analysis

Research summary

Analysis of FTSE100 risk reporting trends indicates many companies will be looking to further improve how they report and manage the risks of the future

Introduction

- Marsh Advisory is delighted to publish research on the FTSE100 risk trends and risk management information for the July 2018 to July 2019 reporting period

- The report summarises over 1,200 combined risks extracted from annual reports and provides cross-industry analysis on risk section maturity and corporate governance alignment

Key Results

- The whitepaper presents rare analysis into overall reporting trends of large UK listed companies and concludes that;
  - In most cases, companies have a short risk identification horizon with themes such as climate risk and pandemics not receiving sufficient prominence
  - Few companies were meeting the Financial Reporting Council's (FRC) updated guidance on emerging risk themes prior to the implementation date

- In light of Covid-19, a retrospective analysis is provided on the level of information contained on pandemic risks and associated controls.

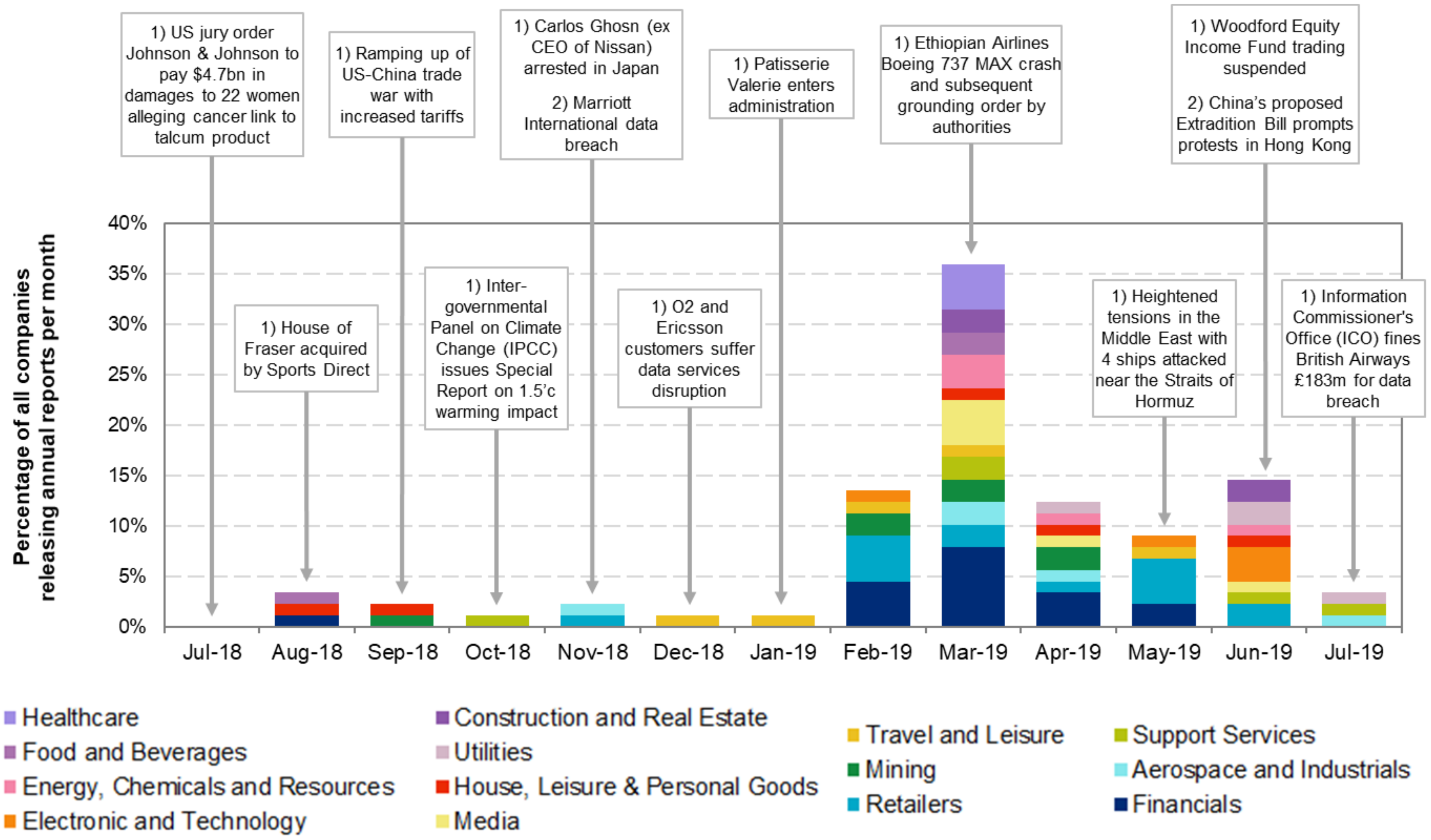
Concluding Remarks

- Our research highlights potential risk blind spots as well as an opportunity to provide a greater level of information on the risk practices in place within companies listed on the London Stock Exchange (LSE) Main Market.

Source: *Marsh Ltd. Research conducted based upon publically available Annual Reports and Accounts.*

Annual Report Publication Timeline

Summary of key risk events from July 2018 to July 2019



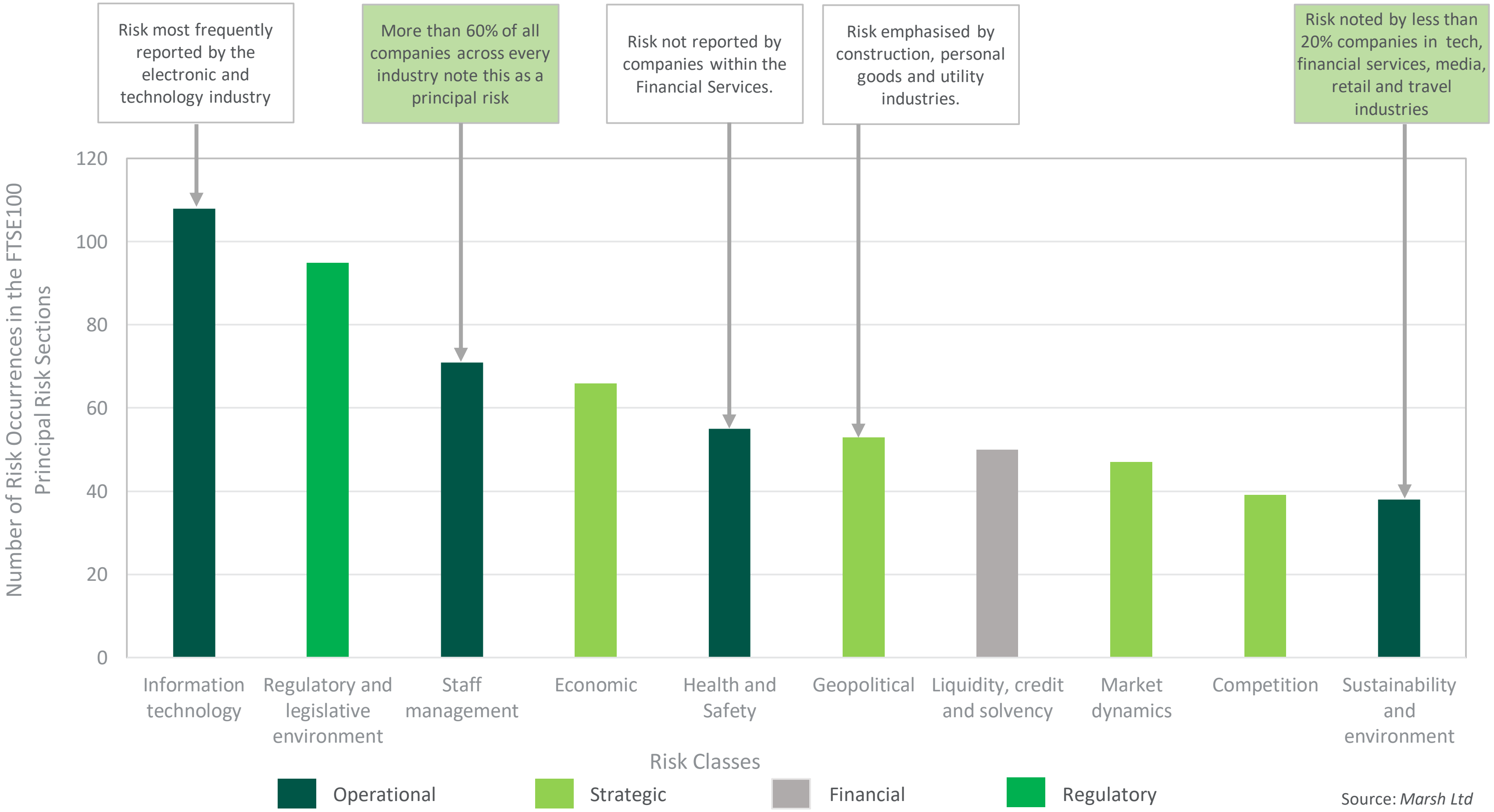
Source: *Marsh Ltd*

Principal Risk Classes

Top 10 risk classes in the FTSE100 ranked by their total number of occurrences

80% of the top 10 principal risks were categorised as either operational or strategic

- Distribution of the top 10 principal risks by risk category is shown below



Source: *Marsh Ltd*

Principal Risk Priorities

Top 5 risks ranked by occurrence for each industry

	Operational								Strategic						Financial					Regulatory	
	Contractor / third party management	Health and Safety	Information technology	Project management	Supply chain, Procurement	Sustainability and environment	Staff Management	Quality Management	Competition	Economics	Geopolitical	Innovation	Market dynamics	Strategy and planning	Capital allocation / structure and financing	Commodity Price	Credit and counterparty	Insurance	Liquidity, credit and solvency	Conduct / ethics	Regulatory and legislative environment
Financials			2														5	4	3		1
Retailers		5	1								4								3		2
Aerospace and Industrials			1		5		3			2											4
Mining		1		2		4										3					5
Support Services		5	1				4		3												2
Travel and Leisure	4	3	1				5			2											
Media			1				2			3			5								4
Electronic and Technology			1				2		4			5									3
House, Leisure & Personal Goods		2	4		5		3														1
Energy, Chemicals and Resources		1	3																5	2	4
Utilities		4	3			1					5										2
Food and Beverages			2			1	5	4		3											
Construction and Real Estate		4					5			3	1				2						
Healthcare			1				3			4				5							2
Mean Risk Rank	4.0	3.0	1.5	2.0	5.0	2.0	3.5	4.0	3.5	3.0	3.0	5.0	5.0	5.0	2.0	3.0	5.0	4.0	3.5	2.0	2.5

Industry Risk Rank: Rank 1 Rank 2 Rank 3 Rank 4 Rank 5

Source: *Marsh Ltd*

Principle Risk Controls (1 of 2)
We examined how different industries utilised key words to outline risk controls

Table shows the percentage of companies in each industry which mention using a specific control at least once

- E.g. 71% of companies in the Aerospace and Industrials industry mention insurance as a key control to mitigate risk at least once
- Monitor, planning, security, policy and engagement represent the most frequently used words to describe risk control measures

Industry	#	Insurance	Transfer	Supply Chain	Contract	Policy	Procedures	Assurance	Resilience	Continuity	Crisis	Security	Planning	Contingency	Engagement	Monitor	Culture
Aerospace and Industrials	7	71%	14%	86%	71%	86%	57%	43%	43%	57%	29%	100%	100%	14%	86%	86%	29%
Construction and Real Estate	4	75%	25%	75%	100%	100%	75%	25%	75%	100%	50%	100%	100%	25%	100%	100%	50%
Electronic and Technology	6	17%	17%	17%	33%	67%	50%	33%	33%	67%	33%	83%	83%	17%	83%	83%	50%
Energy, Chemicals and Resources	5	40%	20%	60%	60%	40%	60%	60%	40%	40%	20%	40%	60%	0%	40%	60%	60%
Financials	20	45%	10%	5%	25%	55%	50%	45%	35%	45%	5%	65%	95%	40%	40%	95%	40%
Food and Beverages	4	0%	25%	25%	50%	100%	75%	75%	0%	75%	50%	75%	100%	50%	75%	100%	75%
Healthcare	4	50%	0%	50%	0%	25%	75%	75%	25%	50%	25%	75%	100%	25%	50%	100%	50%
House, Leisure & Personal Goods	6	67%	0%	83%	67%	100%	83%	33%	17%	50%	0%	67%	100%	17%	83%	100%	50%
Media	6	0%	0%	50%	67%	50%	50%	50%	67%	83%	33%	100%	100%	33%	100%	100%	67%
Mining	7	29%	0%	29%	43%	86%	43%	71%	14%	43%	29%	86%	86%	14%	86%	86%	14%
Retailers	11	45%	18%	91%	55%	82%	73%	27%	55%	64%	36%	91%	100%	55%	82%	100%	36%
Support Services	7	43%	14%	29%	29%	71%	71%	43%	43%	29%	0%	86%	86%	14%	43%	86%	29%
Travel and Leisure	7	29%	0%	57%	57%	57%	71%	43%	43%	57%	43%	86%	86%	43%	57%	86%	29%
Utilities	5	60%	0%	40%	60%	80%	60%	60%	80%	80%	40%	100%	100%	40%	80%	80%	40%

Source: *Marsh Ltd*

Principle Risk Controls (2 of 2)

We examined how different industries utilised key words to outline risk controls

This table shows the percentage of companies in each industry which mention using a specific control more than once

- E.g. 43% of companies in the aerospace and industrials industry mention insurance more than once in their principle risk controls
- Monitor and planning occur frequently across all industries whereas security, engagement and policy are less frequent

Industry	#	Insurance	Transfer	Supply Chain	Contract	Policy	Procedures	Assurance	Resilience	Continuity	Crisis	Security	Planning	Contingency	Engagement	Monitor	Culture
Aerospace and Industrials	7	43%	0%	57%	29%	71%	14%	14%	29%	0%	14%	43%	86%	0%	43%	86%	29%
Construction and Real Estate	4	0%	25%	0%	25%	75%	0%	0%	25%	50%	0%	75%	100%	0%	50%	100%	0%
Electronic and Technology	6	17%	0%	0%	17%	33%	17%	17%	17%	0%	0%	50%	67%	0%	50%	83%	17%
Energy, Chemicals and Resources	5	20%	0%	20%	20%	20%	40%	40%	0%	0%	0%	20%	60%	0%	40%	60%	40%
Financials	20	35%	0%	0%	10%	35%	15%	20%	20%	15%	5%	35%	65%	20%	35%	85%	20%
Food and Beverages	4	0%	0%	25%	50%	75%	0%	25%	0%	0%	0%	75%	75%	0%	75%	100%	50%
Healthcare	4	25%	0%	50%	0%	25%	0%	25%	0%	0%	0%	25%	75%	0%	25%	100%	25%
House, Leisure & Personal Goods	6	17%	0%	50%	33%	33%	50%	17%	0%	17%	0%	33%	100%	0%	67%	83%	17%
Media	6	0%	0%	0%	33%	50%	33%	17%	33%	17%	0%	67%	100%	0%	83%	100%	67%
Mining	7	29%	0%	29%	43%	57%	43%	43%	0%	29%	29%	57%	71%	14%	57%	86%	0%
Retailers	11	9%	0%	36%	18%	45%	45%	18%	9%	27%	18%	45%	100%	18%	64%	100%	9%
Support Services	7	29%	0%	0%	29%	57%	43%	0%	0%	14%	0%	14%	71%	0%	14%	86%	0%
Travel and Leisure	7	14%	0%	43%	29%	43%	29%	0%	0%	14%	0%	57%	86%	14%	14%	71%	0%
Utilities	5	0%	0%	40%	20%	60%	40%	60%	40%	40%	40%	40%	100%	20%	80%	60%	40%

Source: *Marsh Ltd*

airmic

Pandemic risk: looking back to learn going forwards

We examined retrospectively how the FTSE100 evaluated the emerging risk landscape, particularly in reference to their preparedness for COVID-19

- Analysis provides a unique opportunity to review perspectives on pandemic pre-COVID-19.
- With the annual reports representing the 2018-2019 reporting period, societal risks were not given as high a prominence (see table)[1]
- The number of words related to "pandemic" appearing is low. Where it was mentioned, focus was given to potential flu outbreaks

		Causes					Consequences					Controls				
Industry	**#**	Pandemic	Flu	Virus	outbreak	Mean	Pandemic	Flu	Virus	outbreak	Mean	Pandemic	Flu	Virus	outbreak	Mean
Aerospace and Industrials	7	14%	57%	0%	0%	18%	0%	14%	0%	0%	4%	0%	14%	0%	0%	4%
Construction and Real Estate	4	0%	25%	0%	0%	6%	0%	25%	0%	0%	6%	0%	25%	0%	0%	6%
Electronic and Technology	6	0%	17%	0%	0%	4%	0%	33%	0%	0%	8%	0%	33%	0%	0%	8%
Energy, Chemicals & Resources	5	0%	20%	0%	0%	5%	0%	20%	20%	20%	15%	0%	40%	0%	0%	10%
Financials	20	0%	35%	0%	0%	9%	0%	0%	0%	0%	0%	0%	5%	0%	0%	1%
Food and Beverages	4	0%	25%	0%	0%	6%	0%	25%	25%	0%	13%	0%	25%	0%	0%	6%
Healthcare	4	0%	0%	0%	0%	0%	25%	25%	0%	25%	19%	0%	0%	0%	0%	0%
House, Leisure & Personal Goods	6	0%	17%	0%	0%	4%	0%	17%	0%	0%	4%	0%	33%	0%	0%	8%
Media	6	0%	0%	0%	0%	0%	0%	33%	0%	0%	8%	0%	50%	0%	0%	13%
Mining	7	0%	43%	0%	0%	11%	0%	29%	0%	0%	7%	0%	14%	14%	0%	7%
Retailers	11	0%	9%	0%	0%	2%	0%	36%	0%	0%	9%	0%	18%	0%	0%	5%
Support Services	7	0%	14%	0%	0%	4%	0%	29%	0%	0%	7%	0%	14%	14%	0%	7%
Travel and Leisure	7	29%	14%	0%	14%	14%	0%	0%	0%	0%	0%	0%	29%	14%	0%	11%
Utilities	5	0%	80%	0%	0%	20%	0%	20%	20%	0%	10%	0%	60%	0%	0%	15%
All Sector Average	**99**	**3%**	**25%**	**0%**	**1%**	**7%**	**2%**	**22%**	**5%**	**3%**	**8%**	**0%**	**26%**	**3%**	**0%**	**7%**

Source: *Marsh Ltd*

1. Given the impact of COVID-19, Marsh anticipates this will change substantially in the 2020 reports

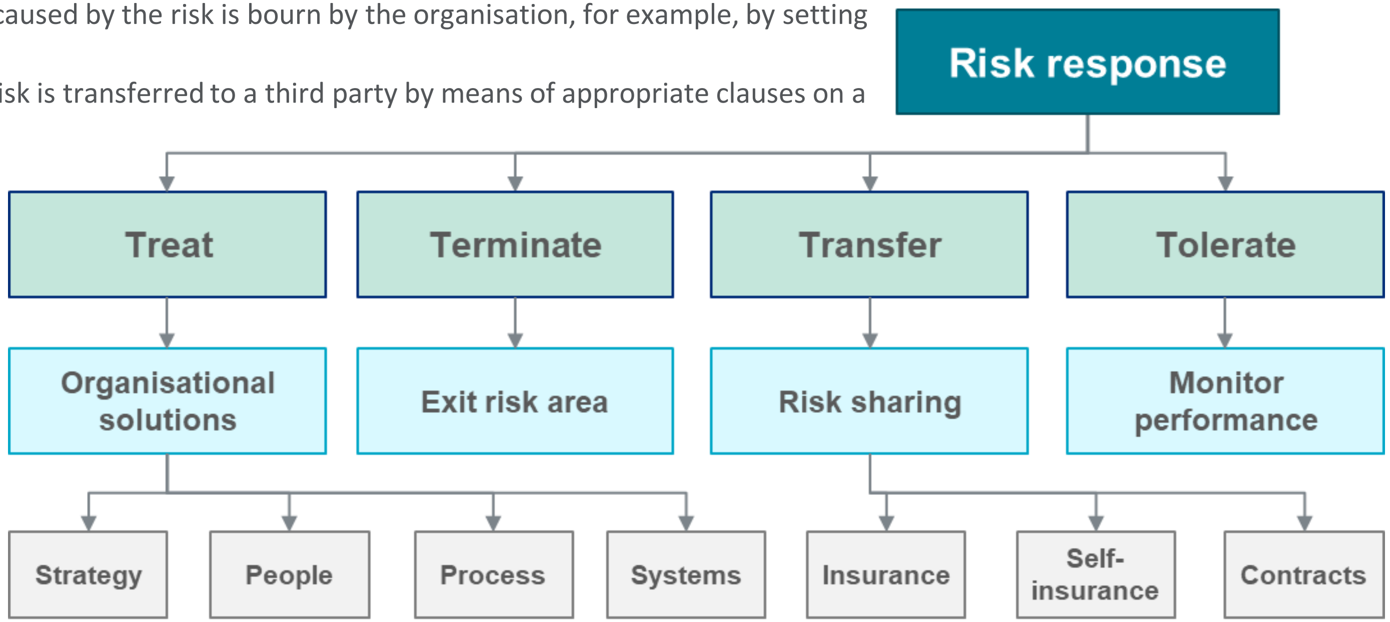
4. Exploration of Common Themes

Risk response

Measures define how the risk should be addressed, given its estimated impact on the organisation's objectives

Broadly risk response types are described by 4 "T"s concept, and in practice is the combination of them:

1) "**To treat**" action means putting controls in place to prevent, detect or mitigate the occurrence of a risk or reduce its impact
2) "**To terminate**" action implies involves ceasing the activity to which the risk is associated, e.g. changing the scope, procurement route, and supplier etc.; this approach is usually adopted when the risk exposure is deemed too great
3) "**To transfer**" action Involves transferring the risk exposure elsewhere by:
   - Insurance – a premium is paid to an insurance company. For this option the risk needs to be insurable, and weigh the cost of the insurance against the value of the risk
   - Self-insurance – the cost of the potential loss caused by the risk is bourn by the organisation, for example, by setting aside funds to meet the cost of the loss
   - Contracts – the financial consequence of the risk is transferred to a third party by means of appropriate clauses on a contract
4) "**To tolerate**" is a conscious and deliberate action to retain the risk, having evaluated that it is more economical to do so that to attempt any risk control action, and that the exposure is within the group's risk appetite



Source: *Marsh Ltd*

Risk treatment

Introducing different types of risk controls in place to reduce risk exposure by addressing likelihood and impact

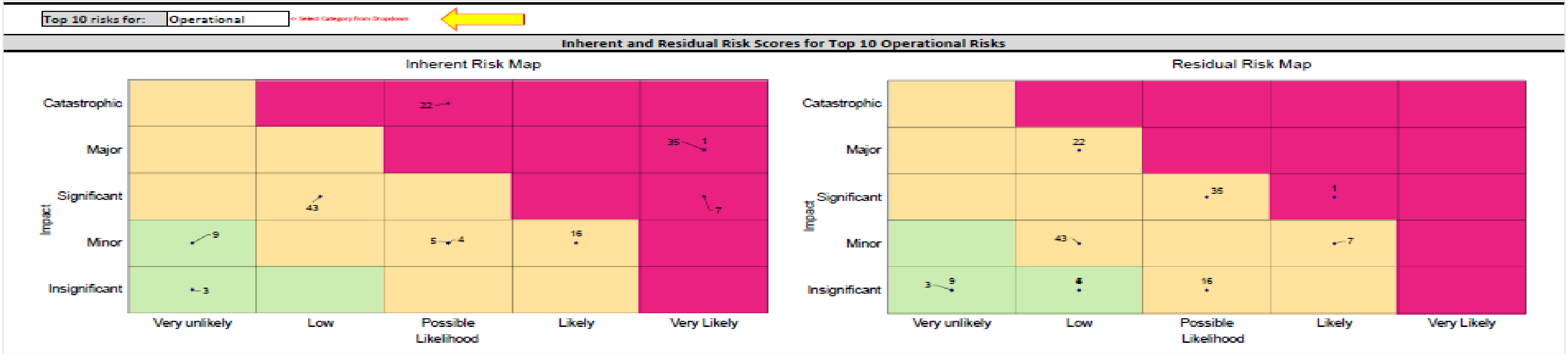
- Risk control is a measure or action that modifies the risk, reducing the either the risks probability of occurrence or impact
- Controls can include policies, practices, processes, technologies, methods, devices etc.
- The bow-tie diagram below illustrates the types of controls in relation to the risk event
  - **Preventative controls** typically are designed to reduce the likelihood of risk happening (e.g. security at the entrance, operational monitoring systems, personnel training)
  - **Mitigating controls** typically address risk impacts and are designed to limit or correct the outcomes, should the risk happen (e.g. emergency or crisis response plan execution)

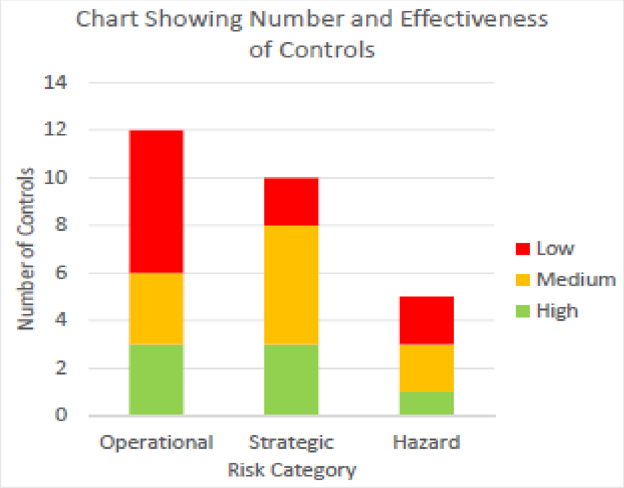
Source: *Marsh Ltd*

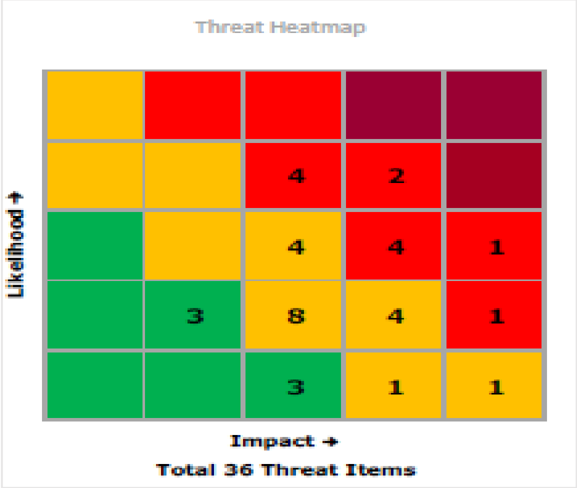
Risk management information dashboards

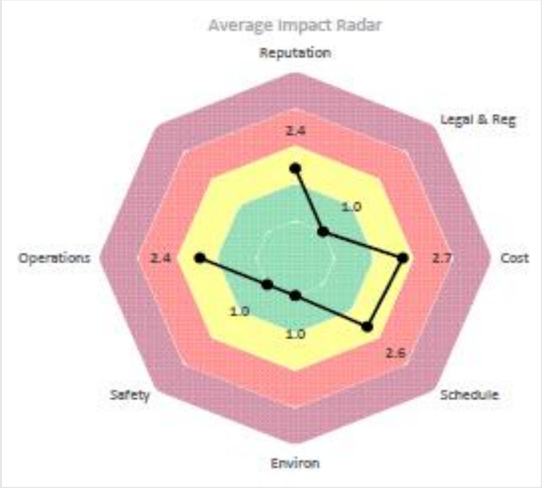
Monitor, review and reporting

EXAMPLE









Source: *Marsh Ltd*

5. Practical internal audit considerations

Why connect Internal Audit to the Risk function?
Benefits of Combined Assurance

Coordinated assurance efforts are directed towards the risks that matter most

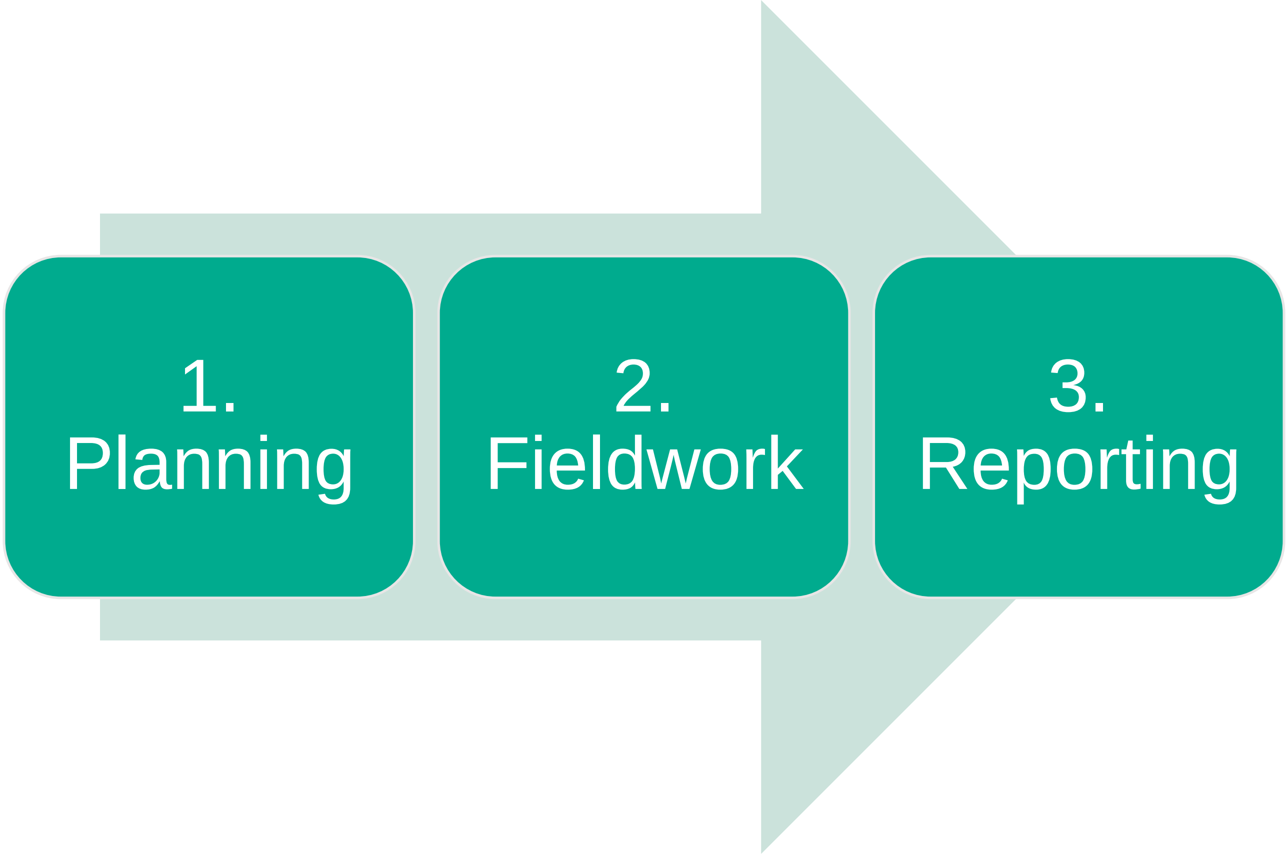
Valuable, integrated data, based on collaboration

Reduction in assurance costs through better resource allocation

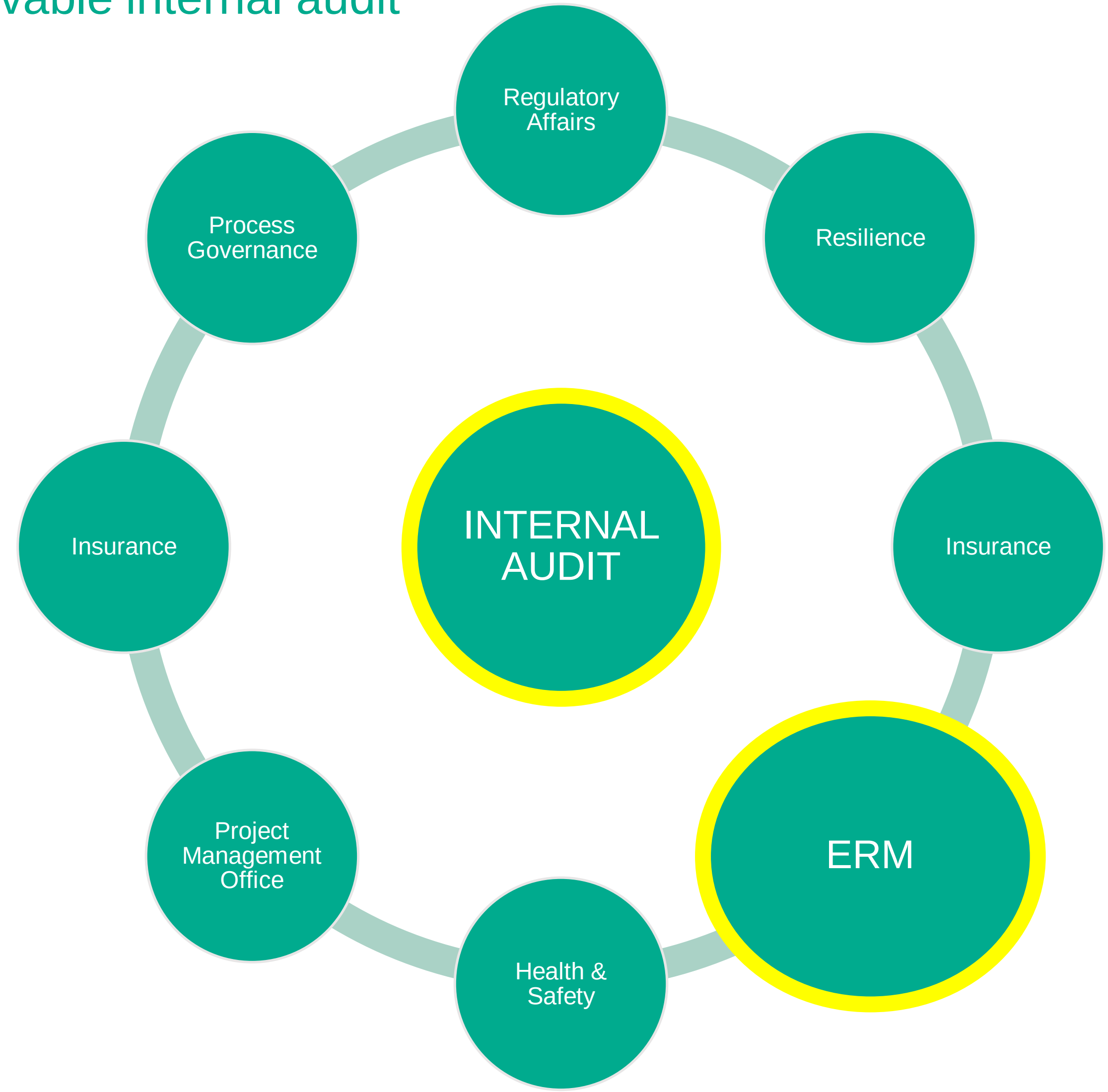
A reduction in the number of reports by different teams, resulting in more efficient reporting

A comprehensive and prioritised approach in the tracking of remedial actions on identified risks

Internal Audit stages



Planning stage - capturing all 2nd line assurance activities
E.g. Accounts Receivable internal audit



airmic

Planning Stage – using 2nd line risk data to create the internal audit programme

E.g. Accounts Receivable internal audit

Objectives	Risk Description	Risk Categories	Risk Owner
Inherent Risk Score	Controls	Control Type	Control Owner
Control Effectiveness	Key Risk Indicators	Residual Risk Score	Risk Assessment Justification
Risk Appetite	Risk Actions	Risk Action Owner	Risk Action Deadline

AUDIT PROGRAMME						
RISK	EXPECTED CONTROL	ACTUAL CONTROL	CONTROL REF	CONTROL DESIGN	CONTROL ADEQUACY	REMEDIAL ACTION

Fieldwork Stage – auditing the risk
E.g. Accounts Receivable internal audit

ACCOUNTS RECEIVABLE RISK REGISTER			
OBJECTIVE	**RISK**	**RISK OWNER**	**RISK CATEGORIES**
Bad debt < £100k in FY	Allowing customers credit levels beyond their capacity or willingness to pay may result in payment defaults which will ultimately damage financial performance	Financial Controller	Financial

Fieldwork Stage – auditing the controls
E.g. Accounts Receivable internal audit

ACCOUNTS RECEIVABLE RISK REGISTER			
CONTROLS	**CONTROL OWNER**	**CONTROL TYPE**	**CONTROL EFFECTIVENESS STATEMENT**
Credit checks undertaken prior to allowing credit	Account Clerk	Preventative	Ineffective
Credit limits regularly reviewed	Treasury Manager	Preventative	Effective
Automated credit limit indicators	Treasury Manager	Detective	Effective

2 Key Questions:

1. Controls designed adequately?
2. Controls operating effectively?

airmic

Fieldwork Stage – auditing the risk assessment

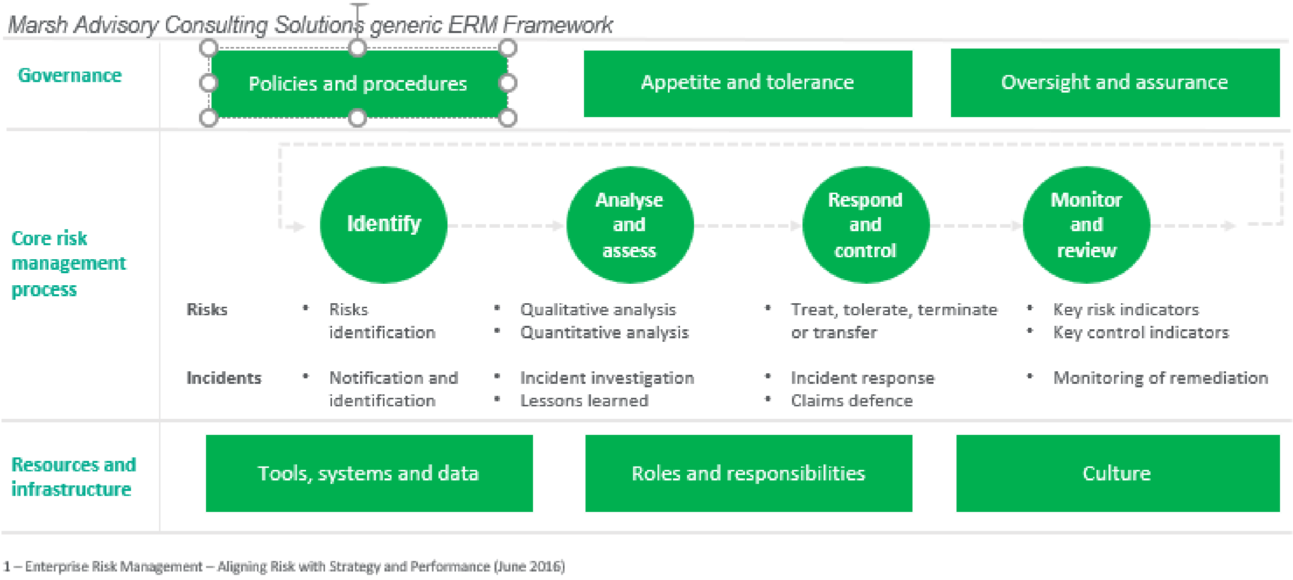
E.g. Accounts Receivable internal audit

ACCOUNTS RECEIVABLE RISK REGISTER						
INHERANT IMPACT	**INHERANT LIKELIHOOD**	**INHERANT RISK SCORE**	**RESIDUAL IMPACT**	**RESIDUAL LIKELIHOOD**	**RESIDUAL RISK SCORE**	**KEY RISK INDICATOR**
3	5	15	3	3	9	5% increase in customer credit limit total
RISK ASSESSMENT JUSTIFICATION This risk remains stable since the last formal review in Q1 evidenced by the static customer credit limit total						

airmic

Reporting Stage – feeding the 3rd line opinion back into 2nd line risk framework
E.g. Accounts Receivable internal audit

INTERNAL AUDIT REPORT



6. Conclusions

Source: *Marsh Ltd*

Conclusions

In Marsh’s experience, the following are characteristics of best practice

#	Area of best-practice ERM
1	**Visible** buy-in, communication and advocacy - “Tone from the Top” and “Tone from the Middle”.
2	**Clarity** on roles, responsibilities and accountabilities of key stakeholders, with good communication flows.
3	**Embedding** of the risk cycle across the company, with analysis informed by data and subject matter opinions.
4	**Accurate** articulation of risk information (including incidents and near misses), timely sharing and transparency of assumptions to inform decision making.
5	**Effective** risk monitoring system in place to track risk status and control effectiveness. Information is reported on residual risk positioning in relation to risk appetite.
6	**Robust** and consistent core culture across the company, regardless of reporting lines and geographies.
7	**External drivers** of risk and stakeholders influences are regularly reviewed and managed.
8	**Interrelationships** between risk activities (e.g. GRC; strategic planning; financial analysis and control; insurance; operational risk incl. BCM, & HSE; Cyber) are understood and initiatives joined up where appropriate.
9	**Scenario analysis** is undertaken, in addition to the regular cycle of risk activities, to stress test the strength and long term viability of the company and help plan future risk mitigations.
10	**Tools** are made available and are suitable to record, analyse and manage risks and inform strategic decision making.

Next Steps

We suggest you do the following after this session

- Review your control effectiveness criteria and the application within the Risk and Audit Framework
- Speak to your Internal Audit team to see where you can create further synergies between the second and third lines to enhance integrated assurance benefits to the organisation
- Review your use of technology and data across Risk and Audit and flag areas of improvement with the oversight committee

Q & A

With regard to Marsh Ltd content herein:

"The information contained herein is based on sources we believe reliable and should be understood to be general risk management and insurance information only. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such. Statements concerning legal, tax or accounting matters should be understood to be general observations based solely on our experience as insurance brokers and risk consultants and should not be relied upon as legal, tax or accounting advice, which we are not authorised to provide."

Airmic promotes and supports the planning, undertaking and subsequent recording, of Continuous Professional Development (CPD).

Subject to the CPD scheme you belong to, this event may qualify for CPD hours.