ISCA INSTITUTE OF SINGAPORE CHARTERED ACCOUNTANTS

KPMG

Driving Value: Risk Transparency and Culture

A study of Singapore-Listed Companies 2016

Supported by:

SGX

Table of Contents

1 Introduction

> Following the announcement that the CG Code may be reviewed in due course, this comprehensive second study provides timely insights and identifies opportunities to enhance the CG Code, in areas such as risk culture and risk disclosures. Risk management is integral to all companies as they grow. Proper risk management and internal controls help companies understand their risk exposure with mitigating controls in place to effectively pursue their objectives. Just as companies evolve, enhancing an organisation's risk governance is also a journey.

Ho Tuck Chuen
Chairman, ISCA Corporate Governance Committee
ISCA

> The study highlights the disparity between disclosures of a structural versus behavioural nature. The focus of the CG Code is primarily on structural elements, such as having a committee or policy in place, and we have seen a robust improvement in these disclosures since the CG Code was introduced. However, disclosures relating to behavioural factors such as risk culture are not as forthcoming and are not currently featured in the CG Code. The impending review of the CG Code provides an opportunity to consider incorporating more of the behavioural aspects influencing risk, and risk culture will be a critical element of this.

Irving Low
Partner
Head of Risk Consulting
Head of Markets
KPMG in Singapore

> This study is a timely reminder that effective risk governance is not just structural, but also cultural. It is more than developing a risk appetite statement, establishing risk committees or charting risk heat maps. The Board also needs to inculcate and embed a risk governance culture and values, including respect for the company's control environment. Risk management performance indicators should be set in a way that creates awareness, accountability and incentivises performance in risk governance.

Tan Boon Gin
Chief Regulatory Officer, Singapore Exchange

Companies need a strong risk management framework in place now more than ever. A rapidly changing business risk environment, increasing digital disruption, cyber security threats and speedy information dissemination are all posing challenges to companies globally. More transparent risk management practices and an enhanced risk culture can allow companies to gain a competitive advantage through more agile decision-making as they seize opportunities and minimise unwanted surprises in performance or compliance.

It is with this in mind that the Institute of Singapore Chartered Accountants (ISCA) and KPMG in Singapore embarked on a study of risk governance disclosures in 2013. A representative sample of 250 listed Singapore companies (2013 Study) was examined. This was conducted at a pivotal time in Singapore's corporate governance history. The Singapore Exchange (SGX) had issued the new Listing Rule (LR) 1207 (10) in 2011 requiring the Board to provide an opinion on the adequacy of internal controls. The Singapore Code of Corporate Governance (CG Code) had also been revised in 2012, incorporating new requirements relating to risk governance.

The focus then was to examine the extent of disclosures in relation to the new requirements in the SGX LR 1207(10) and CG Code. Particular attention was paid to the roles, responsibilities and risk management practices of the Board and board risk oversight committee. The board's conclusion on the adequacy and effectiveness of risk management and internal controls, internal audit and whistle-blowing were also studied. Some companies were found to be early adopters, but a number of companies had not yet reflected the new disclosure requirements.

This report captures the results of the recent 2016 Study, which is supported by SGX.

The findings are consistent with the recent SGX-KPMG Corporate Governance Disclosure Study 2016 that examined corporate governance disclosures for 545 Mainboard-listed companies in Singapore. The results provide another useful reference point for strengthening disclosure requirements.

The 2016 Study revisits the 2013 Study focus areas and includes new areas relating to risk tolerance, risk policies, risk culture, risk types and fraud risk management.

An improvement in disclosures for a majority of the key focus areas was observed over time, regardless of the Company's size or industry. Not surprisingly, new areas of the study, which are considered better practice areas, were not as well disclosed. There is thus a need to raise awareness of the value and importance of these practices, particularly in relation to risk culture and fraud risk management.

Interviews with independent directors and leading risk practitioners were also conducted. They provide further insights into the progress and key challenges in establishing adequate and effective risk management and internal control systems.

We hope you find this report useful in further understanding the key risk governance practices and disclosure requirements as you look for ways to continually improve in these areas.

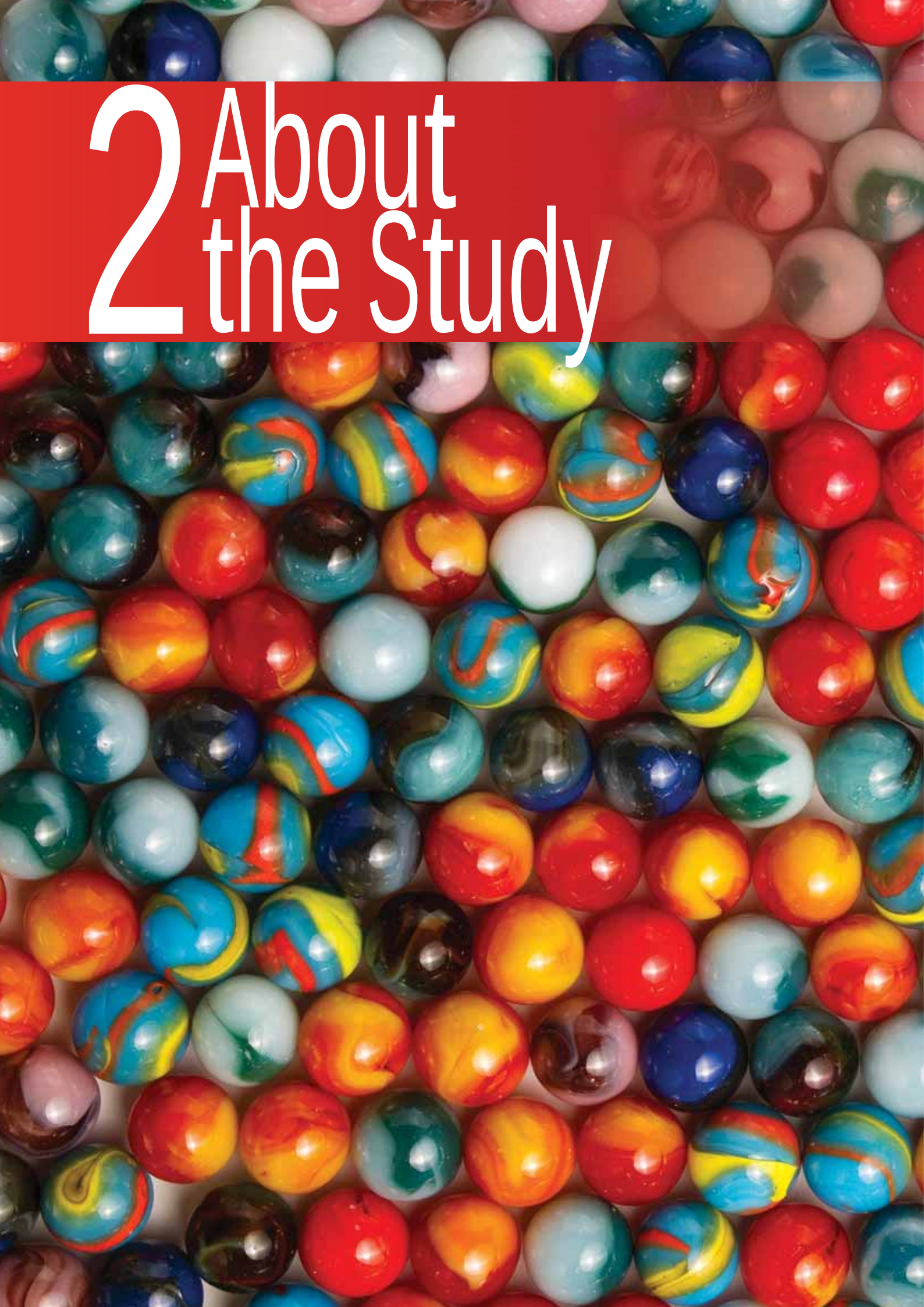
Ho Tuck Chuen

Chairman, ISCA Corporate Governance Committee
ISCA

Irving Low

Partner
Head of Risk Consulting
Head of Markets
KPMG in Singapore

1 ISCA-KPMG 'Towards better risk governance': A study of 250 listed Singapore companies, 2013
2 SGX-KPMG Corporate Governance Disclosure Study, 2016



2 About the Study

2.1 Objectives

Our study, jointly conducted by ISCA and KPMG and supported by SGX, is a time-based study to observe the risk governance disclosures of a sample of Singapore-listed companies in 2013 and 2016.

The study analysed disclosures found in annual reports relating to board risk governance, risk management capabilities and structures, risk management practices, internal audit and fraud risk management. It also looked at the extent to which companies have adopted the requirements of the CG Code relating to risk governance and the SGX LR 1207 (10).

2.2 Research Approach

A sample of 250 Singapore listed companies (from the SGX Mainboard and Catalist) was selected for the initial 2013 Study. At the time, this sample was reflective of the SGX profile of listed companies. For the purposes of the study, secondary listings, newly listed companies, real estate investment trusts, companies that had not released any annual reports for FY11/12 and companies under judicial management were excluded from the sample. Data was collected for the current study using the annual reports for FY15/16 that were publicly available as at 30 April 2016.

The same sample of 250 companies was selected for the current 2016 Study. However, only a total of 219 companies were available for analysis, as 31 companies were excluded from the scope due to their delisting or delays in the release of their annual reports.

The study's limitations are set out in Appendix A.

2.2.1 Market capitalisation

For comparability with 2013, the 219 sampled companies were sorted into three groups based on their market capitalisation (Cap) as at 31 December 2015 according to the same definition previously used[3]. Chart 1 highlights that Small Cap companies comprise a significant proportion of the sample size (72%), followed by Large Cap (16%) and Mid Cap (12%)[4] .

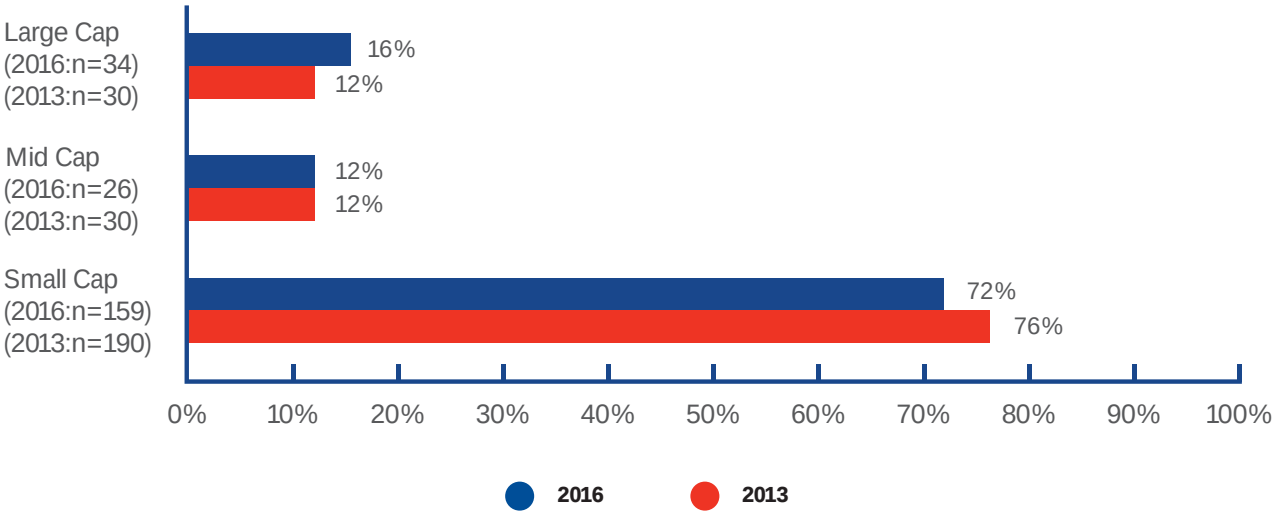


Chart 1: Company distribution by market capitalisation

[3] SGX does not provide criteria for determining Large, Mid and Small Cap companies. The thresholds proposed and used in the 2013 and 2016 Study are based on the Singapore Corporate Awards criteria.
[4] Companies are considered Large cap if their market cap is S$1 billion and above; Mid cap is S$300 million to less than S$1 billion; Small cap is less than S$300 million.

2.2.2 Sector classification

The samples were grouped into various industry sectors using the same classification outlined by SGX in the 2013 Study. Some sectors were merged to reduce the number of sectors to display (e.g. Real Estate, Others). Refer to Appendix B for an overview of the sector groupings and classification.

Chart 2 summarises the distribution of our sample companies across sectors. The three largest sectors are Manufacturing, Services and Commerce, consistent with the 2013 Study.

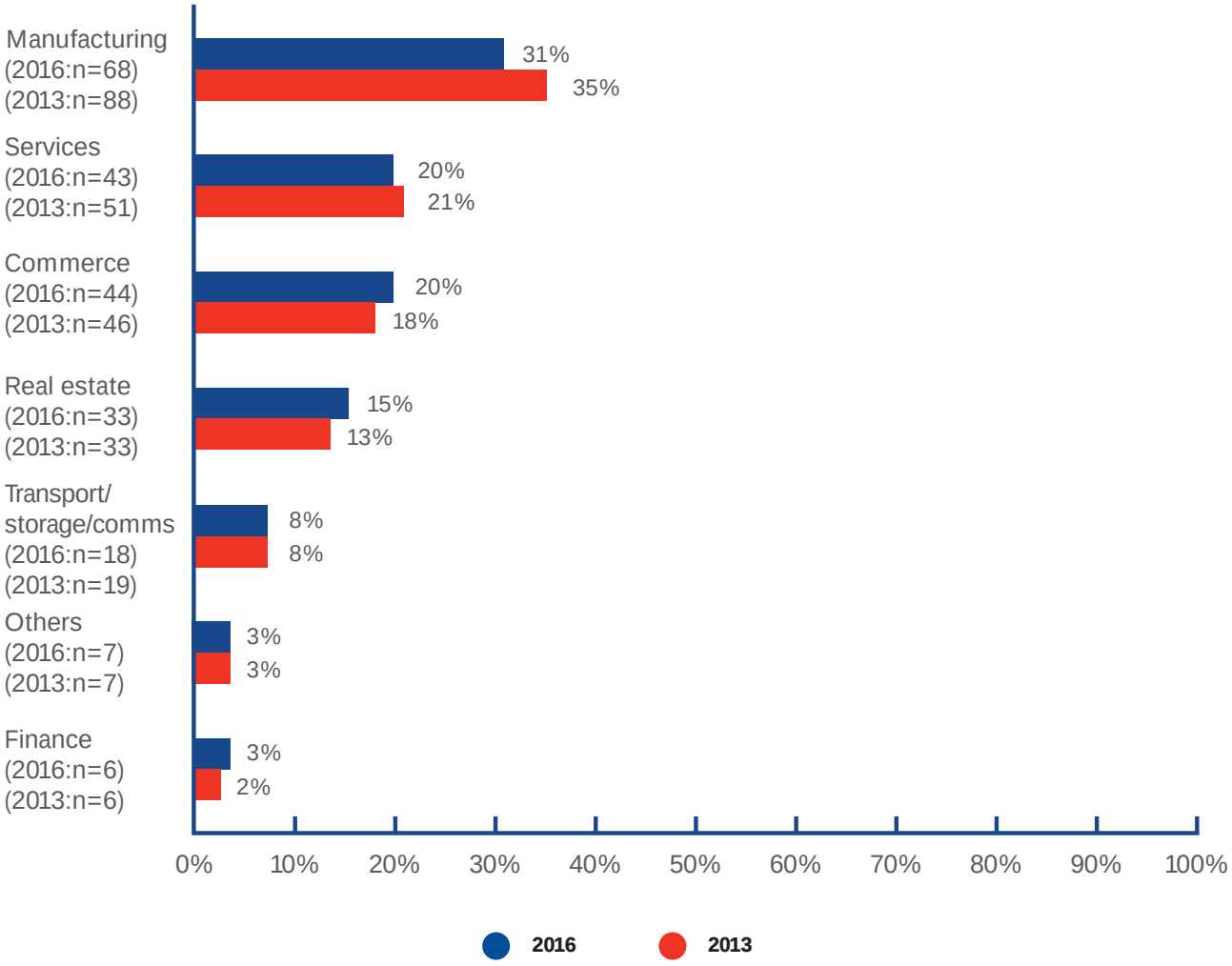


Chart 2: Company distribution by Sector

2.2.3 Government-Linked Corporations (GLCs)

Chart 3 summarises the distribution of our sample of companies according to whether they are classified as a GLC or not.

For the current study, we defined a company as a GLC if one of the substantial shareholders (either direct or indirect) is Temasek Holdings or a government/statutory body and they hold at least 15% shareholding[5] as compared to the definition in the 2013 Study[6] .

[5] The definition of a GLC for the 2016 Study is based on a paper by Associate Professor Mak Yuen Teen for the EU Asia Corporate Governance Dialogue 2015: "Governance of Government-Linked Companies in Singapore"
[6] The definition of a GLC in the 2013 Study was based on an IMF paper by Carolos D. Ramirez and Ling Hui Tan: "Singapore Inc. Versus the Private Sector: Are Government-Linked Companies Different?", 2004.

The performance of GLCs compared to other privately run companies is of interest to stakeholders concerned about the management and return of Singapore's reserves. Temasek Holdings is a GLC and is accountable to the government for its performance. This requires it to develop risk management strategies and capabilities, while taking calculated risks aimed at growing the value of its investments or portfolios over time[7, 8].

Overall, the GLCs represent 7% of the population of companies in the study which is similar to the 2013 Study composition. There have been slight movements within each of the market capitalisation categories due to some changes in the size of the companies and the change in GLC definition.

A significant portion of the Large Cap companies are considered GLCs which is consistent with the previous study (2016: 35%; 2013: 40%).

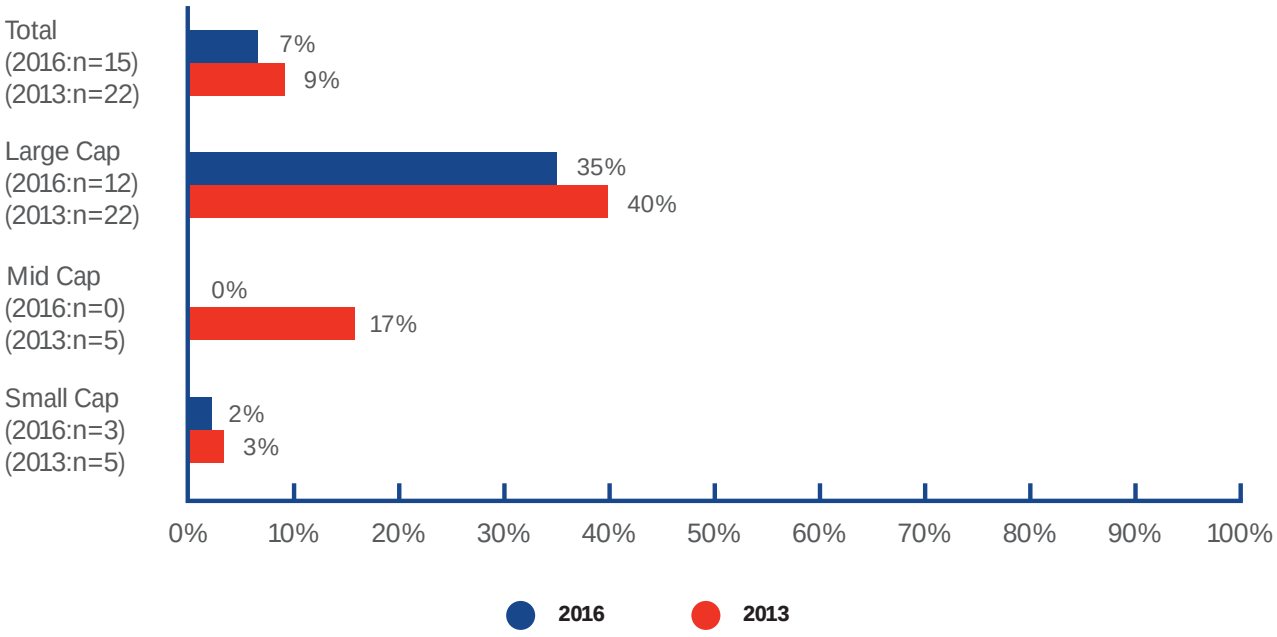


Chart 3: Company distribution of GLCs

2.3 Research Framework and Methodology

To conduct a review of the risk management landscape in Singapore, the collected data – taken from information disclosed in the annual reports of the sampled companies – was mapped against the key regulations and better practices for risk management and internal controls set out by SGX and the Monetary Authority of Singapore (MAS).

Figure 1 provides a summary of our study's approach. Our study focused on two key areas: the risk management capabilities (comprising structure and practices) and the Board's conclusion on the adequacy and effectiveness of risk management and internal controls (as outlined in SGX LR 1207 (10) and Principle 11 of the CG Code).

Figure 2 highlights the difference in requirements between the two corporate governance instruments regarding the conclusion to be formed over the adequacy and effectiveness of risk management and internal controls. The SGX LR 1207 (10) requires the Board to provide an opinion over the adequacy of internal controls, whereas the CG Code Principle 11 requires the Board to comment on the adequacy and effectiveness of internal controls and risk management.

[7] Address by Mr Tharman Shanmugaratnam, Deputy Prime Minister and Minister for Finance, at Temasek Holdings' 39th Anniversary Dinner at Ritz Carlton Hotel, 6 August 2013.
[8] GIC FAQs, "What is the relationship between GIC and the Government?"

State of Adoption

RISK MANAGEMENT CAPABILITIES

1. RISK GOVERNANCE STRUCTURES

1.1 Board
1.2 Board risk oversight committees
1.3 C-suite [chief risk officer (CRO) or equivalent]
1.4 Risk management function (*new*)
1.5 Internal audit (IA) function

2. RISK MANAGEMENT PRACTICES

2.1 Risk Management Framework
2.2 Risk Tolerance (*new*)
2 3 Risk Policies (*new*)
2.4 Risk Categories and Risk Types (*new*)
2.5 Risk Culture (*new*)
2.6 Fraud Risk Management (*new*)
2.7 Whistle-blowing Policies

BASIS OF BOARD OPINION

3. BOARD'S CONCLUSION ON RISK MANAGEMENT AND INTERNAL CONTROLS

SGX LR 1207(10) and PN 12.2

3.1 opinion on the **adequacy** of internal controls

3.2 basis for opinion on internal controls

CG Code (Principle 11)

3.3 comment on **adequacy** and **effectiveness** of:
- internal controls
- risk management systems

3.4 assurance to the board by Chief Executive Officer (CEO) & Chief Financial Officer (CFO)

Figure 1: Summary of approach

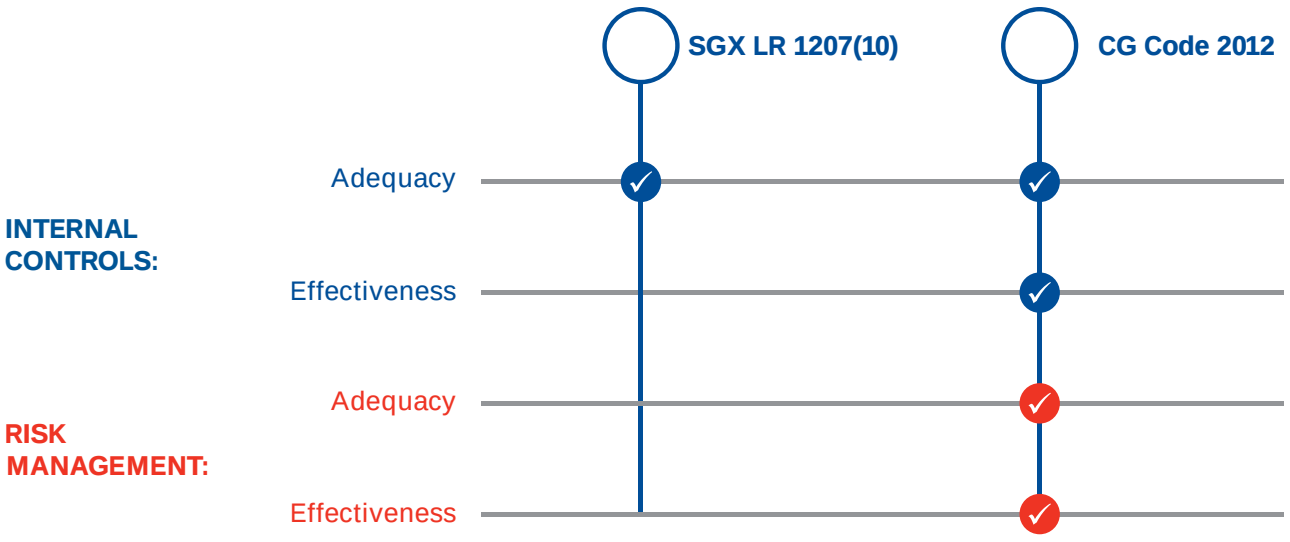
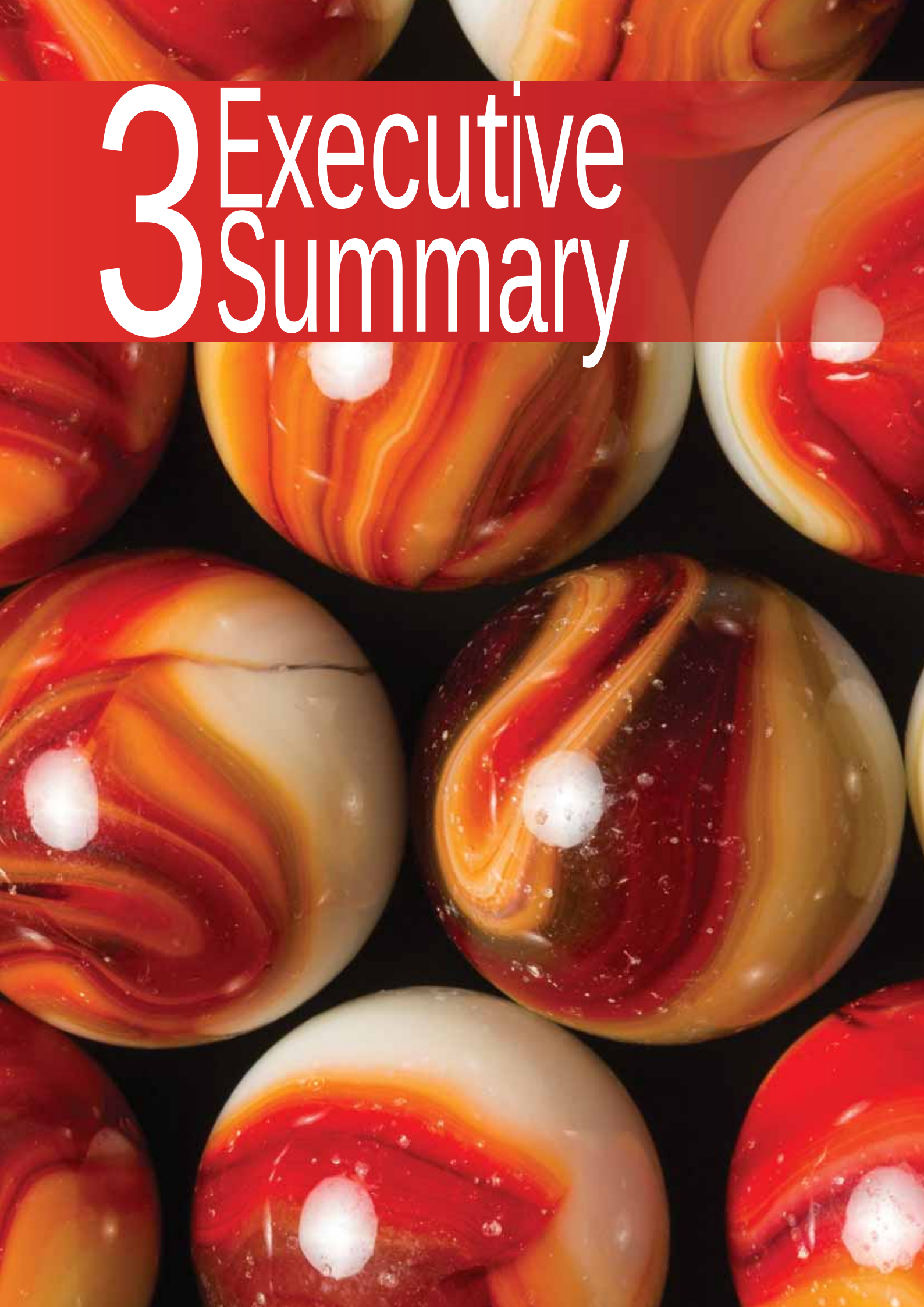


Figure 2: Comparison of requirements regarding the adequacy and effectiveness of risk management and internal controls

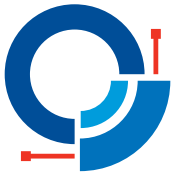


3 Executive Summary

3.1 State of Adoption

3.1.1 Risk management disclosures have improved over time

Disclosures relating to risk governance, risk management practices and the Board's conclusion on the adequacy and effectiveness of risk management and internal controls have improved over time. Where risk structures and practices are specified in the SGX LR or CG Code, there is a trend of improvement. However, for additional areas not specified in the guidelines, such as risk culture and fraud risk management, disclosures were less forthcoming at 19% and 5% respectively.

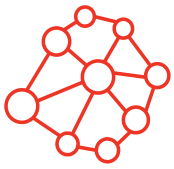


3.1.2 Large Cap companies have more forthcoming disclosures than Mid and Small Cap

Large Caps outperformed other companies especially in the areas of accountability like the 'Board assuming responsibility for risk management' and 'Assurances from the CEO and CFO'. They also did better in the areas of the 2016 Study which have been included for the first time, like risk policies; risk tolerance; risk culture and a dedicated risk function. Disclosures by Large Caps were significantly higher than their counterparts by 18% to 40% in these areas. This could reflect the scale and complexity of risks in these organisations and importance they place on communicating these practices to key stakeholders to enhance confidence in their ability to manage risks.

3.1.3 GLCs continue to have more forthcoming disclosures than non-GLCs

GLCs consistently provided more forthcoming disclosures than non-GLCs on their risk governance and risk management practices. The biggest gaps between GLCs and non-GLCs were for disclosures on having a risk management framework (93% compared to 62%); a Board Risk Committee (BRC) (80% compared to 12%), a CRO (33% compared to 7%) and Management Risk Committee (MRC) (53% compared to 17%) and an established Risk Culture (67% compared to 15%).



3.1.4 Sector influences the disclosure of risk governance structures and practices

The analysis by industry indicates that disclosures were consistent across sectors for areas that are specified in the corporate governance instruments, such as assigning responsibility for risk to a Board Committee and establishing an IA function. However, for better practice areas not specified in the corporate governance instruments, such as risk culture and establishment of a dedicated risk function, the Finance sector appears to be more advanced, leading 9 out of 14 key aspects considered in the 2016 Study. This is possibly due to the additional guidance offered by the MAS Guidelines on Corporate Governance for Financial Holding Companies, Banks, Direct Insurers, Reinsurers and Captive Insurers which are incorporated in Singapore (FS CG Code).

3.2 Risk Governance Structures

3.2.1 Board level risk responsibilities are more clearly disclosed

All companies disclosed that the Board is responsible for risk. This is a significant improvement from the 2013 Study where only 34% indicated this was the case. In addition, the percentage of companies that have formally constituted an Audit and Risk Committee (ARC) has increased from 2% in 2013 to 16% and who have established a separate BRC from 12% in 2013 to 16%.

The value of having a BRC in terms of bringing focus, attention and allocation of resources is evident as significantly more companies that have a BRC in place also have a CRO, MRC and dedicated risk function. However, companies should determine the appropriate risk governance structure relevant for the scope, nature, size and complexity of their company.

3.2.2 Management level risk responsibilities and resource disclosures require improvement

While the percentage of companies that disclosed having a dedicated CRO in place increased to 9%, a significant percentage of companies (66%) still did not specify the executive at senior management level responsible for risk in the organisation. Whether this is a single person or a collective group, companies should enhance disclosures in this regard. In addition, while 20% of companies disclosed having a MRC in place, only 5% indicated there is a dedicated risk function. Given the importance of managing risks to help companies achieve their objectives, more could be disclosed about the resources and capabilities of the risk function and personnel.

3.3 Risk Management Practices

3.3.1 Disclosure of risk culture and risk behavioural practices lacking

While 64% of companies disclosed information in relation to having established a risk management framework (including a risk assessment and monitoring process) and 68% of companies disclosed having a risk management policy in place, there are some areas of risk management practices that could be enhanced. In particular, disclosures relating to risk culture are lacking as only 19% of companies made some mention of it. 41% of companies mentioned setting risk tolerance limits while only 19% disclosed aligning remuneration and risk policies, both of which are key elements in establishing an effective risk culture. Only 4% of companies disclosed having a formal process in place to assess and measure the organisational risk culture.

3.3.2 Risk category and risk type disclosure could be improved

A majority of companies did not disclose specific risk type information, but they disclosed high-level risk categories such as financial, operational, compliance and information technology (IT) categories. Disclosures on the risk description and mitigating actions were less forthcoming. In particular, strategic and cyber risks were significantly under-represented with disclosures at 31% and 5% respectively.

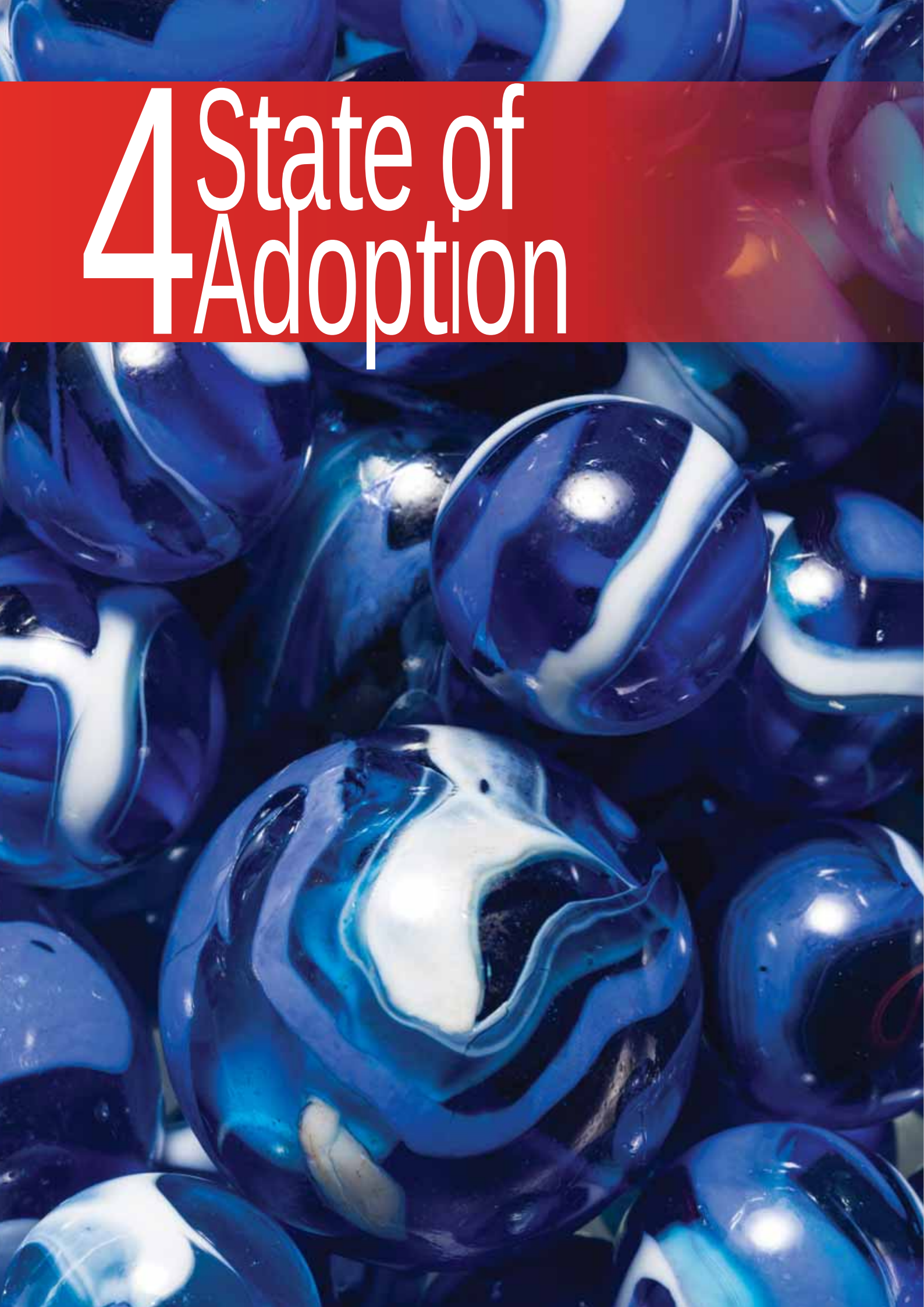
3.3.3 Fraud risk management disclosures revolve around whistle-blowing

Although the study found 95% of companies disclose some fraud risk measures, in the majority of cases this is a whistle-blowing policy. Only 5% of companies or less disclosed information related to a broader fraud risk management framework, anti-fraud policies, or a focus on establishing an anti-fraud culture. While this is encouraging, given that studies have shown that whistle-blowing and tip-offs are the most common method of fraud detection, the introduction of other fraud risk management tools is recommended particularly as technology is enabling new methods of fraud which can more easily circumvent internal controls.

3.4 Board's conclusion on risk management and internal controls

While the SGX LR 1207 (10) has certainly brought focus to all listed companies in ensuring that they comply with the requirements, there remains some confusion in disclosures, particularly with regard to terminology used and the scope of the Board's conclusion. A significant majority of companies (84%) provide an 'opinion' from the Board on the adequacy of internal controls, though a number of companies (13%) adopted other terms such as 'is of the view', 'is satisfied'. The use of the word 'opinion' is required by the listing rule and indicates a higher level of confidence and robustness legally, than the 'comment' afforded by the Code. In addition, not all companies satisfy the CG Code Guideline 11.3 which requires the Board to comment on the adequacy and effectiveness of risk management and internal control systems. There are inconsistencies in the use of the terms adequacy and effectiveness and the concepts of risk management and internal controls. More effort is required to raise awareness of these terms and apply them in practice and disclosures.

4 State of Adoption



Overall, disclosures relating to risk governance, risk management practices and the Board's conclusion on the adequacy and effectiveness of risk management and internal controls have improved since the 2013 Study (refer Chart 4[9]).

The study was expanded to include disclosures on additional aspects, specifically risk policies, risk tolerance, risk culture, risk function and fraud risk management.

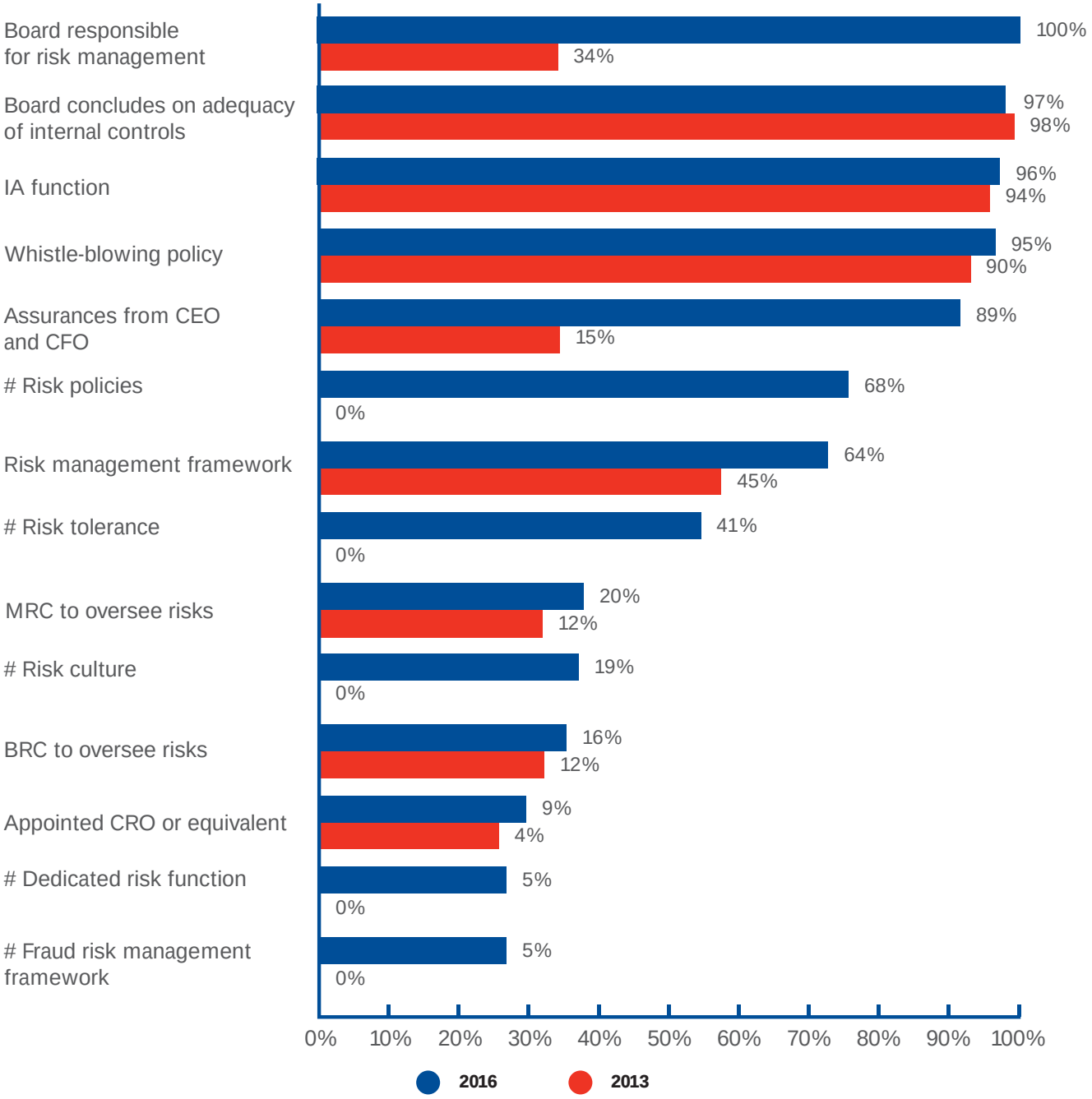


Chart 4: Comparison of risk governance structures and practices
refers to new additional aspects previously not included in the 2013 Study

[9] It should be noted that two adjustments were made to the results of the 2013 Study to enable a more consistent analysis
- In the 2013 Study, the ARC was bundled with the BRC, whereas for the 2016 Study, the ARC and BRC were analysed separately. For comparability, the BRC and ARC data has been retrospectively reclassified and analysed.
- In the 2013 Study, CRO was previously defined as persons described as having risk management responsibilities. In the 2016 Study, the CRO is now defined as persons in an executive position, primarily in a dedicated capacity, carrying an explicit title of CRO For comparability, the CRO data has retrospectively reclassified and analysed.

The 2016 Study found that for a majority of risk governance structures and practices, Large Cap companies had more forthcoming disclosures compared to Mid and Small Cap companies (refer Appendix C.1). Where there were slight decreases in Large Cap disclosures regarding certain risk governance structures and practices during this time, this was due to a reclassification of companies within the Large Cap category rather than companies ceasing to conduct a certain practice.

GLCs provided more forthcoming disclosures than non-GLCs for almost all risk governance aspects (refer Chart 5). In particular, GLCs were significantly more forthcoming about the risk management framework, establishing a MRC, appointing a CRO, establishing a BRC to oversee risks and establishing risk culture.

In addition, the 2016 Study compared the risk governance disclosures across Sector classifications (refer Appendix C.2). The results indicate that disclosures were more forthcoming for the more structural areas such as assigning responsibility for risk to a board committee and establishing an IA function. However, in the emerging areas such as risk culture and establishment of a dedicated risk function, the Finance sector appears to be more advanced, possibly due to the additional guidance offered by the FS CG Code.

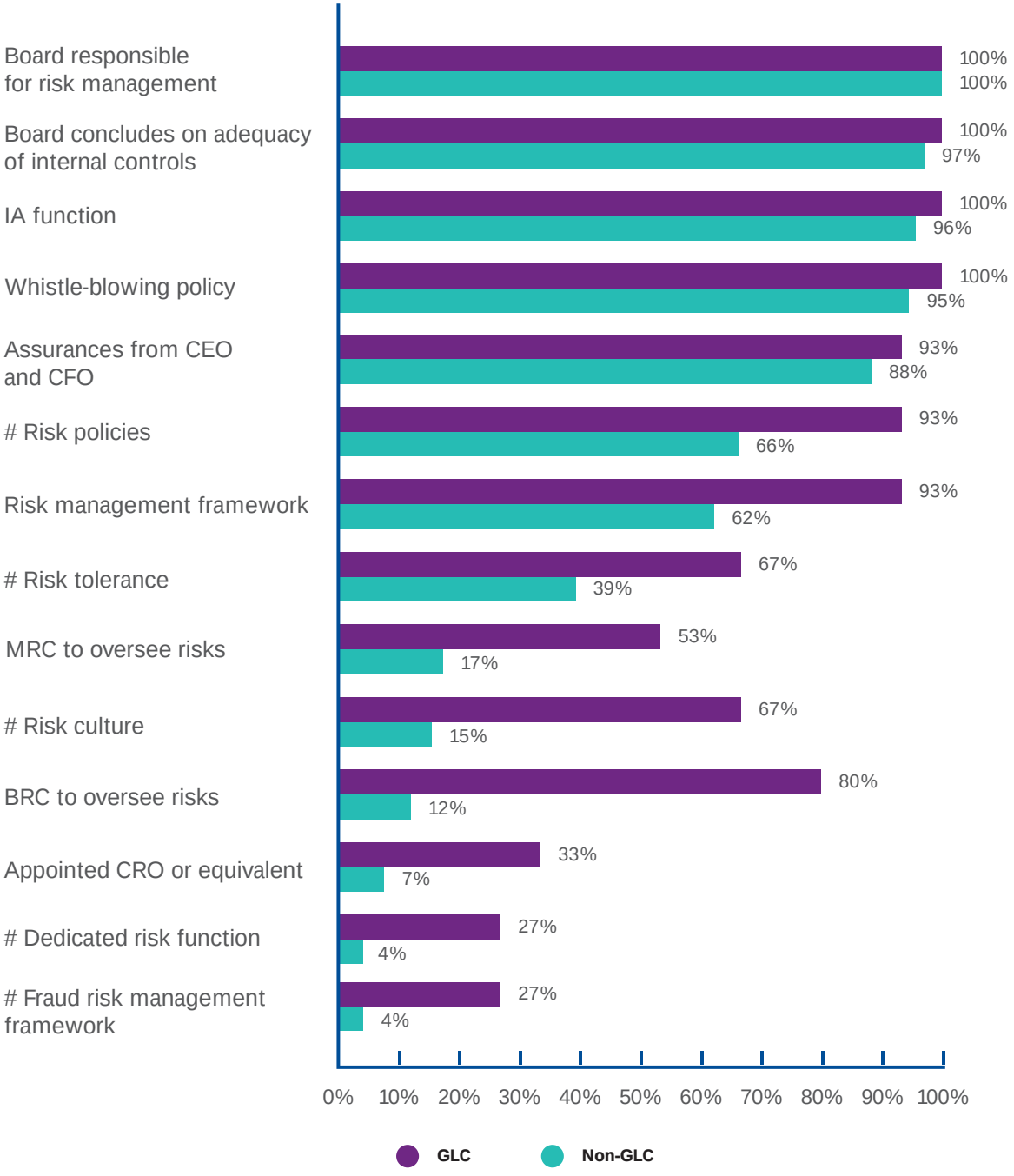


Chart 5: Comparison of GLC and non-GLC risk management practices
refers to new additional aspects previously not included in the 2013 Study

5 Risk Governance Structures

KPMG's 4 Lines of Defence model, as outlined in Figure 3 below, can serve as a useful basis to further understand the key elements and roles within the overarching risk governance and oversight structure. This model highlights that management is the first line of defence in identifying and mitigating risks by establishing policies and implementing operational/financial governance. Additional risk management functions and activities form the second line of defence, while IA and other independent assurance functions form the third line of defence. Finally, the board and board committee structures form the fourth line of defence. Our study explored elements of the 4 Lines of Defence and the related key findings are outlined in this section of the report.

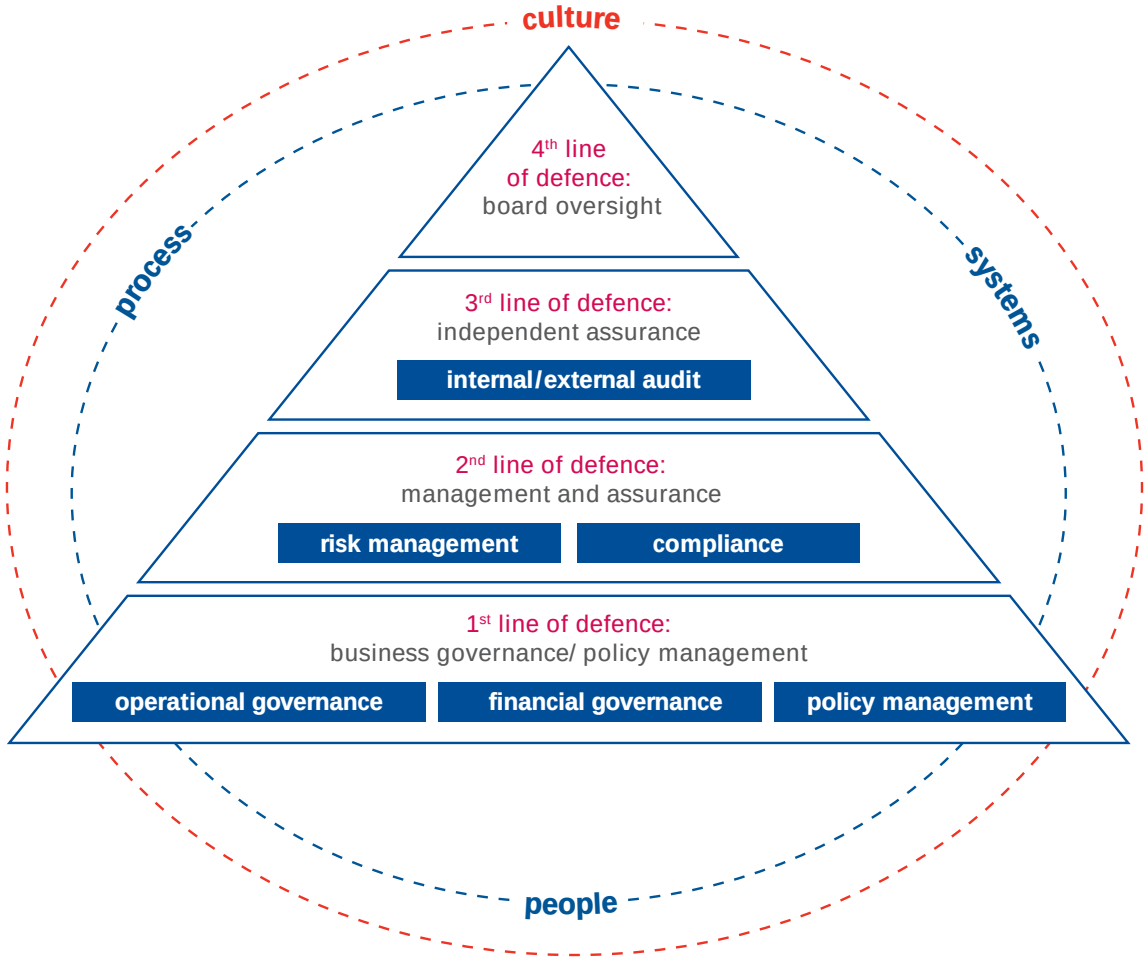


Figure 3: KPMG's 4 Lines of Defence Model

The next section of the report will address the 4th line of defence, followed by the 2nd line of defence and then the 3rd line of defence. The 1st line of defence was not covered as part of this study.

5.1 4th Line of Defence: Board Risk Oversight

5.1.1 Board

> Principle 11: The board is responsible for the governance of risk. The board should ensure that management maintains a sound system of risk management and internal controls to safeguard shareholders' interests and the company's assets, and should determine the nature and extent of the significant risks which the board is willing to take in achieving its strategic objectives.

The CG Code places the responsibility for the governance of risk on the board. The introduction of such guidelines clarifies for stakeholders that the board indeed has overall responsibility for risk oversight matters, even if the board sets up separate board committees to assist it with its risk governance responsibilities.

Chart 6 shows that the percentage of companies which disclose that the board is responsible for risk management improved significantly from 2013. This highlights that there is a much stronger recognition that the Board retains ultimate accountability for managing risks in the business.

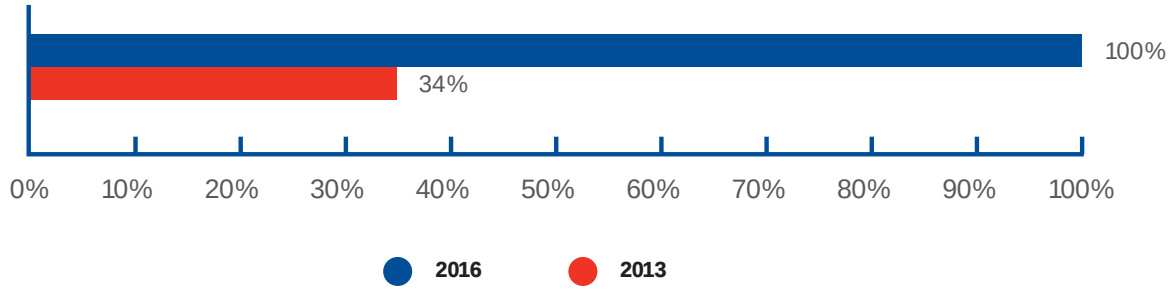


Chart 6: Percentage of companies stating the board is responsible for risk

5.1.2 Board committees

> Guideline 11.4: The board may establish a separate board risk committee or otherwise assess appropriate means to assist it in carrying out its responsibility of overseeing the company's risk management framework and policies.

There have been interesting trends in the board risk oversight committee structures since the 2013 Study. While the proportion of companies with an Audit Committee (AC) decreased by 14% across the population (refer to Chart 7), the proportion with an ARC increased by 14% (refer to Chart 8). This indicates there has been a restructuring of committees from AC to ARC by these companies. Encouragingly the percentage of companies with a BRC increased to 16% compared to 12% (refer Chart 9).

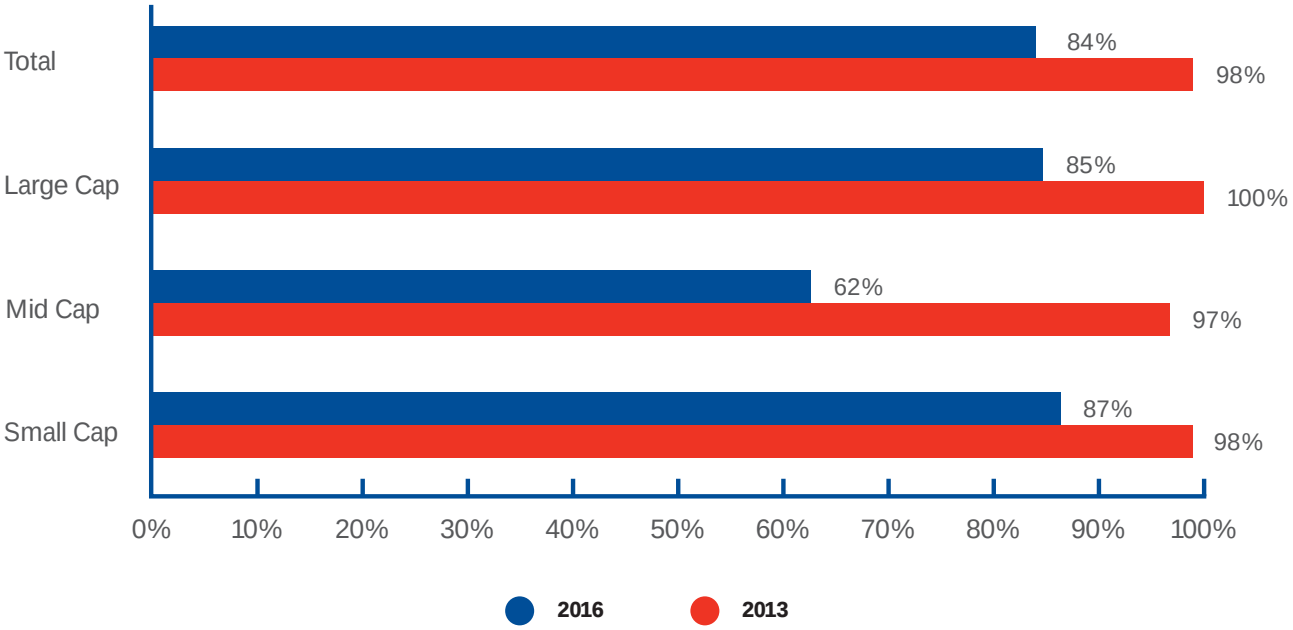


Chart 7: Percentage of companies with an Audit Committee

The analysis becomes even more interesting when examining the results across market capitalisation (refer Chart 7, 8 and 9). For Large Cap companies, a significant proportion established separate BRCs (65%). In addition, the percentage of ARCs increased to 15% (reflecting a change in title from the previous AC).

While Mid Cap companies had the most significant decrease in ACs (35%), they had an equivalent increase in ARCs. The percentage of Mid Cap companies with BRCs slightly decreased (by 4%) between 2013 and 2016 which was driven by a reclassification of the market capitalisation of some Mid Cap companies from the 2013 Study rather than companies ceasing to have a BRC in 2016.

Small Cap companies also restructured their risk oversight committees, with an increase in ARCs to 13% and BRCs to 6%.

This general restructuring of risk oversight committees during the past three years reflects the response of companies to the increasing complexity of the risk landscape confronting them, and the increased workload of the AC. Many companies have opted to restructure their committees to either have a formally constituted ARC or a separate BRC.

> "When the board considers what the right board committee structure should be, it needs to take into account the size, nature and complexity of the business. For some companies, typically larger and more complex ones, having a separate committee structure allows the members to focus in a consistent manner. The AC typically evaluates things that have happened, while the BRC should be forward looking. There is quite a difference between the two and for some companies it makes sense to have them separate with clearly defined responsibilities."
>
> **Danny Teoh**
> Independent Director

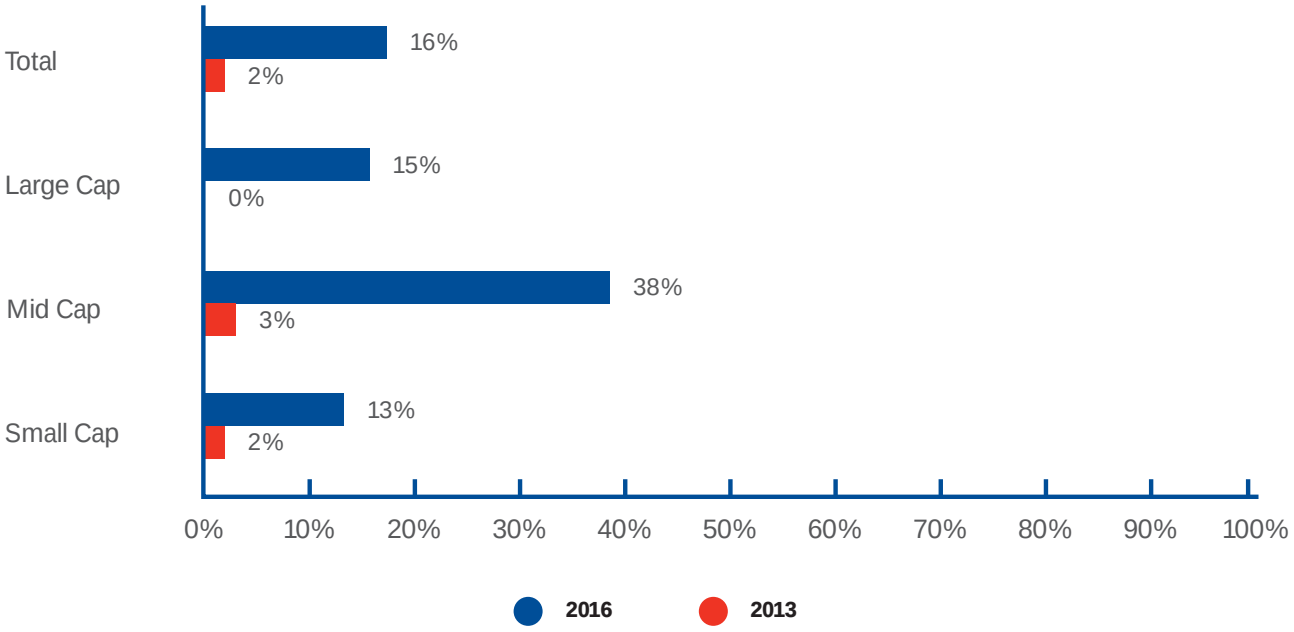


Chart 8: Percentage of companies with an Audit and Risk Committee

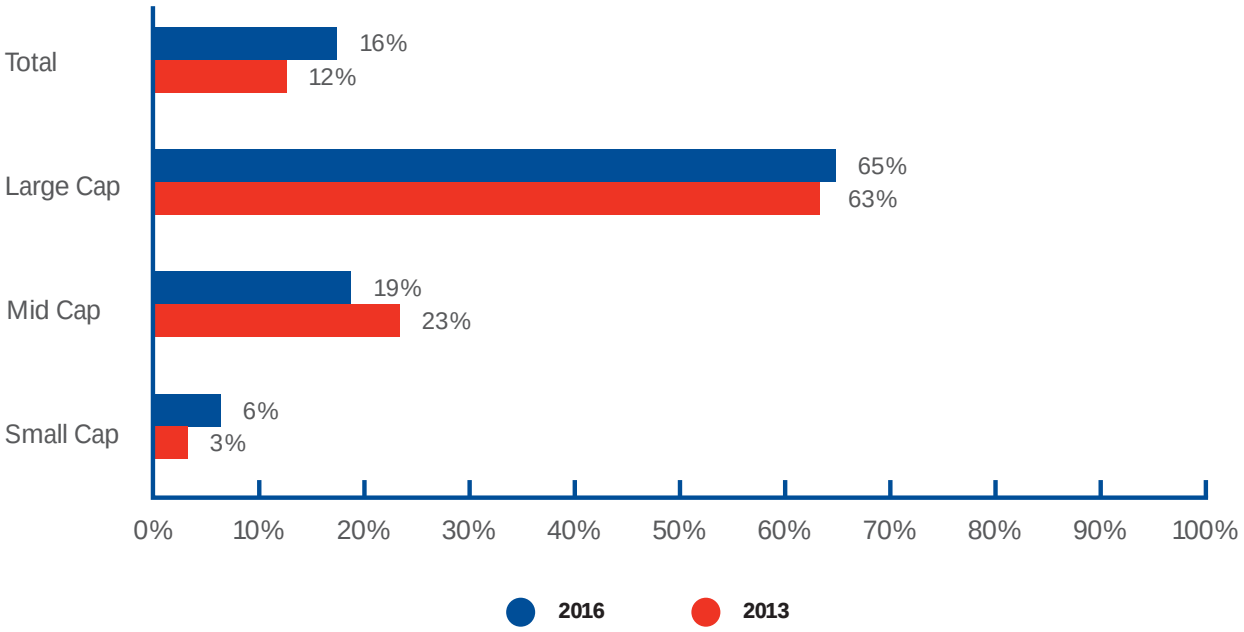


Chart 9: Percentage of companies with a Board Risk Committee

The study also considered the extent to which the board committee terms of reference found within the annual reports of companies included reference to the board committee's roles and responsibilities in relation to risk management. As shown in Chart 10, the percentage of companies stating that the ARC has responsibility for risk management remained consistent. For those with BRCs, all state that the BRC is responsible. These results are in line with expectations, given that both the introduction of a BRC, or the restructuring of the ACs into an ARC, indicate an increased focus on these committees as being ultimately accountable for risk.

However, there was a significant increase (from 29% to 83%) in the percentage of companies stating that the AC has some responsibility for risk management.

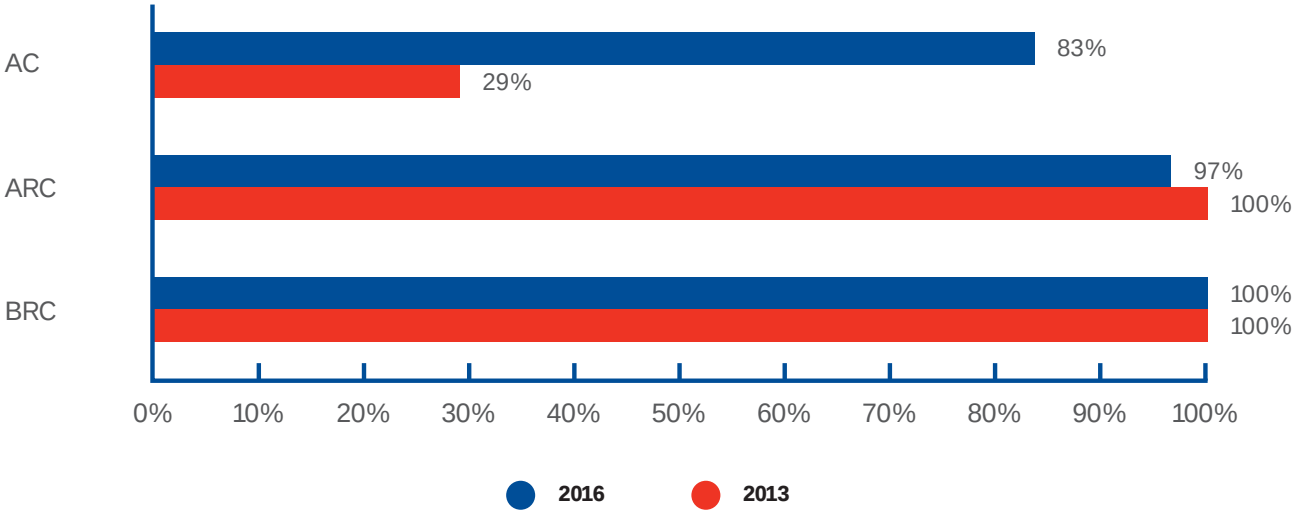


Chart 10: Percentage of companies specifying board committee responsibility for risk

Chart 11 provides a further breakdown to identify the percentage of ACs that were a 'stand-alone' AC with no separate BRC (71%) and those that had a separate BRC (12%) in place.

For the 'stand-alone' ACs, it is encouraging to see that a majority specified responsibility for risk in their terms of reference (as in this scenario they are generally the primary Board committee responsible for risk). However, 9% failed to do so. For the ACs with a separate BRC, a proportion (12%) specified a role in relation to risk management. This could reflect a split in responsibilities between the AC and BRC (such as the AC taking responsibility for financial reporting risk and the BRC taking responsibility for all other risk types).

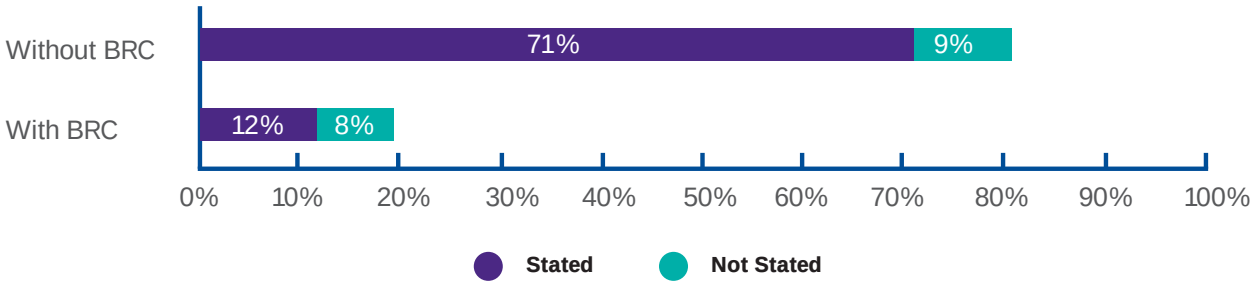


Chart 11: Percentage of companies specifying the AC responsible for risk (comparing those with and without a separate BRC)

Our study also considered the results for GLCs and non-GLCs regarding the risk oversight structures. Chart 12 highlights that 100% of GLCs had an AC with no GLCs having an ARC (refer Chart 13). The percentage of GLCs with a separate BRC (refer Chart 14) increased significantly to 80% (from 55% in 2013), indicating this is the preferred risk governance structure amongst GLCs. In comparison, non-GLCs opted for ARCs, with 15% moving from an AC to an ARC model. Only 12% of non-GLCs established a separate BRC. The GLCs could therefore be seen to be leading the way in terms of focusing attention on risk.

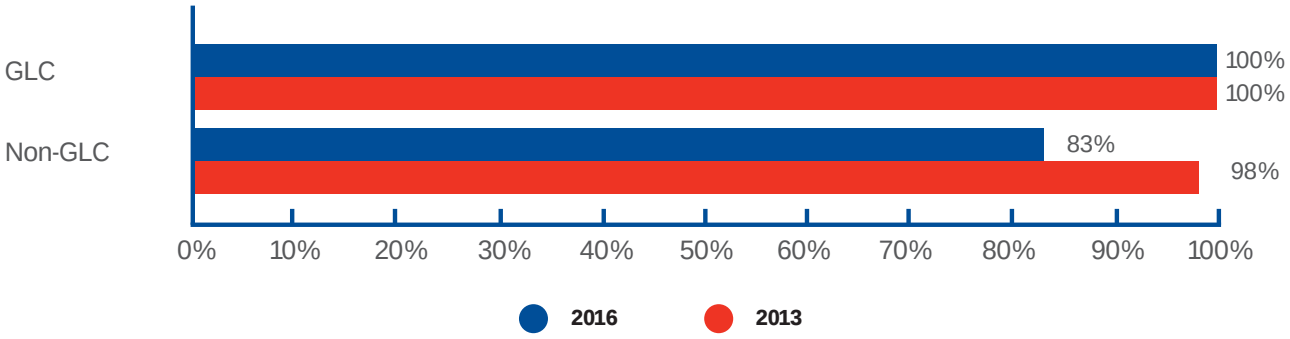


Chart 12: Comparison of GLC and non-GLC companies with Audit Committees

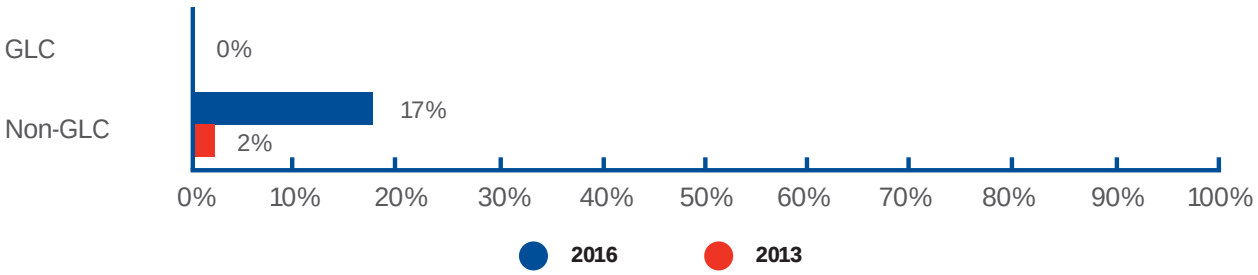


Chart 13: Comparison of GLC and non-GLC companies with Audit and Risk Committees

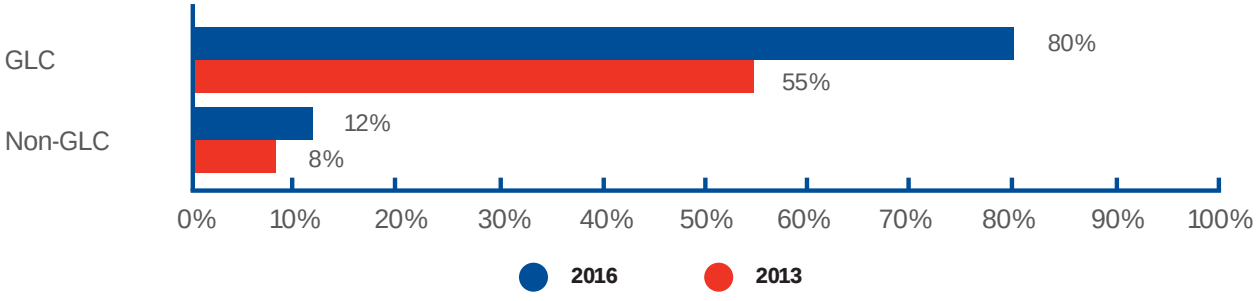


Chart 14: Comparison of GLC and non-GLC companies with Board Risk Committees

5.1.3. Board Committee Composition

Increasingly, the composition of the board committees responsible for risk oversight is critical to maximise the effectiveness and outcomes of the committee.

The study found that the AC and ARC comprised mostly independent directors (IDs) and non-executive directors (NEDs), which is consistent with the requirements of the CG Code. While the AC composition has not changed significantly since 2013 (refer Chart 15), the proportion of IDs on the ARC has increased (refer Chart 16), with a commensurate decrease in the NED percentage. The BRC proportions changed minimally with a slight increase in NEDs in 2016 (refer Chart 17). The inclusion of the EDs on the BRC could also reflect that for a majority of companies (outside the Finance sector) there has been no formal guidance in the CG Code for BRC composition. The recently launched BRC Guidebook seeks to address this gap by suggesting that good practice is to have at least three directors, the majority being NEDs, (including the chairman), with at least one ID[10]. This is consistent with the FS CG Code.

> "The board risk oversight committee structure is unique to every company's circumstances. For some companies, there is a danger that when additional committees are created, accountabilities are diffused. Companies should spend more time focusing on the mandate, size, composition and frequency of meetings for each committee. There needs to be more thinking done about the roles and responsibilities of each committee and assessment of committee member capabilities to ensure there are no gaps in risk oversight mechanisms (particularly beyond financial risks)."
>
> **Professor Mak Yuen Teen**
> NUS Business School

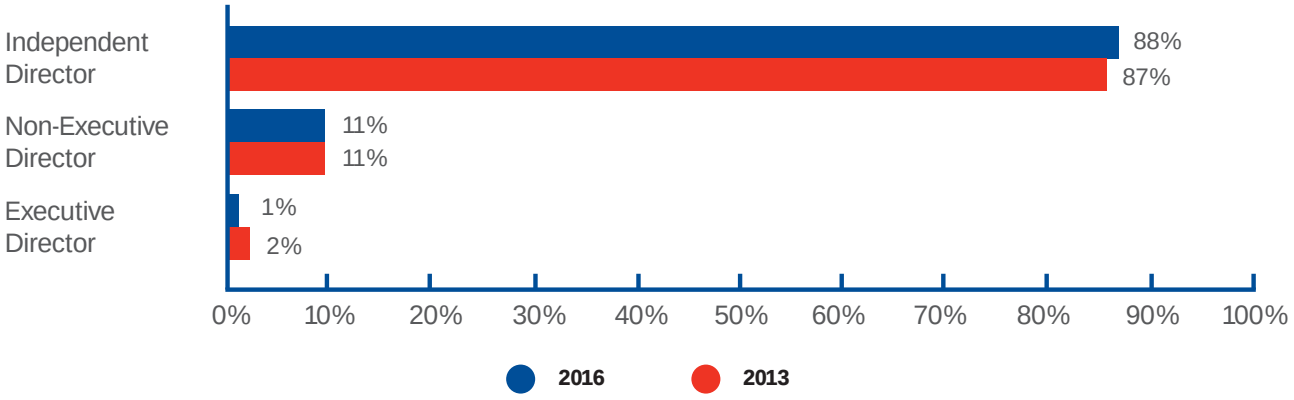


Chart 15: Audit Committee Composition

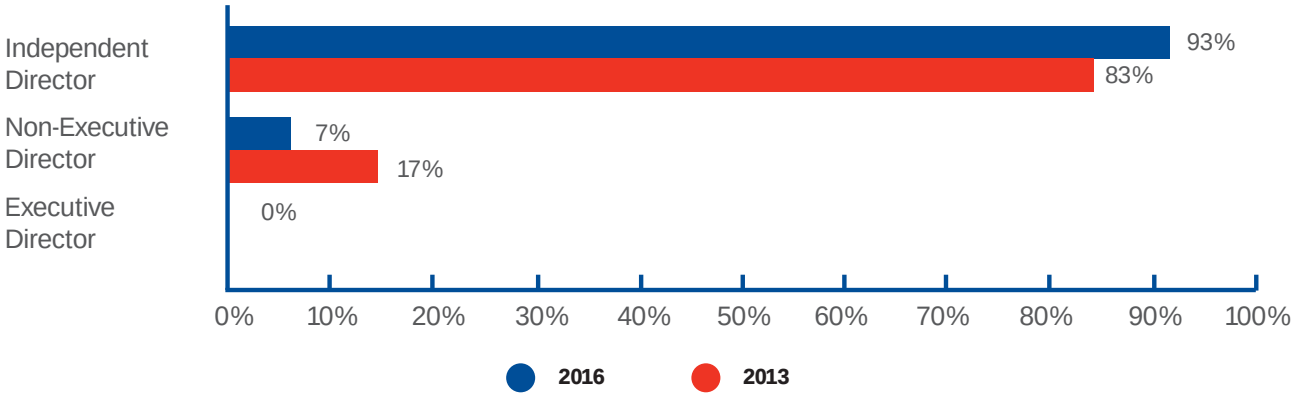


Chart 16: Audit and Risk Committee Composition

[10] SID CG Guides for Boards in Singapore, Board Risk Committee Guide, 2016 (SID BRC Guidebook)

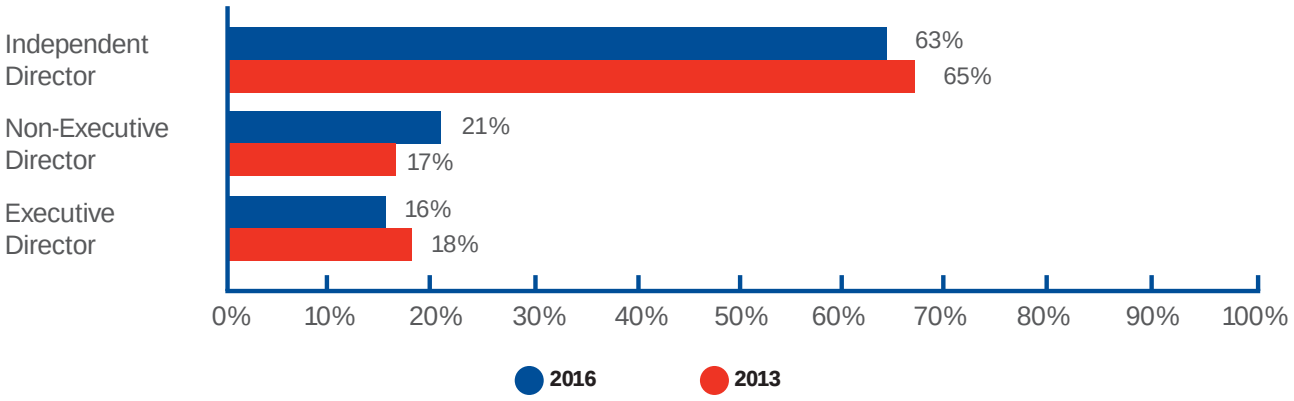


Chart 17: Board Risk Committee Composition

While the Chairman of the AC and the ARC is consistently an ID, this is not the case for the Chairman of the BRC (refer Chart 18). The AC and ARC practices are consistent with the requirements of the CG Code which state in Guideline 12.1 that "the AC should comprise at least three directors, the majority of whom, including the AC Chairman, should be independent." While the CG Code is silent on the composition of the BRC, the FS CG Code guidelines indicate that "the board risk committee should comprise at least 3 directors, a majority of whom, including the Chairman of the board risk committee, should be non-executive directors." As such, it is not uncommon for the BRC Chairman to be a NED.

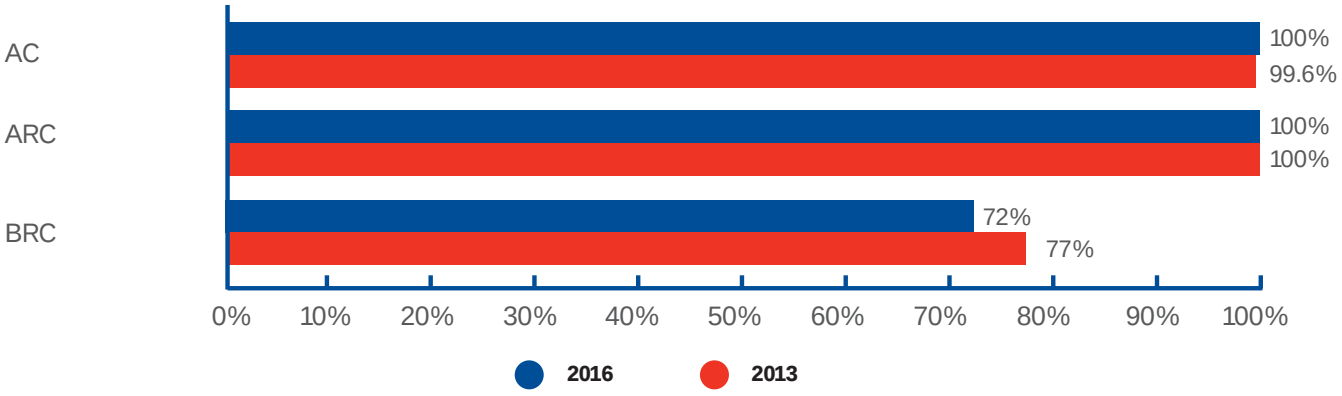


Chart 18: Percentage of companies with an Independent Committee Chairman

> "Since the financial crisis, there has been an acknowledgement that it is inadequate to rely solely on quantification models and historical technical analysis. This needs to be complemented by judgment calls based on subjective degrees of belief or a nuanced understanding about an uncertain future. To give yourself the best chance of navigating such ambiguity, you need the right mix of skills, experience and instincts, starting with the Board and the Audit or Risk Committees."
>
> **Mr Tan Boon Gin**
> Chief Regulatory Officer, Singapore Exchange

5.1.4. BRC Qualifications and Experience

The background of board committee members is an important element in their ability to act cohesively and make well-informed decisions on the range of issues which confront them. The CG Code encourages the board to "ensure that the members of the AC are appropriately qualified to discharge their responsibilities. At least two members, including the AC Chairman, should have recent and relevant accounting or related financial management expertise or experience, as the Board interprets such qualification in its business judgment.[11]" In addition, the FS CG Code indicates that for a BRC, "at least 2 members should have the relevant technical financial sophistication in risk disciplines or business experience, as the Board interprets such qualification in its judgment.[12]"

Our study shows that the background of both the BRC Chairman and members is mostly in finance, business operations and accounting (refer Chart 19). Fewer specialise in risk management, legal and IT. This shows that currently the traditional boardroom skillsets are found on these committees, but increasingly IT, risk management and legal skills will be sought after for these positions, as the nature of the risk environment evolves and its complexity increases.

The Nomination Committee plays a pivotal role in board member selection and appointment. It needs to be clear about what skills it is looking for when it searches for new committee members, and to properly understand the risk management credentials of the potential candidates. However, it is important to be able to clarify and define what risk management credentials are sought after. These could range from technical risk management qualifications to having risk oversight experience (at C-Suite level) to on-the-job experience of managing significant business operations and major projects.

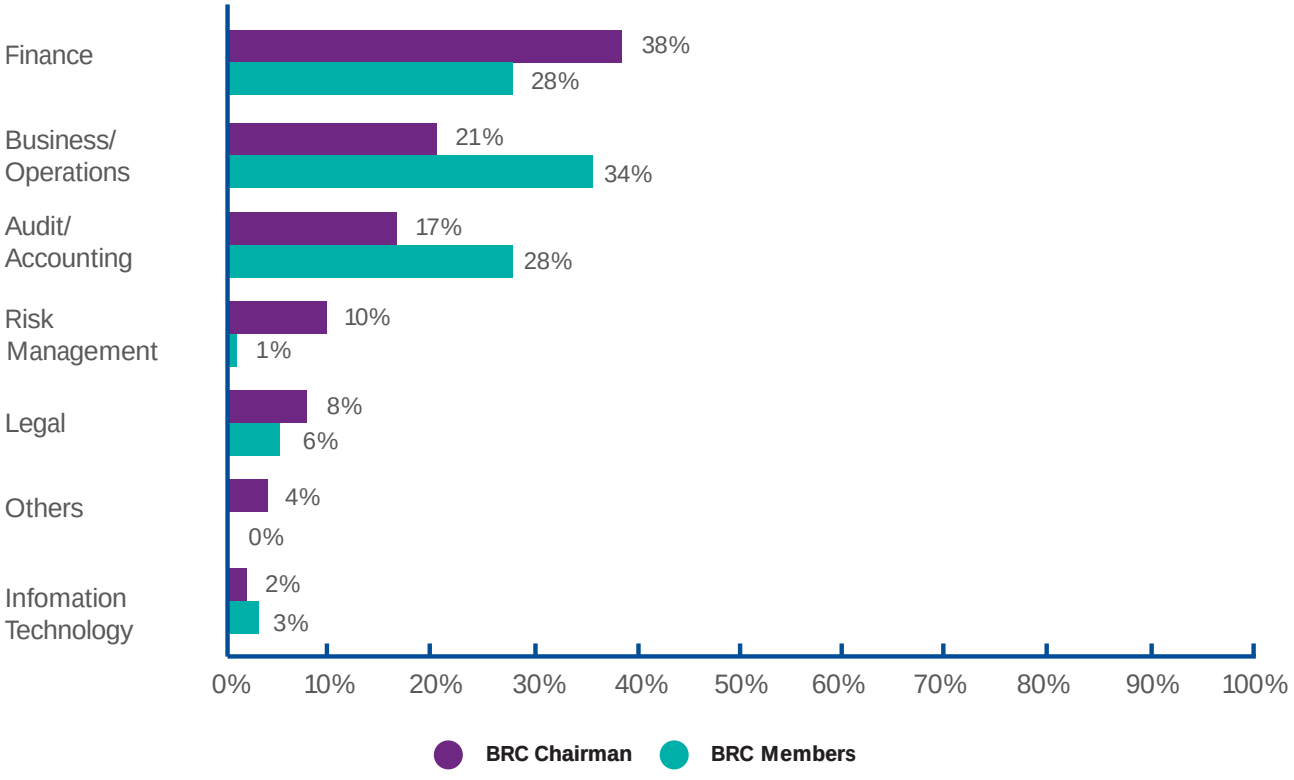


Chart 19: Background of BRC Chairman versus Members (multiple responses were allowed for this chart)

[11] CG Code Guideline 12.2
[12] FSCG Code Guideline 11.12

5.2 2nd Line of Defence: Risk Management

5.2.1 Chief Risk Officer

Overall, while the proportion of companies with a dedicated CRO (9%) increased (refer Chart 20), the role remains uncommon across the Singapore market. For the purposes of the 2016 Study, a CRO (or Head of Risk Management) has been defined as a person who has been appointed in a dedicated capacity, at a senior management level, to drive and oversee the risk management efforts across the organisation. Where an existing executive, such as the CFO, Treasurer or Operational Divisional Head has been appointed to oversee risk management, in addition to their existing roles, these have been excluded from this analysis.

In a 2015 KPMG Study[13], 76% of Singapore Board level respondents (61% globally) declared that improving risk-related information flowing to the board was a focus for them in response to the increasing complexity of the business and risk environment. This reinforces the view expressed in the 2013 Study that senior executives find the assessment and management of risks for their companies as becoming increasingly challenging. Directors expressed concern that the quality and quantity of information they receive may hinder their oversight, and without a dedicated CRO, the provision of increased risk information to board committees falls to already overstretched management.

> "At more of our board retreats, workshops, and strategy sessions, where we used to have economists come in to brief us, we're now seeing training sessions built around cyber security.
>
> Getting directors comfortable with the realisation that you can't just rely on the 'Digital Director' to deal with cyber security and digital risk is essential - it's every director's responsibility to be comfortable with the subject and to learn enough about it. They don't have to be a detailed expert but they need to understand the risks."
>
> **Adrian Chan**
> Independent Director

The companies which do have a CRO tend to be Large Cap, with nearly one third of Large Caps having a CRO. This could reflect the size, scale and complexity of operations and broad range of risks to be monitored.

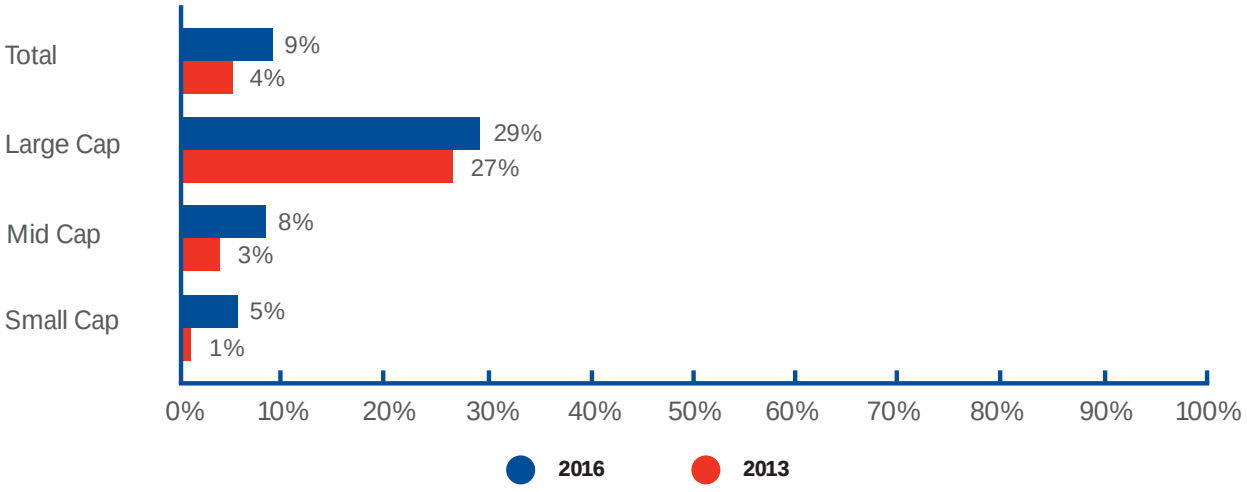


Chart 20: Percentage of companies with a Chief Risk Officer

An analysis by industry (refer Chart 21) shows that the Finance sector has the highest proportion of dedicated CROs. While this is not a mandated industry requirement, it is strongly recommended by the FS CG Code, which states that "depending on the scale, nature and complexity of its business, the Board may appoint a CRO to oversee the risk management function."

[13] KPMG Audit Committee Institute – Global Pulse Survey "Calibrating Strategy and Risk: A board's eye view" 2015

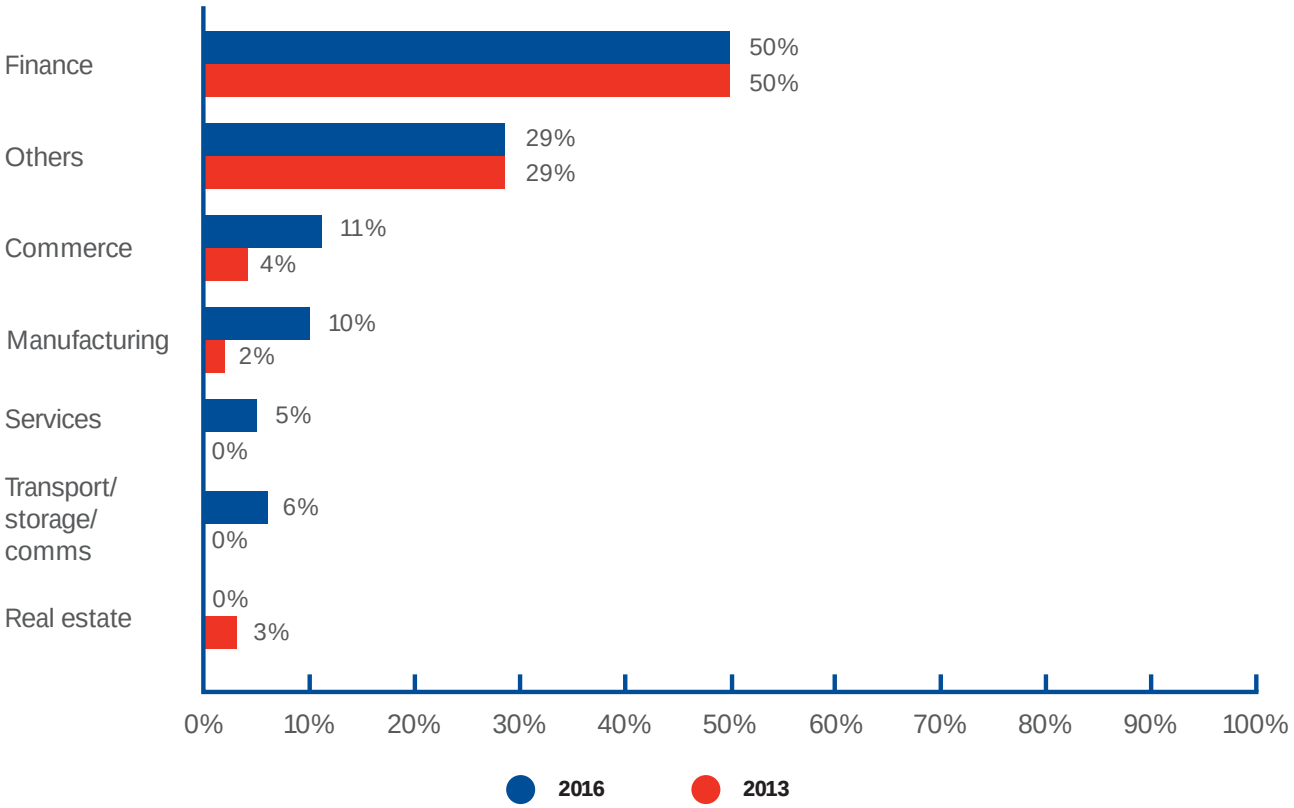


Chart 21: Percentage of companies with Chief Risk Officers by Sector

> "The role of the CRO and risk management function has expanded significantly demonstrating the emphasis on good risk management and governance in our Group. Besides establishing and maintaining the risk management framework, I am also responsible for business continuity management and I oversee complex and high risk projects that involve many business and functional groups so as to ensure a coordinated approach in managing risk project implementation. The risk team is also facilitating the implementation of Control Self Assessment."
>
> **Jeanne Cheng**
> Chief Risk Officer, Singapore Power

While there was a 19% improvement in the percentage of companies disclosing the senior manager responsible for risk management, a significant proportion (66%) of companies did not disclose who is responsible for risk (refer Chart 22). For the 34% that did disclose, the CRO (9%), CFO (7%) and CEO (4%) were the most prevalent responses.

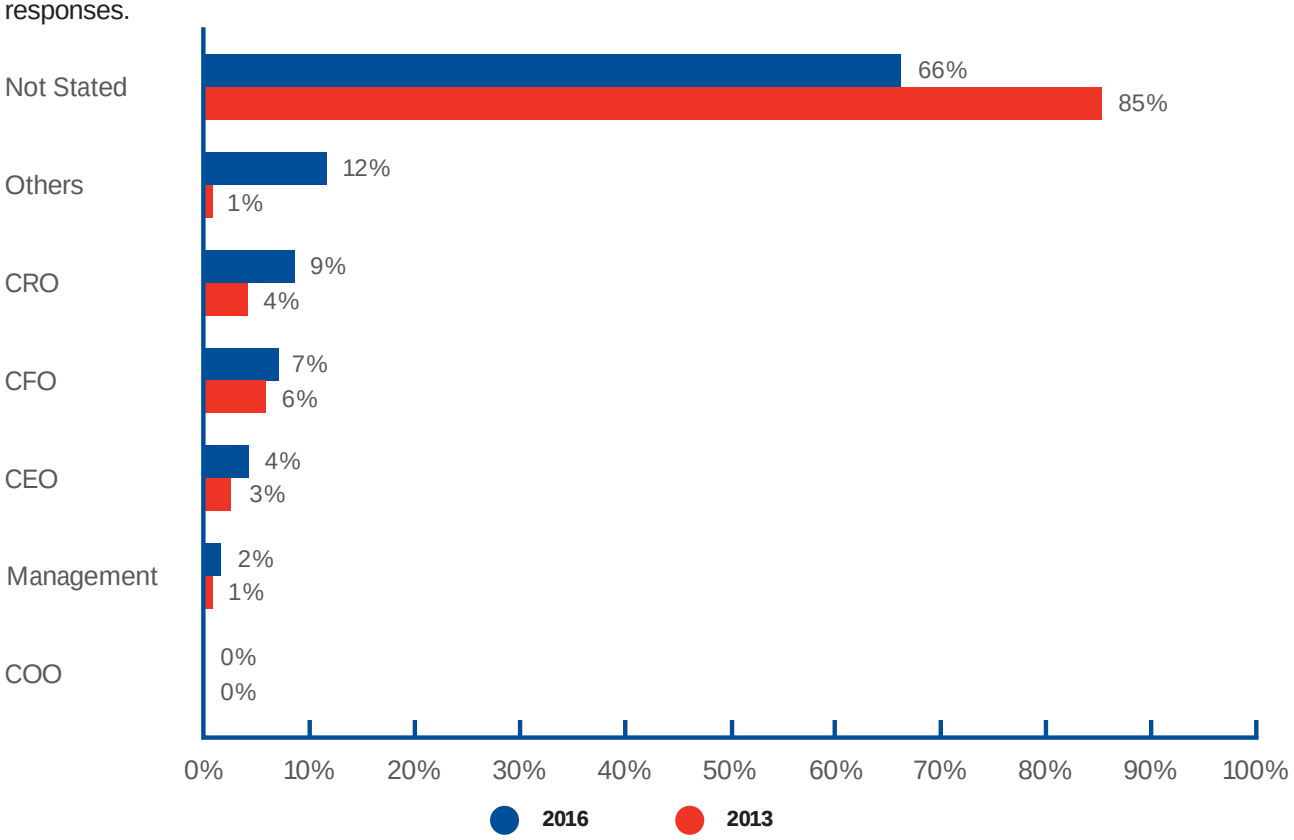


Chart 22: Percentage of companies specifying the senior manager responsible for risk management (multiple responses were allowed for this chart)

Where a C-Suite executive is responsible for risk management, it is interesting to see the change over time in the background of these executives. While in the 2013 Study, 63% had an audit/accounting background, in 2016 there was a more even spread across audit/ accounting, business/ operations and finance taking on the risk management oversight role (refer Chart 23). This reflects the need for broader experiences and skill sets beyond the traditional accounting skillset.

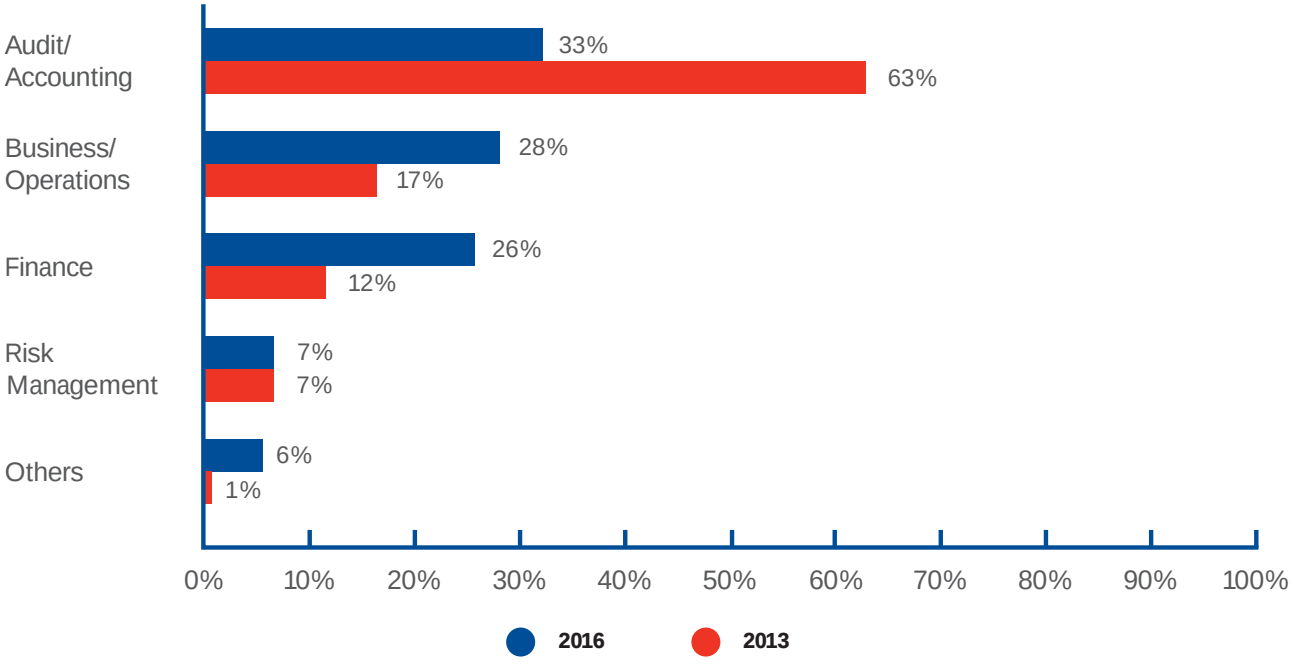


Chart 23: Percentage of backgrounds disclosed for C-Suite executives responsible for risk (multiple responses were allowed for this chart).

5.2.2 Management Risk Committee

While there was an 8% increase in the percentage of companies disclosing having a MRC, the disclosure of non-board MRCs remains uncommon (refer Chart 24). An MRC that consists of members from different business units or functions can evaluate risks from multiple vantage points within the company in order to see how risks and mitigating actions are connected or common. This ability to link the risks that a company faces is valuable to the board in terms of risk governance, and it may be even more important if the company does not have a dedicated C-suite executive, such as a CRO, in charge of risk management oversight.

> "An effective risk management function requires a mix and broad range of skill-sets. Beyond the risk management process and framework, which people can be trained on and can develop through on-the-job learning, it is becoming increasingly critical for risk managers to bring technical knowledge, business understanding and industry expertise to ensure they can challenge and bring value to the business."
>
> **Jeanne Cheng**
> Chief Risk Officer, Singapore Power

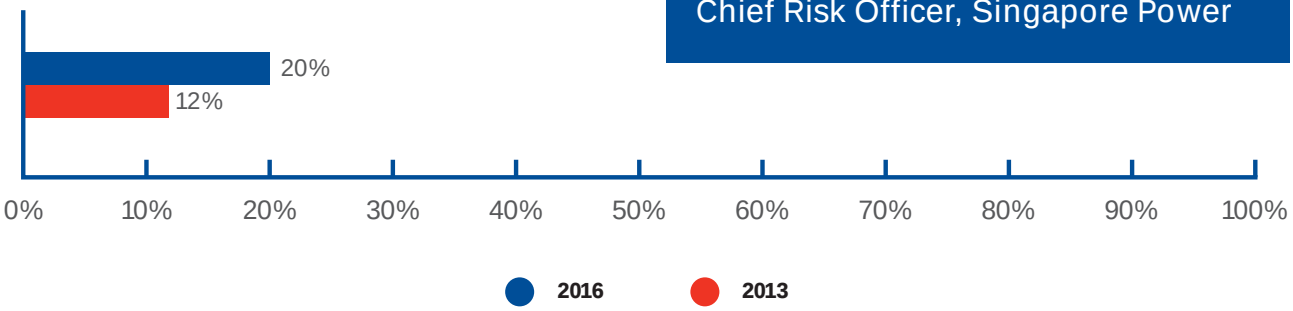


Chart 24: Percentage of companies with a Management Risk Committee

5.2.3 Correlation between companies with BRCs in place

Interestingly, where a company has a BRC in place, it is also more likely to have an MRC and a CRO. Chart 25 highlights that 53% of companies that had a BRC also had an MRC (compared to only 13% of companies without a BRC). 31% of companies that had a BRC also had a CRO (compared to only 5% of companies without a BRC). 31% of companies that had a BRC also had a dedicated risk function (compared to only 1% of companies without a BRC).

This is consistent with the finding of the 2013 Study and possibly reflects the greater risk complexity in these companies with BRCs. It also tends to indicate a higher level of risk management maturity, reflected in the increased sophistication of the framework. This could also reflect the fact that a BRC drives the demand for more risk reporting and analysis, causing management to respond by implementing a more formalised structure for assessment and reporting.

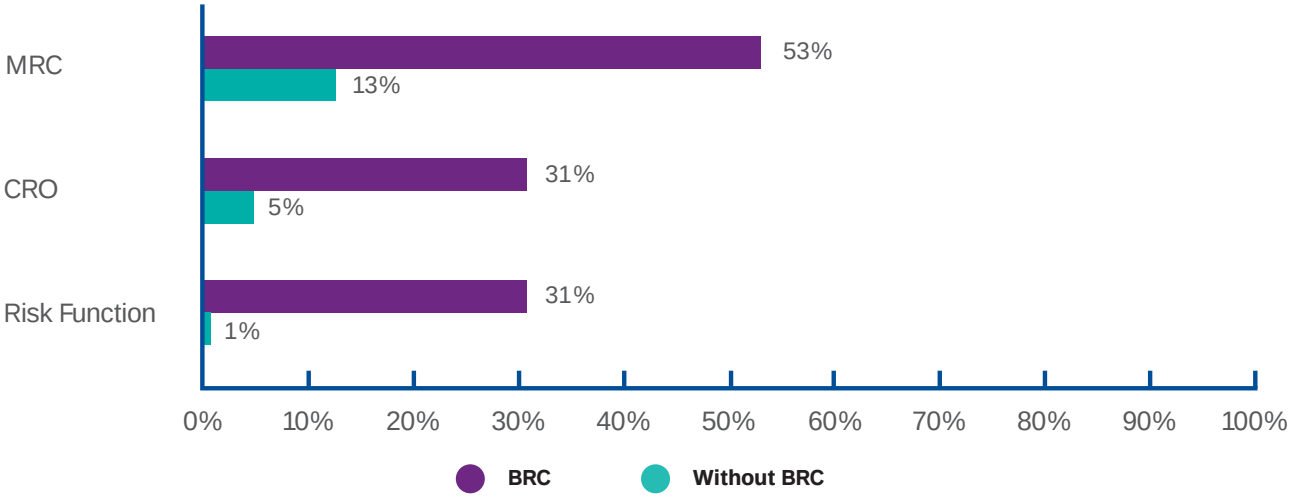


Chart 25: Percentage of companies with BRCs that have an MRC, CRO and Risk Function

5.2.4 Dedicated risk management function

The existence of a dedicated risk function is another key element of a robust risk management framework, and an indicator of the maturity of risk management in a company. While only 5% of sampled companies disclosed having a dedicated risk function in place (refer Chart 26), our experience suggests that the risk management function is still in an emerging state of maturity and often combined with other functions. Nearly one quarter of large caps had a dedicated risk function, reflecting the increased size and possible complexity of their business.

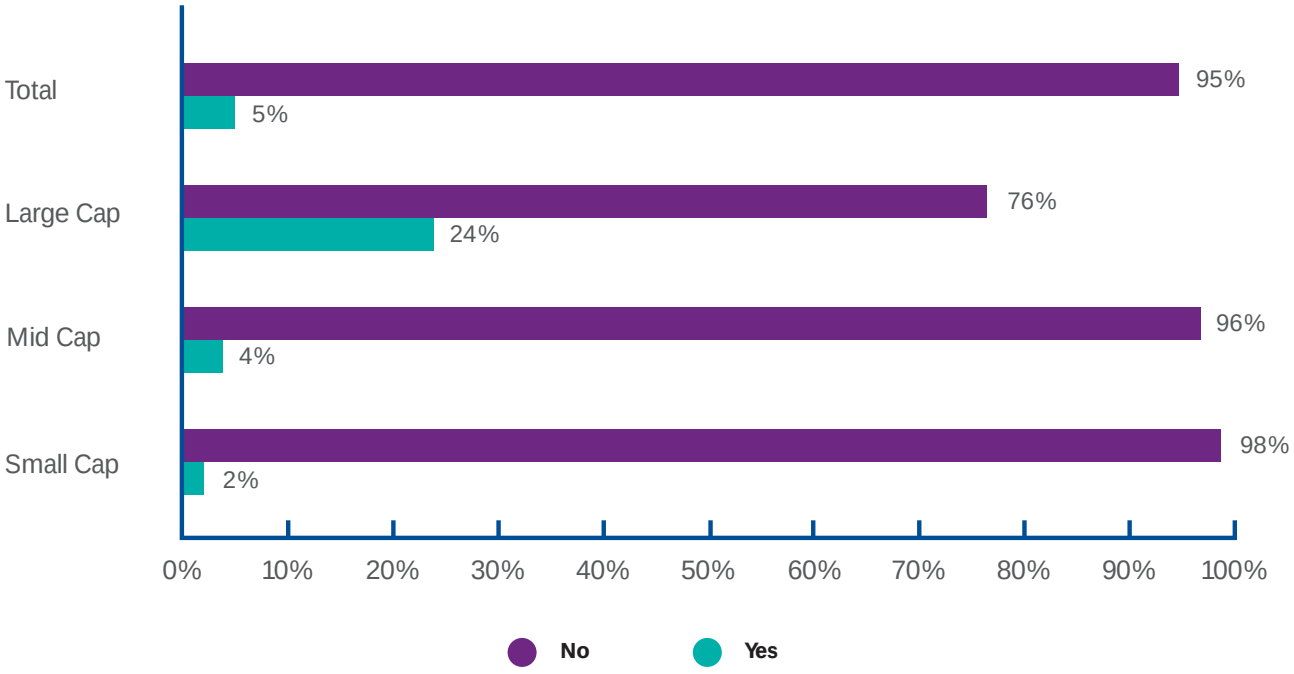


Chart 26: Percentage of companies with a dedicated risk function

In summary, there is an increasing trend in the introduction of CROs and MRCs. But there is still a lack of clarity about who is responsible for risk, with no requirement to disclose these and other details of the risk management structure. A CRO, MRC and a dedicated risk management function are all critical factors in a company's ability to assess and report on its management of risks, yet the level of transparency in disclosures regarding these areas is falling short.

This is particularly evident when contrasted with the level of disclosures found in relation to internal audit - a critical aspect of the independent assurance (3rd line of defence). This may represent an opportunity to review and refresh the existing guidelines relating to the risk management structure, function and resources found in the CG Code. Until then, greater awareness of the importance of establishing and disclosing these practices is required to give stakeholders sufficient transparency over the robustness of risk management frameworks at a company level.

> "I think, that most people think that internal audit and risk management are one and the same. That's the common misconception on the ground - that IA looks at risk management and internal controls and everything in between. So risk management and internal audit are always spoken of in the same breath. I think the CG Code could be clearer in actually defining what the different responsibilities are and how they should be separately resourced."
>
> **Adrian Chan**
> Independent Director

5.3 3rd Line of Defence: Internal audit

Principle 13 states "The company should establish an effective internal audit function that is adequately resourced and independent of the activities it audits."

It is encouraging to see that an IA function was established for all Large and Mid Cap companies, with only a small percentage of Small Cap companies not yet having an IA function in place (refer Chart 27).

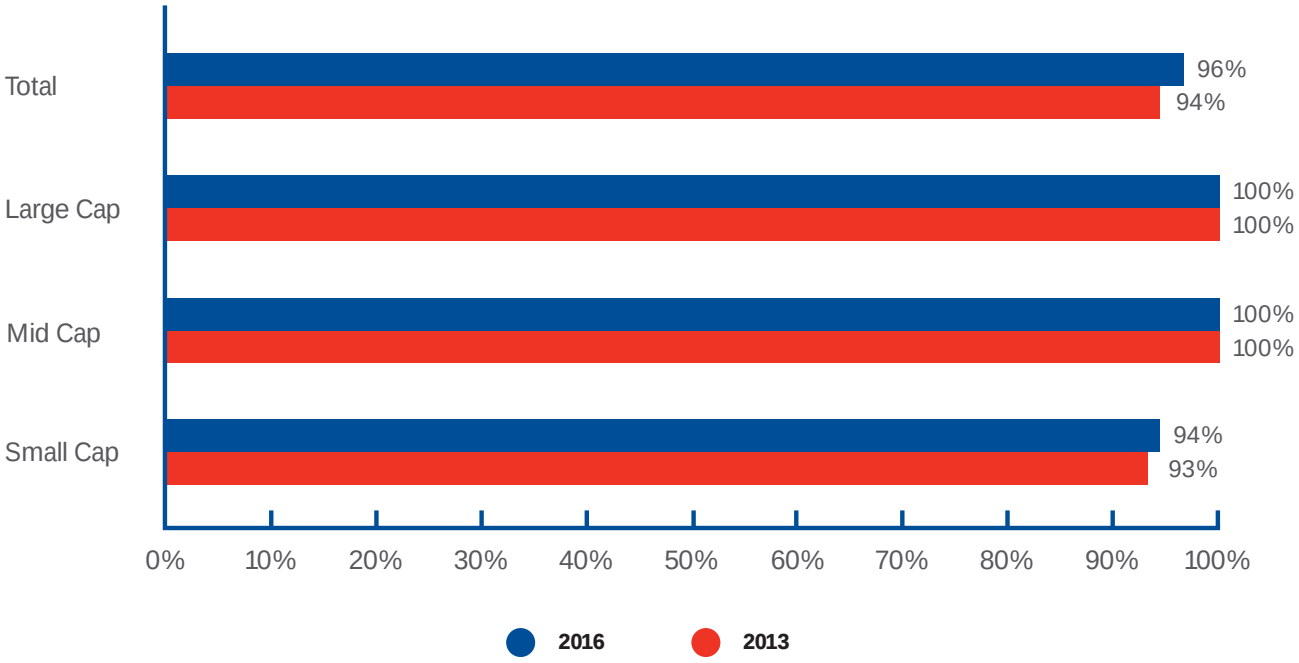


Chart 27: Percentage of companies with an IA function in place

When analysing the IA function model, our study found that a majority of companies outsource their IA function (63%), a result that increased since 2013 (refer Chart 28). Approximately 20% of companies had an in-house IA function, with very few disclosing adopting a co-sourced[14] IA model.

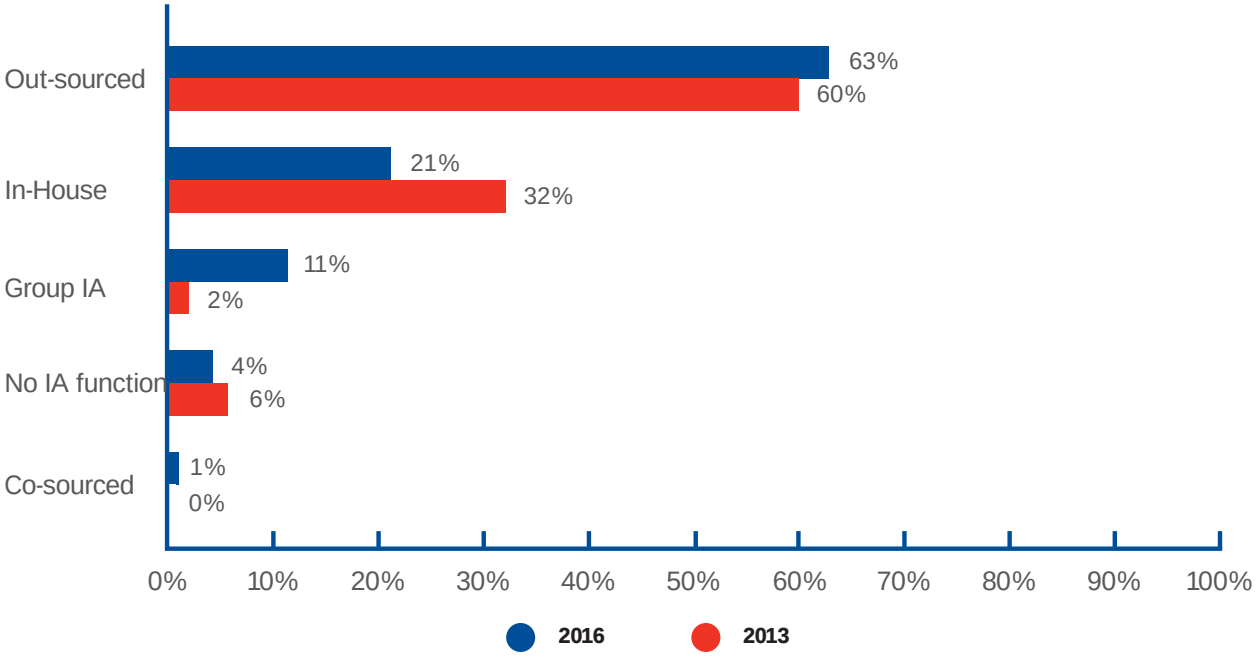


Chart 28: Percentage of companies disclosing the IA function model

[14] Disclosures relating to a co-sourced IA model were separately captured in the 2016 Study (not previously captured in the 2013 Study).

When analysing the IA model across market capitalisation, the results show that in-house IA functions are more prevalent amongst Large Cap companies, whereas Mid and Small Cap companies tend to adopt an outsourced IA model (refer Chart 29).

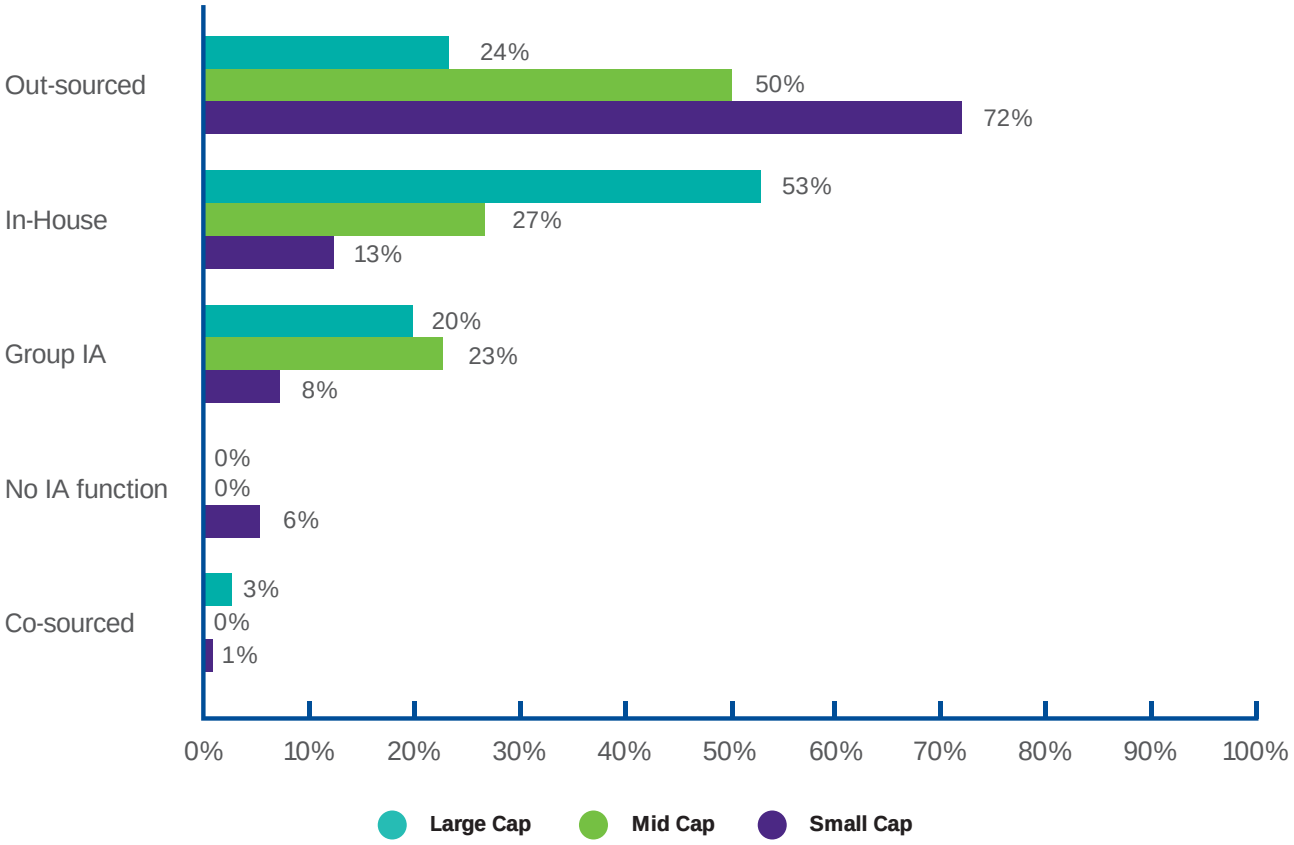
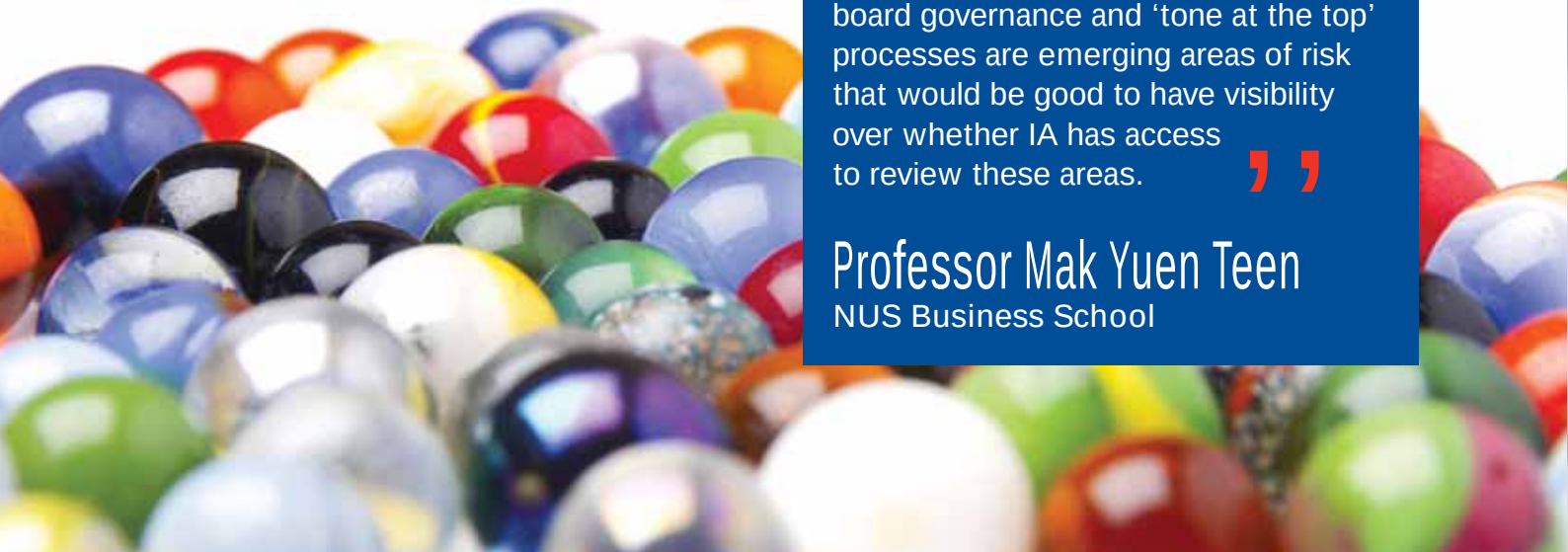


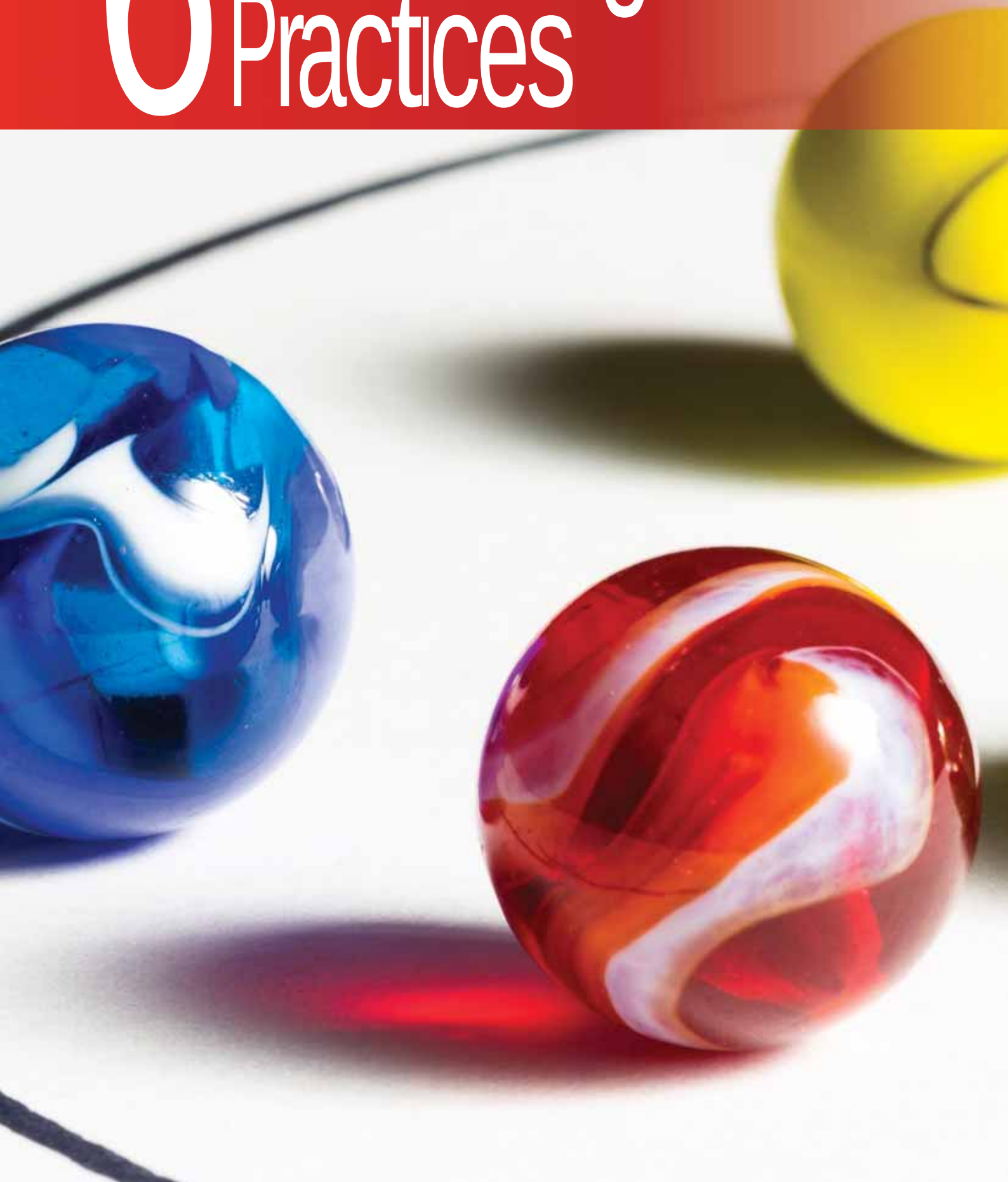
Chart 29: Percentage of companies disclosing the IA function model by market capitalisation

While the 2016 Study focused on whether an IA function exists and how it is structured, and did not specifically test the extent to which companies disclose details of the IA plan, it was generally observed that companies disclosed very little in terms of the scope and coverage of business processes, entities or divisions or frequency of reviews. This could be an area of future improvements for IA disclosures.

> "While a majority of companies have established an IA function, disclosures are currently limited as they do not indicate the scope of the IA plan. By disclosing such information, stakeholders can ascertain the coverage, frequency and the levels within the organisation that IA has access to. For example, the board governance and 'tone at the top' processes are emerging areas of risk that would be good to have visibility over whether IA has access to review these areas."
>
> **Professor Mak Yuen Teen**
> NUS Business School



6 Risk Management Practices



The complex business environment of today means that companies face a variety of risks at multiple levels that may determine their success or failure. Boards and management, especially those working in companies operating in diverse environments or industries, may struggle to fully understand the full spectrum and complexity of the risks their companies may face.

To manage risks effectively, the process of risk identification, assessment and reporting should be formalised in the form of a risk management framework. This should allow the board and management to take a more structured and disciplined approach towards managing risks, as well as enabling more informed decision-making.

6.1 What constitutes a Risk Management Framework?

There are many risk management frameworks for companies to select from to either adopt in full or adapt to their company's circumstances. KPMG's Global Enterprise Risk Management (ERM) Framework (refer Figure 4) captures the key elements companies should consider establishing and disclosing in relation to how they manage risks.

These mechanisms form the foundation of the risk management framework as they help to guide organisational behaviours around decision making. Decisions are the way that risks and opportunities present themselves to the business. As more and more companies have a devolved decision-making structure, key stakeholders (investors, board and management) rely on these mechanisms being in place and working effectively. Further guidance on all aspects of the risk management framework can be found in the SID Board Risk Committee Guidebook.

Figure 4: KPMG's Global ERM Framework

Our study shows that 64% of companies disclosed having a risk management framework, a significant increase from 45% in 2013 (refer Chart 30). This means that more companies are specifying that they have formally adopted a risk management framework, such as International Organization for Standardization (ISO) 31000 or Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) or more commonly, they have established a tailored risk management framework for their company's circumstances.

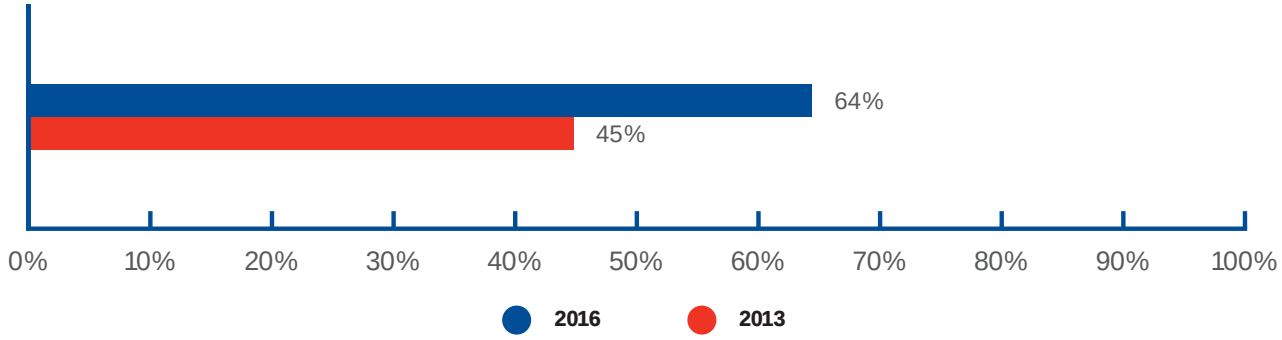


Chart 30: Percentage of companies disclosing a risk management framework

6.1.1 Risk strategy and appetite

Guideline 11.1 states "The board should determine the company's level of risk tolerance."

Risk appetite and risk tolerance are key elements of a robust risk management framework. Risk appetite refers to the amount and type of risk that a company is willing to pursue or retain in the pursuit of its long-term strategic objectives. Risk tolerance then indicates the boundaries of risk-taking outside of which the company is not prepared to venture in the pursuit of its long-term business objectives. For the purposes of this study, the term risk tolerance will be used.

However, only 41% of the sampled companies disclose their approach to risk tolerance (refer Chart 31). The study found that more Large Caps, compared to Mid and Small Cap companies disclose their risk tolerance approach. This reflects the increased levels of risk management maturity in Large Caps necessitated by the size, scale and complexity of their operations. They also face increased expectations from key stakeholders, such as institutional investors, regarding their risk management disclosures.

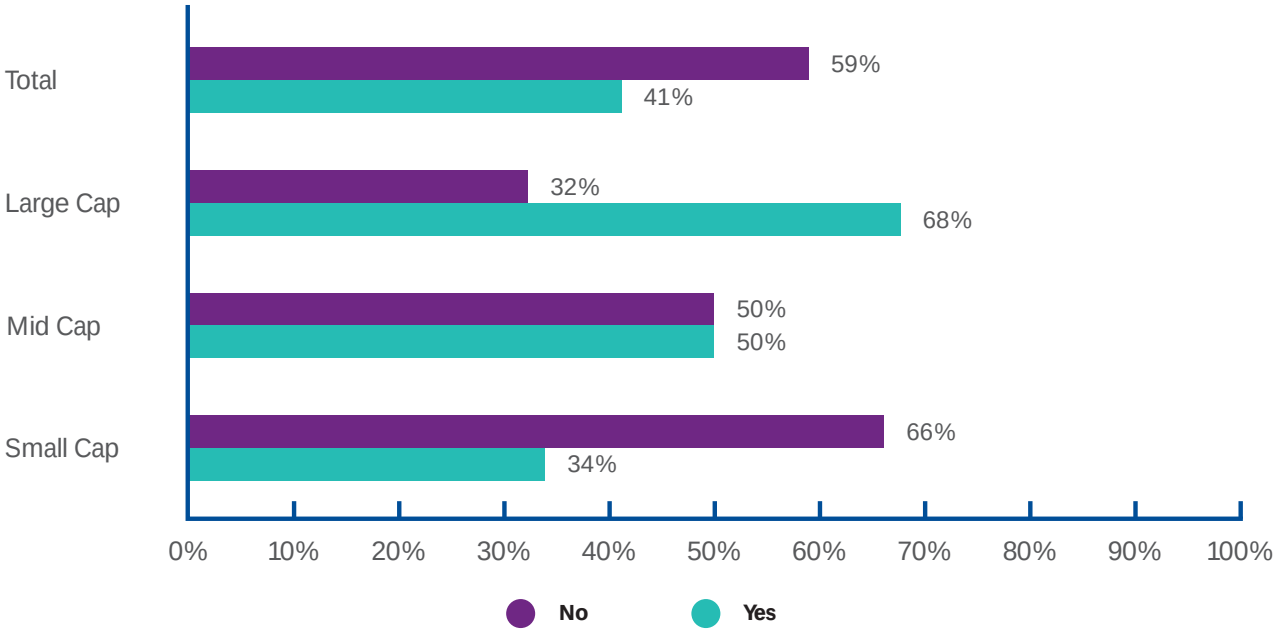


Chart 31: Percentage of companies disclosing risk tolerance

6.1.2 Risk management policies

Guideline 11.1 states "The board should determine the company's risk policies."

A much greater proportion (68%) of companies disclose having a risk policy in place, with nearly all Large Cap companies doing so (refer Chart 32). It is encouraging to see that a high proportion of Mid and Small Cap companies have also mentioned having a risk policy. Through continued awareness of the importance of such a policy to set out the expectations, roles and responsibilities of risk management, disclosures should continue to increase in this area.

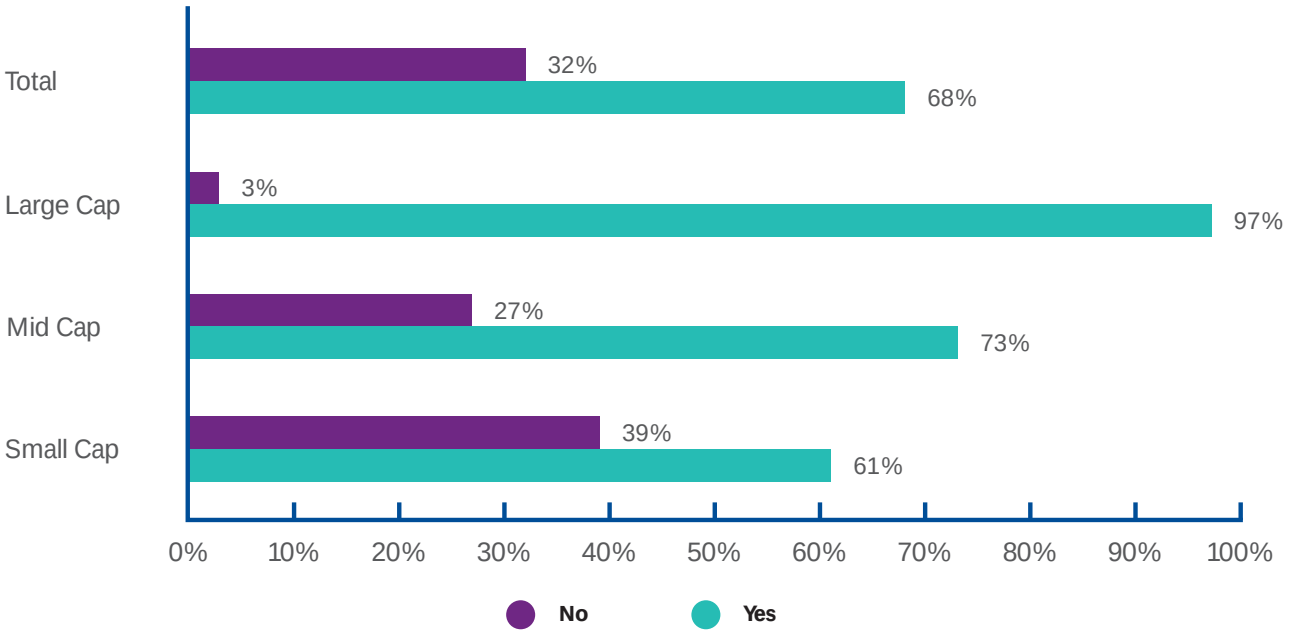


Chart 32: Percentage of companies disclosing risk policies

6.1.3 Risk assessment and monitoring

Guideline 11.1 states "The board should oversee management in the design, implementation and monitoring of risk management and internal control systems."

The study assessed the extent to which companies disclosed the way that risks were identified, assessed, reported, managed and monitored. The results indicate that a majority of companies (63%) have disclosed some information about the company's risk assessment and monitoring processes, with Large and Mid Cap companies leading the way (refer Chart 33).

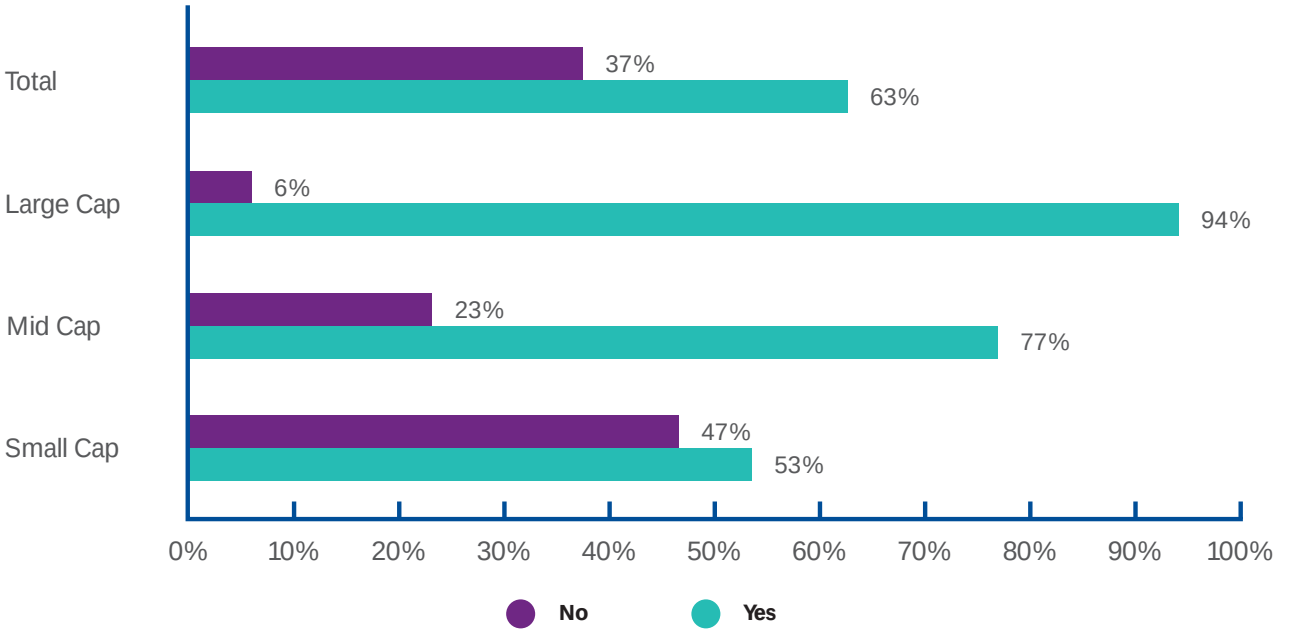


Chart 33: Percentage of companies disclosing risk assessment and monitoring processes

6.1.4 Risk insights

Our study reviewed the key risk categories that were being disclosed. Key risk categories are defined as the grouping of similar risk types to enhance the review and reporting process[15]. The SGX LR 1207 (10) specifies three broad risk categories – financial, operational and compliance. The CG Code, meanwhile, specifies four broad risk categories – financial, operational, compliance and information technology.

Not surprisingly all companies disclosed their financial and operational risks and almost all companies disclosed compliance and information technology risks (which align to the key risk categories specified in the SGX LR 1207 (10) and CG Code Principle 11).

There were two additional risk categories added for the purposes of this analysis – strategic risk and cyber risk. While cyber risk could be considered as part of the IT risk category, for the purposes of this study, it was analysed as a separate risk category given the significant concern and focus of many companies in this area.

However, the percentage of companies disclosing in relation to strategic and cyber and risk categories were significantly lower (refer Chart 34). Some companies described 'other' risk categories relevant to their business such as Political, Economics, Environment and Social, which were grouped together for this analysis. In the current environment, strategic and cyber risks arguably can present the greatest risk to companies, and can cause the greatest damage to the company in the shortest time. In recent years, the number of companies which are victims of cyber-attacks has been on the rise. Their systems were compromised by malware and were held at ransom by hackers to pay a fee to have them recovered[16]. Companies could be more forthcoming in relation to these risk categories and types.

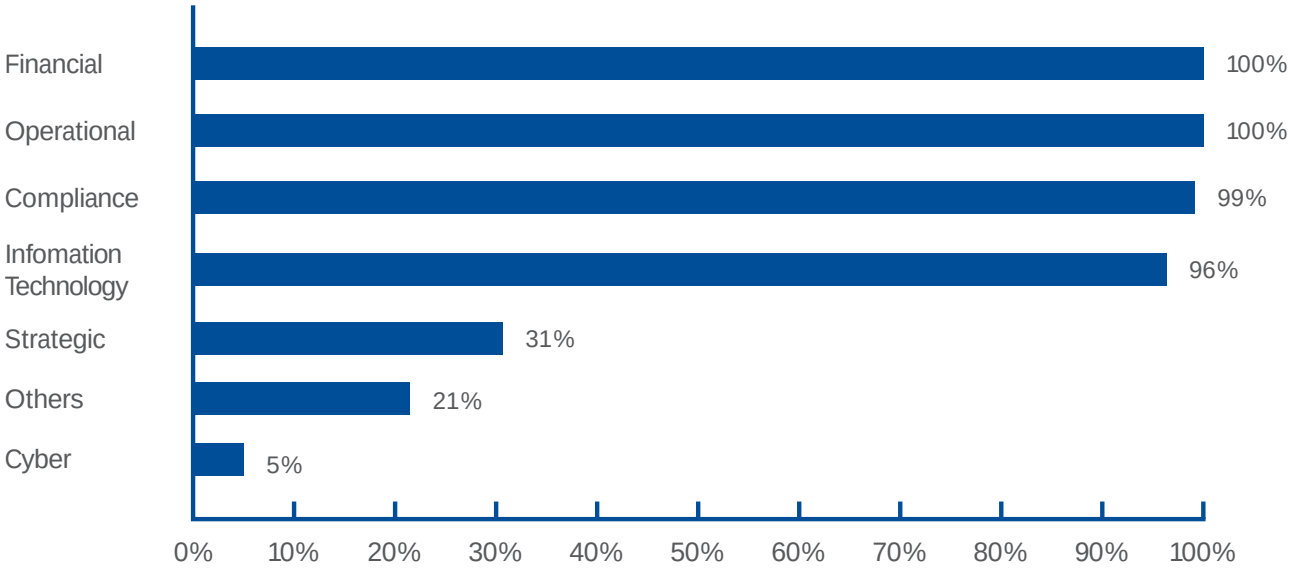


Chart 34: Percentage of companies disclosing key risk categories

[15] SID BRC Guidebook Appendix 4C Glossary of key risk terms
[16] The Business Times: Singapore sees spike in number of cyberattack-for-ransom cases.

The study also examined the extent to which companies disclosed specific risk types. A risk type is defined as a specific risk example with a succinct description or title[17]. It provides more insight than merely stating a broad risk category. For example, health and safety, product reliability, customer experience, geopolitical risks etc. A majority of companies (61%) did not disclose the key risk types at all with 39% providing some mention (i.e. a short description) of the risk types (refer Chart 35) which indicates disclosures could be more forthcoming in this area.

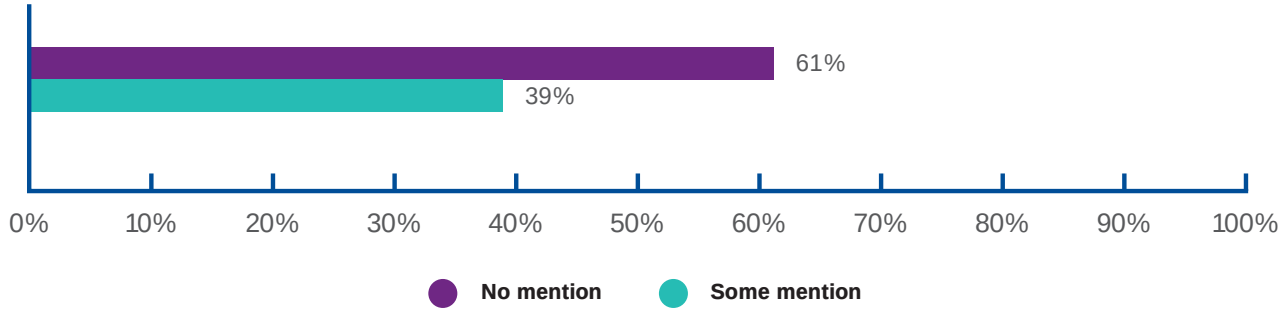


Chart 35: Percentage of companies specifying the key risk types

6.2 Risk Culture

Risk culture is an emerging area in risk management, but has moved rapidly up the agenda in recent years as organisational culture has been blamed for multiple instances of misconduct in different industries. Culture is fundamental to an organisation's management of risk as it directly affects the manner in which individuals at the organisation approach business decisions. A strong risk culture supports effective risk management; a weak risk culture is a risk in itself.

An organisation's risk culture is made up of its employees shared belief systems, norms, and values in relation to risks. To optimise their performance, organisations should strive for a culture in which relevant risks are identified, assessed, and acted upon in an efficient and professional manner.

6.2.1 Risk culture disclosure

Our study showed that 19% of all companies mentioned risk culture and the board's role in establishing a strong risk culture (refer Chart 36). A significant proportion (59%) of Large Caps mention risk culture, which is reflective of the importance they place on this as part of the overall risk management framework. Overall, this is an encouraging result, given the emergent nature of this focus of risk management in the region, although more awareness amongst all companies is required to enhance disclosures in this area.

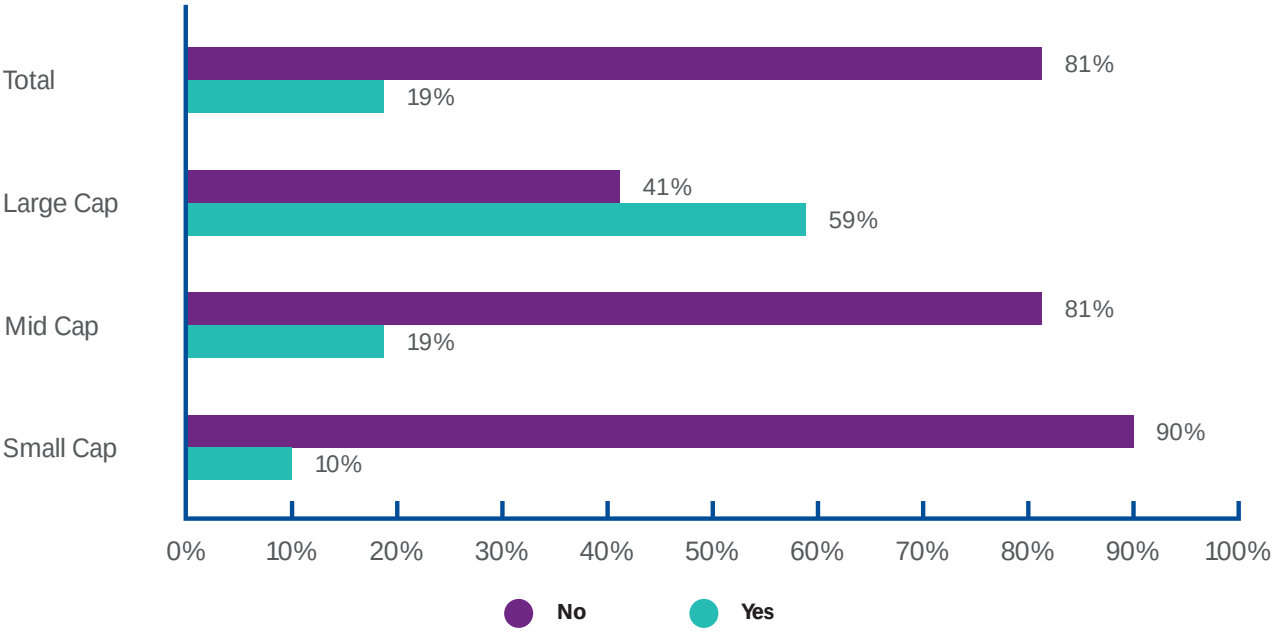


Chart 36: Percentage of companies disclosing information about the risk culture by market capitalisation

[17] SID BRC Guidebook Appendix 4C Glossary of key risk terms

In addition, when we review the disclosure by industry we can see that the Finance sector is clearly stronger in this regard than the other sectors (refer Chart 37). This is not surprising given the FS CG Code, which states that the responsibilities of the Board include, "setting the tone from the top, and inculcating an appropriate risk culture throughout the firm (11.6 (a))".

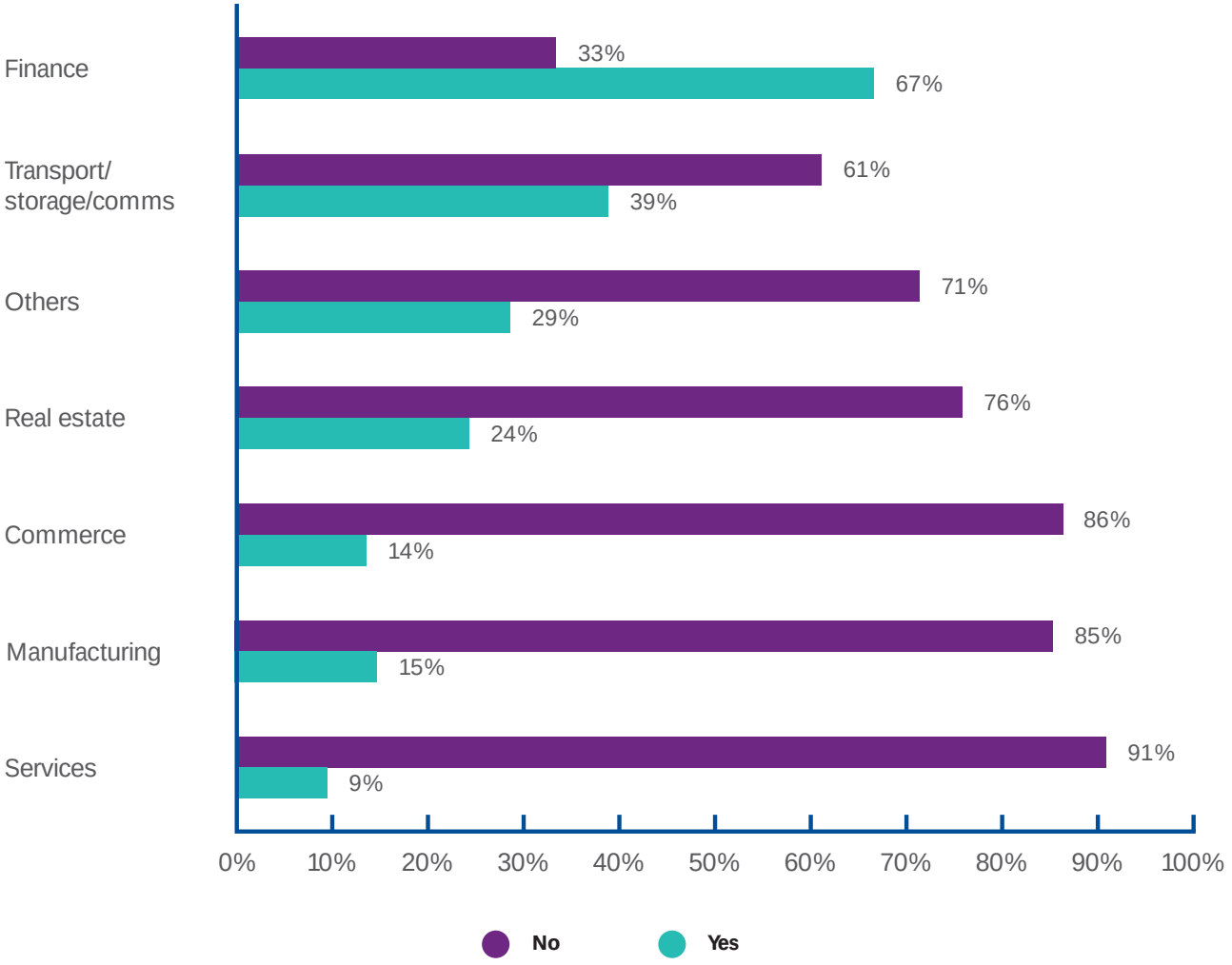


Chart 37: Percentage of companies disclosing information about the risk culture by sector

6.2.2 Risk culture assessment and measurement

However, when we look at whether companies have disclosed that they assess and measure risk culture, the results are not as compelling. Whilst 19% of companies disclosed having a risk culture, only 4% of the population disclosed that they have a framework and process for assessing and measuring risk culture (refer Chart 38). Scientific studies[18] have shown that organisations that intentionally manage their culture outperform similar organisations that do not.

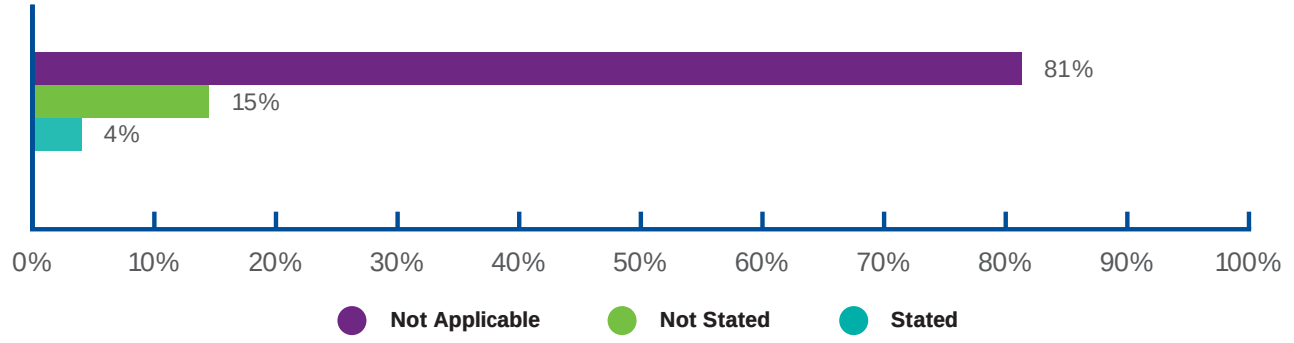


Chart 38: Percentage of companies disclosing information about the assessment and measurement of risk culture

[18] Studies by Kaptein, M. University of Rotterdam (1998-2011)

6.2.3 Aligning remuneration and risk policies

Guideline 8.1 states "A significant and appropriate proportion of ….remuneration…should be structured so as to link rewards to corporate and individual performance….It should take into account the risk policies of the company, be symmetric with risk outcomes and be sensitive to the time horizon of risks."

One of the key drivers of a strong risk culture is a remuneration structure that rewards employees for responsible behaviour and disciplines them for irresponsible performance.

Our study found that only 19% of companies specified that there is an alignment between their remuneration and risk policies despite this being a requirement in the CG Code (refer Chart 39). Slightly more Large and Mid Cap companies specified the link compared to Small Cap. However, more can be done to enhance disclosures in this area as this is a key aspect of ensuring an appropriate risk culture, with the right cultural drivers, is in place.

> "Risk culture is not something new. It is the 'tone at the top', values and ethics and essentially means doing the right thing. Risk culture red flags start at the top. Is there a dominant Chairman and/or CEO? Is there a balanced approach to growth and risk taking? How many resources are invested in risk and audit? How does the CEO react to risk and audit issues arising?
>
> We have started the process to take stock of risk culture by looking at how people in the organisation react to scenarios mostly through training sessions and workshops. We are continuing to evolve in this area."
>
> **Danny Teoh**
> Independent Director

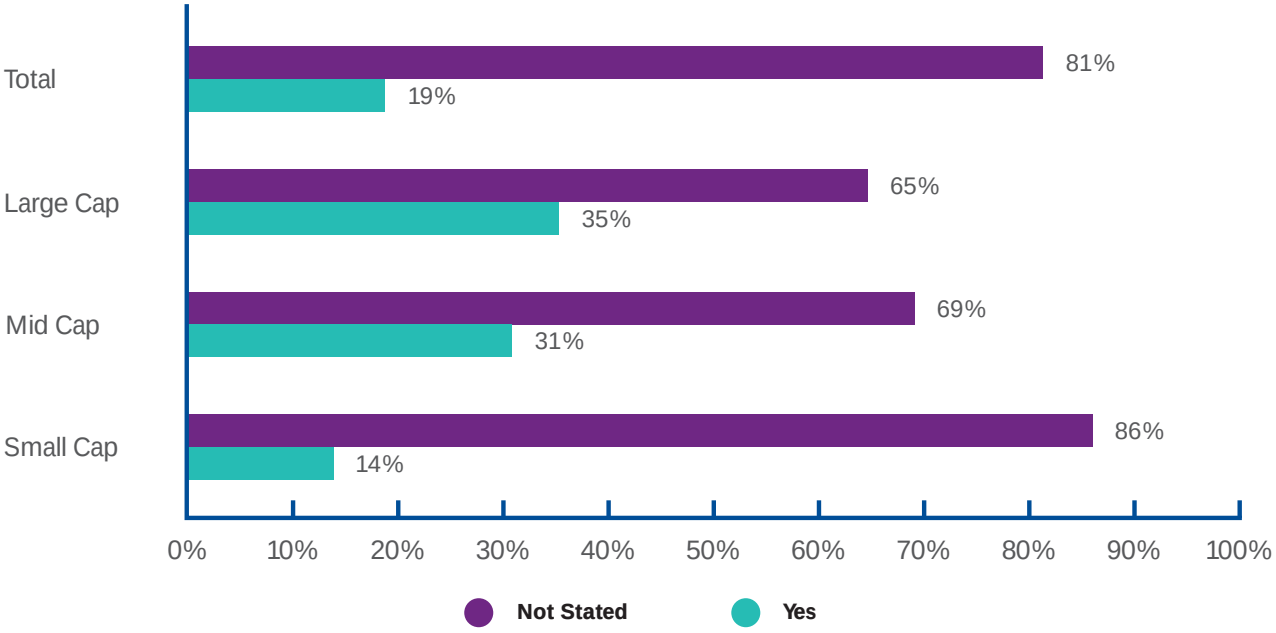


Chart 39: Percentage of companies that disclose a link between remuneration and risk policies by market capitalisation

Another aspect of this is shown in Chart 40. While it is encouraging to see that 26% of companies have included risk management as part of the Board performance management process, only 2% of companies have referred to it as being part of the management level. A significant proportion of companies (72%) do not state whether risk management practices are considered as part of the performance management process. This is another area for improvement to enhance transparency of the link between remuneration, performance, risk and culture.

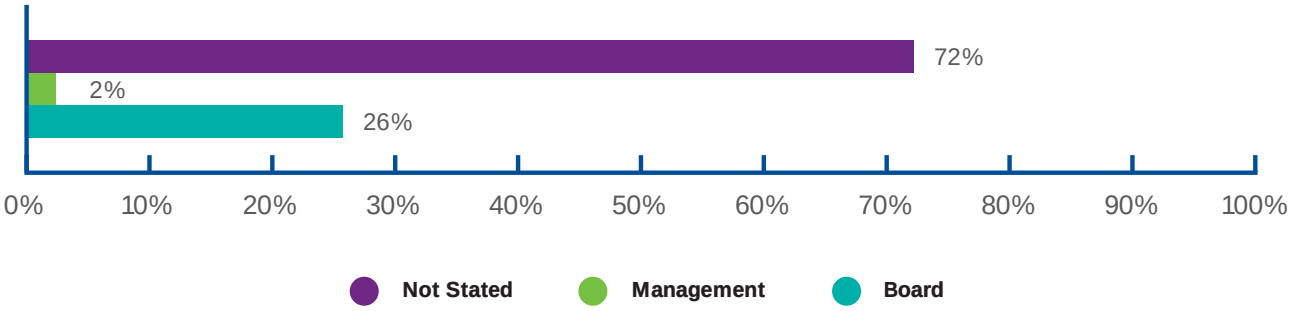


Chart 40: Percentage of companies disclosing whether risk management practices are incorporated into Board and Management performance management processes

6.3 Fraud Risk Management

Guideline 12.7 states "The AC should review the policy and arrangements by which staff of the company and any other persons may, in confidence, raise concerns about possible improprieties in matters of financial reporting or other matters…The existence of a whistle-blowing policy should be disclosed..."

Fraud risk management provides a framework which helps to prevent, detect and respond to fraud through taking corrective action. It can include mandatory conflict of interest declarations, implementation of whistle-blower policies, and Codes of Conduct and Ethics to establish a clear tone at the top with regard to employees' business and ethical conduct. Although there is currently no mandatory requirement for Singapore companies to have whistle-blowing policies in place, the CG Code recommends companies do so. However, there is no other mention within the CG Code regarding anti-fraud policies or procedures.

KPMG's Global profiles of the fraudster study[19] found that notification by employees via whistle-blowing channels is one of the most common methods for the detection of fraud (20%). When tip-offs from customers and employees via other channels is included, the proportion rises to 44%. Thus, having a rigorous process to capture and respond to such notifications is critical.

6.3.1 Whistle-blowing policies and protocols

Our study showed that a majority of companies (95%) disclosed having a whistle-blowing policy in place which has slightly improved since 2013 (refer Chart 41).

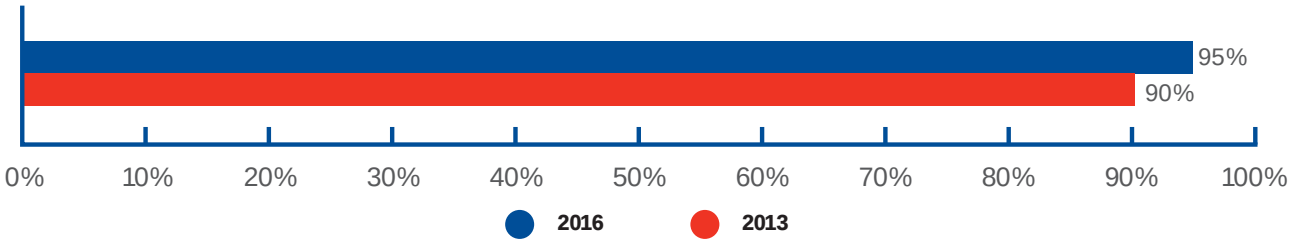


Chart 41: Percentage of companies disclosing whistle-blowing policies

[19] Global profiles of the fraudster: technology enables and weak controls fuel the fraud, May 2016 https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/profiles-of-the-fraudster.pdf

For a whistle-blowing programme to be effective, it is critical to instil staff confidence and trust in the programme and in the organisation's response to an incident. The recipient should also ensure the confidentiality of the whistle-blower's identity at all times. Some tools that can minimise fear of retaliation or identification of the whistle-blower include anonymous hotlines and web-based feedback portals. Where the whistle-blower can be identified, steps should be taken to ensure that the whistle-blower is not subjected to reprisals.

Chart 42 highlights that of the companies that disclosed having a whistle-blowing channel, most companies encourage whistle-blowers to report to the Audit Committee (74%), followed by IA (14%) and management (14%). Both the AC and IA are considered to be independent and free from bias, and it is encouraging to note that the percentage of non-independent channels such as management or HR has reduced since the prior study.

The consideration of an appropriate whistle-blowing channel is crucial as employees may not consider HR or management to be independent, given they generally report to the C-suite. It is important that whistle-blowers do not have reason to fear exposure or reprisal which could come from their identity being exposed.

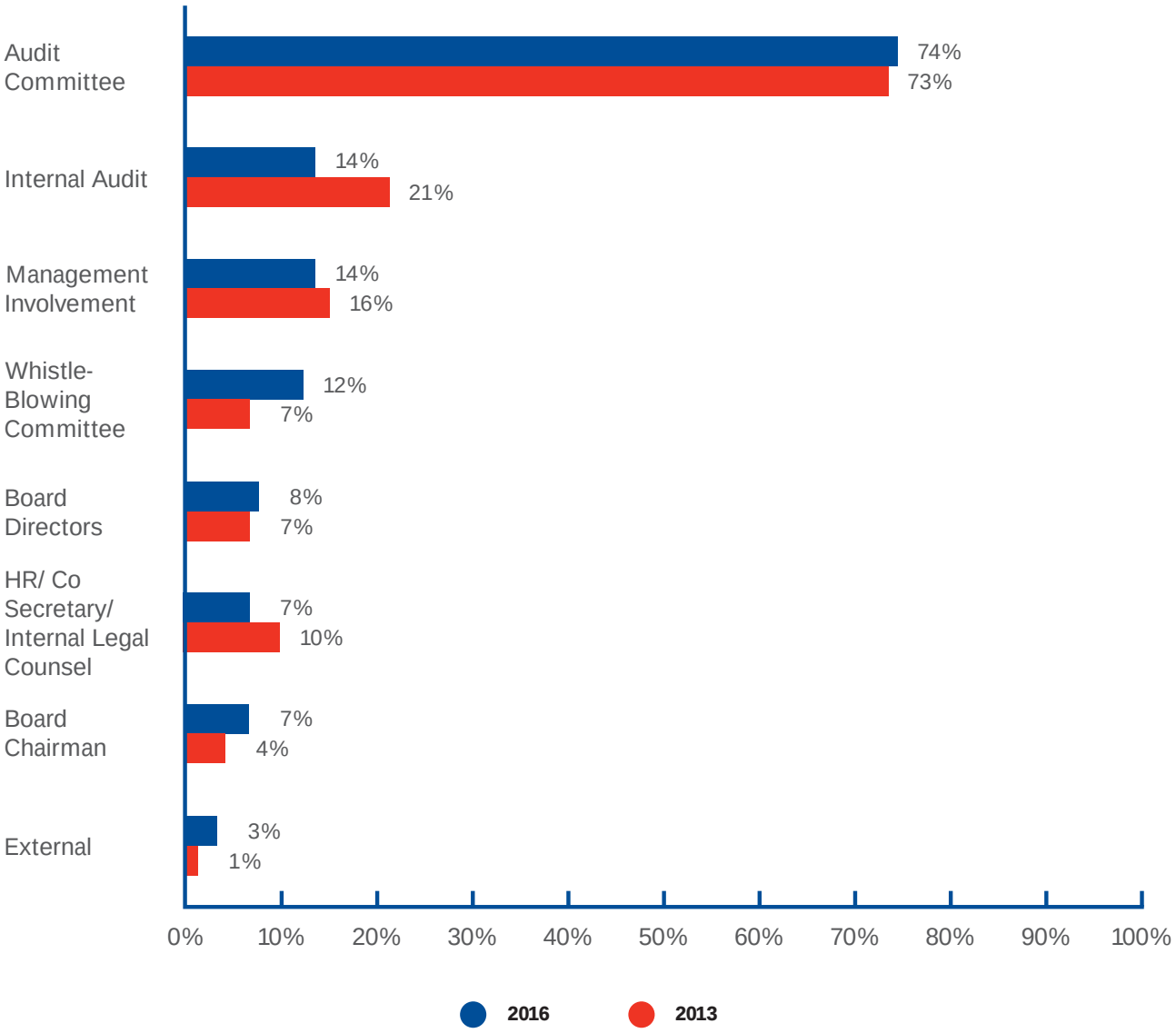


Chart 42: Percentage of companies disclosing the whistle-blowing reporting channel (multiple responses were allowed for this chart)

A majority of companies do not disclose details of how many whistle-blowing incidents were reported during the year (refer Chart 43). However, the percentage of companies stating that no whistle-blowing incidents were reported has increased. KPMG's Fraud Survey found that whistle-blowing channels were used by employees to report fraud in 20% (15% in 2011) of cases. However, they could not determine whether the occurrences are increasing or companies are simply getting better at detecting fraud.

Where companies disclose that no whistle-blowing incidents were reported during the year, it may be an indicator that the whistle-blowing policy and processes are not effective. In these circumstances, companies could consider whether disclosing more information about steps taken to embed a fraud risk culture and whistle-blowing process would be beneficial to stakeholders reading and using the annual reports.

Overall, one of the most important factors in fraud prevention is having well-trained and security-conscious staff members as the crucial first line of defence. The quality of training is therefore important in raising employees' awareness of fraud risks and anti-fraud policies, and the training needs to be tailored to make it relevant to different employee levels and functions.

Also critical is establishing reporting channels where actual or suspected fraud can be reported in confidence without fear of reprisal, and training employees and external parties on how to make use of these channels.

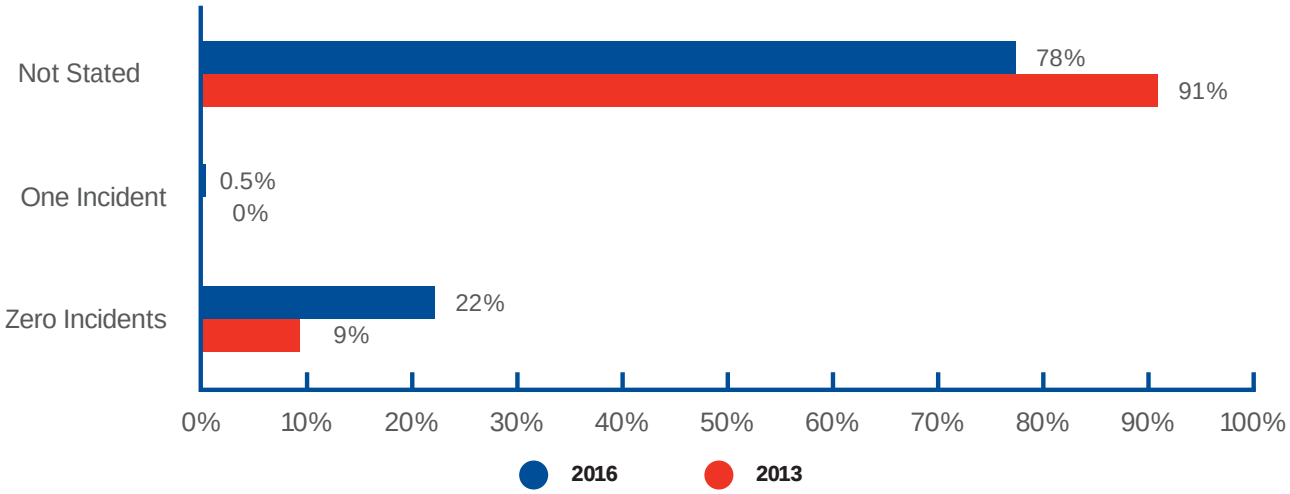


Chart 43: Percentage of companies that disclose the number of incidents reported during the year

6.3.2 Broader aspects of fraud risk management

Our study examined the extent to which disclosures were forthcoming in relation to fraud risk management. For instance, whether a fraud risk management framework was in place, whether there was specific mention of creating a fraud awareness culture, and whether there was broader anti-fraud policy (which included reference to a whistle-blowing policy and approach).

The results of the study indicated that very few companies have mentioned anything in relation to the broader fraud risk management framework, broader fraud policies or anti-fraud culture (refer Chart 44). Given the importance of fraud awareness driven by Anti-Money Laundering and Anti-Bribery and Corruption regulations and many recent corporate scandals, companies should consider disclosing more broadly in relation to this vital aspect of risk management framework.

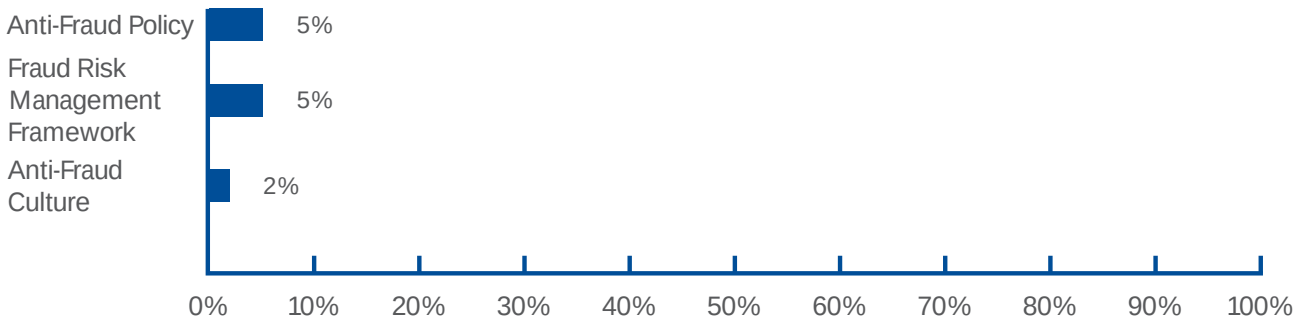
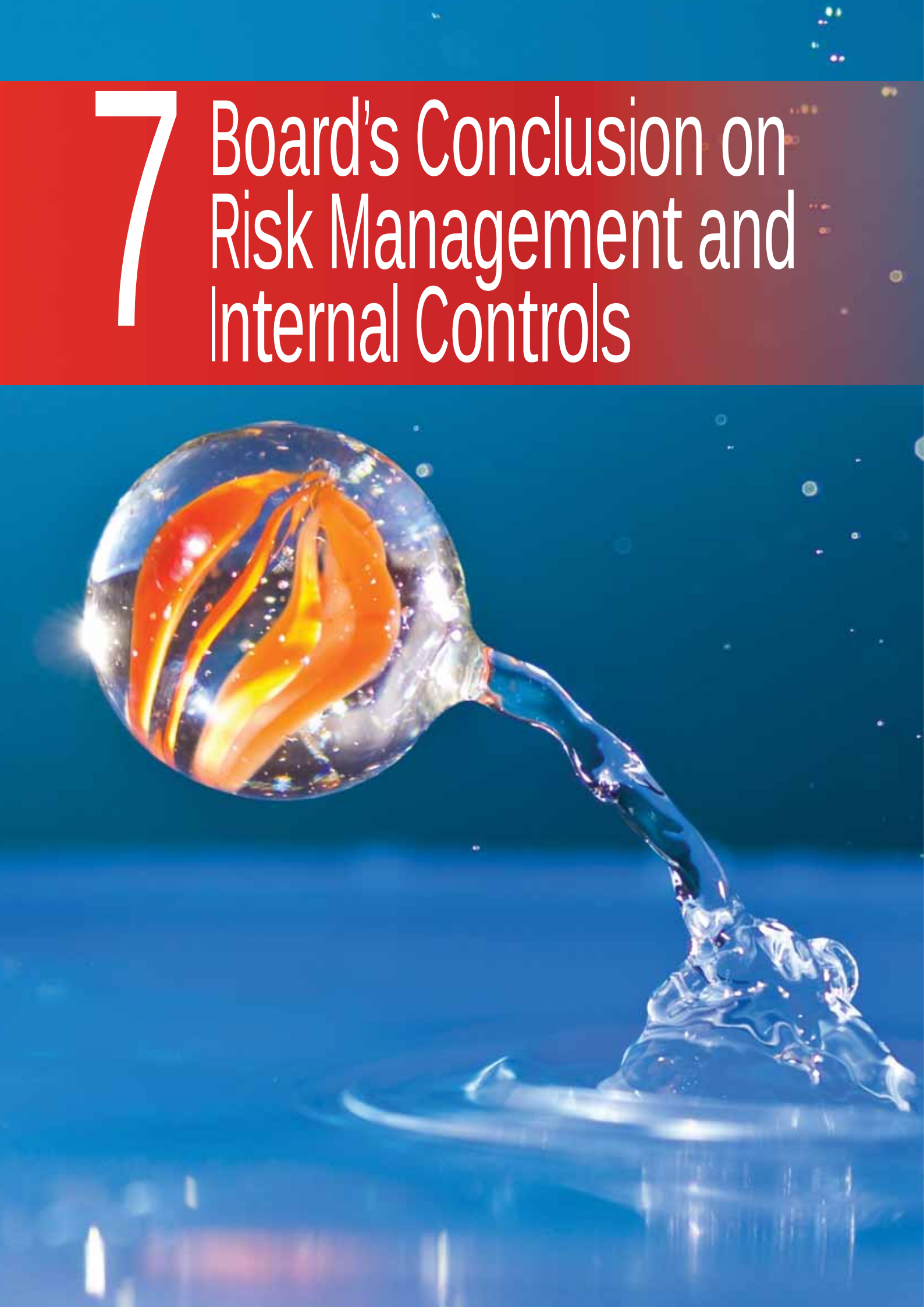


Chart 44: Percentage of companies disclosing fraud risk management measures

7 Board's Conclusion on Risk Management and Internal Controls



The board is required to conclude on the adequacy and effectiveness of risk management and internal controls. In order to do so, it must gather enough evidence through the risk governance structures and risk management practices (as described in the previous sections of the report). Another mechanism specified in the CG Code is to obtain assurances from the CEO and CFO.

7.1 CEO and CFO assurances (Guideline 11.3)

Guideline 11.3(b) states "The Board should also comment…on whether it has received assurance from the CEO and the CFO…regarding the effectiveness of risk management and internal control systems."

The study found a significant improvement in the disclosure of the CEO and CFO assurances over the effectiveness of risk management and internal control, with 89% of companies satisfying this requirement (refer Chart 45). This is a significant improvement on 2013, where only 15% of the companies disclosed that this internal assurance was being provided. This is due to the timing of the previous study, as this was a new requirement of the revised CG Code and as a result, many companies had not yet established practices for this.

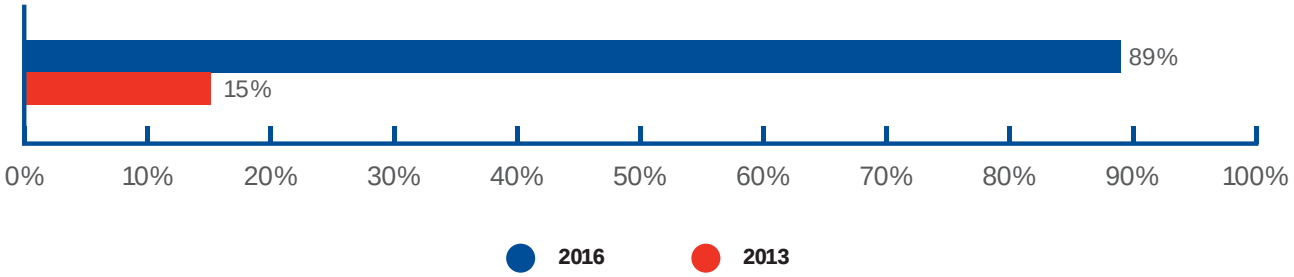


Chart 45: Percentage of companies disclosing whether the CEO and CFO provided assurance

While the CG Code only specifies providing assurance on the effectiveness of risk management and internal controls, it is also encouraging to see companies adopting leading practice and providing an assurance over the adequacy of risk management and internal controls as well as the effectiveness (refer Chart 46).

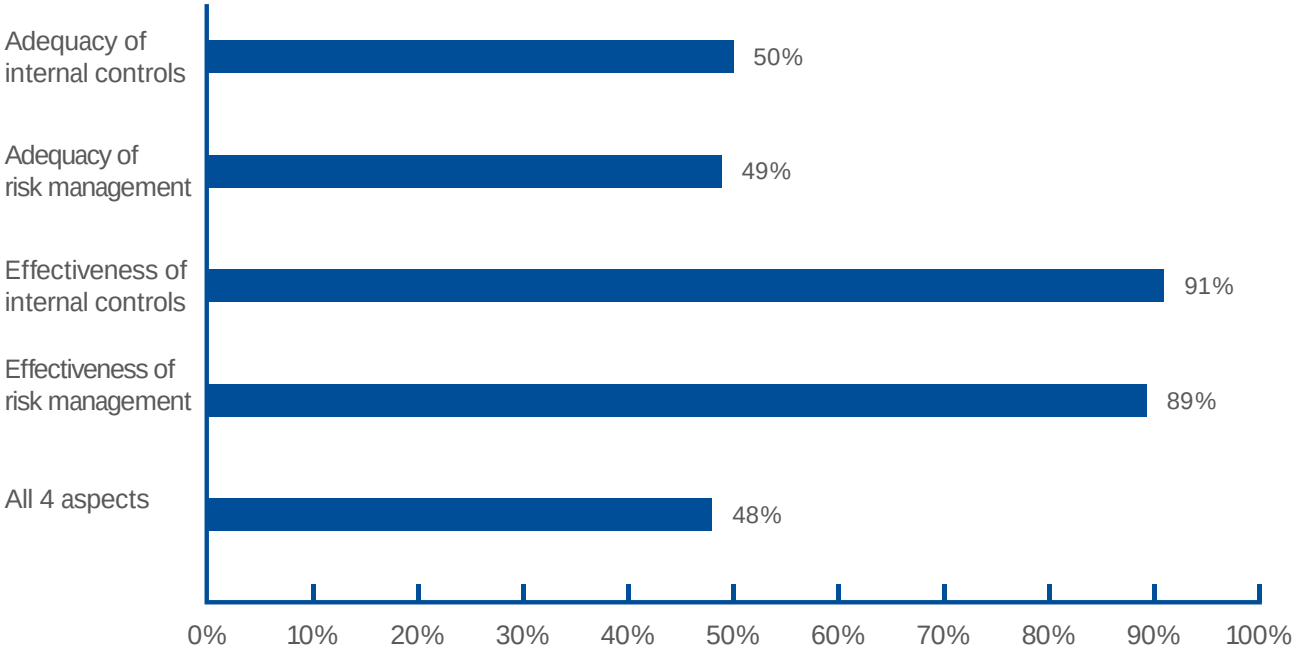


Chart 46: Percentage of companies disclosing the scope of the CEO and CFO assurances

7.2 Board's opinion (SGX LR 1207 (10))

SGX LR 1207 (10) states "Opinion of the board, with the concurrence of the AC, on the adequacy of the internal controls, addressing financial, operational and compliance risks".

SGX LR PN 12.2 states "Where the board and the AC are satisfied that the issuer has a robust and effective system of internal controls, the disclosure must include the basis for such an opinion."

Companies are required to comply with the mandatory SGX LR 1207(10). Our study found that while 97% of companies provided a statement in relation to the Board's conclusion on the adequacy of internal controls, only 84% of companies sampled specifically stated the term 'opinion'. Instead they used other language such as 'is of the view', 'is satisfied' or 'believes'. To comply with the SGX LR 1207 (10) it is recommended that companies adopt the wording as specified in the SGX LR.

On a positive note, quite a large proportion of companies provided a 'combined' opinion which captures the requirements of the CG Code regarding the adequacy of risk management and effectiveness of risk management and internal controls (refer Chart 47).

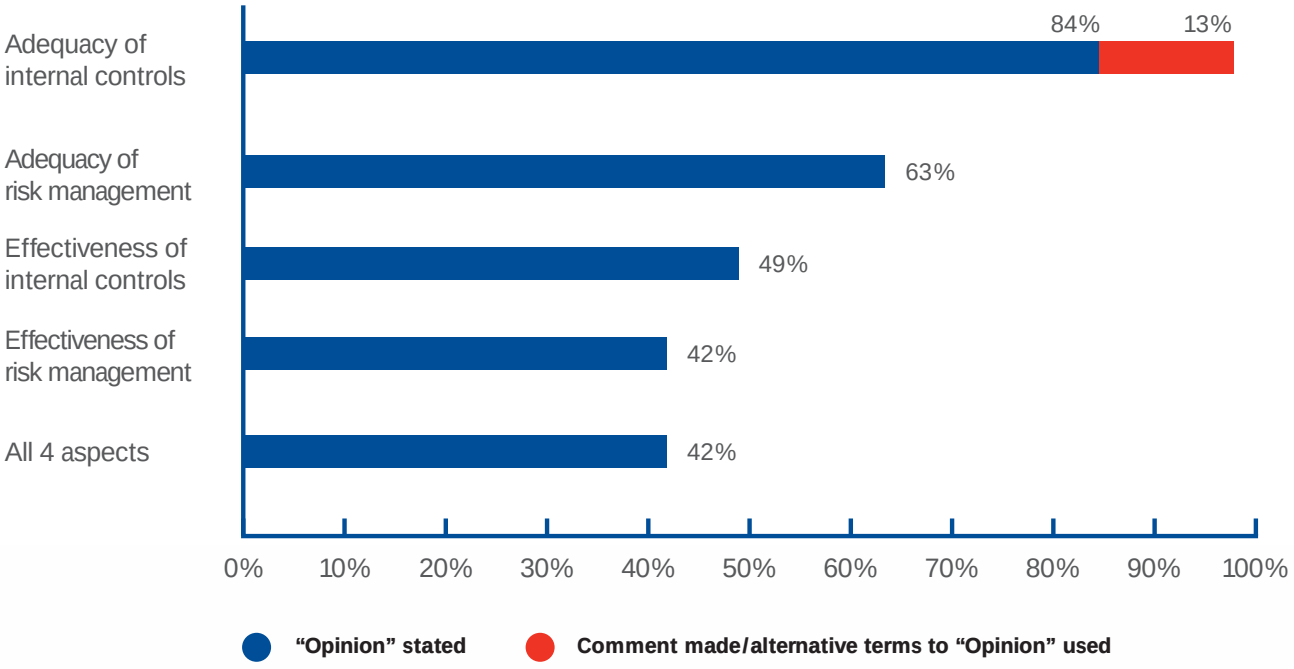


Chart 47: Percentage of companies disclosing the board's opinion in relation to the adequacy of internal controls

7.3 Board's comment (Guideline 11.3)

Guideline 11.3 states "The board should comment on the adequacy and effectiveness of the internal controls, including financial, operational, compliance and information technology controls, and risk management systems, in the company's Annual Report."

Our study found that there was a significant improvement across all aspects of the disclosures relating to the Board's comment on adequacy and effectiveness of risk management and internal controls as shown in Chart 48. In particular, comments on the adequacy and effectiveness of risk management increased by 40-50%. However, a large proportion of companies (41%) did not adopt all aspects of the disclosure requirements specified in the CG Code.

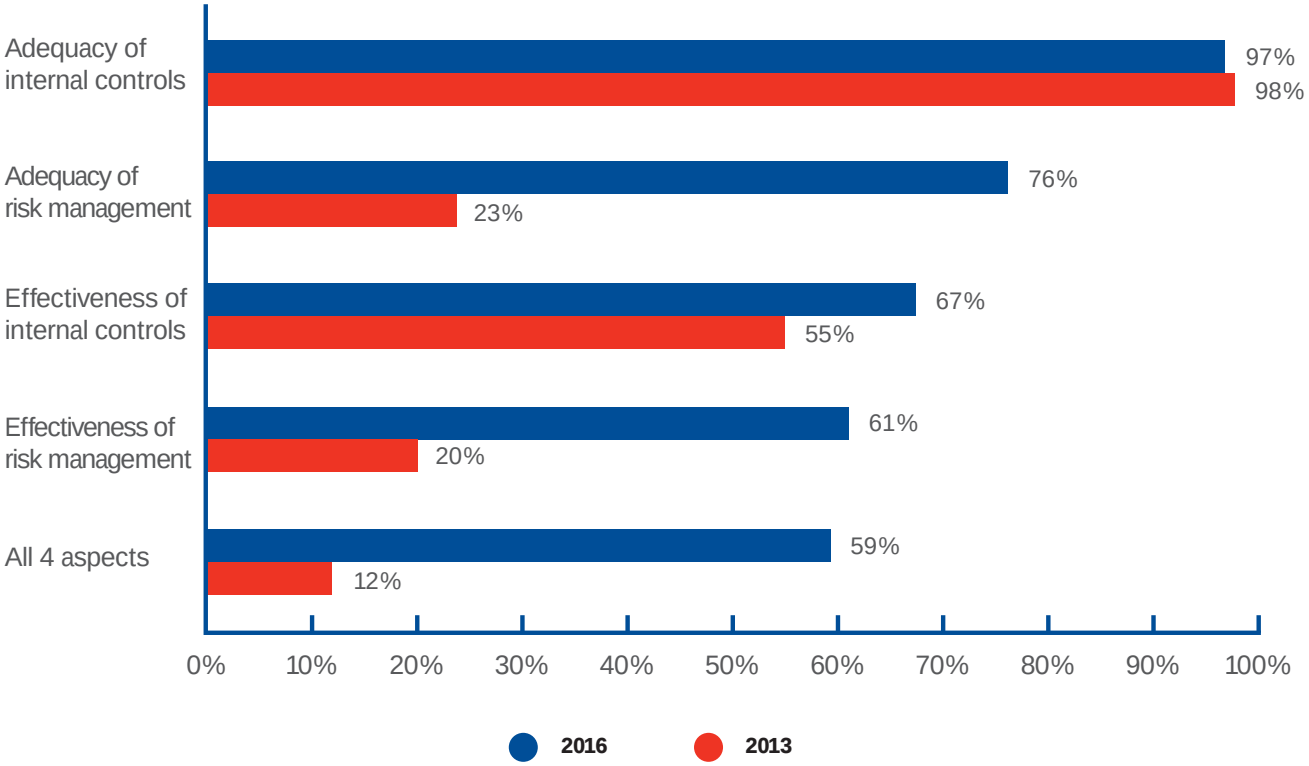
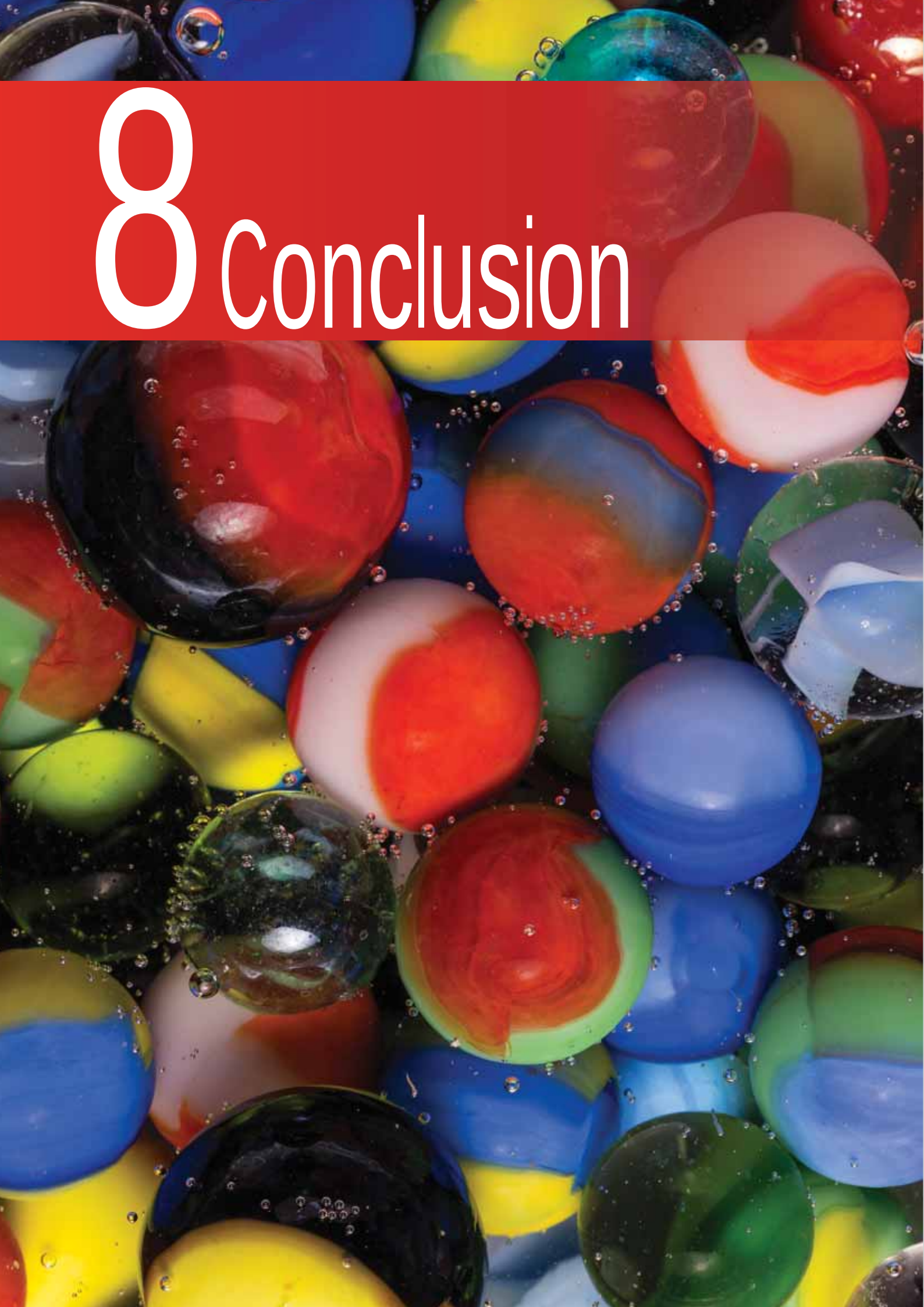


Chart 48: Percentage of companies disclosing the board's comment in relation to the adequacy and effectiveness of risk management and internal controls



8 Conclusion

It is encouraging to see that companies have been progressively improving their disclosures relating to risk governance over time. Companies gave more information on disclosures that are more structural in nature (such as the Board being responsible for risk governance, assigning responsibilities across board committees, setting up key risk and whistle-blowing policies and establishing an IA function). Less forthcoming disclosures are observed in emerging areas of risk governance or areas not specified in the CG Code. These include risk tolerance, risk culture, fraud risk management and the risk management function.

Companies typically stay silent when they have not implemented the underlying process or the process is not fully put in place. Possible reasons for non-disclosure of such information could be a lack of awareness of the need to, or lack of requirement to, disclose.

Changes could be on the way based on a recent announcement by the Monetary Authority of Singapore indicating that the CG Code may be reviewed[20]. This Study has identified opportunities to enhance the existing CG Code requirements. This in turn can bring focus and attention to key risk governance disclosure areas to assist companies to drive further enhancements in underlying practices.

The areas of risk governance for regulators to consider when refreshing the CG Code and for companies to further develop in practice[21] include:

Risk Governance Structures – while most companies continue to assign responsibility for risk governance to the AC, an increasing percentage are establishing an ARC or BRC. Companies should conduct a holistic review of the board governance structure as emerging committees such as the Corporate Governance Committee and Sustainability Committee also start to gain momentum.

Risk Culture – companies should establish a risk culture framework. Formal risk culture frameworks are often more commonly disclosed in companies operating in more regulated industries, though non-regulated businesses are increasingly deriving value from adopting a more formal approach to risk culture. This involves:

- Defining the 'tone at the top' and formalising the expected values and behaviours across the organisation, typically through a Code of Conduct
- Embedding risk culture into daily business activity. An effective way is to establish, communicate and monitor risk tolerance limits, for example, by pledging zero tolerance for fraud. Another way is by changing the organisational mindset towards an activity, such as mandating health and safety sharing sessions at the beginning of every meeting
- Establish a formal risk management training programme. Training at all levels in the company (directors, management and employees) is a key aspect to building capabilities, clarifying roles and responsibilities and explaining risk management concepts in practical terms
- Establishing mechanisms (such as surveys, interviews and workshops) to measure the effectiveness of risk culture. This is critical for identifying areas of deficiency and continuous improvement.

Fraud Risk Management – as the frequency and scale of fraud-related events increase, companies should review the holistic fraud risk management framework in place to manage such risks. The 2016 Study found that companies typically only disclose having a whistleblowing policy and procedure in place. However, this represents only one aspect of the framework focused on providing a reporting channel. Fraud risk management should be integrated as part of the Enterprise Risk Management framework to minimise duplication of effort and standardise the tools and approach to identify, assess, manage and mitigate fraud risks.

[20] "Good time to review S'pore's Code of Corporate Governance: MAS", The Business Times, 27 September 2016
[21] For further practical guidance relating to risk governance, refer to the SID Board Risk Committee Guidebook, 2016

Risk management function resources and capabilities – stakeholder expectations continue to increase in relation to risk governance, requiring companies to consider the right operating model for risk management activities. Clarifying the senior executive responsible for directing and overseeing the risk management framework is the starting point. The key to success is to define the scope and objectives of the risk function. This will then determine the structures, resources and capabilities required. The risk management function provides valuable support to the business in managing risks. Disclosures relating to this could be enhanced to provide stakeholders with more comfort over the level of investment and prioritisation of risk resources in the business.

Risk disclosures – while the SGX LR 1207 (10) and CG Code encourage companies to disclose key risk categories, a specific directive does not yet exist to disclose more detailed risk information. However, as disclosure requirements continue to evolve, with increasing emphasis on identifying key risks, it is hoped that risk disclosures will become more transparent. Upcoming requirements, such as the new Key Audit Matter disclosure requirements and disclosures on material sustainability issues will necessitate change. Stakeholders are looking for comfort and assurance that the company has identified the key risks and is monitoring their potential severity, likelihood and velocity of impact. In short, stakeholders want to know the company is doing everything it can to mitigate the risk.

Internal Audit – while the structure and role of Internal Audit is relatively well defined in the CG Code, there are opportunities for further enhancement. Even though companies are required to disclose having an IA function in place, there is no visibility on the scope and depth of coverage in the audit plan for the year. The role of IA could also be more clearly defined to include not only looking at financial, operational, compliance and information technology processes and controls. It could be empowered to review the adequacy and effectiveness of major cross-organisational frameworks such as governance and culture, enterprise risk management, fraud risk management, compliance, crisis management and learning and development.

Other areas – taking stock of the progress that other jurisdictions have made in risk governance is also key to further developing the Singapore corporate governance landscape. For example, the South African King Code III[22] is currently under review with new areas of corporate governance being incorporated into the draft King Code IV[23]. Such developments include (but are not limited to) recommending companies to 'apply or explain' whether the Board is responsible for governing the Technology and Information framework (including a specific and separate responsibility for governing cyber security risk frameworks), that the Board conducts a review of the adequacy and effectiveness of the Technology and Information function, that the Board conducts a review of the adequacy and effectiveness of the Compliance function and that the AC oversees the implementation of a Combined Assurance Model.

For a risk management framework to be adequate and effective, companies need both the structural and behavioural elements to be well-defined, embedded and disclosed. Only then can companies provide the full picture to key stakeholders.

[22] Institute of Directors, Southern Africa, King Code III of Governance for South Africa 2009
[23] Institute of Directors, Southern Africa, Draft IV Report on Corporate Governance for South Africa 2016

Appendix A. Limitations and Disclaimers

A.1 Completeness of information

The study relied on annual reports for FY14/15 that were publicly available as at 30 April 2016. The extent to which companies disclosed additional information outside of the annual report was not captured. In addition, the extent to which companies issued supplementary corporate governance disclosure information after the published annual report (e.g. through announcements on the SGXNet) was also not captured.

A.2 Subjectivity and interpretation

The study is predominantly a qualitative approach that involves an assessment of the extent to which a company has made a disclosure in relation to the corporate governance disclosure requirements and areas of better practice. While efforts were made to standardise the assessments and calibrations in the study, there was an element of subjectivity and interpretation, which may impact the results.

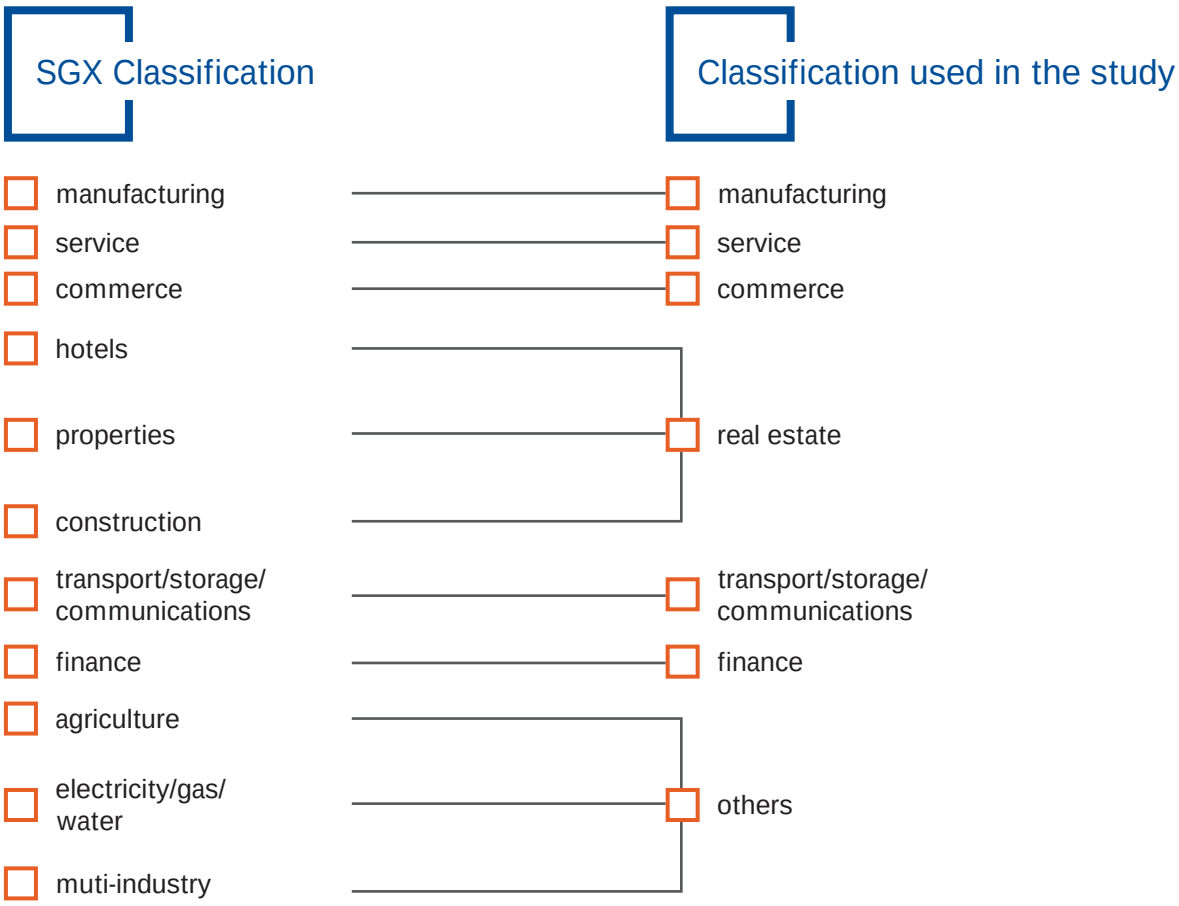
A.3 Levels of compliance

The study focused on corporate governance disclosures relating to risk governance and risk management. It did not test the underlying practices within each company to verify whether the disclosures were accurate and complete.

A.4 Comparative data from 2013 Study

To the extent possible, the results from the 2013 Study have been retained. However, to enhance the clarity and consistency of comparative results, some results from the 2013 Study were adjusted. Where this has occurred, explanations are provided in the narrative text.

Appendix B. Sector Classification



Appendix C. Risk Governance Structures and Practices Comparison

C.1 Comparison by Market Capitalisation (2016)

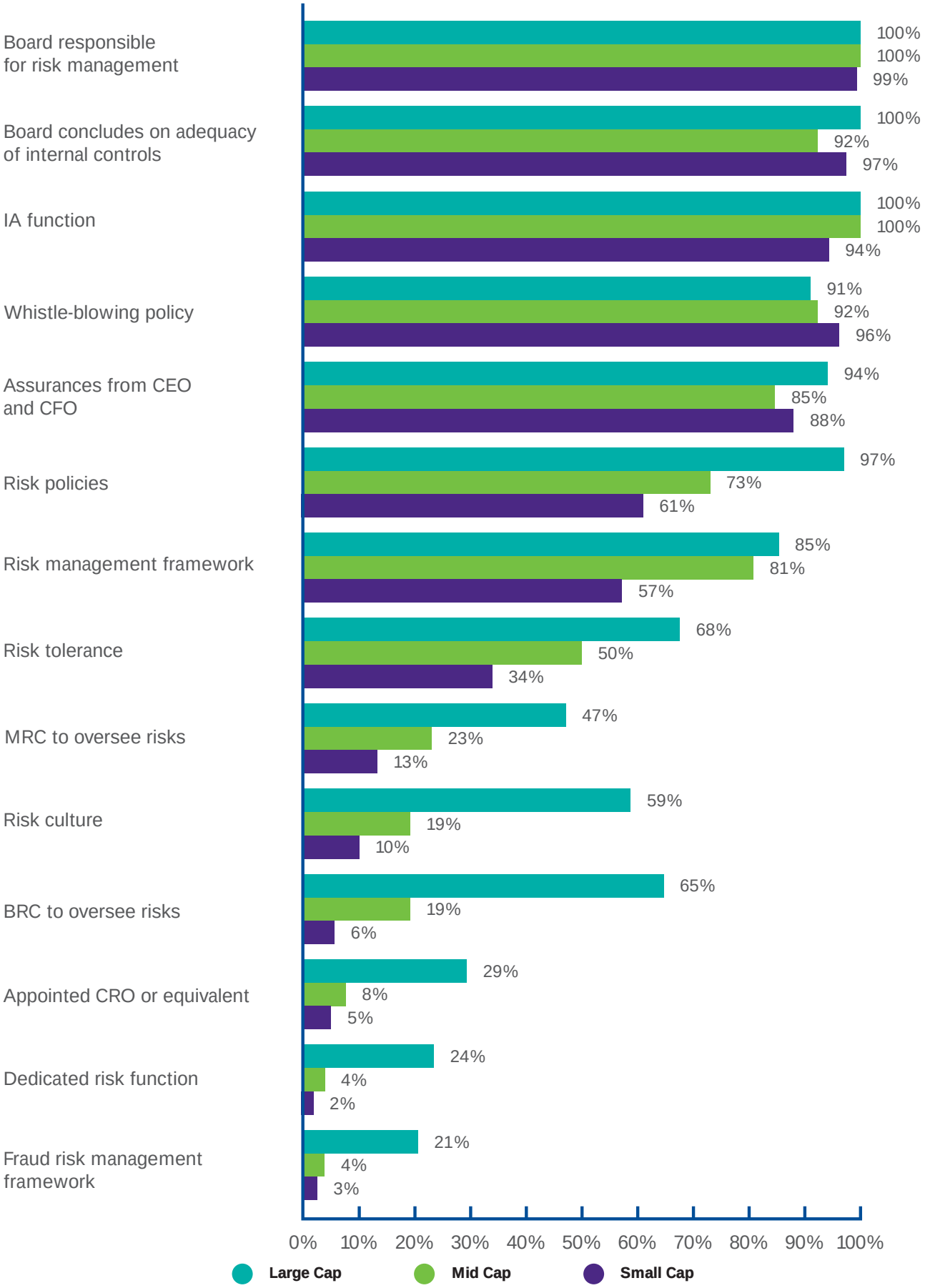


Chart 49: Comparison of risk governance structures and practices by market capitalisation

C.2 Comparison by Sector (2016)

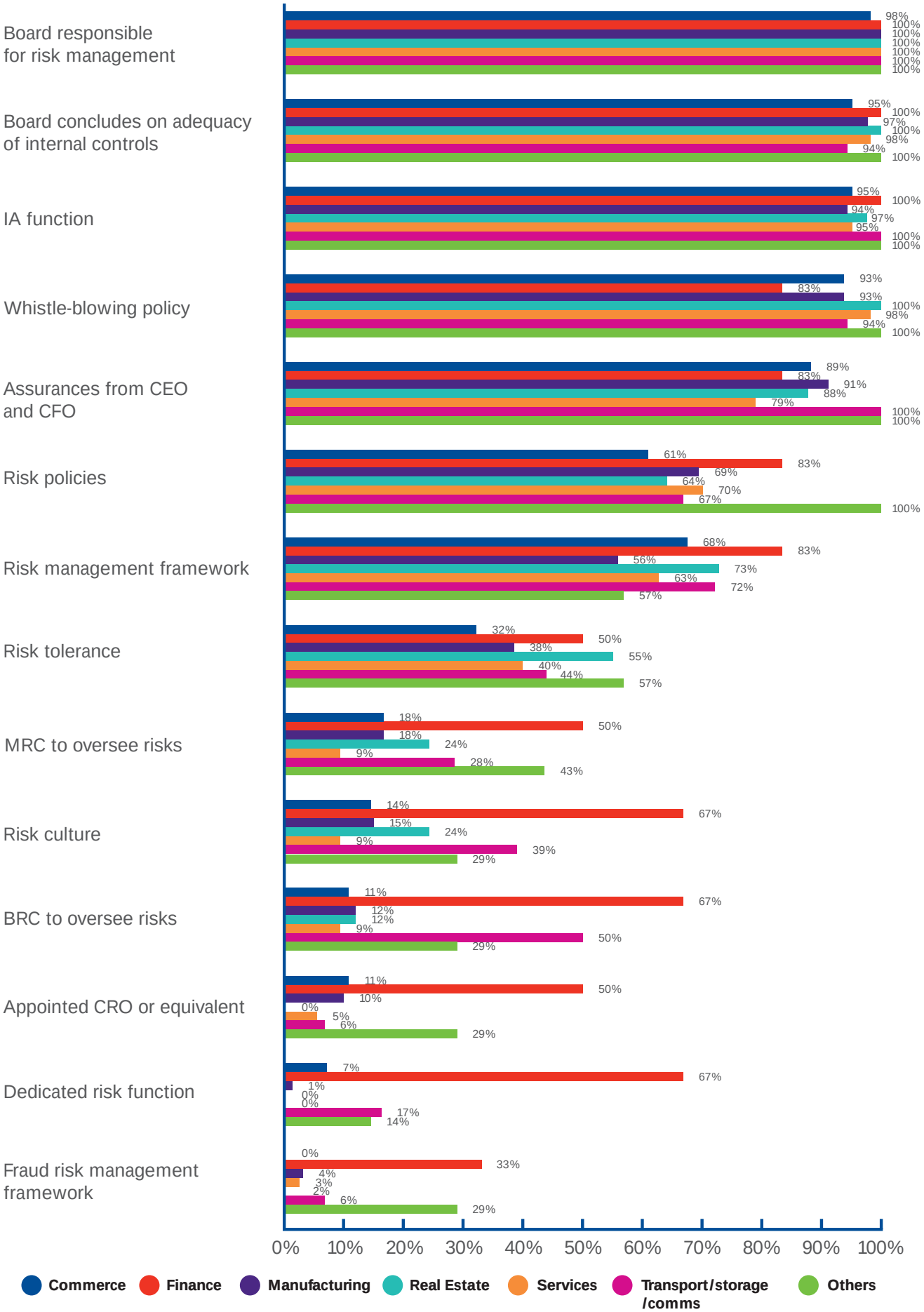


Chart 50: Comparison of risk governance structures and practices by sector

CONTACT US

ISCA

HO TUCK CHUEN
Chairman
ISCA Corporate Governance Committee
T: +65 6749 8060

KPMG

IRVING LOW
Partner
Head of Risk Consulting
Head of Markets
KPMG in Singapore
T: +65 6213 2017
E: irvinglow@kpmg.com.sg