MARSH

INSIGHTS | AUGUST 2020

Beyond Compliance

Evaluating Risk Reporting Trends in the FTSE100

MARSH & McLENNAN COMPANIES

INSIGHTS | JULY 2020

Table of Contents

Principle Risks Analysis

Risk reporting in the annual reports of FTSE100 companies generally lacks clarity, which could raise concerns related to companies' insurance programs, including directors and officers (D&O) liability, according to recent Marsh research. Companies could improve reporting transparency in their reports through such measures as presenting relevant global risk trends, outlining risk controls, and adopting — or highlighting existing — enterprise risk management (ERM) frameworks. Such risk reporting is likely to face greater scrutiny in the post-COVID-19 era.

Crises and business failures, along with investor pressures and consumer expectations of transparency, have raised the bar on governance expectations for UK listed companies. Updates to corporate governance codes have increased risk reporting requirements and provided guidance to boards to enable effective risk management implementation. However, an examination of annual reports found that risk reporting often lacks clarity.

All companies have entered a new chapter in global commerce due to the economic downturn resulting from the COVID-19 pandemic. This uncertainty is heightened for UK listed companies due to the country's departure from the European Union.

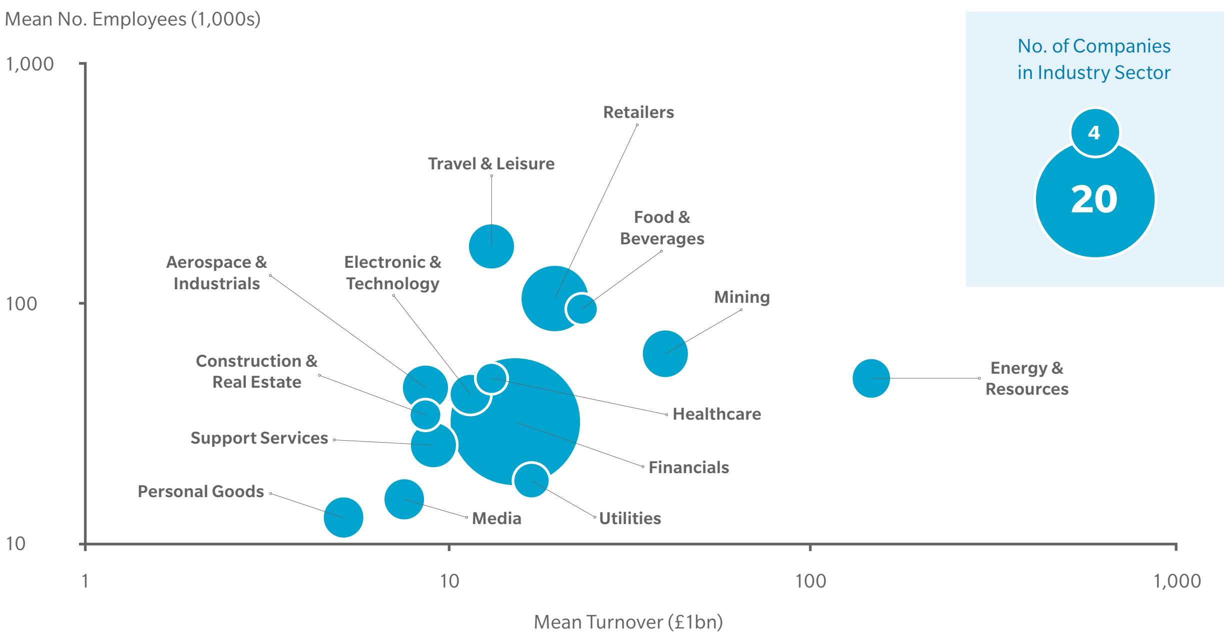
Both events will amplify the need for guidance bodies and companies to consider the effectiveness of their risk management frameworks, how they report principal risks, and associated risk management activities.

Marsh, in partnership with Cranfield University, conducted research exploring the state of risk reporting for the FTSE100 in late 2019, before the onset of the COVID-19 pandemic (see Figure 1). We analysed the risk sections of annual reports for trends and keywords relating to various risk management characteristics in order to determine which risks were key concerns among the FTSE100, and where there were gaps when comparing to the World Economic Forum's The Global Risks Report 2020[1].

FIGURE 1

Financial services firms form the largest segment of FTSE100 companies when segmented by industry. (Data reflects FTSE100 composition as of July 2019).

SOURCE: MARSH



[1] World Economic Forum, Global Risk Report (2020).

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.[2]

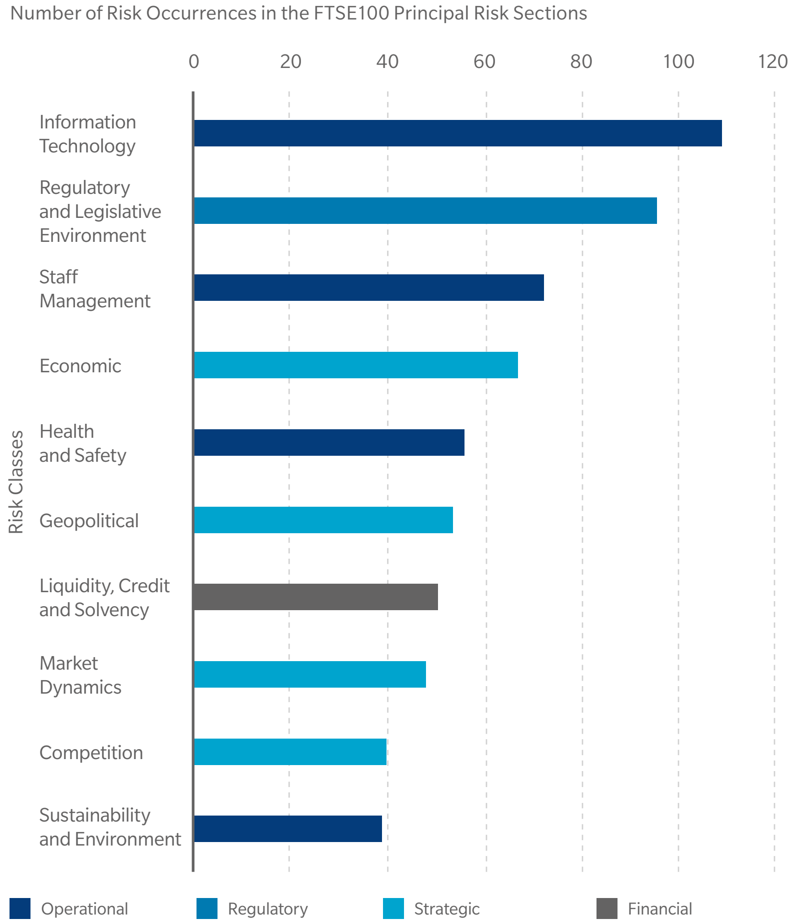
Financial Reporting Council.

Annual reports from FTSE100 companies contained 1,200 risks. We assigned these risks to four major classes – strategic, operational, financial, and regulatory – and subdivided them into 68 sub-classes for purposes of comparison and analysis.

FIGURE **2**

Information technology was the top risk class across 1,200 principal risks listed by FTSE100 companies.

SOURCE: MARSH



From the FTSE100 reports examined, only 64% of companies reported on risk trends. The top two risk classes across all industries were "information technology" and "regulatory and legislative environment" (see Figure 2). This is in line with the prominence of cyber risk and the political uncertainties experienced during 2018 and 2019 due to Brexit and other national protectionist policies globally. Further, we found that eight of the top 10 principal risks were categorised as either operational or strategic.

35%

The majority of companies (35%) issue annual reports in March.

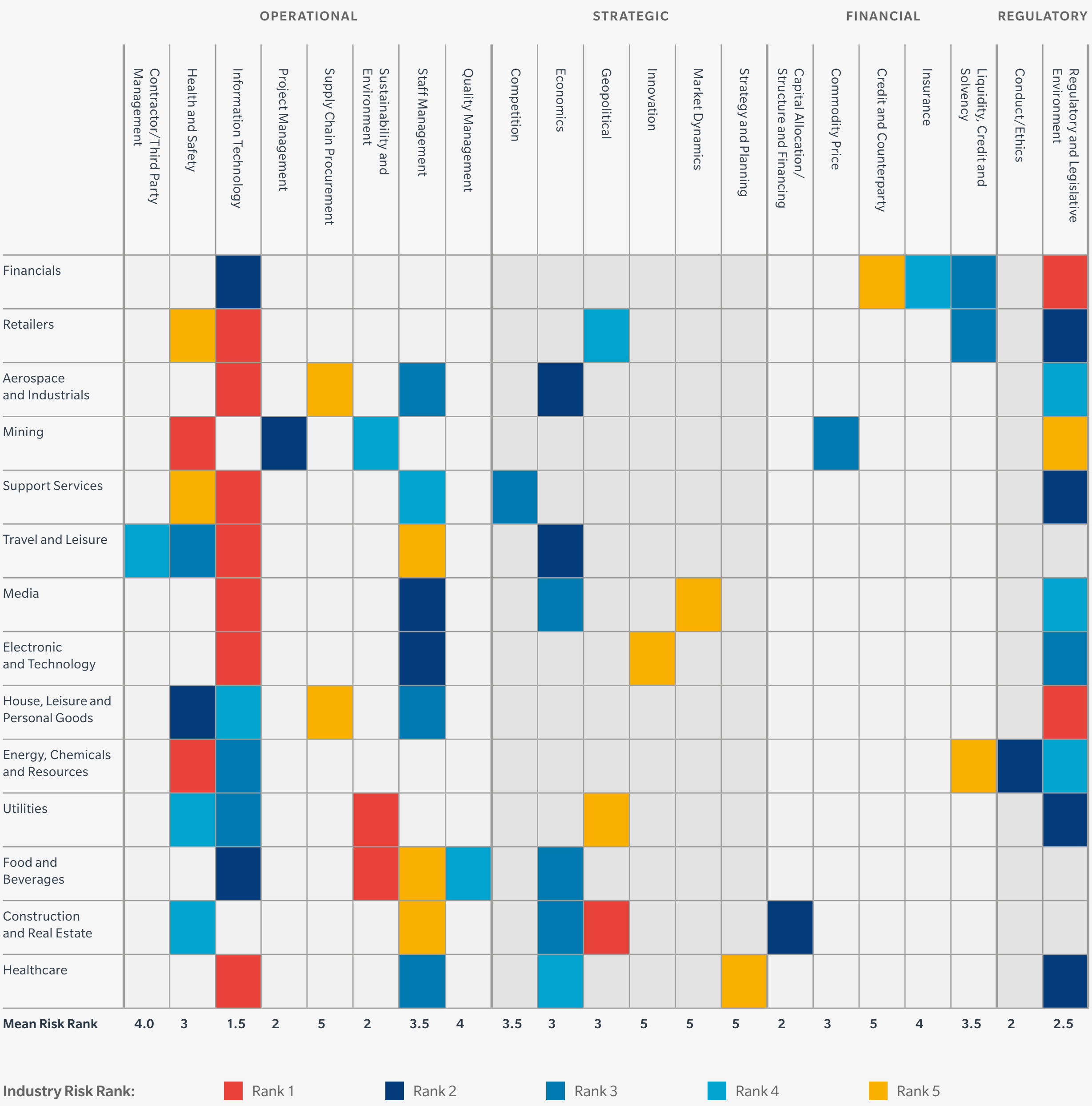
[2] Financial Reporting Council, UK Corporate Governance Code, July 2018, Principle O.

One striking trend is the relatively low rank of the 'sustainability and environment' risk class. This is in contrast to The Global Risks Report 2020, which ranked this risk as both high in likelihood and high in impact in 2020. While The Global Risks Report 2020 is a trend report with a time horizon of 15 years, the contrast suggests that industry leaders' opinions (through the WEF risk perception survey) are out of sync with company leaders on the prominence of climate and environmental risks.

FIGURE 3

Information technology cited most often as top risk by industry.

SOURCE: MARSH



Managing and Controlling Risks Within Risk Appetite

The role of enterprise risk management (ERM) is more important than ever. Boards are ultimately responsible for company performance and for the oversight of the principal risks to achieving strategic objectives. For their part, directors' risk responsibilities include conducting risk assessments, presenting risk information to shareholders, defining and articulating the risk appetite, and communicating and embedding staff behaviours that create a robust risk and control environment. ERM is defined as "the culture, capabilities, and practices, integrated with strategy and execution that organisations rely on to manage risk in creating, preserving and realising value.[3]"

An effective ERM framework necessitates embedding risk management and internal controls in a company's business processes. The FTSE100 companies typically provide control information on their principal risks and the supporting management activities.

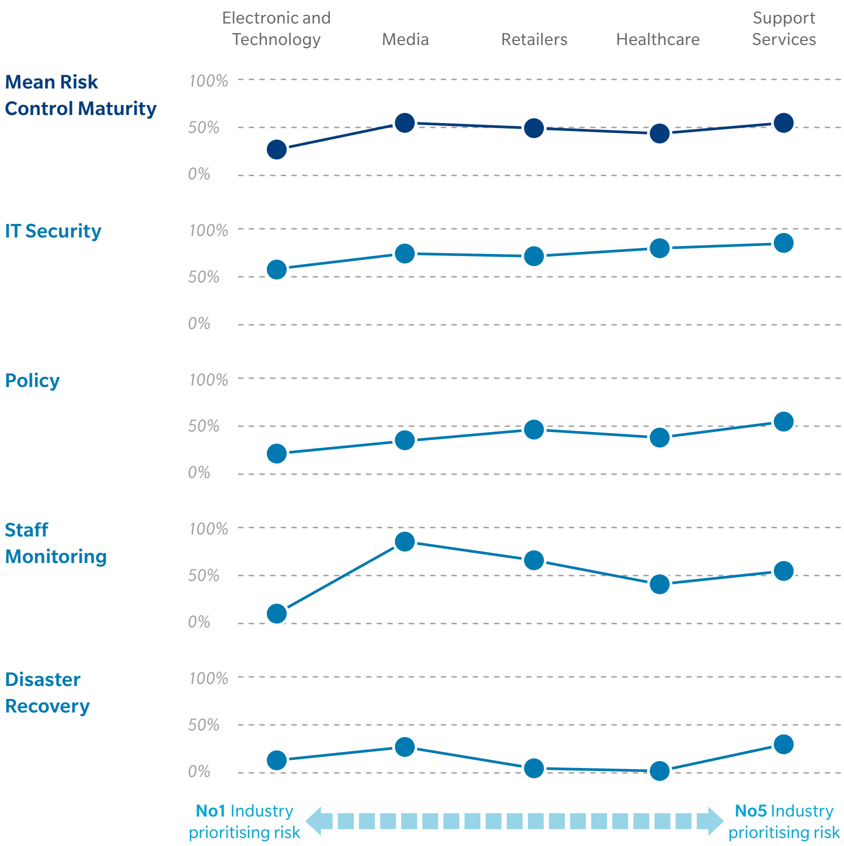
Despite information technology being the top-ranked risk class, word analysis of the reported risk control information shows that keywords such as "policy", "staff monitoring", and "disaster recovery" were under-reported for the risk class in the majority of cases (see Figure 4). These are all areas key to information technology and its management.

In addition, the word "insurance" appeared in only 41% of annual report risk sections. All listed companies have insurance in place to mitigate at least some of the consequences of principal risks. This omission suggests there are either reporting siloes or a lack of integration between business risk, insurance, and audit practices in many companies – at least in terms of reporting the "combined assurance and control" practices.

FIGURE
4

Certain expected risk control terms are often missing within discussions of information technology risks.

SOURCE: MARSH



RISK DEFINITION:

- Includes, cyber risk, data theft/loss, malicious attack, system impairment, infrastructure failure.

OBSERVATIONS

- Although the **Electronic and Technology** industry sector note IT risk as the most frequently occurring, the controls they discuss within their annual report are consistently poor.
- ~75% of all companies in the top 5 industries mention security and protection within their risk controls.
- Overall, the **Support Services** industry performed the best in mentioning key words within their risk control sections.

[3] Abstracted from The Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management – Aligning Risk with Strategy and Performance, June 2016.

Very few organisations included information on pandemic risk in their 2019 report.

This report offered the unique opportunity to review perspectives on pandemic pre-COVID-19. With the annual reports representing the 2018-2019 reporting period, societal risks were not at this time given high prominence. This is demonstrated by the table below. The number of words related to "pandemic" that appeared in the risk sections was quite low. Where there was mention, notable focus was given to a potential flu outbreak. Given the impact of the COVID-19 pandemic, Marsh anticipates this will change substantially in the 2020 reports, with significantly more attention given to this area.

FIGURE 5

Pandemic Risk: Understanding how companies viewed pandemic risk before COVID-19.

SOURCE: MARSH

		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 and 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 and 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%**

The revised Corporate Governance Code has increased the requirement on companies to report on emerging risks and to provide information on how they are managing and controlling them. Since this requirement applies to reporting periods commencing 1 January 2019, it is not surprising that only 31% of companies listed their emerging risks. However, only 15% of all companies summarised their procedures to identify emerging risks, and even fewer (11%) provided information on their controls to manage such risks. We anticipate this to change in annual reports in 2020.

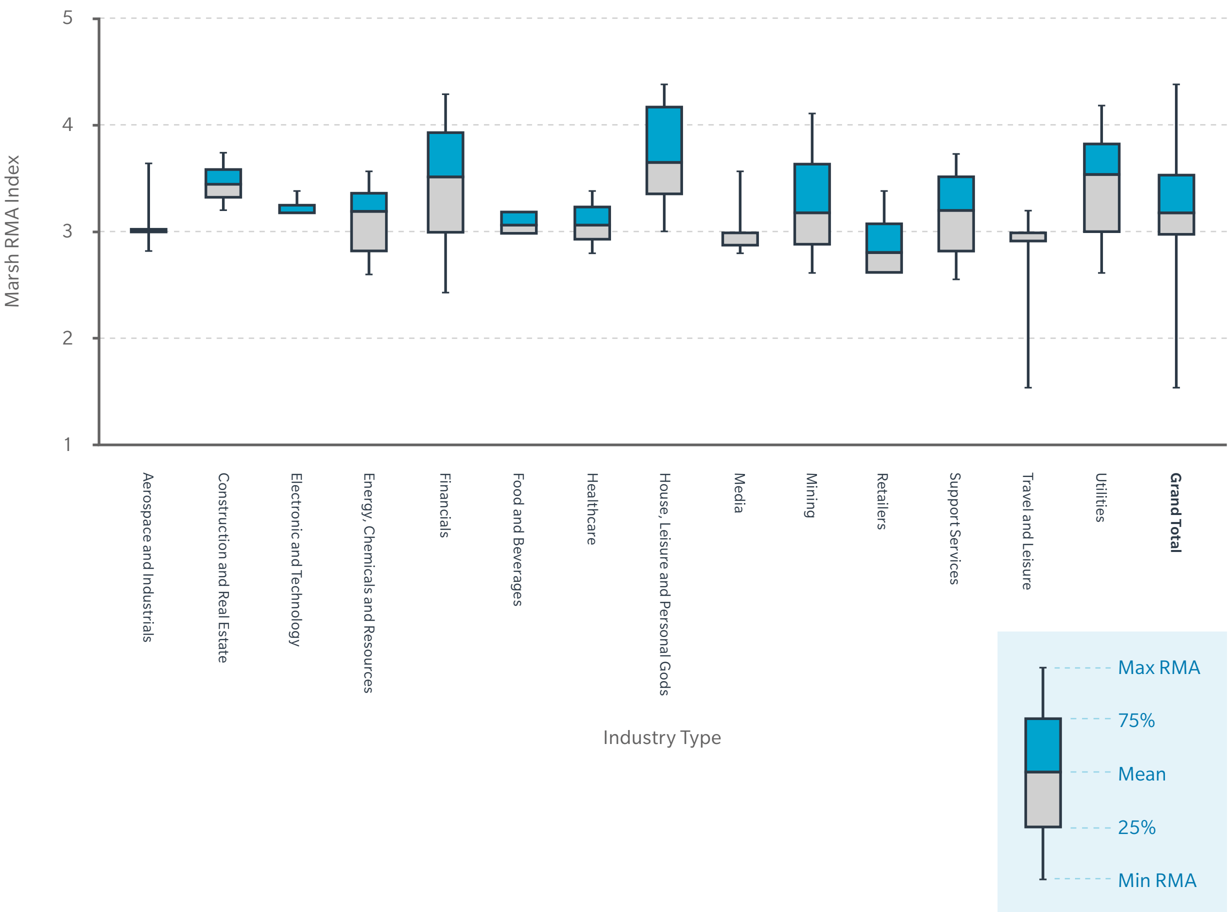
While the revised Corporate Governance Code is applicable to accounting periods commencing 1 January 2019, some companies were already reporting good information.

Based on the information provided in each company's annual report, Marsh calculated an approximate score for ERM risk maturity (see Figure 6). We calculated the score using a ranking system for the clarity of risk information provided on principal risks and controls, risk trends, risk appetite, viability statements, and risk governance. These results, grouped by industry, show that the majority of industries have above average ERM practices (score above 3), and are entering into maturity with their provision. Overall, the house, leisure, and personal goods; utilities; and financial institutions sectors performed best, with the travel and leisure and retail sectors performing worst, based upon the information within the annual reports.

FIGURE 6

Most FTSE100 companies score above average for risk maturity within their industry.

SOURCE: MARSH



“The risk management and internal control systems encompass the policies, culture, organisation, behaviours, processes, systems, and other aspects of a company.[4]”

Financial Reporting Council.

The Role of Enterprise Risk Management and Responsibilities for Risk Management

Companies should have ERM frameworks in place to set risk governance requirements. The framework should specify the cycle of risk management activities and the associated staff responsibilities and infrastructure, such as risk monitoring and reporting software. A well-informed ERM framework enables better decision making and provides greater certainty over outcomes.

The research shows that the main reporting line for risk and assurance within the FTSE100 is to a risk committee, with 54% of the FTSE100 stating that such a committee is in place. The majority of companies (59%) do not name the role responsible for chairing this committee, and, of those that do, the most common chairperson is the CEO. The average frequency of these meetings is five times per year.

Risk management culture is set and monitored by the board, and implemented by senior leadership. As is evident from historical corporate crises, enabling and maintaining an effective risk management culture is a prerequisite for effective ERM.

Conclusion

Our research shows that while all FTSE100 companies meet Financial Reporting Council (FRC) requirements for risk reporting, there is a considerable variation in the detail and insight provided. Keyword search analysis and comparison to The Global Risks Report 2020 suggests that the reporting of risk needs to provide additional information on emerging risks and the connectivity between risk management activities. Further, the COVID-19 crisis and the resulting spiral of economic implications necessitates that companies re-assess their risk frameworks to ensure the accuracy of risk profiles, appetite, controls, and governance in order to protect value and to create value once market upturns materialise.

An effective ERM framework assesses data and subject matter opinion to analyse principal uncertainties and then plans and implements controls and actions to create and protect value to your company.

Companies seeking to create and protect value, especially in the wake of current political, social, health, and economic crises should ensure they have an effective ERM framework in place to help them assess data and subject matter opinion, analyse principal uncertainties, and then plan and implement appropriate controls and actions.

Methodology

FTSE100 companies are required to report their principal risks within the strategic report section of annual reports. In the Summer of 2019, we examined the 2018-2019 reporting period of FTSE100 companies. We abstracted and analysed over 1,200 risks from annual reports to determine trends. These risks were categorised under operational, strategic, financial, or regulatory headings and further divided into 68 sub-classes to decode company principal risks into comparable risk types.

[4] Financial Reporting Council, Guidance on Guidance on Risk Management, Internal Control and Related Financial and Business Reporting, September 2014.

Key Requirements and Guidance

Companies listed on the London Stock Exchange main market have been required to provide risk management information to external parties within their annual reports since the creation of the UK's Corporate Governance Code in the early 1990's. The FRC published the revised UK Corporate Governance Code in July 2018 and also issued "Guidance on Board Effectiveness" at the same time.

The UK Corporate Governance Code sets out the "comply or explain" requirements for risk reporting under Principle O. Further information is provided within the FRC's Guidance on Risk Management, Internal Control and Related Financial and Business Reporting,[5] which is expected to be updated later this year following a review of the role and requirements for audit. For non-listed companies, the FRC's Wates Corporate Governance Principles for Large Private Companies[6] provides opportunity and risk guidance.

Over and above the requirement for providing risk information within the annual report, the Duty of Fair Presentation requirement within The Insurance Act 2015 stipulates the necessity for the (re)insured to provide the (re)insurer with "every material circumstance", and sufficient and accurate risk information.

[5] Financial Reporting Council, Guidance on Risk Management, Internal Control and Related Financial and Business Reporting, September 2014.

[6] Financial Reporting Council, The Wates Corporate Governance Principles for Large Private Companies, December 2018.

ABOUT MARSH

Marsh is the world's leading insurance broker and risk adviser. With over 35,000 colleagues operating in more than 130 countries, Marsh serves commercial and individual clients with data driven risk solutions and advisory services. Marsh is a wholly owned subsidiary of Marsh & McLennan Companies (NYSE: MMC), the leading global professional services firm in the areas of risk, strategy and people. With annual revenue over US$15 billion and 75,000 colleagues worldwide, MMC helps clients navigate an increasingly dynamic and complex environment through four market-leading firms: Marsh, Guy Carpenter, Mercer, and Oliver Wyman. Follow Marsh on Twitter @MarshGlobal; LinkedIn; Facebook; and YouTube, or subscribe to *BRINK*.

For further information, please contact your local Marsh office or visit our website at marsh.com.

DAVID STARK
+44 (0)20 7357 5033
david.stark@marsh.com

Insurance Brokers
Chartered