ISCA-KPMG risk management study

Towards better risk governance

A study of Singapore listed companies 2013

INSTITUTE OF SINGAPORE CHARTERED ACCOUNTANTS
Formerly ICPAS

KPMG
cutting through complexity

Contents

Introduction

Risk governance has emerged as one of the top key concerns for boards and senior management in recent years. The 2008 financial crisis, which cost the global economy an estimated US$2.3 trillion based on estimates by the International Monetary Fund (IMF),[1] revealed that inadequacies in risk management practices and a lack of awareness regarding risk exposures among many financial institutions and listed companies were key contributing factors. Regulatory reviews of the crisis found that the lapses and deficiencies in risk management played a critical role in exacerbating the crisis.[2,3]

The 2008 crisis clearly highlighted the importance of businesses having strong risk management practices to help them identify, assess and manage risks. To raise awareness and promote stronger risk management practices in Singapore, the Monetary Authority of Singapore (MAS) introduced more robust guidelines that require boards to provide commentaries and disclosures regarding risk management and internal controls in the revised Code of Corporate Governance (Code) 2012. It also issued the Risk Governance Guidance for Listed Boards in May 2012. In addition, the Singapore Exchange (SGX) Listing Rule (LR) 1207(10) was amended in 2011 to strengthen corporate governance (CG) practices.

To gather insights on the pace and adoption of risk management practices, the Institute of Singapore Chartered Accountants (ISCA) and KPMG jointly conducted a study of the risk management landscape in Singapore. Our study examined the risk management capabilities of listed companies and the quality of risk management disclosures in their annual reports. In addition, we assessed the state of adoption for Principle 11 of the revised Code 2012 and SGX LR 1207(10) to identify more effective approaches to enhance the adoption of risk management practices.

We hope this risk governance study will be of use to boards and management, as well as regulators. Specifically, we hope it will be useful in terms of raising awareness and enhancing understanding of the existing guidelines and practices required to strengthen risk management capabilities and move towards a higher standard of risk governance.

R. Dhinakaran
Vice-President
Chairman, ICSA Corporate Governance Committee
ISCA

Irving Low
Partner
Head of Risk Consulting
KPMG in Singapore

[1] International Monetary Fund, "Global Financial Stability Report", April 2010.
[2] Senior Supervisors Group, "Risk Management Lessons from the Global Banking Crisis of 2008", Financial Stability Board, 21 October 2009.
[3] Anil K Kashyap, University of Chicago, Booth School of Business and NBER, "Lessons from the Financial Crisis for Risk Management – Paper Prepared for the Financial Crisis Inquiry Commission", 2 February 2010.

About the study

Objectives

Our study is a joint effort by ISCA and KPMG to gather insights on the risk management landscape in Singapore. It provides an understanding of the risk management capabilities and structures of listed companies in Singapore, as well as risk management disclosures in their annual reports. In addition, it also assesses the state of adoption of risk management practices among listed companies in accordance with the revised Code 2012 Principle 11 and SGX LR 1207(10).[4]

Research approach

Data was collected from a total of 250 companies listed on the SGX.[5] For the purpose of our study, secondary listings, newly listed companies, real estate investment trusts, and companies that have not released any annual reports for FY11/12, including companies under judicial management, were excluded from the sampling.

The 250 sampled companies were sorted into three groups based on their market capitalisation (market cap) (see Table 1). A total of 30 large-cap, 30 mid-cap and 190 small-cap companies were randomly selected across the three groups.

Data was collected using the annual reports for FY11/12 that were publicly available as at 31 December 2012.[6]

Profile of companies

The samples were grouped into various industry sectors using the classification outlined by SGX, with some sectors merged to reduce the number of sectors to display

table 1: market capitalisation of companies (as at 30 Dec 2011)[7]

market capitalisation[8]	number of samples selected	% breakdown[9]
large-cap (companies with market cap of S$1 billion and above)	30	12%
mid-cap (companies with market cap of S$300 million to less than S$1 billion)	30	12%
small-cap (companies with market cap of less than S$300 million)	190	76%
total	250	100%

report legend

to assist the reader distinguish between key categories of data we have adopted the following symbols:

○ = market capitalisation

□ = sector

◇ = government linked companies (GLCs) /non-government linked companies (non-GLCs)

[4] Our study acknowledges the possibility that some of the sampled companies may have already adopted various risk management practices but decided not to disclose this information in their annual reports. Where possible, our study has indicated this non-disclosure, but for all other analyses, we assume that the companies were not ready to disclose the relevant information as a result of incomplete adoption or implementation of all the risk management practices.

[5] Total number of SGX listed companies as at 31 December 2012 was 776. Source: SGX.

[6] Many of these annual reports were published before the revised Code 2012 came into effect on 1 November 2012.

[7] The study was initiated during 2012 with the selection of the samples being based on the "Ranking of Singapore companies by market capitalization as at 30 Dec 2011" published by The Business Times.

[8] SGX does not provide criteria for determining large/mid/small cap. The thresholds proposed and used in this study are based on Singapore Corporate Awards criteria.

[9] The proportion of the samples across the three groups is with reference to the 250 sampled companies.

(e.g. Real Estate, Others) (refer to Appendix 1). Figure 1 summarises the breakdown of our sample companies across sectors. We also show how the sector breakdown compares to the SGX listed companies breakdown (using available SGX data, 6 Sep 2013). Refer to Appendix 2 for a further breakdown of companies by sector and size.

Most companies in our sample have total assets of at least S$100 million (71%). More than half of the companies have a turnover of more than S$100 million (60%). (Refer to Figures 2 and 3).

government-linked companies (GLCs)

The performance of GLCs compared to other privately run companies is also of interest to stakeholders. Tasked to manage and grow Singapore's reserves, both Temasek Holdings and GLCs are accountable to the government for their

figure 1: sector representation

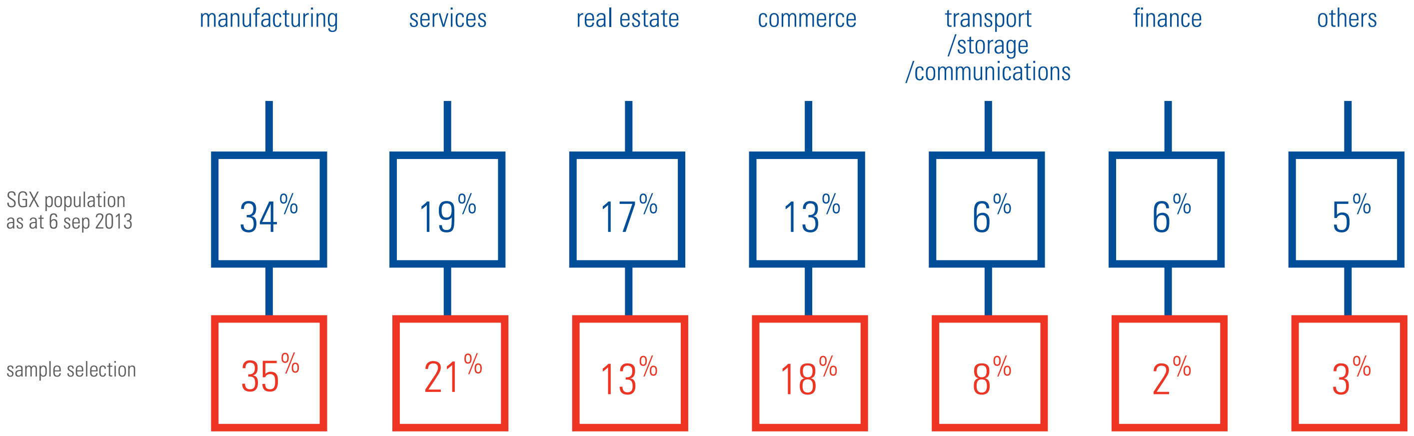


figure 2: sample companies by total assets

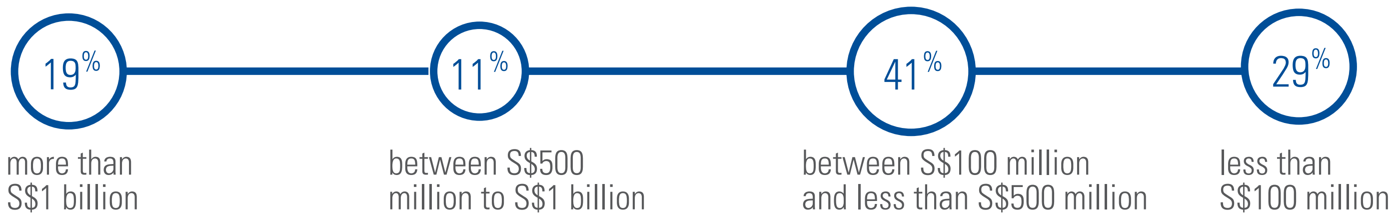


figure 3: sample companies by turnover

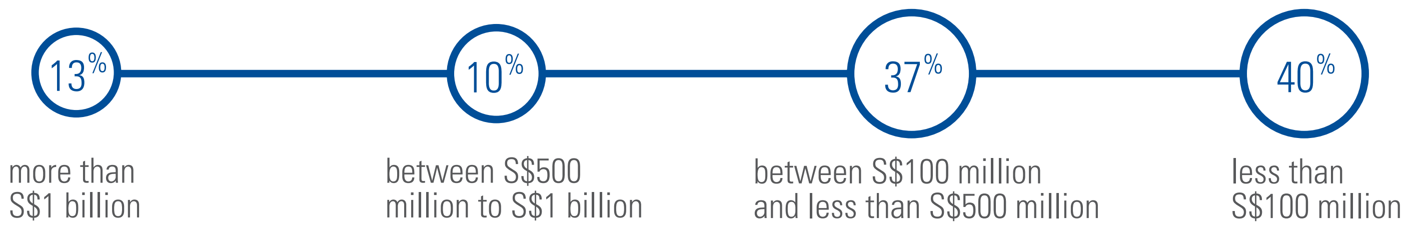
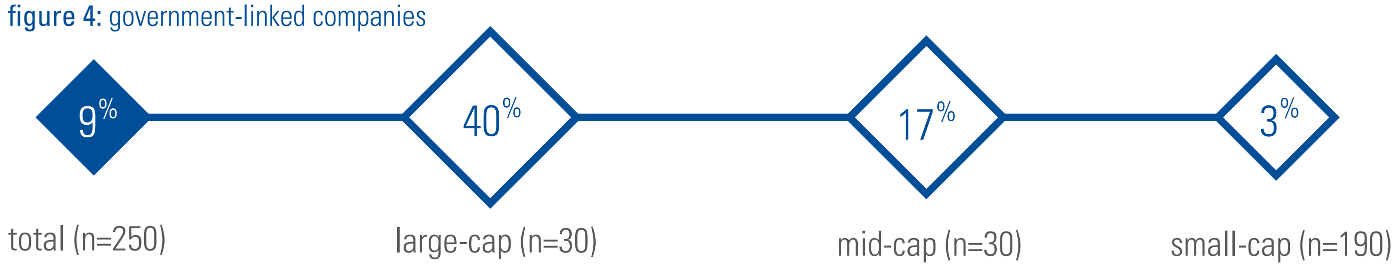


figure 4: government-linked companies



performance. This requires them to develop risk management strategies and capabilities, while taking calculated risks aimed at growing the value of their investments or portfolios over time.[10,11]

To examine any differences in the risk management practices between GLCs and non-GLCs, our study considers a company to be a GLC if one of the substantial shareholders is Temasek Holdings or a government/statutory body.[12] As our sample was randomly selected prior to being subjected to the GLC definition test, only a portion of Singapore's GLCs were included in our study. Overall, 22 out of the 250 sampled companies (9%) are considered GLCs, as shown in Figure 4. Among the large-cap companies in our sample, 40% are categorised as GLCs.

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 new regulations and best practices for risk management and internal controls set out by SGX and MAS. Figure 5 provides a summary of our study's approach. Our study focused on two key areas: annual report disclosures and risk management capabilities (comprising structure and system).We analysed the quality and substance of risk management disclosures based on requirements outlined in SGX LR 1207(10) and Principle 11 of the revised Code 2012.

We then analysed the key elements of the risk management and internal control system in place to support the disclosures regarding adequacy and effectiveness.

Annual report disclosures

The revised Code 2012 has raised the standard of risk management disclosure. It is now no longer sufficient for the board to review and comment on the **adequacy** of the company's risk management and internal control system. The board should now also review and comment on the **effectiveness** of the system. In addition, the board should obtain assurances from the chief executive officer (CEO) and chief financial officer (CFO) regarding the effectiveness of these systems.

In addition to the changes to the Code, changes to the SGX Listing Rules have increased the extent of disclosures required in the annual report. It is now necessary for the board to disclose the basis for its opinions on the adequacy of the company's internal controls.[13] Table 2 below provides a summary of the disclosure requirements.

Risk management capabilities: establishing the structure and system

In order to make a disclosure, it is necessary for companies to have the supporting risk management

[10] 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.
[11] GIC FAQs, "What is the relationship between GIC and the Government?".
[12] Our definition of a GLC is based on an IMF paper by Carlos D. Ramírez and Ling Hui Tan: "Singapore Inc. Versus the Private Sector: Are Government-Linked Companies Different?", 2004.
[13] SGX LRs PN 12.2 Adequacy of Internal Controls.

and internal control structures and systems in place. The changes to the guidelines and rules emphasise the board's responsibility for the governance of risk. Existing rules and guidelines also provide further guidance to the board on establishing the necessary structures and systems to help the board with its oversight role with respect to risk management and internal control.

Beyond the oversight of internal controls carried out by the AC, the board may also establish a BRC to assist it in overseeing risks. In addition to establishing a BRC at the board level, the board may also appoint a CRO to provide oversightof risks at the C-suite level. The board should also establish an effective IA function to assist the board by providing independent and objective assurance regarding internal controls.

The revised Code 2012 further stresses the need for companies to have a sound system of risk management and internal control in place. This can include risk management frameworks and policies, as well as whistle-blowing policies that may provide a structured and disciplined approach to managing risks for the company.

figure 5: summary of approach

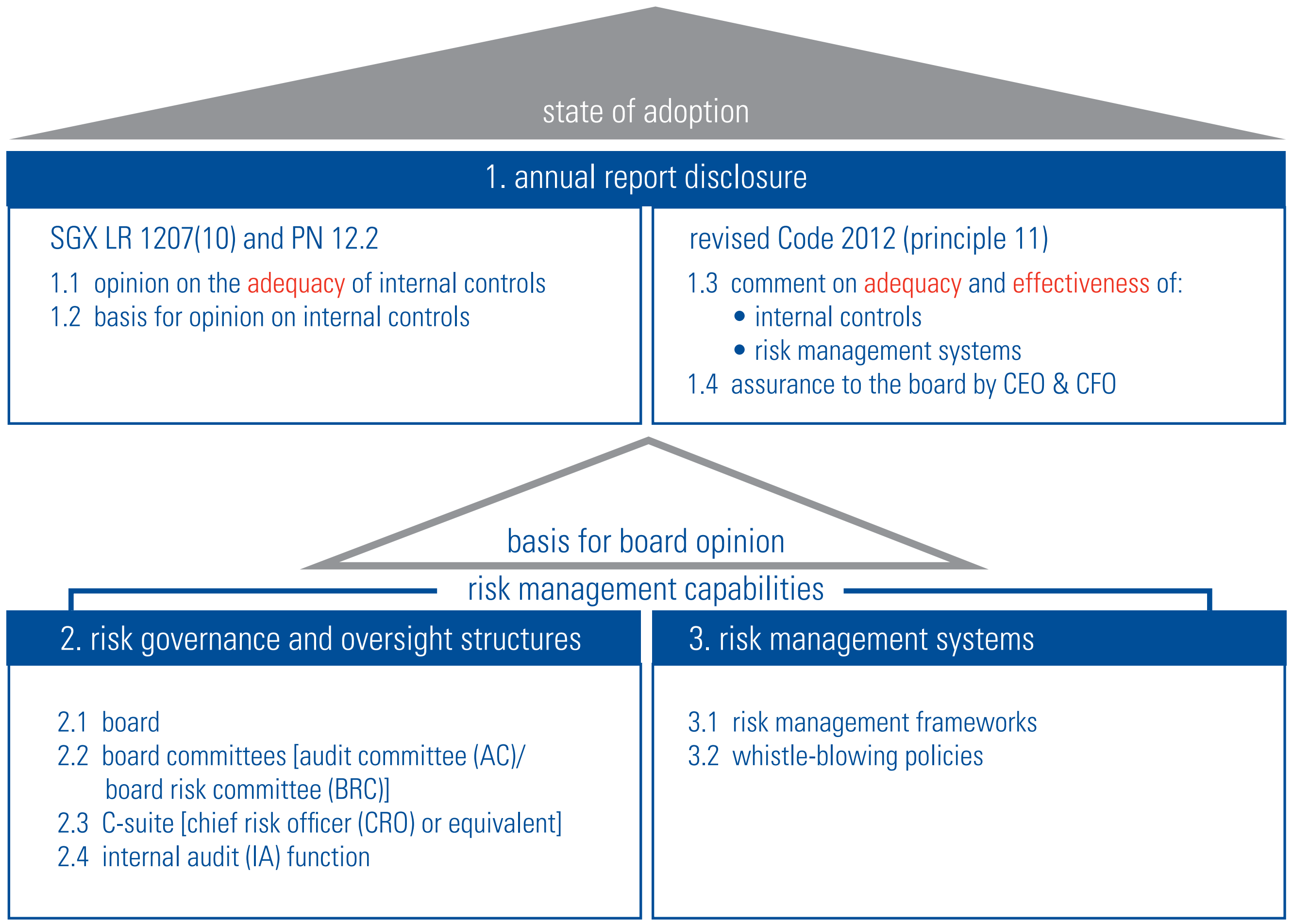


table 2: comparison of requirements regarding adequacy and effectiveness of risk management and internal control systems

		code 2005	guidelines on CG 2010	SGX 1207(10)	code 2012
internal controls:	adequacy	✓	✓	✓	✓
	effectiveness				✓
risk management:	adequacy	✓	✓		✓
	effectiveness				✓

Key take-aways

Regulations drive higher compliance

Adoption of new requirements encouraging

Size, complexity of industry and stakeholder expectations drive adoption rates

Low rate of disclosure of board assurance from CEO and CFOs

Greater transparency of risk oversight responsibilities at board committee level required

Separate risk structures remain uncommon

IA is an essential component of the assurance framework; capabilities must evolve to meet expectations

Low rates of disclosure of risk frameworks

Whistle-blowing disclosures must go beyond policies; channels to report and procedures to resolve equally important

Executive summary

Compliance is higher when risk management is regulation-based, compared to when risk management is principle-based.

Our study found that 98% of the sampled companies complied with the SGX LR 1207(10) requirement for disclosure of an opinion regarding the adequacy of internal controls and that 80% disclosed a basis for their opinion.[14]

However, we found that the adoption rates were lower for compliance with all elements of the revised Code 2012 Principle 11: only 12% of companies commented on the adequacy and effectiveness of the risk management and internal control system. Surprisingly, only 23% of sampled companies complied with the previous Code 2005, which required disclosure of the adequacy of internal controls and risk management.

These low take-up rates for the voluntary Code highlight two things: First, very few companies are early adopters of the requirements in the revised Code 2012 Principle 11. Second, companies are still facing challenges interpreting requirements and determining what and how much information to disclose, despite the 'comply or explain' regime being effective since 2005.

The adoption rate for risk management is encouraging given that it is early days for the revised Code 2012.

We found that 12% of the sampled companies have complied with the revised Code 2012 Principle 11 compared to 23% compliance with Code 2005. Even though both rates appear to be on the low side, it is encouraging to see that the adoption rate for the revised Code 2012 is already half of the rate for Code 2005 given that the revised Code 2012 came into effect for companies with financial years commencing only 1 November 2012. A key driver of the improved adoption rate of the Code 2012 is the introduction of SGX LR 1207(10), which requires companies to disclose deviations from the Code with explanations.

Bigger companies, companies in the finance sector, and GLCs have adopted and disclosed better-developed risk management practices.

However, there is room to improve for all in terms of disclosing board responsibility for risk; establishing appropriate risk oversight structures within the board, board committees and management committees; and disclosing assurances to the board by the CEO and CFO regarding the effectiveness of the risk management and internal control system.

Low rate of adoption for board assurance from CEOs and CFOs.

Only 15% of companies sampled disclosed that the CEO and CFO provide assurance to the board regarding the effectiveness of risk management and internal control. This is partly due to the timing of this study, but it also reflects that companies are challenged by this requirement in determining the extent of assurance required, what needs to be done to support the assurance and how it should be disclosed.

Greater transparency of risk oversight responsibilities at board committee level required; scope and responsibilities remain relatively unchanged.

Our study found that very few companies have established a separate BRC (14%) and that instead they typically rely on the AC to provide risk oversight on behalf of the board. However, our results show that there is no significant difference in the frequency of meetings, or the committee size, between ACs with risk management responsibilites and those ACs without risk management responsibilites.

Separate risk structures remain uncommon; smaller companies have less established risk management structures and systems.

Only 5% of companies have a dedicated CRO in place and only 12% have established a separate management risk committee (MRC).

While a majority of small-cap companies disclosed having an IA function (93%) and whistle-blowing policy (91%) in place, only 34% disclosed that their board is responsible for risk governance and only 4% have established a BRC to help the board oversee risks. In addition, only 1% disclosed having a CRO to provide executive oversight and only 38% disclosed and explained having a risk management framework.

It should be noted that the number of small-cap companies with outsourced IA functions in place seems relatively high (68%) compared to the results of a recent survey conducted jointly by the Singapore Accountancy Commission (SAC) and KPMG titled "Taking the Pulse – A Survey of IA in Singapore 2013" which indicated only one third of Singapore companies surveyed had an outsourced IA function. The lack of information about the nature, scope, coverage and spend on IA functions in annual reports highlights the challenges in relying solely on disclosures.

IA is an essential component of the assurance framework; capabilities must evolve to meet expectations.

A critical element of establishing an effective framework to check the adequacy and effectiveness of the risk management and internal control system is IA. Whilst 94% of companies sampled disclosed that they have an IA function in place, only 39% disclosed that their IA function meets the Institute of Internal Auditors (IIA) Standards. Results of the recent SAC-KPMG survey titled "Taking the Pulse – A Survey of IA in Singapore 2013" highlighted that greater demands are being placed on the IA function to provide assurance to the AC regarding the risk management and internal control system. Therefore, ensuring that IA functions are adequately resourced and positioned in the organisation is critical to success and satisfying compliance requirements.

Boards can improve the disclosures regarding their risk management and internal control system and the mechanisms in place to check the system's adequacy and effectiveness.

In addition to the low rate of disclosures regarding the adequacy and effectiveness of their risk management and internal control system, the study found that only 32% of the sampled companies disclosed and explained their risk management framework.

Whistle-blowing remains a key pillar in the risk management and internal control assurance framework.

Whilst 90% of sampled companies disclosed having a whistle-blowing policy in place, further work is required to enhance disclosures regarding the channels for reporting concerns and the procedures for addressing claims. The majority of companies (73%) indicated that the AC is the primary channel for reporting concerns.

[14] SGX Listing Rules Practice Note 12.2 Adequacy of Internal Controls.

ISCA and KPMG observations and comments

The state of risk management and internal controls in Singapore has improved and is becoming more mature. However, further work is required by boards of listed companies to ensure there is an adequate and effective system of risk management and internal control within their organisation and that the annual report disclosures reflect this.

The timing of this joint study is important. ISCA and KPMG embarked on this study in 2012 and reviewed annual reports for 250 Singapore listed companies for the financial year 2011/12. Despite the fact that for a majority of companies, the official compliance date for the revised Code 2012 is not until the end of 2013, the timing of the study enables important distinctions to be made at a point in time. In particular, the study highlights characteristics of early adopters and identifies critical gaps in existing disclosures. This provides a timely opportunity to generate awareness and education around the key challenges facing boards and C-suite management in adopting the requirements.

This study has revealed that there are gaps regarding the substance and quality of disclosures, which can be improved significantly.

// What is evidently clear, however, is that with the introduction of the SGX LR 1207(10) on 29 September 2011, it has made a significant difference in the adoption of more formal risk management and internal control structures and frameworks. It has pushed and propelled a significant majority of the listed companies to at least have some form of formal internal control framework /systems in place. //

Irving Low
Partner
Head of Risk Consulting
KPMG in Singapore

Companies in our sample have performed better when disclosing the adequacy of internal controls and traditional assurance functions such as IA and whistle-blowing, which were the focus of the previous Code (2005). However, there are limitations to continuing with this approach. By focusing only on adequacy, companies could end up designing the best (rather than fit-for-purpose) risk management and internal control systems.

The developments in the regulatory environment and CG Code to incorporate effectiveness and risk management seek to address this gap and are an essential step forward in the CG framework in Singapore. Without a process in place to understand whether the risk management and internal control system is operating as intended, both boards and ACs are exposed. This is especially true for large companies with diverse operations, wide geographical spread, and/or complex holding/ subsidiary company structures, which could pose significant strategic, reputational, financial and operational risk if not well governed.

The regulatory and better practice regime in Singapore is not intended to replicate the Sarbanes-Oxley style regime in the US or be onerous in nature. However, boards of listed companies in Singapore need to ensure that the levels of assurance that they are receiving from various channels (e.g. risk and controls self-certification, risk-based internal audit plans, control self-assessments, independent audits, etc.) provide them with the comfort they need to satisfy the requirements.

Companies should adopt the CG requirements not just from a compliance tick-the-box perspective, but also to promote their organisation's long-term sustainability. With the effective date of compliance with the revised Code 2012 imminent, now is the time for companies to not only review their current risk management and internal control systems, but also the frameworks they have in place to check the adequacy and effectiveness of their systems.

// Effective risk governance is an ongoing commitment and ISCA encourages companies and businesses to think seriously about how to adopt the best practices in the revised Code of Corporate Governance. Adoption will help them deal with risks much better in the present complex and uncertain business environment. Hence, the aim of our joint study is to help them look at risk governance in greater depth and hopefully follow up with the adoption of the best practices. //

R. Dhinakaran
Vice-President
Chairman, ISCA Corporate Governance Committee
ISCA

This study provides a call to action for boards, ACs and management to confirm:

- Is the risk management and internal control framework appropriate vis-a-vis the business model and risks?
- From an oversight perspective, where/what are the sources of assurance for SGX Listing Rule 1207(10) and Principle 11?
- As CEO/CFO – how effectively do the 'lines of defence' interact with each other?
- How does the board interact with CEO/CFO on risk management and internal controls i.e. are they 'connecting the dots' with risk management and internal control information?

Key findings

98% disclose an opinion on the adequacy of internal controls, only 80% disclose a basis

29% state that AC is responsible for risk but 57% did not disclose which board committee is responsible

12% are early adopters of the revised Code 2012; already half the rate of companies complying with Code 2005

although 94% disclose having an IA function in place; only 39% disclose meeting IIA standards

only 15% adoption for board assurance from CEO/CFO

14% have BRCs

12% have MRCs

5% have CROs

whilst 90% disclose whistle-blowing policies, only 36% disclose channels for reporting; and only 16% disclose procedures to resolve

Key findings: State of adoption

Following the global financial crisis (GFC) in 2008, the CG landscape in Singapore has seen significant changes in three major areas: the Singapore Companies Act (amendments expected to be tabled in Parliament by end-2013[15]), the SGX Listing Rules and the Code.

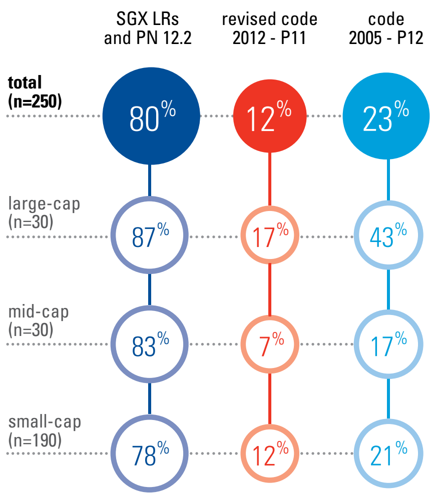
Among the changes introduced, the amendments to SGX LR 1207(10) and Principle 11.3 of the revised Code 2012 are considered significant for boards. These rules and guidelines require them to disclose the board's opinion regarding internal controls (as well as risk management, in case of the revised Code 2012) in the annual report.

While the revised SGX Listing Rules came into effect on 29 September 2011, the revised Code 2012 will take effect only for financial years commencing 1 November 2012. Although compliance with the revised Code 2012 is not mandatory, listed companies are required under the SGX Listing Rules to disclose their CG practices[16] and explain any deviations from the Code.

Higher adoption of regulatory requirements

Our findings in Figure 6 show that 80% of the sampled companies have complied with the mandatory SGX LR 1207(10) requiring disclosure of an opinion regarding the adequacy of internal controls and have provided a basis as recommended in SGXs Practice Note 12.2. While adoption rates for the revised Code 2012 and Code 2005 (specifically with regard to the adequacy and effectiveness of risk management and internal control systems) are significantly lower. In the short period since the revised Code 2012 has come into effect, 12% of companies have already fully complied with Principle 11.3 of the revised Code 2012. In comparison, only 23% of companies complied with the components relating to risk management and internal control in the 'old' Code that has been in existence since 2005.

figure 6: has the board commented on risk management and internal controls as per the SGX LRs and CG Code (2005 and 2012)?



Looking at the revised Code 2012, SGX LR 1207(10) and the Risk Governance Guidelines for listed Boards 2012, we identified 10 risk management practices to be the most relevant for our study. These 10 areas are relevant as they highlight compliance with or adoption of the new regulations and best practices that will enable the board to carry out its risk governance responsibilities more effectively. The 10 areas are shown in Table 3 overleaf.

Of note, our study found that many companies have also formed a MRC as an additional structure to assist their boards in the governance of risks. This is a measure beyond the revised guidelines, as the guidelines suggest only that the board consider appointing a CRO to provide executive oversight of risks.

Bigger companies have better risk management practices

Out of the 10 risk management practices selected for analysis, the compliance and adoption rates among large-cap companies were consistently higher than those of the mid-caps and small-caps in 7 of the 10 areas, as shown in Figure 7.

Many of the large-cap companies, if not all, are operating in multiple jurisdictions beyond Singapore. The greater complexity of their operating environments may mean higher standards of risk management are a necessity in their daily operations.

GLCs have better risk management practices

Our study found that the compliance and adoption rates for risk management practices were higher among GLCs compared to non-GLCs. Among the 10 risk management practices selected for analysis, GLCs achieved higher compliance and adoption rates in nine of them (refer to Figure 8).

[15] Ministry of Finance, "Ministry of Finance's Responses to the Report of the Steering Committee for Review of the Companies Act", 4 December 2012.
[16] SGX, "Guide to Sustainability Reporting for Listed Companies".

table 3: 10 risk management practices

risk management practice	code of corporate governance 2012	risk governance guidelines	SGX LR 1207(10)	other references
board assumes responsibility for risk management	principle 11	appendix M		
established BRC to manage risks	principle 11.4	appendix A		
appointed CRO or equivalent		appendix A		
established MRC to manage risks				17
established IA function	principle 13	appendix L		
established risk management framework	principle 11.1	appendix C & L		
explained risk management framework	principle 11.1	appendix M		
established whistle-blowing policy	principle 12.7	appendix L		
positive opinion with basis	principle 11.3	appendix G & H	1207(10) & PN 12.2	
assurances from CEO and CFO	principle 11.3(b)	appendix M		

Finance sector has better risk management practices

The GFC in 2008 revealed weaknesses in the risk management practices of the finance sector. Since then, many financial institutions have enhanced their risk management capabilities to address these weaknesses. In Singapore, the finance sector is also subjected to more stringent MAS regulations.[18]

Based on disclosures in annual reports, when it comes to risk management capabilities, the finance sector outperformed all other sectors (refer to Figure 9). Among the 10 risk management practices selected for analysis, the finance sector came out top in nine areas.

However, it should be noted that two out of six finance sector companies did not disclose information regarding key elements of risk management, which impacted the overall adoption rate for that sector.

[17] KPMG International, "Expectations of Risk Management Outpacing Capabilities – It's Time For Action", 2013.
[18] MAS, "Guidelines on Corporate Governance for Banks, Financial Holding Companies and Direct Insurers which are incorporated in Singapore", March 2013.

figure 7: risk management practices – compliance and adoption rates across market caps

	large-cap (n=30)	mid-cap (n=30)	small-cap (n=190)
board assumes responsibility for risk management	33%	33%	34%
established BRC to manage risks	63%	27%	4%
appointed CRO or equivalent	37%	7%	3%
established MRC to manage risks	53%	17%	5%
established IA function	100%	100%	93%
established risk management framework	84%	53%	37%
explained risk management framework	67%	30%	27%
established whistle-blowing policy	83%	90%	91%
positive opinion with basis	87%	83%	76%
assurances from CEO and CFO	13%	13%	16%

Note: Leading practices identified by filled in shapes

figure 8: risk management practices – compliance and adoption rates by GLCs and non-GLCs

	GLCs (n=22)	non-GLCs (n=228)
board assumes responsibility for risk management	41%	33%
established BRC to manage risks	55%	10%
appointed CRO or equivalent	32%	5%
established MRC to manage risks	45%	9%
established IA function	100%	94%
established risk management framework	73%	42%
explained risk management framework	45%	31%
established whistle-blowing policy	91%	90%
positive opinion with basis	86%	78%
assurances from CEO and CFO	14%	15%

figure 9: risk management practices – compliance and adoption rates across industries

	commerce (n=46)	finance (n=6)	manufacturing (n=88)	real estate (n=33)	services (n=51)	transport/storage /communications (n=19)	others (n=7)
board assumes responsibility for risk management	22%	67%	35%	42%	39%	21%	29%
established BRC to manage risks	9%	67%	8%	15%	10%	42%	29%
appointed CRO or equivalent	13%	67%	3%	3%	4%	5%	29%
established MRC to manage risks	13%	67%	6%	9%	6%	32%	43%
established IA function	96%	100%	92%	97%	96%	95%	100%
established risk management framework	48%	83%	47%	42%	29%	53%	71%
explained risk management framework	33%	83%	35%	36%	12%	32%	71%
established whistlee-blowing policy	89%	100%	88%	94%	96%	84%	86%
positive opinion with basis	78%	100%	76%	79%	80%	74%	86%
assurances from CEO and CFO	20%	17%	11%	24%	12%	21%	0%

Key findings: 1. Annual report disclosure

1.1 and 1.2 'Opinion with basis'

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

SGX LRs PN 12.2: 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.

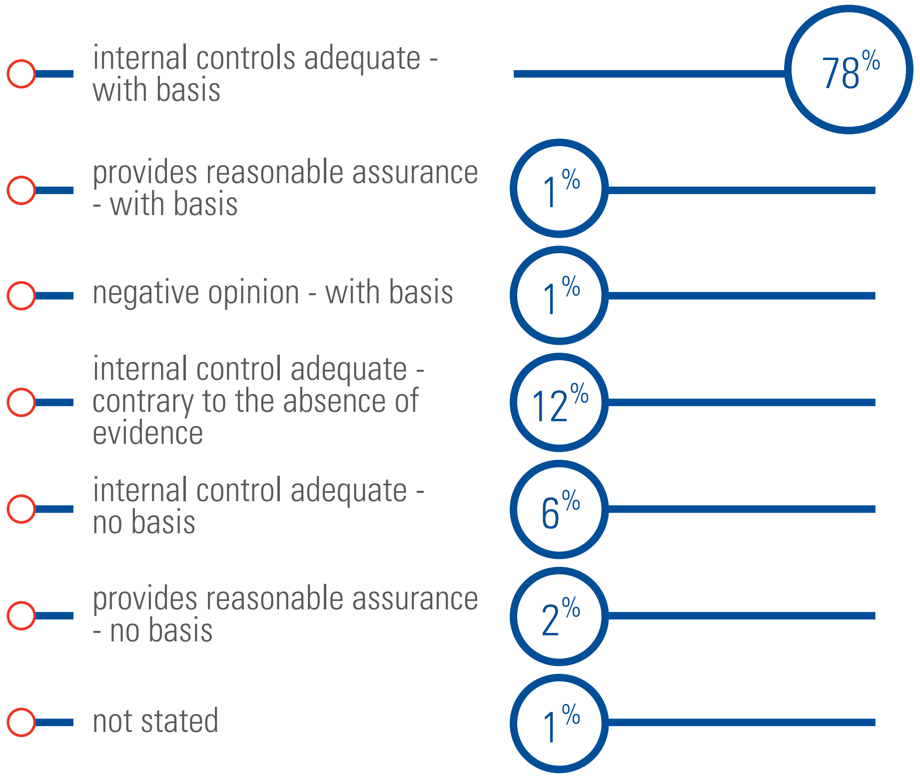
A majority of companies comply with regulatory disclosure requirements, although further work is required to disclose the basis of the opinion

Our study found that most companies have complied with SGX LR 1207(10). As shown in Figure 10, 78% of sampled companies provided positive opinions on the adequacy of their internal controls – including the basis for the directors' opinion – in their annual reports. Looking at our data in Figure 11, large-cap companies (87%) led the pack in complying with the rule compared to mid-caps (83%) and small-caps (76%).

Of the 250 sampled companies, 20% are considered by our study to have not provided a basis for the board's opinion, whether the opinion was stated as adequate internal control or otherwise (refer to Figures 10 and 12). The small-cap category of our sampled companies made up the bulk of the companies that do not provide a basis for their opinions (21% of 190 samples, Figure 12). On the other hand, companies in the finance sector have fully complied with this requirement.

Examples of the different types of opinions given can be found in Appendices 3a and 3b.

figure 10: what is the board's opinion on the adequacy of internal controls? (n=250)



Note: Statistics do not add up to 100% due to rounding

figure 11: percentage of boards stating that internal controls are adequate with basis

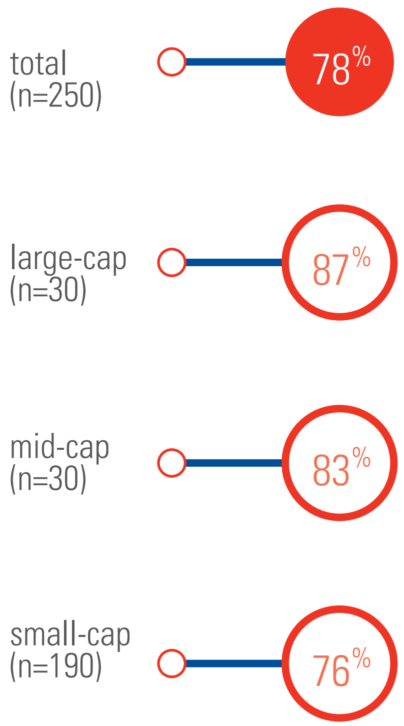
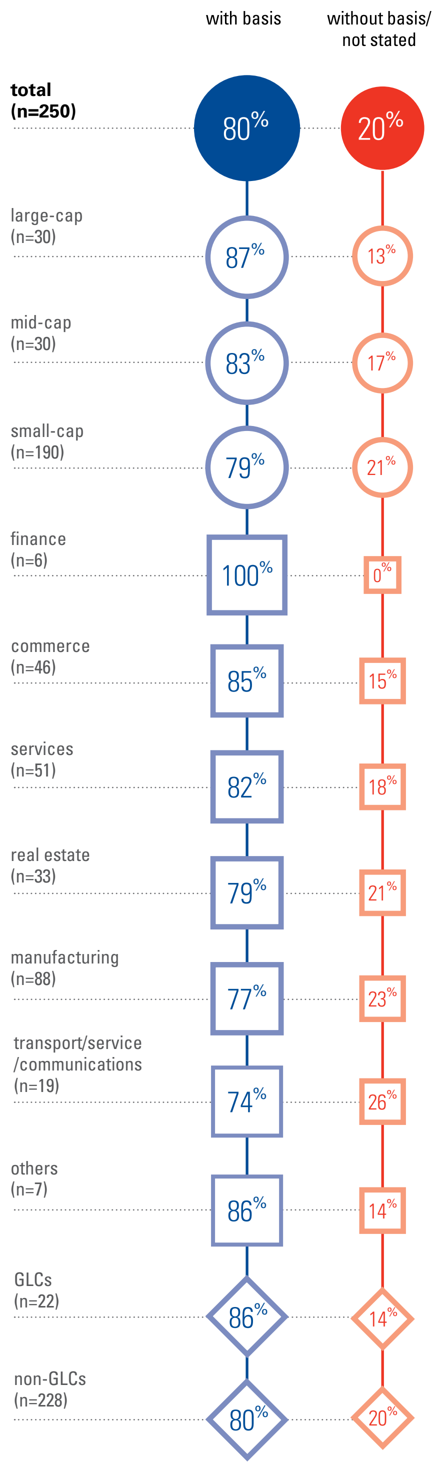


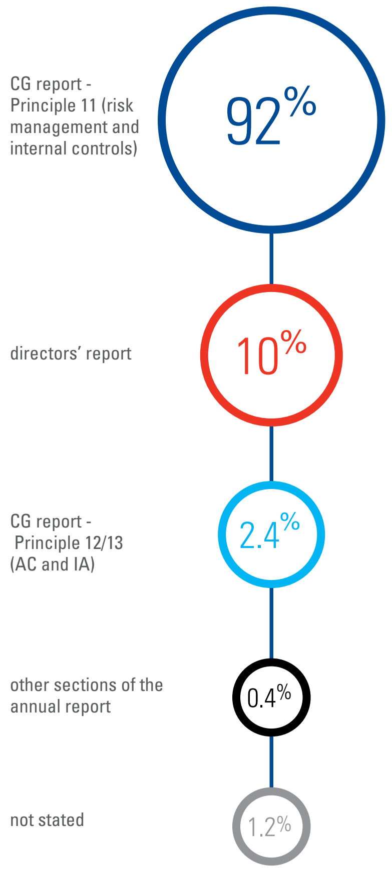
figure 12: board's opinion on internal controls (adequate or otherwise) – with basis or without basis



A majority of companies disclose the board's opinion in the CG report

For compliance with SGX LR 1207(10), SGX recommends that the opinion on internal controls be disclosed in the directors' report or the CG section of the annual report.[19] Our study found that 92% of sampled companies disclosed their opinions in the CG report while 10% of the sampled companies did so in the directors' report (Figure 13).

figure 13: disclosure of the board's opinion on the adequacy of internal controls with basis



Note: Figures add up to more than 100% as companies may report in more than one location.

1.3 'Comply or explain'

P11.3: 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.

Further work is required across all companies to enhance disclosures regarding adequacy and effectiveness of risk management

As shown in Figure 14, our study found that most sampled companies gave an opinion or commented on the adequacy of internal controls (98%) and slightly more than half (55%) also commented on the effectiveness of internal controls. However, only 23% of the sampled companies provided comments on the adequacy of their risk management systems and only 20% of the sampled companies did so for the effectiveness of their risk management systems.

Our findings show that compliance with the mandatory SGX LR 1207(10) is high at 98% for overall sampled companies (Figure 14 and 15). Our mid-cap samples had a 100% compliance rate (Figure 15).

However, only 12% of sampled companies adopted and complied with both the mandatory SGX LR 1207(10) and the full guidelines in

[19] SGX, "SGX-ST LRs Practice Note 12.2: Adequacy of Internal Controls", 2 April 2013.

figure 14: whether the board commented or opined on the adequacy and effectiveness of the company's internal control and risk management systems

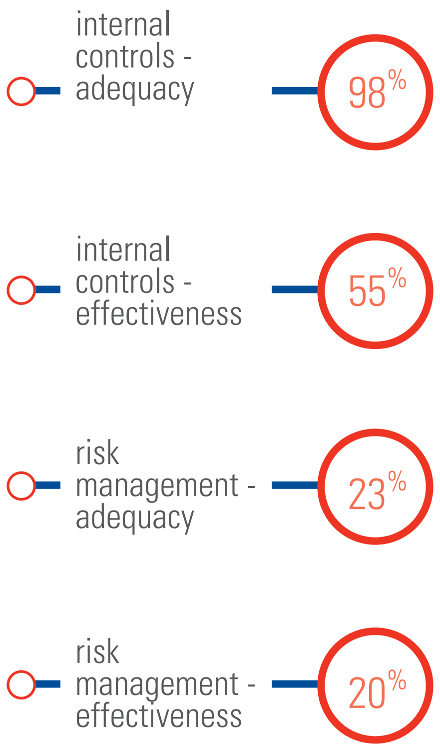
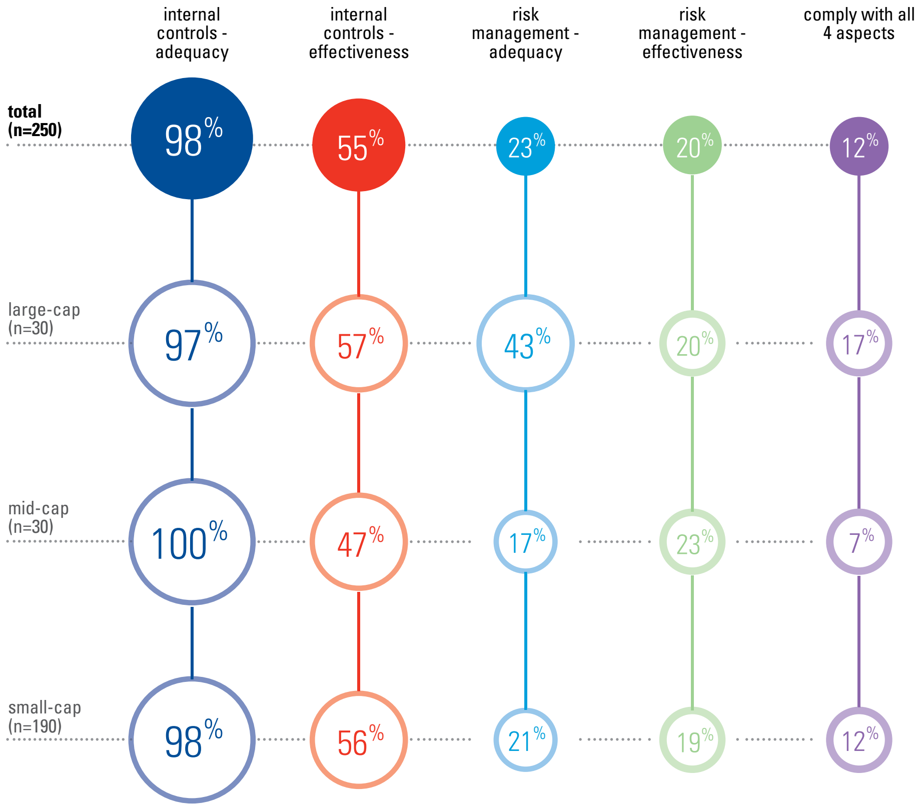


figure 15: whether the board commented or opined on the adequacy and effectiveness of the company's internal control and risk management systems (by market cap)



the revised Code 2012 (i.e. provided an opinion or comment on all four aspects listed in Figure 15). All market capitalisation segments showed only a minority of sampled companies addressing all four aspects of the adequacy and effectiveness of internal controls and risk management. Our data further revealed that large-cap companies are much more likely to comment on the adequacy of risk management compared to mid-cap or small-cap companies (43% versus 17% and 21%, respectively, as shown in Figure 15).

Figure 16 highlights the rate of compliance between GLCs and non-GLCs. Figure 17 shows a similar rate of compliance and adoption of SGX LR 1207(10) (including Practice Note 12.2) across sectors, with the finance sector complying in full. To boost compliance with the SGX LR, further work is required across sectors to disclose the basis of opinion. For the revised Code 2012 and Code 2005, our results indicate that adoption remains low across all sectors and GLCs/ non-GLCs.

figure 16: adoption and compliance rates (GLCs and non-GLCs)

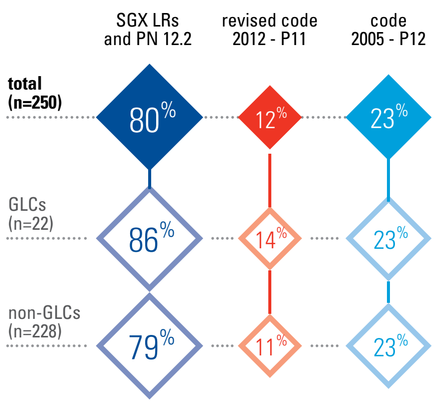
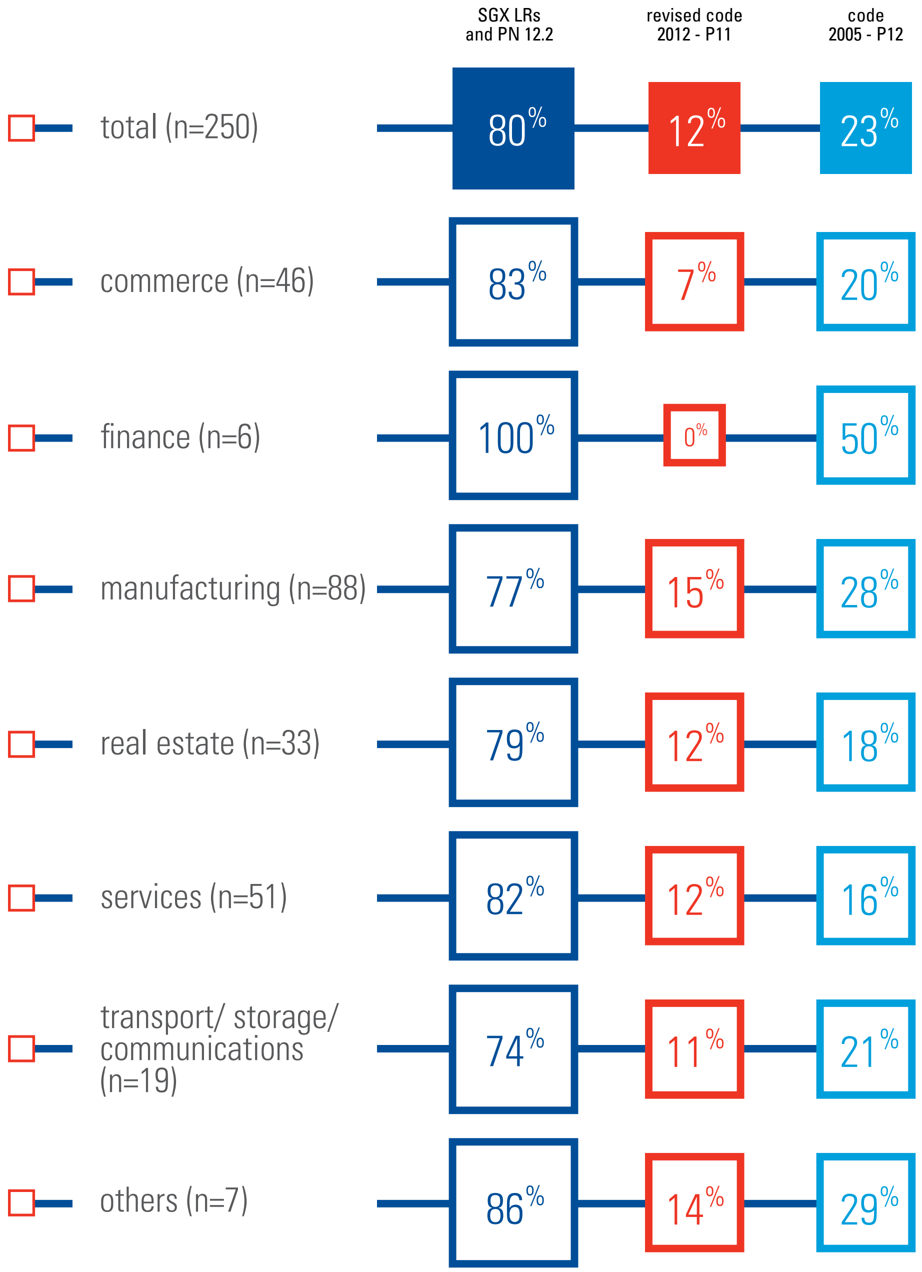


figure 17: adoption and compliance rates across sectors



1.4 Assurance from the CEO and CFO

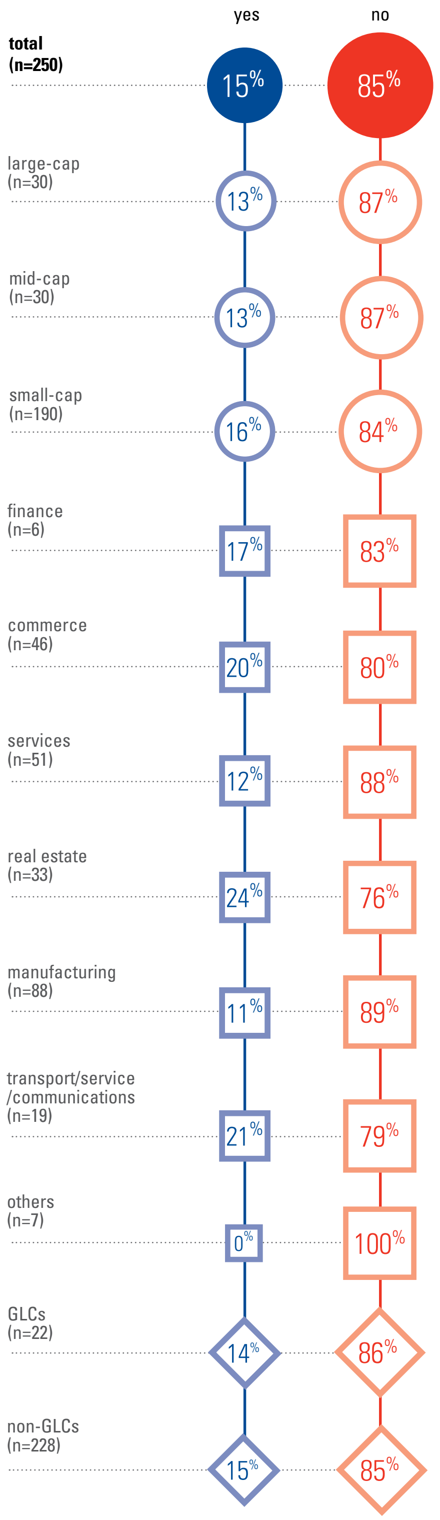
P11.3(b): The board should also comment in the company's annual report on whether it has received assurance from the CEO and CFO regarding the effectiveness of the company's risk management and internal control systems.

The revised Code 2012 has raised the standard for risk management disclosures beyond simply requiring the disclosure of the board's opinion on the company's risk management and internal control systems. The Code 2012 advocates that the board comment on whether it has received assurance on the effectiveness of the company's risk management and internal control systems from the CEO and CFO.

Our study found, as Figure 18 shows, that only 15% of all sampled companies disclosed having received assurances regarding the effectiveness of risk management and internal control systems from their CEO and CFO. Further analysis revealed that this low rate is consistent across all market capitalisations and all sectors, as well as across both GLCs and non-GLCs.

Key findings: 2. Risk governance and oversight structures

figure 18: did the company disclose that the CEO and CFO provided assurance?



Given the low 15% disclosure rate across all sampled companies (Figure 18) for whether the board has received assurance regarding the effectiveness of the company's risk management and internal control systems from the CEO and CFO, we conducted further analysis to understand whether the disclosure rate varies depending on different profiles. As shown in Figures 19, 20 and 21, we found no significant differences across profiles.

figure 19: assurance from CEO and CFO when the BRC or AC oversees risk management

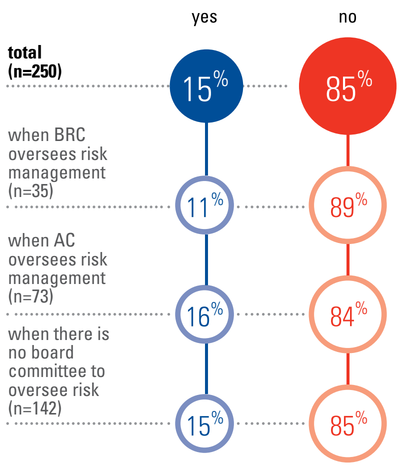


figure 20: assurance from CEO and CFO when there is a CRO

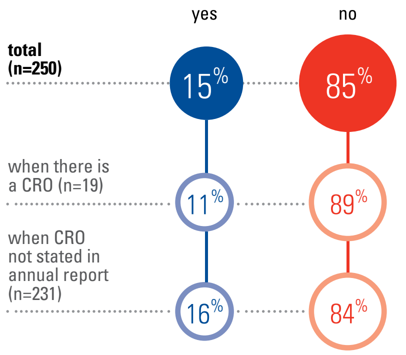
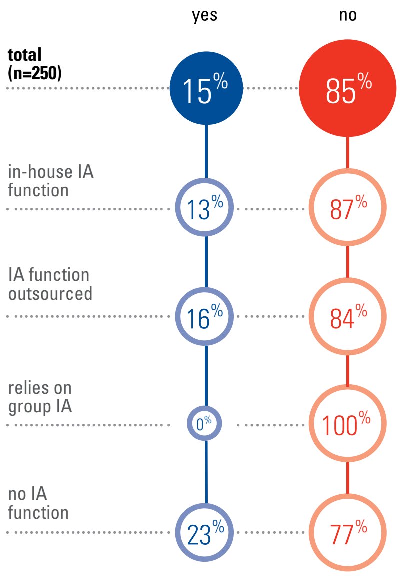
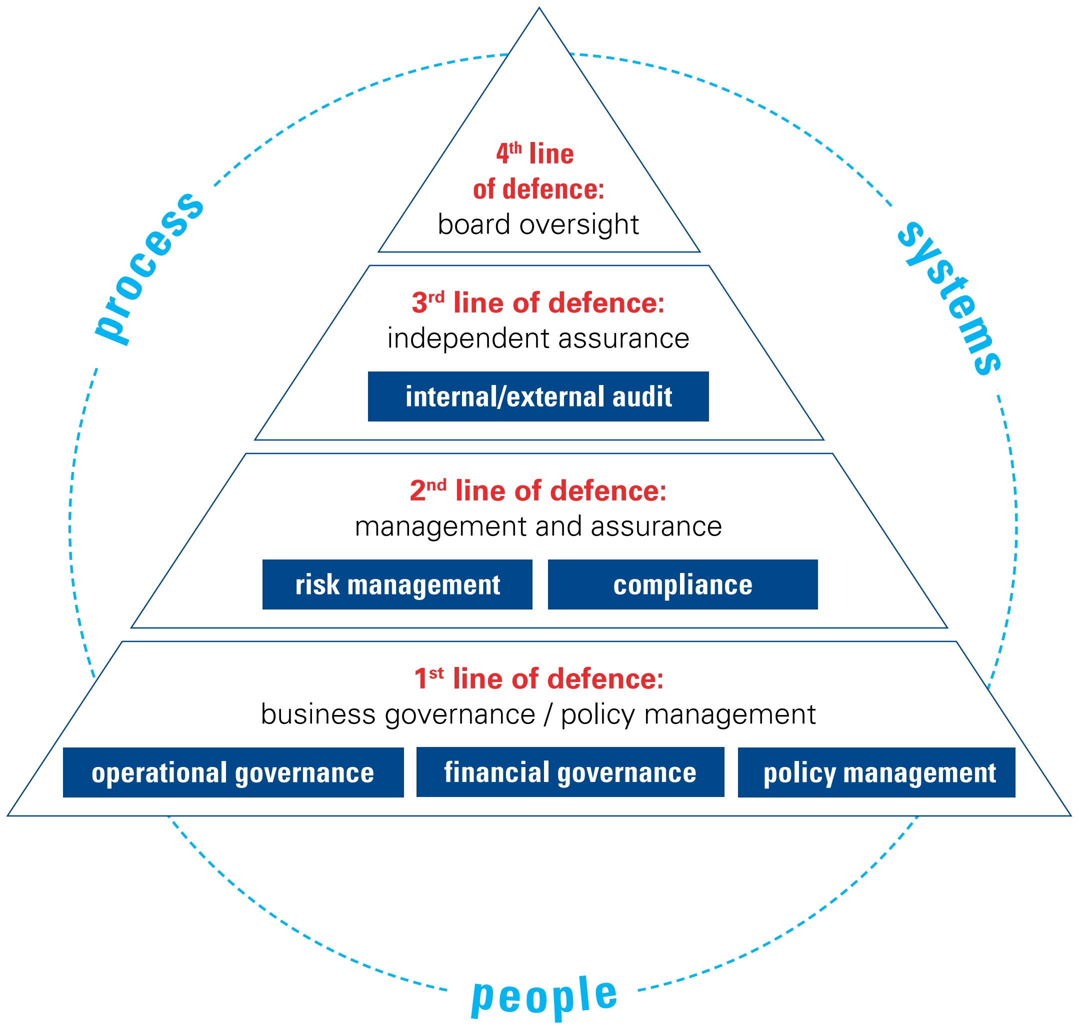


figure 21: assurance from CEO and CFO when there is an IA function



KPMG's 4 Lines of Defence model, as outlined in Figure 22 below, can serve as a useful basis to further understand the key elements of 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 22: KPMG's 4 Lines of Defence model



2.1 Board

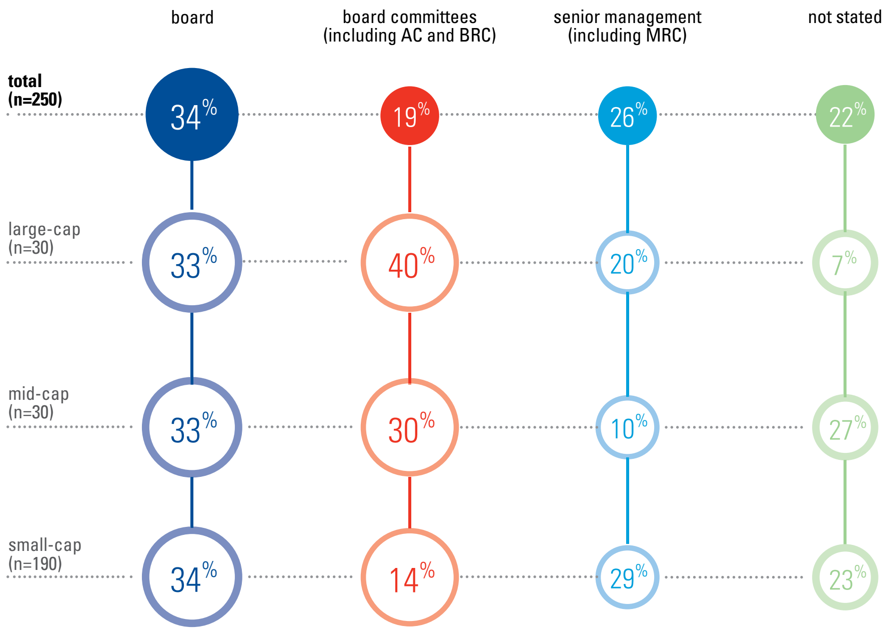
P11: The board is responsible for the governance of risk. The board should ensure that management maintains a sound system of risk management and internal controls to safeguard shareholders' interests and the company's assets, and should determine the nature and extent of the significant risks which the board is willing to take in achieving its strategic objectives.

The revised Code 2012 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.

Inconsistent disclosure of ultimate responsibility for risk

Our study shows in Figure 23 that companies are not consistent in disclosing who is responsible for risk governance in their organisation. Only 34% of companies disclosed in their annual report that their board is responsible for risk governance – this is consistent across the large-cap, mid-cap and small-cap companies sampled. Among all companies sampled, 19% rely on their board committees for risk governance; 26%, particularly among the small-caps, stated that management is responsible for risk governance; and 22% did not disclose who is responsible for risk governance.

figure 23: who is responsible for governance of risk?



Note: Statistics do not add up to 100% due to rounding. Also a number of annual reports did not identify those responsible for risk governance clearly. The researchers have coded the information using their best judgment.

2.2 Board committees

P11.4: 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.

The revised Code 2012 expresses that the board is responsible for risk governance. To receive assistance in carrying out the risk oversight function effectively, the board may consider setting up a separate BRC. Given the increasingly complex business environment, especially for companies operating in multiple jurisdictions, setting up a BRC may be necessary to provide adequate oversight of risk matters.

BRCs are becoming more common, although there is a need for improved clarity regarding committee roles related to risk

Overall, 43% of the 250 sampled companies have either the BRC (14%) or AC (29%) assist the board in risk management. Based on market capitalisation, our study found that 63% of sampled large-cap companies have formed BRCs, compared to just 27% of sampled mid-cap companies and 4% of sampled small-cap companies. Mid-caps and small-caps tend to incorporate the risk oversight function in the responsibilities of the AC (43% and 27%, respectively).

In some sampled companies, ACs that have been tasked with risk oversight responsibilities were renamed as audit and risk committees (ARC) or something similar. For the purpose of our study, both BRCs and ARCs are collectively referred to as BRCs.

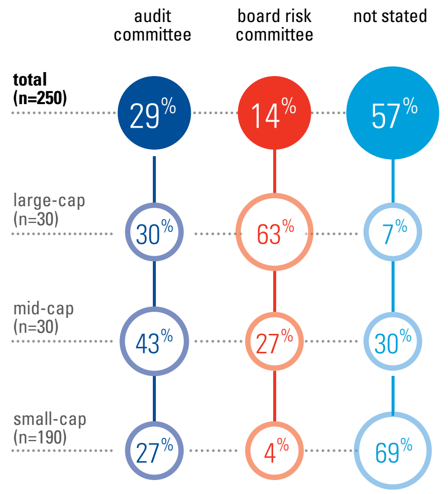
Our study found that 57% of the sampled companies failed to disclose having either their AC or BRC to support the board in carrying out its risk oversight responsibilities (see Figure 24). This figure is driven predominantly by the small-cap companies, of which 69% failed to state which board committee is responsible for risk oversight.

Clarifying the role of the board and board committees is an essential part of the disclosure process to assist stakeholders in understanding where ultimate accountability for risk sits. It also helps them understand how the interrelationships between the board and board committees are structured to ensure that there are no gaps or duplication of effort.

Our study found that BRCs are more common among GLCs (55%) than non-GLCs (10%) as shown in Figure 25.

Figure 26 shows by sector, that the finance sector leads the pack with 67% of the sampled companies in this sector having formed a BRC. The transport/storage/communications sector comes in second with 42% having formed BRCs. These findings indicate that companies operating in sectors deemed more complex and demanding – for example, finance and communications – have taken steps to enhance their risk management capabilities or structures even though the Code 2005 did not mention BRCs.

figure 24: which board committee helps the board to oversee risks?



Note:
For the purpose of this study, BRCs and ARCs are collectively referred to as BRCs

figure 25: companies with BRC (GLCs and non-GLCs)

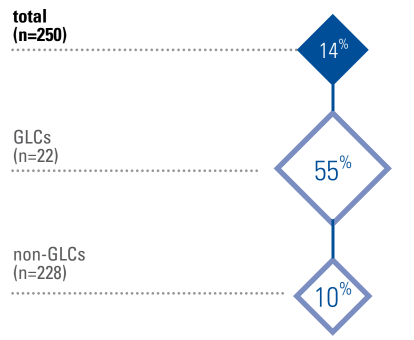
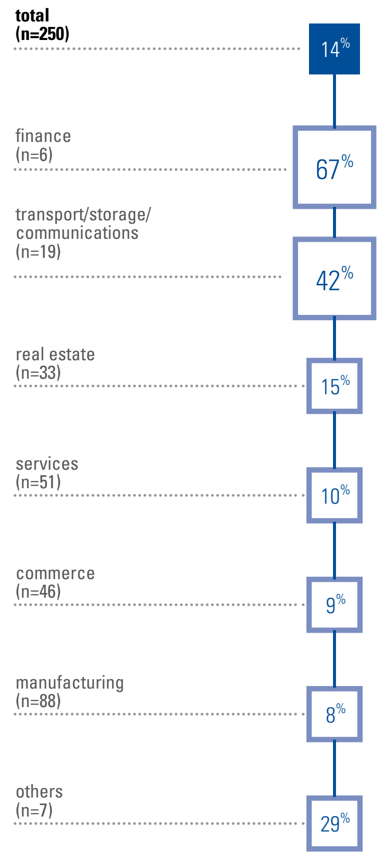


figure 26: companies with BRC (by sector)



BRCs have a strong independent composition

The ability of the board to provide independent oversight is a key pillar of effective governance. Among the sampled companies with a BRC, 80% disclosed that their BRC chair is independent as highlighted in Figure 27. This is in line with the general principles of the Code, which advocate that the chairman of a board committee should be independent.

Furthermore, our study found that among the 35 sampled companies with a BRC, 72% reported that independent directors make up more than half of the BRC's composition (see Figure 28). Having more than half of the BRC made up of independent directors was more common among large-cap companies (79%) than among mid-caps and small-caps (both at 63%).

figure 27: is the BRC chairman independent?

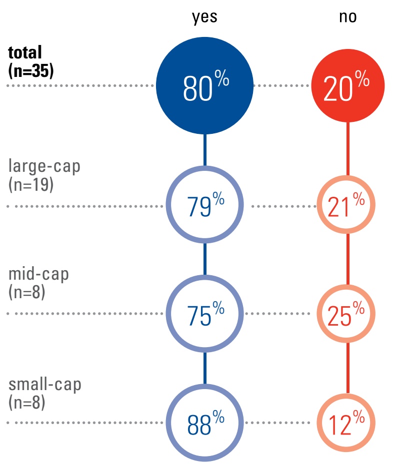
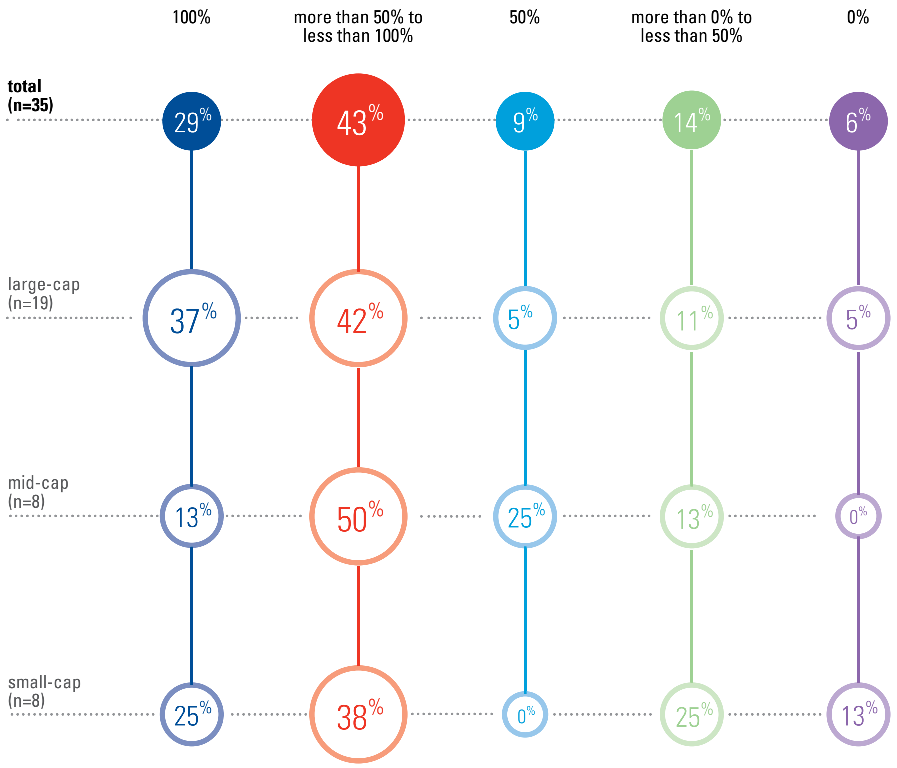


figure 28: proportion of independent directors on the BRC



Note: Statistics do not add up to 100% due to rounding

BRC committee size and frequency of meetings similar to AC

Our study found that the average committee size and number of meetings for BRCs is similar to those of ACs. On average, a BRC has four directors and meets about four times per year (see Figure 29). In addition, our findings show that there were no significant changes to the BRC committee size and number of meetings over the past two financial reporting periods (FY10/11, FY11/12).

However, the number of BRC meetings held by the sampled small-cap companies with BRCs (n=8) increased substantially in FY11/12. Further analysis indicates that the higher number of meetings recorded for some small-cap companies (n=3) was due to the formation of an ARC to provide oversight of financial reporting matters, audit activities and risk functions. Whilst the sample size is small, it is encouraging to see a slight increase in the frequency of meetings as this reflects recognition of the increase in responsibilities.

Common membership between AC and BRC

According to the Risk Governance Guidance for Listed Boards 2012, it is important that communication is maintained between the BRC and AC.[20] Our findings indicate that overlapping membership by individual directors across the two board committees is relatively common. Only a minority (14%) of the sampled companies' BRCs had no BRC members who also sit on the AC of the same board (see Figure 30).

We note that overlapping membership across both the BRC and AC within the same company is relatively common. Of the 35 sampled companies with a BRC, 60% indicated that at least half of their BRC members also sit on the AC of the same board. BRCs of small-cap companies have the highest proportion of cross-membership spanning the two board committees. Whilst this is effective for sharing of information, care must be taken to plan AC and BRC agendas and meetings to optimise time and clarify the roles of each committee.

[20] MAS Corporate Governance Council, "Risk Governance Guidance for Listed Boards", 10 May 2012.

figure 29: average BRC size and number of meetings held (n=35)

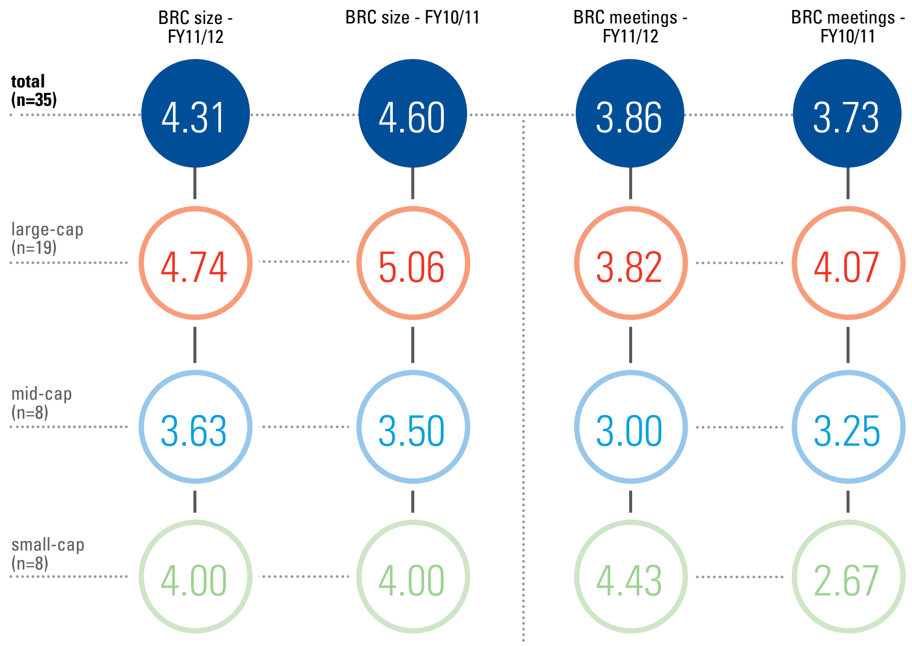
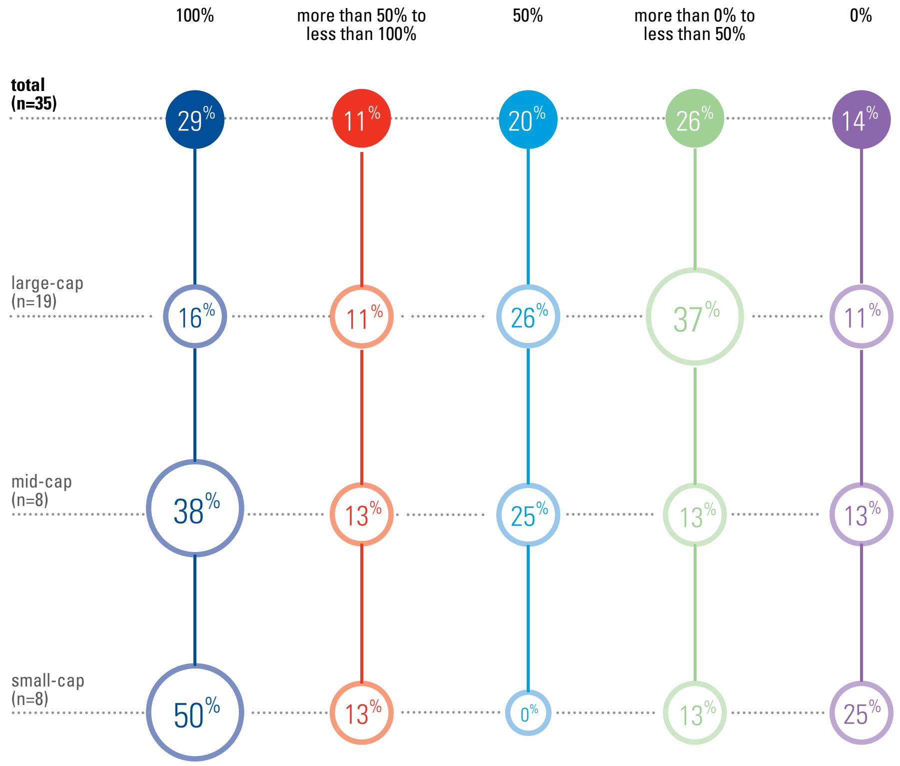


figure 30: percentage of BRC members who are also AC members on the same board



Note: Statistics do not add up to 100% due to rounding

BRCs are linked to more mature risk management practices

Based on the risk management disclosures made in the annual reports we reviewed, we found that the sampled companies with BRCs are more likely to have established other risk management structures. Our study found that the boards of sampled companies with BRCs are more likely to appoint a CRO (34% versus 3% for companies without a BRC; see Figure 31), establish an in-house IA function (69% versus 27% for companies without a BRC; see Figure 32) and disclose their risk management framework (71% versus 40% for companies without a BRC; see Figure 33).

figure 31: do companies with a BRC disclose having a separate CRO?

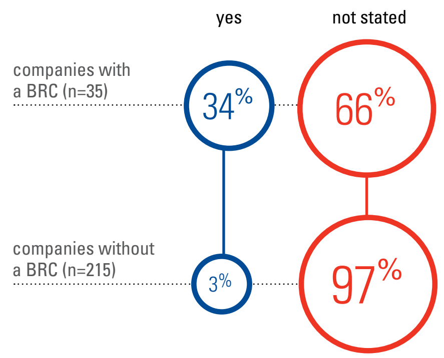


figure 32: do companies with a BRC have an IA function?

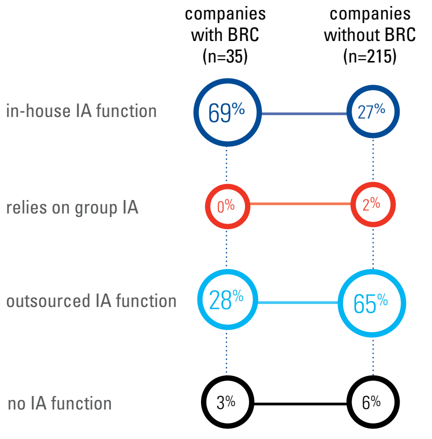
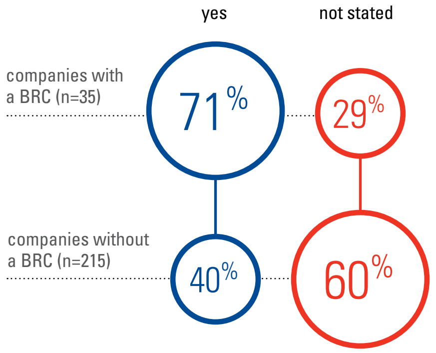


figure 33: do companies with a BRC disclose their risk management framework?



AC composition remains the same but frequency of meetings has increased, reflecting an increased role

Our study found that 29% of sampled companies rely on their AC for the oversight of risks (see Figure 24). This highlights that in addition to overseeing risks pertaining to the integrity of the financial statements[21], ACs have the added responsibility of risk management. Among the 250 companies included in our study, 73% of them have three directors on the AC (see Figure 34). While a majority of the large-cap companies have three or four directors on the AC, most mid-cap and small-cap companies have only three directors on their boards – the minimum number required by legislation (Companies Act and Code). This finding is consistent across all sampled sectors (see Figure 35).

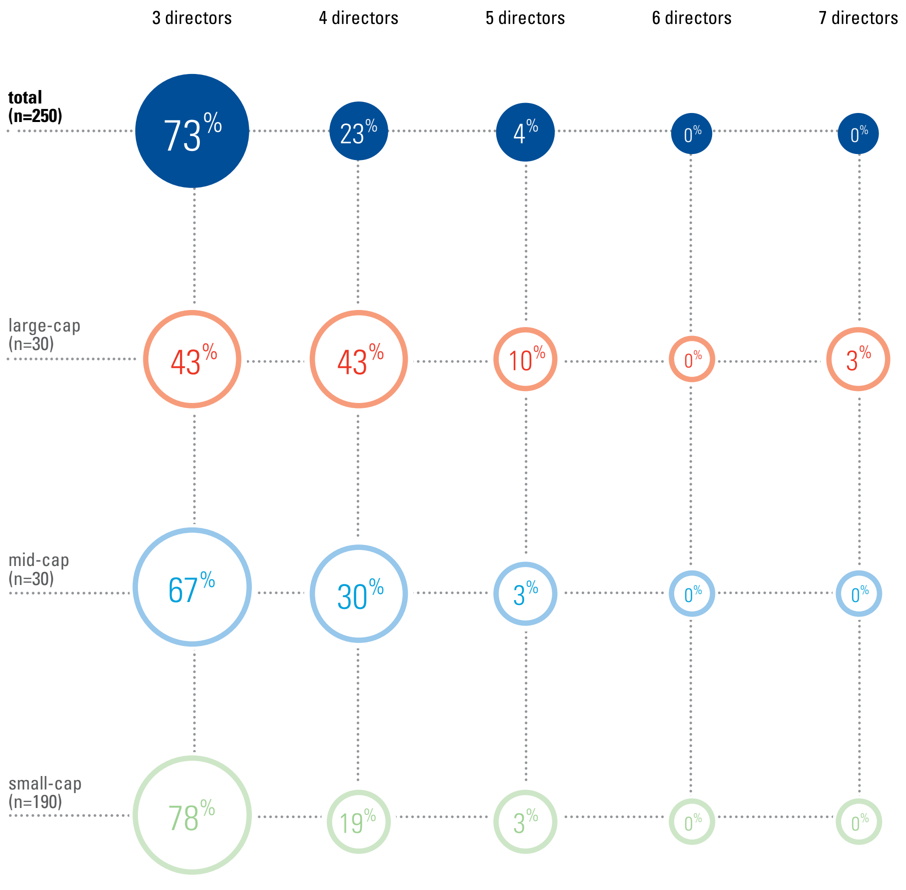
Despite the increased emphasis on risk management during the past few years, AC size and activities remained fairly consistent across the past two financial reporting periods (FY10/11 and FY11/12). Our findings indicate that sampled large-cap companies have slightly larger ACs compared to the mid-caps and small-caps. In addition, the ACs of large-cap companies met more frequently, averaging 5.1 meetings in FY11/12 compared to the overall average of 4.08 meetings for all sampled companies (see Figure 36). This is consistent with the reporting requirements of SGX LR 705, which requires companies with market capitalisation exceeding S$75 million to perform quarterly reporting of their financial results.

Among the 29% of sampled companies that rely on their AC to help the board provide oversight of the company's risk governance and management (see Figure 24), it would be reasonable to expect the size of these companies' ACs to increase and for their members to meet more often. This expectation would make sense given the need to discharge expanded responsibilities beyond the traditional AC scope, which includes financial reporting, internal controls and audit.

However, our study found few differences among the sampled companies to differentiate those with ACs bearing expanded risk management responsibilities and those with ACs not disclosed as bearing these additional responsibilities. Across these two groups of ACs, there were comparable results (see Figure 37) for number of directors (about 3) and number of meetings per year (about 4).

The only notable difference was in the number of meetings per year among large-cap companies. The ACs of sampled large-cap companies did meet more frequently (5.44 times) when they are in charge of risks compared to ACs of sampled large-cap that do not explicitly state that they are responsible for risk management (4.50 times).

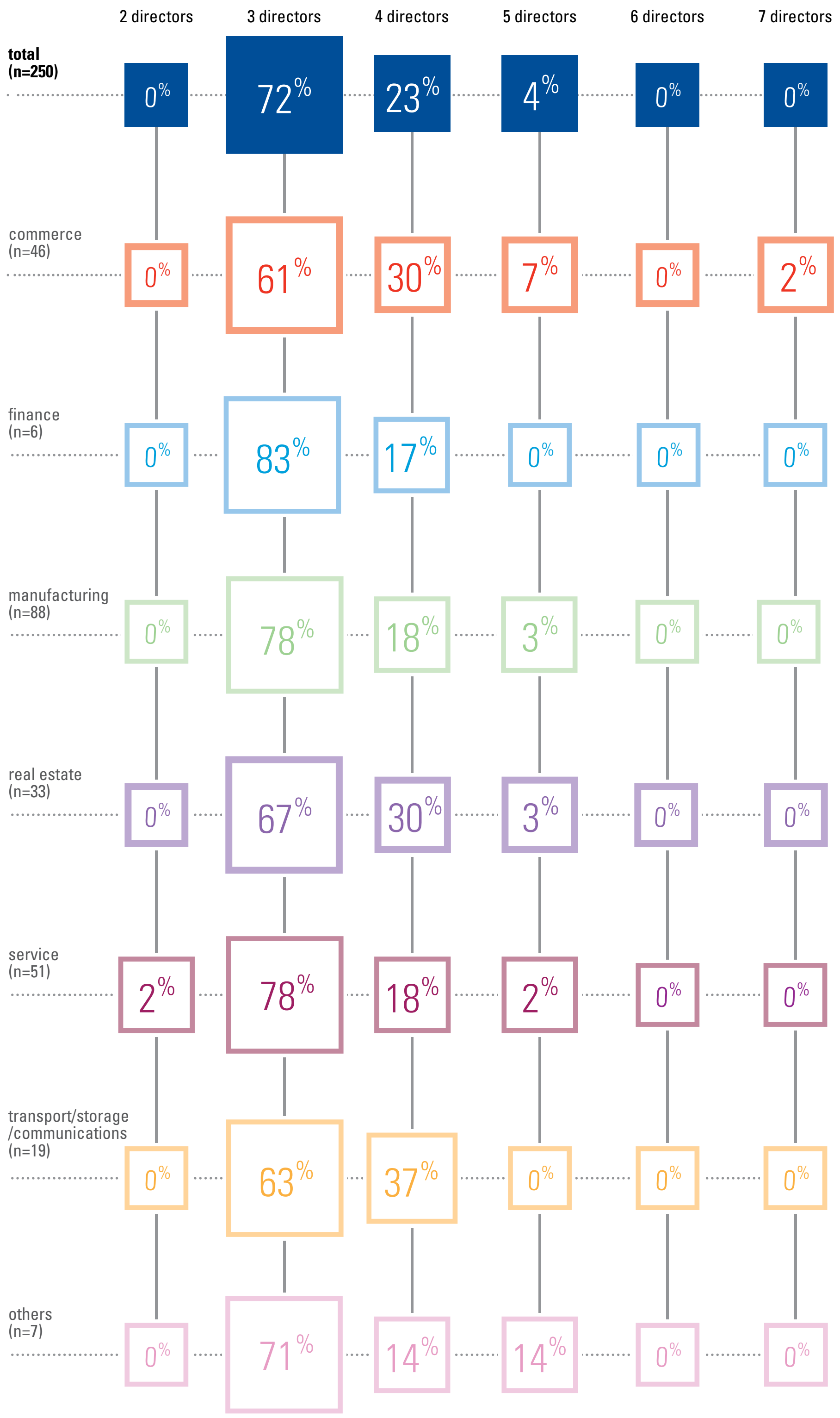
figure 34: AC size – number of directors by market cap



Note: Statistics do not add up to 100% due to rounding

[21] MAS Corporate Governance Council, "Risk Governance Guidance for Listed Boards", 10 May 2012.

figure 35: AC size – number of directors by sector



Note: Statistics do not add up to 100% due to rounding figure 36: average AC size and number of meetings held

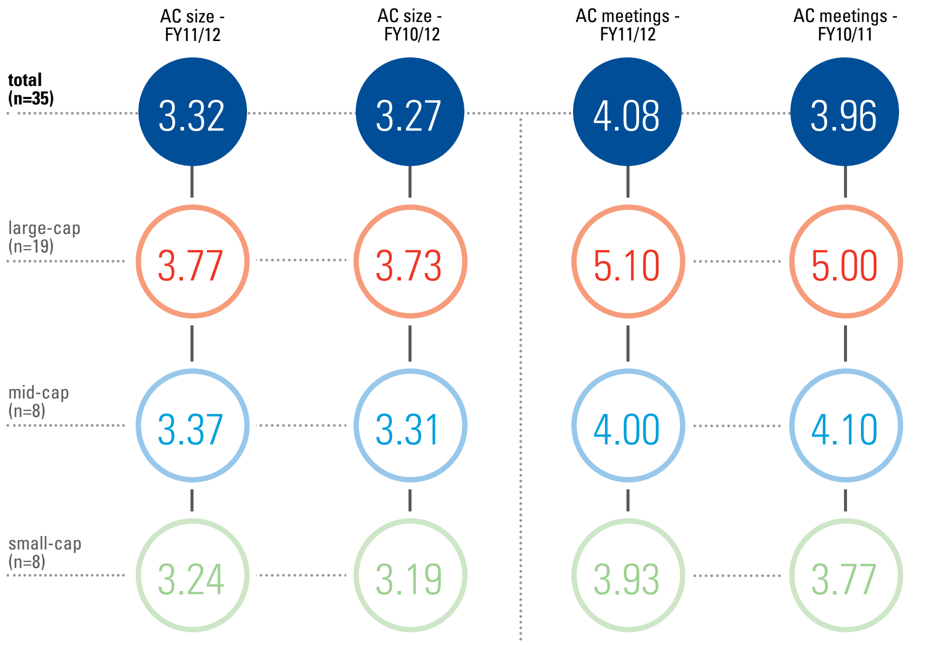
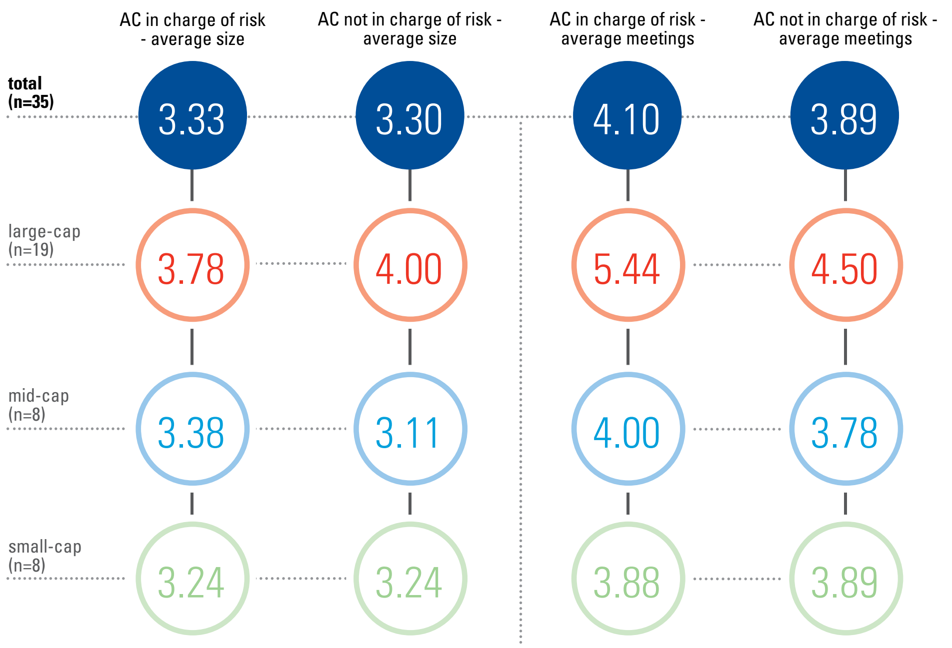


figure 37: comparison of ACs with and without risk management responsibilities



2.3 Management (C-suite)

Varied disclosures regarding responsibility for risk at the C-suite level

A global study conducted by KPMG found that risk management is deemed essential by C-suite executives for adding value to their businesses.[22] Despite its importance, our study revealed that only 15% of the sampled companies disclosed that their C-suite is responsible for risk management. While half of the sampled large-cap companies disclosed in their annual report that someone at the C-suite level is responsible for risk management, only 19% of the mid-caps and 10% of the small-caps did the same (Figure 38).

Our further analysis shows that among the mid-caps and small-caps that made this disclosure, it was most commonly the CFO who took on the addition role of risk management oversight. 70% among mid-caps (i.e. 14% out of 20% that disclosed) and 44% among small-caps (i.e. 4% out of 9% disclosed). On the other hand, large-cap companies were most likely to assign the risk management duties to a CRO (60%).

Incidentally, our study also found that of the 35 sampled companies with a BRC, 34% also have a separate CRO (Figure 31). This is a significantly higher proportion than the 3% seen for sampled companies without a BRC (Figure 31). This suggests that it is more common for companies with a BRC to appoint a C-suite executive to oversee risk management and is reflective of the increased focus on establishing an effective risk management framework.

The role of a dedicated CRO remains uncommon

The KPMG global study revealed that senior executives find that the assessment and management of risks for their companies is becoming increasingly challenging.[23] This corresponds with the findings from an earlier ISCA study that surveyed 144 CFOs in Singapore. In that study, 76% of the respondents indicated they spent moderate or most of their time on risk management matters.[24]

The findings from these KPMG and ISCA studies appear to indicate that CFOs are spending more of their time on risk management relative to their more traditional role of overseeing the financial aspects of the business. These findings suggest that boards of listed companies should consider appointing a CRO to provide executive oversight of risk management efforts if circumstances and resources allow them to do so.

However, our recent study shows that most companies do not appoint additional C-suite executives to provide oversight of either risk management or internal controls. Only 5% of all sampled

figure 38: who is responsible for risk management at the C-suite level?

figure 39: companies with a CRO

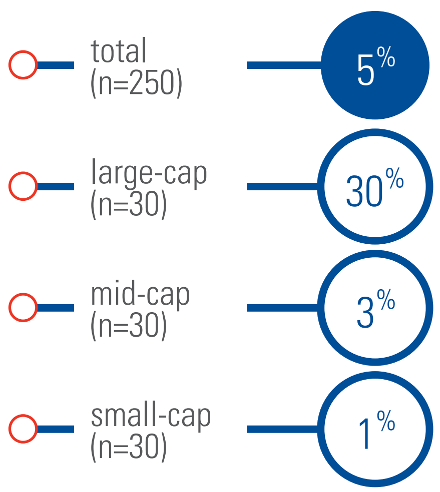
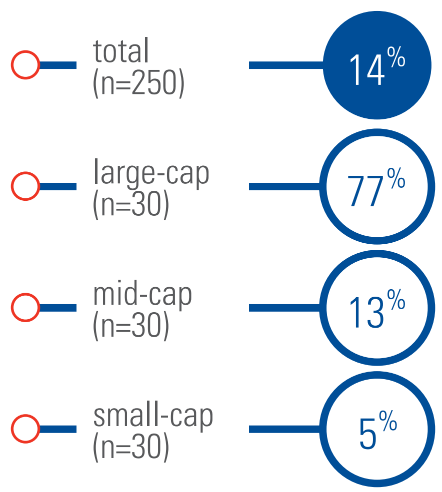


figure 40: companies with a CAE



[22] KPMG International, "Expectations of Risk Management Outpacing Capabilities – It's Time For Action", 2013.

[23] KPMG International, "Expectations of Risk Management Outpacing Capabilities – It's Time For Action", 2013.

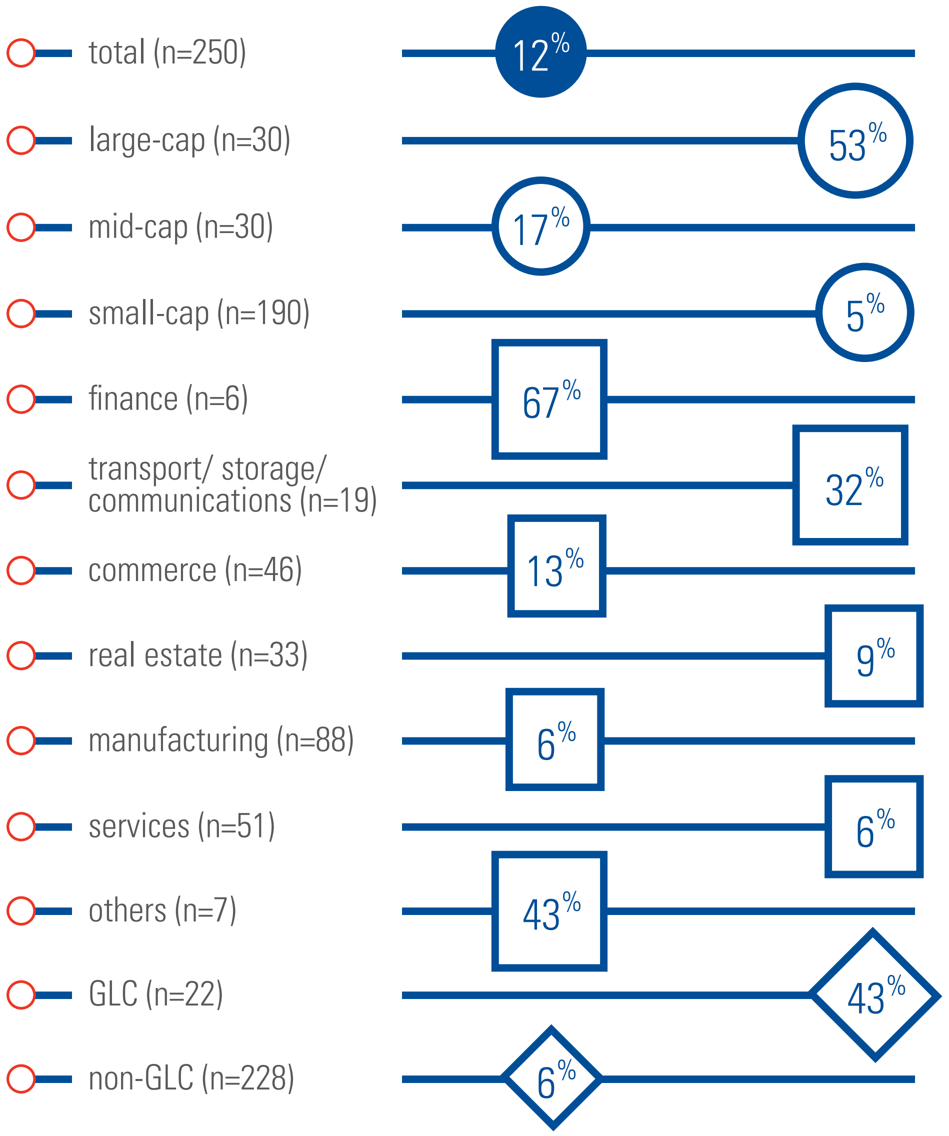
[24] Institute of Singapore Chartered Accountants (formerly Institute of Certified Public Accountants of Singapore), "ICPAS CFO Study – Beyond Finance: Competencies for the Modern CFO", October 2012.

companies have a CRO or its equivalent, and only 14% have a chief audit executive (CAE) (see Figures 39 and 40).

The companies that have higher instances of appointing additional C-suite executives tend to be the sampled large-cap companies. This could be due to the size of such companies and the complexity of their operations.

Among the companies that have appointed a CRO to assist the board in risk oversight, only a handful disclosed background information about their CRO in their annual report. This information may be as important to shareholders as information about the rest of the C-suite. As such, guidance from the authorities regarding what information to disclose in annual reports may be helpful.

figure 41: companies with a MRC



Disclosure of non-board MRCs remains uncommon

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 are linked.[25] 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.

Apart from appointing a CRO to provide executive risk oversight, our study found that 12% of the sampled companies disclosed that they have formed an MRC to manage risks (see Figure 41). Among these 30 sampled companies, 53% are large-caps, 17% are mid-caps and 5% are small-caps. The two sectors with the highest percentage of companies with an MRC are the finance sector (67%) and the transport, storage and communications sector (32%). In addition, nearly half (45%) of the GLCs in our sample have established an MRC as part of their risk management structure.

[25] KPMG International, "Expectations of Risk Management Outpacing Capabilities – It's Time For Action", 2013.

2.4 Internal audit function

P13: The company should establish an effective internal audit function that is adequately resourced and independent of the activities it audits.

According to the IIA, internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by applying a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.[26]

To assess the adequacy of internal controls, addressing financial, operational and compliance risks, the board and AC should seek support from the management, IA, compliance and risk management functions (if applicable) to monitor the existing activities and records relating to risk management and internal controls. IA is one of the sources that can assist the board in forming the basis of its opinion as required under SGX LR 1207(10). In addition, an effective IA function enhances corporate governance, risk management and internal controls.

The IA function, which can be in-house or outsourced, plays an important role to provide reasonable assurance and validation of existing internal controls. While having an internal auditor is currently seen as best practice, there are investor groups advocating for an independent IA function to be part of the SGX Listing Rules and for companies to include the IA report in their annual reports.[27]

Most companies have an IA function

As illustrated in Figure 42, our findings show that the majority of the sampled companies (94%) have an IA function. By market capitalisation, the majority of the large-cap companies have in-house IA function (90%), while most mid-caps and small-caps outsource their IA function (67% and 68%, respectively). This finding is consistent with the findings of another recent study performed by KPMG in which 44% of CAEs indicated that co-sourcing or outsourcing is the most cost-efficient means to obtain a diverse range of skill sets, which otherwise may not be fully utilised in an in-house setup.[28]

However, it should be noted that the number of small-cap companies with outsourced IA functions in place seems relatively high (68%) compared to the results of a recent survey conducted jointly by the SAC and KPMG titled "Taking the Pulse – A Survey of IA in Singapore 2013" which indicated only one third of Singapore companies surveyed had an outsourced IA function.

The lack of information about the nature, scope, coverage and spend on IA functions in annual report disclosures creates challenges for users of this information to draw conclusions as to the effectiveness of the IA functions to support board, AC and management to validate the adequacy and effectiveness of the risk management and internal control system. This anomaly highlights the challenges in relying solely on disclosures.

Further work is required to disclose adoption of IIA Standards

The IIA, which is a global guidance-setting body, provides IA professionals worldwide with useful guidance. The IIA Standards (Standards) are meant to be principle-focused and provide a framework for performing and promoting internal auditing.

The Standards include statements outlining the basic requirements for the professional practice of internal auditing and for evaluating the effectiveness of the function. This helps to establish the basis for the evaluation of IA performance and can be useful in improving organisational processes and operations. A company's IA function may be perceived to be

[26] The IIA, "Definition of Internal Auditing", taken from the International Professional Practices Framework (IPPF) 2013 Edition
[27] Jared Heng, "Internal Audit Should be Part of SGX's LRs: SIAS", 11 October 2011.
[28] SAC and KPMG, Internal Audit Survey 2013.

relatively more effective or of higher quality if it is aligned with international standards. When a company discloses that it has met the Standards, this should be perceived positively amongst stakeholders.

Of the 237 companies in our study that have disclosed that they have an IA function, we found that only 39% have disclosed that they have met the Standards (Figure 43). By market capitalisation, 77% of the large-cap companies have made such disclosure, while only 43% of the mid-caps and 32% of small-caps have done likewise. The higher percentage of large-cap companies disclosing they have met the Standards may be due to such companies having the scale and resources to ensure compliance with the Standards.

figure 43: proportion of companies disclosing that their IA function meets IIA standards

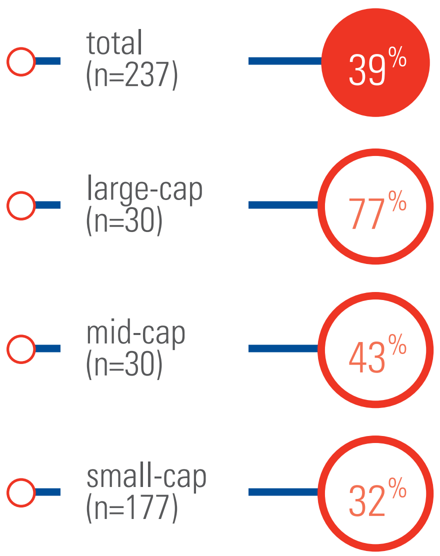
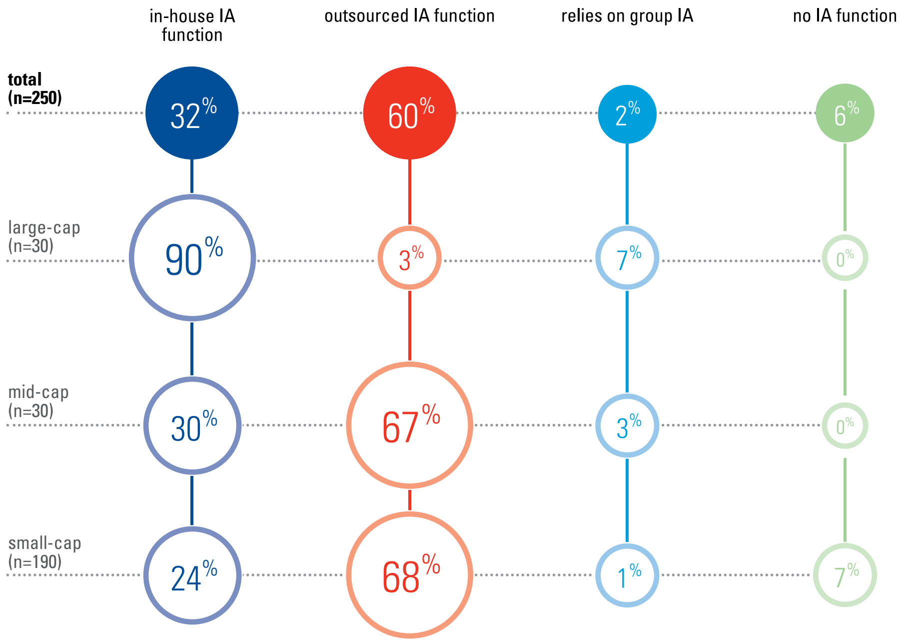


figure 42: IA function



Key findings: 3. Risk management system

3.1 Risk management framework

P11.1: The board should determine the company's levels of risk tolerance and risk policies, and oversee management in the design, implementation and monitoring of the risk management and internal control systems.

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 executives, 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.

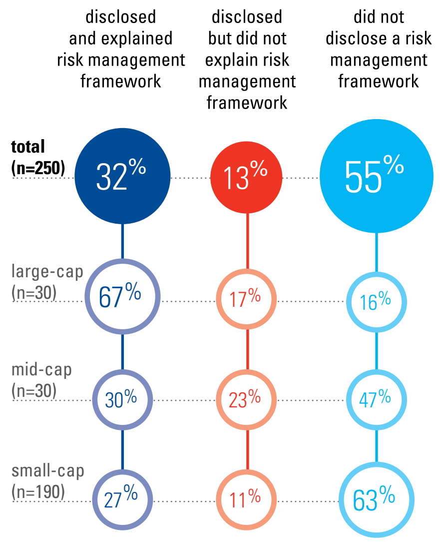
Further work is required to disclose and explain the risk management framework

Our study shows in Figure 44, that only 45% of the 250 sampled companies have 'disclosed' having a risk management framework.

Furthermore, only 32% of sampled companies have explained the framework in their annual report.

Further analysis reveals that a greater proportion of large-cap companies (67% of the large-cap sample) have disclosed and explained their framework compared to mid-caps (30% of the mid-cap sample) and small-caps (27% of the small-cap sample). This suggests that more focus is required by small-cap and mid-cap companies to establish appropriate risk management frameworks, including setting risk policies and risk tolerance levels and establishing a robust process for measuring, monitoring and managing risk.

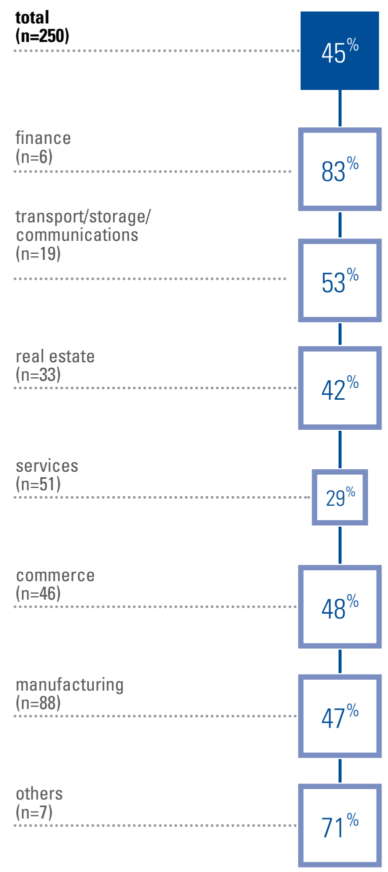
figure 44: disclosure of risk management framework in the annual report (by market cap)



Note: Statistics do not add up to 100% due to rounding

Furthermore, apart from the finance and transport/storage/communications sectors, and excluding the companies categorised in the 'others' sector, less than half of the companies in the remaining sectors have disclosed having frameworks to evaluate and manage their risks (see Figure 45).

figure 45: disclosure of risk management framework in the annual report (by sector)



3.2 Whistle-blowing policy

P12.7: The AC should review the policy and arrangements by which staff of the company and any other person may, in confidence, raise concerns about possible improprieties in matters of financial reporting or other matters. The AC's objective should be to ensure that arrangements are in place for such concerns to be raised and independently investigated, and for appropriate follow-up action to be taken. The existence of a whistle-blowing policy should be disclosed in the company's Annual Report, and procedures for raising such concerns should be publicly disclosed as appropriate.

Setting up formal whistle-blowing procedures within an organisation can help strengthen corporate governance and ethics in the organisation, in addition to being a useful risk management tool. Currently, there is no mandatory requirement for companies under the Companies Act or SGX Listing Rules to have whistle-blowing policies in place in Singapore.

To highlight their importance, the Sarbanes-Oxley Act of 2002 formalised the whistle-blower programmes for publicly held US companies. In Section 301, it requires the AC of a publicly listed company to establish a complaint notification, or whistle-blower, system in order to facilitate the receipt, retention and treatment of complaints received by the issuer regarding accounting, internal accounting controls or auditing matters.

According to a report by the Association of Certified Fraud Examiners (ACFE) titled "2012 Global Fraud Study", whistle-blowing (tips) from employees, customers, vendors, and other sources remained the most common detection method (43%), catching nearly three times as many frauds as any other form of detection.[29] This remains by far the most common means of detection.

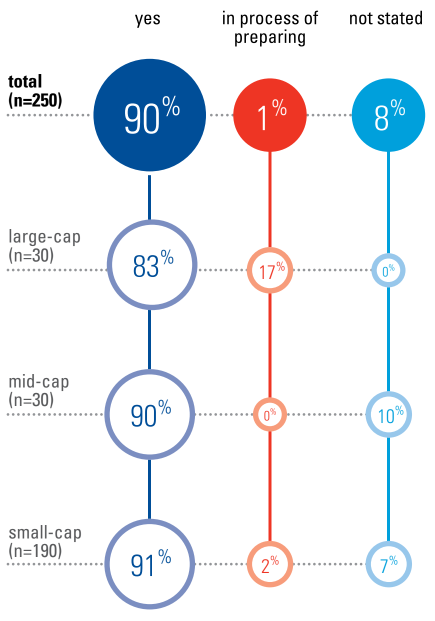
Most companies have a whistle-blowing policy

Our study found that a majority of the sampled companies (90%) have disclosed that they have a whistle-blowing policy in place. Interestingly, the proportion of small-cap companies that have disclosed having a whistle-blowing policy (91%) is slightly higher compared to large-cap companies (83%) (see Figure 46).

Further work is required to disclose whistle-blowing channels

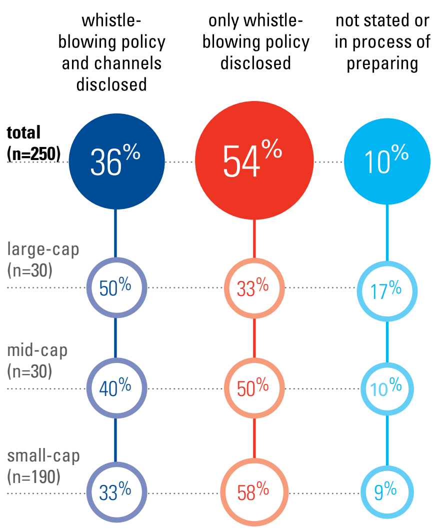
The revised Code 2012 indicates that the AC should ensure that arrangements are in place for whistle-blowing and that independent investigation should lead to appropriate follow-up action

figure 46: is the whistle-blowing policy disclosed?



Note: Statistics do not add up to 100% due to rounding

figure 47: are the whistle-blowing channels disclosed?



being taken. However, our findings show that although a majority of the sampled companies (90%) have disclosed that they have a whistle-blowing policy in place (see Figure 46), 54% of them have not disclosed the channels through which whistle-blowing is handled (see Figure 47).

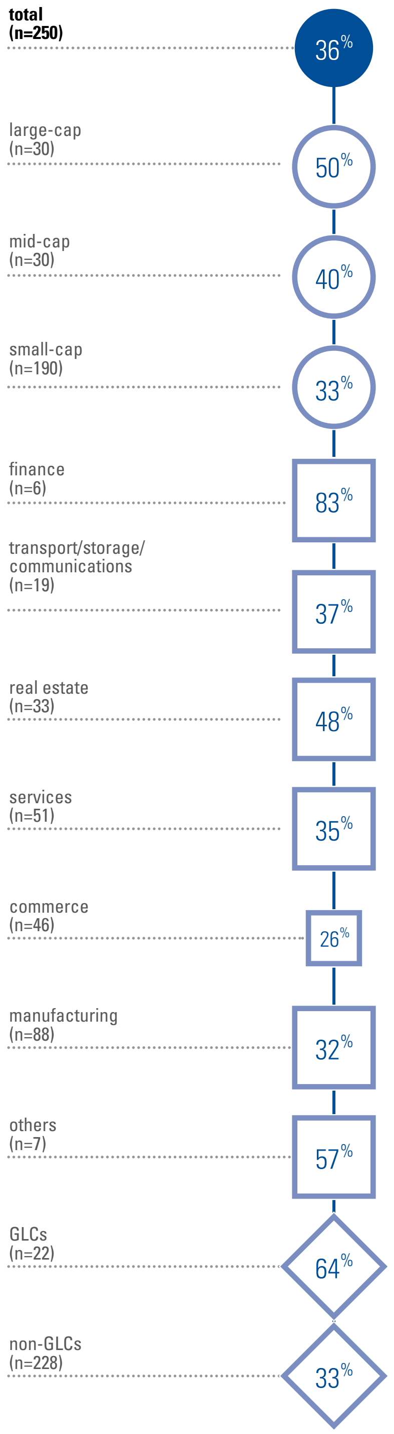
For the purpose of this study, we have defined higher quality disclosure as disclosing a whistle-blowing policy and its related channels, rather than simply mentioning that a whistle-blowing policy exists. On this basis, our results show that 50% of the sampled large-cap companies have higher quality disclosure compared to only 33% of sampled small-cap companies.

As illustrated in Figure 48, our results suggest that large-cap companies and companies in the finance sector are the most likely to disclose their whistle-blowing channels. In addition, we found that 64% of the sampled GLCs disclosed their whistle-blowing channels while only 33% of non-GLCs did the same in their FY11/12 annual reports.

Mixed disclosure of types of whistle-blowing channels

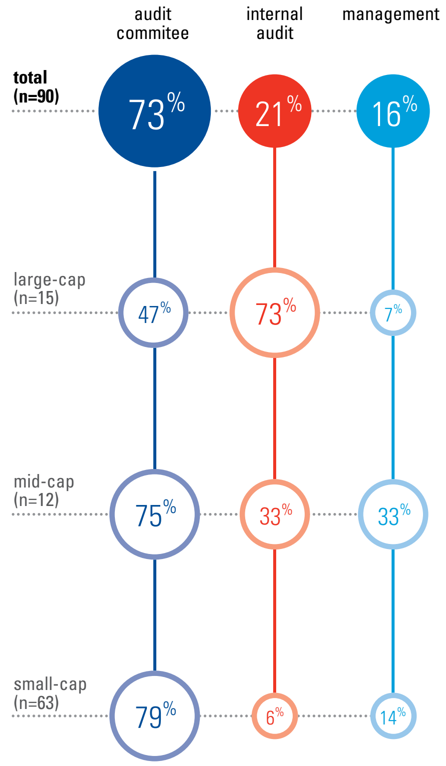
For a whistle-blowing programme to be effective, it is critical to instil staff confidence and trust in the programme and in the organisation's response to an incident. The recipient should also ensure the confidentiality of the whistle-blower's identity at all times. Some tools that can minimise fear of retaliation or identification of the whistle-

figure 48: who discloses whistle-blowing channels?



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.

figure 49: top three whistle-blowing channels (n=90)



Note: Figures add up to more than 100% as companies may have multiple channels

Our study found that only 90 of the selected 250 companies sampled (36%) disclosed their whistle-blowing channels (Figure 47). Figure 49 shows that among these 90 companies, 73% have whistle-blowing channels to the AC; this proportion rises even higher to 79% among small-cap companies. For the 15 large-cap companies that have disclosed their channels, 73% have channels to IA.

[29] ACFE, "2012 Global Fraud Study: Report to the Nations on Occupational Fraud and Abuse", http://www.acfe.com/uploadedFiles/ACFE_Website/Content/rttn/2012-report-to-nations.pdf.

Interestingly, the top whistle-blowing channel for the large-cap companies is IA, while the mid-caps and small-caps prefer the AC. The differences in whistle-blowing channels among large-caps and small-caps could be due to the lower incidence of in-house IA functions among small-caps (Figure 42) and reliance on alerts from employees and other stakeholders regarding areas of concern.

Challenges exist regarding the independence of whistle-blowing channels when the AC and IA function are not utilised

The two most common whistle-blowing channels – the AC and IA – are considered independent as both are supposed to be free of bias. However, our findings show that a significant number of the 90 sampled companies that disclosed their whistle-blowing channels have channels that are deemed to be less or non-independent, such as via management (16%) or via HR/company secretary/in-house legal counsel (10%) (see Figure 50).

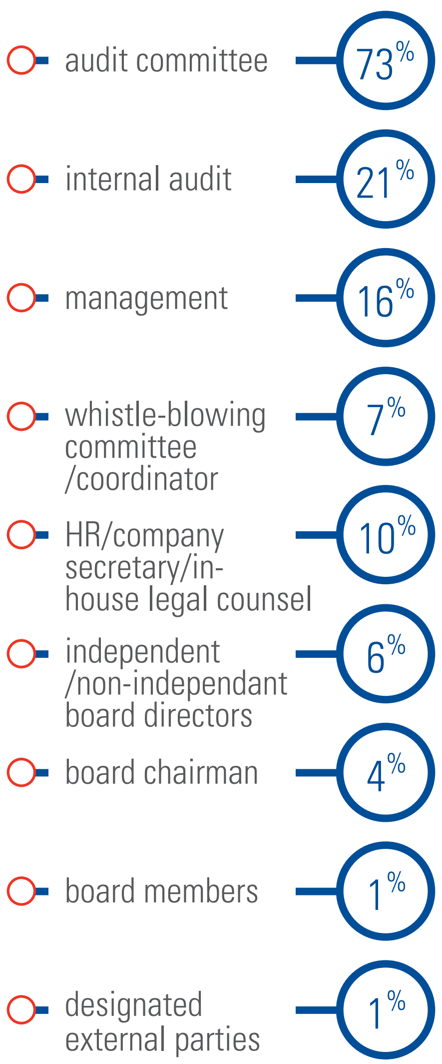
Our analysis found that in the four companies with whistle-blowing channels to the board chairman (4%), all four chairmen are non-independent.

Similarly, our analysis of the companies with whistle-blowing channels to a whistle-blowing committee/coordinator found that almost half of these committees/coordinators are considered non-independent as they report to their management. The remaining half did not disclose the composition/identity of the committee/coordinator.

Non-independent channels may not be able to allay the fears of exposure and reprisals among whistle-blowers. Employees may not consider HR as independent given that HR usually reports to the C-suite, thus making them less suitable as an independent whistle-blowing channel. This highlights the importance of careful consideration and selection of an appropriate whistle-blowing channel.

figure 50: who do whistle-blowers inform? (n=90)

Note: figures add up to more than 100% as companies may have multiple channels.



Interestingly, even though our earlier findings indicate that 60% of the sampled companies have outsourced their IA function (Figure 42), only 1% of the sampled companies have outsourced their whistle-blowing channel (Figure 50). The advantage to using an external party as the whistle-blowing channel is that anonymity can be maintained since the external party would be less likely to recognise the voice or handwriting of the whistle-blower.

Whistle-blowing forms a key part of the assurance framework

According to SGX LR 1207(10), the board has to provide an opinion on the adequacy of its internal controls. The factors considered and deliberated by the board and AC in arriving at the opinion should be disclosed. The board can no longer make a cursory comment on the internal controls for the business operations as a whole without specifying the assessment basis.

Further analysis of our results revealed that among boards with a BRC and disclosed whistle-blowing policies in place, 91% provided a positive opinion with basis (see Figure 51). This seems to suggest that BRCs and whistle-blowing policies are useful for boards in terms of giving them a stronger basis for providing a positive opinion. Of course, boards must recognise that beyond simply establishing such structures or systems, the quality of the structures and systems is also important for effective risk management. Possessing overall effective risk management structures and systems should be the key basis for providing a positive opinion.

figure 51: proportion of companies stating that internal controls are adequate with basis SGX LR 1207(10) and PN 12.2

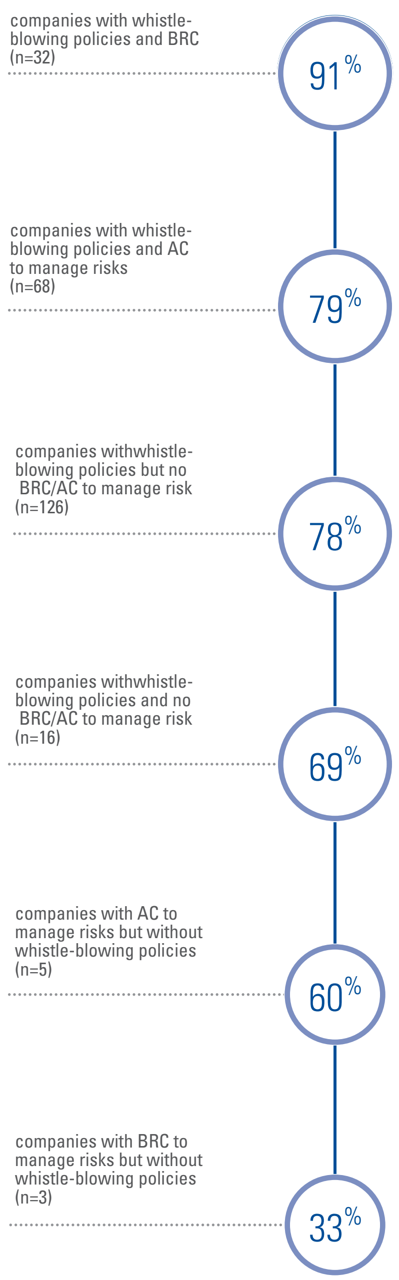
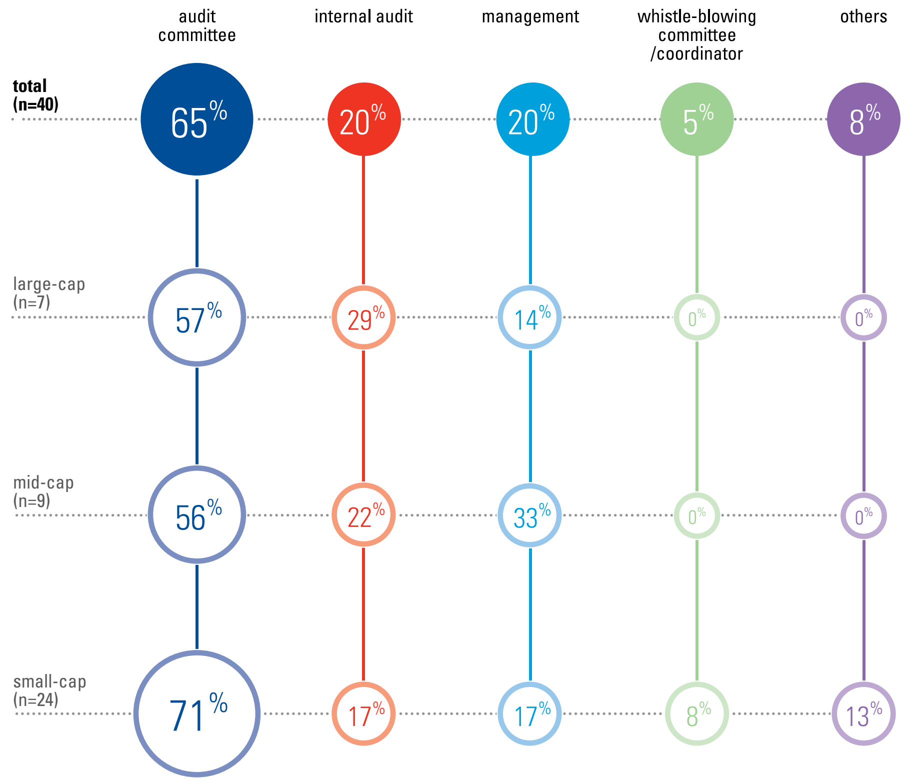


figure 52: who addresses whistle-blowing reports or cases? (n=40)



Note: Figures do not add up to 100% as companies may state multiple options

Limited disclosure of procedures for addressing whistle-blowing claims

A report by the International Finance Corporation (IFC) indicated that organisations need to consider several elements to effectively implement a whistle-blowing policy. These include having procedures to conduct independent investigations.[30]

Our analysis (Figure 46) found that only 40 companies (16%) have further disclosed details on the key people addressing the whistle-blowing reports. As illustrated in Figure 52, these 40 companies appoint mainly independent parties such as the AC (65%) and IA (20%) to address whistle-blowing reports or cases, which is in line with the recommendations of the IFC report.

[30] IFC "Whistle-blowing: Recent Developments and Implementation Issues", Global Corporate Governance Forum, Private Sector Opinion, Issue 5, 2007.

Conclusion

Risk management is no longer just an operational concern for management. Today, it has become a key strategic priority for both the board and management. With the global economy remaining sluggish and facing an uncertain future, weaknesses in many major economies around the world are also becoming more evident. To manage the growing spectrum of risks in the business environment, it is imperative for businesses – particularly those with operations in multiple jurisdictions beyond Singapore – to grow their risk management capabilities.

To raise awareness and promote stronger risk management practices in Singapore, MAS and SGX have introduced more robust guidelines and regulations on risk management and internal controls in the Code of Corporate Governance and the SGX Listing Rules. Specifically, the revised Code 2012 calls for the board to be responsible for the governance of risk. The introduction of this guideline reinforced the notion that risk management should be a key responsibility of the board.

Although the changes have been welcomed by the business community, our study reveals that significant gaps in the risk management capabilities of listed companies remain. Despite most boards stating that their internal controls are adequate (98%), only a small proportion of companies have a dedicated BRC (14%) or a CRO (5%) to oversee risks. Furthermore, only 45% of companies have disclosed in their annual report that they have a risk management framework. This suggests that most companies may still lack the resources and understanding to establish a sound system of risk management.

Despite these gaps, it is heartening to see that companies are complying with CG regulations in Singapore. Almost all the companies in our sample complied with SGX LR 1207(10) to provide their opinion on the adequacy of their internal controls in their annual report. The majority of them have also been able to substantiate their opinions and state that their internal controls are adequate (78%).

In comparison, the adoption rates for the guidelines in the revised Code 2012 are relatively low. Only 12% of our sampled companies have commented on both the adequacy and effectiveness of their risk management and internal control systems. Further, only 15% have disclosed receiving assurances from their CEO and CFO. This suggests that a regulation-based approach may be more effective in promoting better risk management practices in Singapore. However, our study suggests that many smaller companies may find it difficult to adopt risk management practices effectively as they have access to fewer resources.

To help Singapore companies – especially smaller companies – overcome challenges in adopting better risk management practices, the business community should consider working together with all the relevant stakeholders to share best practices in risk management. Closer collaboration among stakeholders will help to promote a higher standard of risk governance within companies in Singapore.

Appendices

appendix 1: sector classification

SGX classification[31]	classification used in the study
manufacturing	manufacturing
service	services
commerce	commerce
hotels	real estate
properties	real estate
construction	real estate
transport/ storage /communications	transport/ storage /communications
finance	finance
agriculture	others
electricity/ gas/ water	others
multi-industry	others

appendix 2: additional sector breakdown by number of companies

	large-cap (n=30)	mid-cap (n=30)	small-cap (n=190)
total (n=250)	30	30	190
commerce (n=46)	3	6	37
real estate (n=33)	4	7	22
finance (n=6)	3	1	2
services (n=51)	3	4	44
manufacturing (n=88)	7	6	75
transport/storage /communications (n=19)	7	4	8
others (n=7)	3	2	2

[31] SGX sector classification as stated on SGX website. http://www.sgx.com/wps/portal/sgxweb/home/marketinfo/sector_summary

appendix 3a: types of board opinions: examples from annual reports (with basis)

type of opinion	actual wording in annual report
internal controls adequate (with basis)	Based on the framework established and the reviews conducted by management and the internal and external auditors, the board opines, with the concurrence of the AC, that there were adequate controls in place within the group addressing material financial, operational and compliance risks to meet the needs of [company] in its current business environment as at [year-end date].
provides reasonable assurance (with basis)	It is the opinion of the board, with the concurrence of the AC that, from the results of reviews and enquiries made, the system of internal controls maintained by the company's management throughout the financial year 2011 provides reasonable assurance against material financial misstatements or loss, and includes the safeguarding of assets, the maintenance of proper accounting records, the reliability of financial information, compliance with appropriate legislation, regulation and best practice, and the identification and management of business risks.
negative opinion	The board, with the concurrence of the AC, is therefore of the view that the system of internal controls and risk management previously maintained by the group in the last financial year was inadequate in terms of financial, operational and compliance risks to safeguard shareholders' investments and the group's assets.

appendix 3b: types of board opinions: examples from annual reports (without basis)

type of opinion	actual wording in annual report
internal controls adequate (contrary to the absence of evidence)	The board believes that, in the absence of any evidence to the contrary, the system of internal controls maintained by the group's management provides reasonable assurance against material financial misstatements or loss, safeguarding of assets, the maintenance of proper accounting records, reliability of financial information, compliance with legislation, regulations and best practices and the identification and management of business risks.
internal controls adequate (no basis)	The board believes with the concurrence of the AC that the system of internal controls including financial, operational and compliance controls and risk management systems maintained by the company's management throughout the financial year is adequate to meet the needs of the company in its current business environment.
provides reasonable assurance (no basis)	The board believes, with the concurrence of the AC, that the system of internal control maintained by the management and that was in place throughout the financial year for the group provides reasonable, but not absolute, assurance against material financial misstatements or loss, and includes the safeguarding of assets, the maintenance of proper accounting records, the reliability of financial information, compliance with appropriate legislation, regulation and best practices, and the identification and containment of business risks.

Glossary

abbreviation	description
AC	Audit Committee
ACFE	Association of Certified Fraud Examiners
BRC	Board Risk Committee
CAE	Chief Audit Executive
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CG	Corporate Governance
Code	Code of Corporate Governance
COO	Chief Operating Officer
CRO	Chief Risk Officer
GFC	Global Financial Crisis
GLC	Government - Linked Companies
IA	Internal Audit
IC	Internal Control
ID	Independent Director
IFC	International Finance Corporation
IIA	Institute of Internal Auditors
IMF	International Monetary Fund
ISCA	Institute of Singapore Chartered Accountants
LR	Listing Rule
MAS	Monetary Authority of Singapore
MRC	Management Risk Committee
Non-GLC	Non Government - Linked Companies
P	Principle
PN	Practice Note
RM	Risk Mangement
SAC	Singapore Accountancy Commission
SGX	Singapore Exchange

Acknowledgements

ISCA Research Team

Mr. Chan Sze Yee – Head, Research

Mr. Shawn Pang – Manager, Research

Ms. Perrine Oh – Manager, Research

Mr. James Shen – Executive, Research

Ms. Kay Zin – Executive Assistant, Research

The ISCA Research team sincerely thanks Mr. Yee Cheok Hong, Executive Director (Policy & Strategic Planning/ Industry Development), ISCA, for his invaluable feedback and guidance with regard to this study.

Former ISCA Research Manager, Mr. Germin Ong also contributed to this study.

KPMG Thought Leaders

Mr. Irving Low – Partner, Head of Risk Consulting

Ms. Emilie Williams – Director, Risk Consulting

KPMG Risk Consulting Professional Team

CONTACT

R. Dhinakaran
Vice-President
Chairman, ISCA Corporate Governance Committee
ISCA

Institute of Singapore Chartered Accountants
60 Cecil Street
ISCA House
Singapore 049709
Tel: +65 6749 8060
Fax: +65 6749 8061

Irving Low
Partner
Head of Risk Consulting
KPMG in Singapore

KPMG Services Pte Ltd
16 Raffles Quay
#22-00 Hong Leong Building
Singapore 048581
Tel: +65 6411 8888
Email: irvinglow@kpmg.com.sg