Director's Quarterly *update*

Deloitte Singapore
Issue 1, May 2015

Through the eyes of the board

Corporate strategy: Dead or alive?

Financial Reporting Surveillance Programme (FRSP): What you need to know

Budget 2015: Many happy (tax) returns

Digital Directors: The board's role in the cyber world

Deloitte.

Contents

Welcome

Philip Yuen
CEO, Deloitte Singapore

The role of directors today has changed significantly and becoming substantially more complex. Many directors find themselves increasingly unprepared for addressing the evolving demands of their role - new accountability and a host of new business issues with which they must deal.

The Director's Quarterly is an e-publication aimed at exploring the challenges of practicing corporate oversight and governance in a world of change, and helping directors increase their relevance of the role they play and the work they do to ensure that their companies continue to create value for their stakeholders.

There are no easy answers but through this e-publication, we hope to promote a dialogue in the critical areas of corporate governance among industry bodies, companies and their boards of directors.

In this first issue, we look at a wide variety of topical issues: everything from how directors need to appreciate that their duties go beyond simply setting the strategy and broad oversight responsibilities to why it is essential that the board promote awareness of quality financial reporting standards and the key tax matters from the 2015 Singapore Budget.

For many companies, big data is critical in keeping the company nimble, competitive and profitable. Directors need to have a grasp of the issues surrounding big data. Equally important, they should be prepared to ask the right questions. This is covered in the 'Crunchy questions for boards' on page 26. The final article talks about how the overwhelming number of cybercrime incidents has forced boards to have to get up to speed with the new digital reality.

We hope that through these pieces, directors can find better ways to successfully navigate the complexity in the business environments and deliver on the promise to protect and increase shareholder value.

For information on Deloitte's Centre of Corporate Governance, please visit us at www.deloitte.com. If you have queries about particular articles, would like to suggest future topics or have feedback, please contact us at enquires@deloitte.com.

I hope you enjoy this first edition of our Director's Quarterly.

Kind regards,

Philip Yuen

Corporate strategy: Dead or alive?

In a VUCA world—one that is volatile, uncertain, complex, and ambiguous—is strategy relevant anymore? According to some, it isn't. They believe that setting strategy is no longer possible when conditions change at increasing speed, quickly disrupting long standing business models. Perhaps, they suggest, organizations would do better to focus on being flexible, adjusting their initiatives as necessary in response to the changes as they occur in the operating environment. In short, they say, strategy is dead. But is it?

In a VUCA world, strategy matters now more than ever. That's because strategy is an integrated set of aligned, reinforcing, and coherent choices about an organization's goals and aspirations, about where to play and how to win, and about the capabilities and management systems required to do so. Strategy is the foundation that drives resource allocation, investment positions, performance expectations, and the design of organizational structures. It is the filter through which organizations distinguish opportunities from distractions, helping management make good decisions about what to do, but as importantly, about what not to do. Strategy, therefore, profoundly influences an organization's position, its potential, and future economics—in short, a well-executed strategy is essential to producing superior financial performance over time.

That is not to say that strategy does not need agility and flexibility. Strategy describes explicit choices for the organization, which are underpinned by a set of assumptions about the organization's industry, competitors, customers, and other factors. Since those factors aren't static, organizations need to periodically re-verify those assumptions and, when they change, organizations need to recheck the choices they made based on those assumptions, and adapt them if necessary. How often should an organization revisit its strategy and underlying assumptions? The right timeline will depend on the "clock speed" of the industry—the clock speed of the technology industry, for example, is much faster than it is for many other industries.

Boards of directors have an important role in strategy. While management is responsible for setting, refining, and executing the organization's strategy, the board's role is to provide oversight and guidance to the direction of the strategy and to weigh its inherent risks.

Part of the board's responsibility is to clearly set appropriate expectations for management and the organization's strategy. Boards should neither set the bar too low—not demanding a strategy and simply allowing management to develop initiatives in an ad hoc way without the context of overall strategic goals—nor set the bar too high—setting unrealistic expectations for the organization based on its starting point and resources. Instead, boards should demand that management develop an explicit strategy that reflects a set of choices and considers alternatives, clearly outlining their consequences, tradeoffs, and risks. Boards should also demand that the strategy be coherent; its choices should make sense and reinforce each other; the choices of the markets the organization will enter should be ones that will enable it to achieve its goals and aspirations; its plans should enable the organization to succeed and connect with its current and future customers; and the required resources to carry out the strategy should be those the organization has or can access in the future.

Boards are also responsible for appropriately evaluating the organization’s strategy and its inherent risks. The board cannot afford to receive management’s proposals uncritically, accepting them without question or query. On the other hand, boards should not attempt to drive the strategic process, which would occur when directors move from constructively probing the strategy and its underlying assumptions and risks to actively defining the strategy and advocating its direction.

Boards and management need to interact productively when defining and refining strategy. There should be a cadence to the interactions between them; the aspects of strategy and the issues being addressed should develop over time, so that their sessions focus on different aspects of strategy and escalate in quality. In a productive relationship, the questions the board asks should be ones that are purposeful and legitimately probe and advance the strategy without grandstanding or attempting to “one up” management. As the organization’s primary steward of risk, the board is responsible for defining the risk appetite for the organization. The expectations the board sets around strategy, and its interactions with management, should be viewed in the context of the risks being borne by the organization and its stakeholders, and how those risks are managed and mitigated.

Boards need to weigh the organization’s various portfolios, and the risks associated with them, and assess different scenarios that change those portfolios—for example, getting out of one business or into another—and their impact on the organization’s basket of risks.

In a VUCA world, management and boards tend to systematically underestimate the risk of the status quo—the current direction and makeup of the organization—and overestimate the risk of doing something different. Just because the current activities and their risks are known does not mean they are less than the risks associated with doing something different.

While setting strategy may be a greater challenge than in the past, the risks of not setting a strategy are also greater today. Boards should connect regularly, visit the organization’s business units, meet with management, and engage industry and subject matter experts so they can better understand, assess, and challenge the strategic choices made by management and the assumptions that underlie those choices.

If the board isn’t satisfied with the strategy proposed by management, the board has a duty to require management to rethink and improve that strategy, but it isn’t the board’s responsibility to take over that role from management.

Questions for directors to ask:

Does our organization have a strategy that we believe will enable it to achieve its future aspirations? Does the organization have the resources—such as a management team with the appropriate leadership abilities, a workforce with the required skills, capabilities, and expertise, and financial and technology resources—necessary to achieve our strategic objectives? Does our board have the right qualifications for the current environment? If we’re lacking any required resources, what is the organization doing to obtain them?

Does our organization suffer from the phenomena that the decisions had been vetted by so many parties that no one person could be held accountable?

How quickly are strategic and operational decisions translated into actions?

What is the board’s working relationship with management? When we interact with management on strategy, is there a constructive, positive dialog among directors and management regarding the strategic choices? Are we confident that management and the board are “on the same page” around strategy?

How quickly does information on the competitive environment get to the board?

Financial Reporting Surveillance Programme (FRSP): What you need to know

By Soh Lin Leng, Audit Partner & How Aylwin, Audit Senior Manager

In April 2014, the Accounting Corporate Regulatory Authority (ACRA) issued the Practice Direction No. 2 of 2014 titled "Directors' Duties in relation to Financial Reporting and Review and Sanction Process of the Financial Reporting Surveillance Programme Administered by ACRA" (the Practice Direction). This Practice Direction sets out the duties of a director in relation to financial reporting and the review and sanction process of the Financial Reporting Surveillance Programme (FRSP).

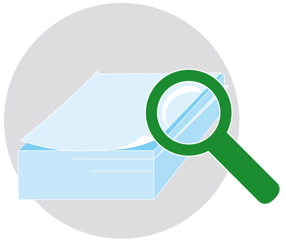
The FRSP is not a new programme. Intended to uphold the transparency, integrity and quality of financial reporting in Singapore, the FRSP was established by ACRA in 2011. Selected financial statements are reviewed to determine if they comply with Accounting Standards[1] issued by the Accounting Standards Council. During its review, ACRA will raise formal enquiry letters to the directors who authorised the financial statements to request for explanation, supporting documents and other records as necessary.

The FRSP has garnered more attention in recent years because increasingly, ACRA recognises that the robust practice monitoring framework surrounding the work of auditors needed to be complemented by a surveillence framework over directors, with whom the ultimate responsibility of providing reliable financial reports lies.

In January 2014, the ACRA and the Institute of Singapore Chartered Accountants (ISCA) signed a Memorandum of Understanding (MOU) which is expected to strengthen the quality of financial reporting in Singapore. The MOU enables ACRA to draw on the expertise of ISCA's Financial Statements Review Committee (ISCA-FSRC) which reviews financial statements as part of industry self-regulation efforts. Potential non-compliances in financial statements will be shared by ISCA-FSRC and ACRA will deliberate and take enforcement action against directors under the Companies Act, if necessary.

[1] Accounting Standards refer to Singapore Financial Reporting Standards (SFRS), Singapore Financial Reporting Standards for Small Entities and Charities Accounting Standards, as issued by the Accounting Standards Council.

How does the FRSP work and what Directors should look out for?

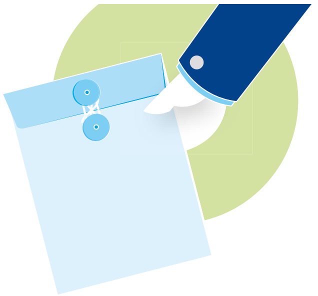


Step 1: Selecting financial statements for review

ACRA adopts a risk-based approach in prioritising the financial statements for review.

Emphasis is placed on financial statements of public and large private companies with certain characteristics, such as those with significant public interest risks, significant change in key stakeholders and operations that require subjective judgement in accounting for transactions.

Step 2: Reviewing and Corresponding with Directors



This step involves the following:

- ACRA will raise formal enquiry letters to directors to request for explanation together with any supporting documents and records as necessary, on any matters that require additional information upon review of the financial statements.
- Directors will have to respond to the enquiry letters within two to three weeks from the date of the enquiry letter.
- On a case-by-case basis, ACRA may request for physical meetings to receive verbal clarifications.

Step 3: Taking firm enforcement action

Depending on the severity of the accounting standard breach(es), the range of sanctions may include:

- Issuance of an advisory letter
- Issuance of a warning letter
- Imposing a fine by offer of composition and
- Prosecution leading to fines and/or imprisonment

Under SGX Rule 704(7)(k) surrounding announcement of appointment of directors, where the director has been the subject of any investigation or disciplinary proceedings, or has been reprimanded or issued any warning by any regulatory authority in Singapore, it should be disclosed. This rule is now extended to sanctions arising from the FRSP.

Step 4: Requirement to rectify deficient financial statements
Where significant prior period corrections have to be made in the next set of annual financial statements as a result of review by ACRA, the company may be required to disclose the fact that the correction arises from ACRA's FRSP review process in the notes to the financial statements explaining the correction.

Depending on the severity of the financial reporting breach(es), the company may also be required to rectify deficient financial statements, have the restated financial statements re-audited; and re-file the restated financial statements together with the most current set of financial statements with ACRA.

Step 5: Reporting to the public
ACRA will publish reports annually summarising the activity and findings of FRSP for the past year.

To guide directors and oher financial preparers, ACRA will also publish areas of the FRSP's review focus for the coming year, in the form of a Financial Reporting Practice Guidance (FRPG).

The FRPG is very useful in guiding directors on the areas of focus by ACRA when they review the financial statements but ACRA reserves the right to conduct review of other areas in the financial statements, aside from those included in Table 1.

Table 1: Areas of review focus

FRPG No. 1 of 2014 (for financial years of 2013)	FRPG No. 1 of 2015 (for financial years of 2014/2015)
• Requirements under FRS 113 Fair value measurement standard newly effective for annual periods beginning January 1, 2013 • Significant accounting policies • Applying the going concern assumption where material uncertanty exists • Disclosures surrounding accounting judgement and estimation uncertainties • Asset value and impairment testing such as goodwill, other intangibles, and property, plant and equipment • Financial risk and capital management disclosures • Adequacy of related party disclosures • Preparation of consolidated financial statements if exemption criteria is not met	• Requirements under new suite of consolidation standards[2] effective for annual periods beginning January 1, 2014 • Accounting for business acquisitions involving separate recognition of intangible assets and contingent share consideration • Classification of cash flows into operating, investing and financing activities within statement of cash flows • Long-life asset value and impairment testing • Computation of basic and diluted earnings per share (EPS) ratios • Operating segment disclosures • Fair value disclosures including justification of fair value hierarchy classification of investment properties and biological assets as Level 2 instead of Level 3, and adequacy of Level 3 disclosures.

[2] Refers to SFRS 110 *Consolidated Financial Statements*, SFRS 111 *Joint Arrangements*, SFRS 112 *Disclosures of Interests in Other Entities*, SFRS 27 *Separate Financial Statements* and SFRS 28 *Investments in Associates and Joint Ventures*

Guidelines for directors in carrying out duties over financial reporting

The FRSP places a notable increased workload on directors who are already tasked with many other responsibilities of corporate governance. In particular, directors with no financial accounting background will find the duties put forth by the FRSP especially challenging. However, here are some general reminders on financial reporting to note as you carry out your duties.

The right mindset

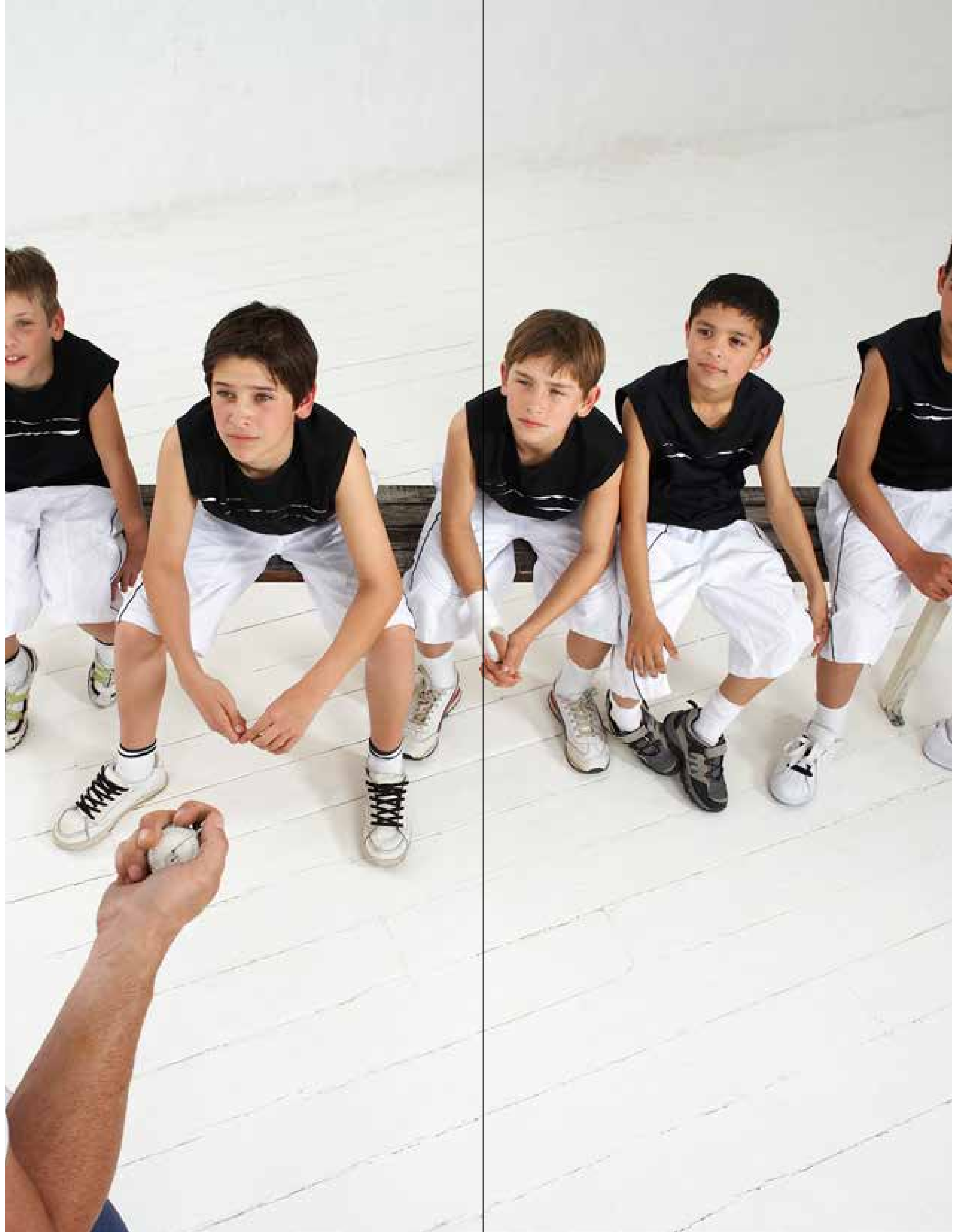
Directors, whether executive or non-executive, are expected to exercise care, competence and diligence in reviewing the financial statements. Directors cannot delegate the task in its entirety to its finance team to work with the auditors. In fact, given the directors' proximity to the business, they are expected to apply professional skepticism when reviewing the financial statements. Even if directors are not accounting experts, they are expected to question as to whether accounting treatments applied reflect the substance of the underlying transaction.

The right skillsets

Directors are not expected to be accounting experts but will need to have up-to-date knowledge of accounting concepts and principles sufficient to perform their review. There are many courses for accounting updates and specific accounting subject matters organised by accounting firms and the Singapore Institute of Directors (SID) collaborated with the Institute of Singapore Chartered Accountants (ISCA) for Directors that are available[3].

The right system

It is also important to devise and maintain a sound system of internal accounting controls over financial reporting so as to ensure assets are safeguarded against loss from unauthorised use and facilitate the proper recording of authorised transactions necessary to prepare true and fair financial statements. The board is also required to opine, with the concurrence of the audit committee, on the adequacy of the internal controls, addressing financial, operational and compliance risks[4].



The right people

Directors are not alone in the journey of preparing quality set of financial statements. Directors are encouraged to call on support from a competent management and finance team, as well as help from external advisors, including working with the independent auditors.

Management team

In building its senior management team, directors should ensure their CEO and CFO have adequate knowledge, competence, experience and integrity to undertake their roles.

Finance team

Directors should ensure that resources in the company's finance team are adequate in preparing high quality financial statements. This includes hiring qualified and competent accountants in their finance teams, as well as ensuring they receive continuous training to keep them abreast of financial reporting developments.

External advisors including independent auditors

Certain complex transactions require engaging help, such as valuation and accounting advice from professional external advisors. Directors should also engage independent auditors on a proactive basis. Although external auditors are not permitted under independence rules to participate in preparing the company's financial statements, engaging them early helps to identify significant audit and accounting issues to be resolved to a timely basis.

Conclusion

Directors need to embrace the new wave of increasing regulatory surveillence surrounding their financial reporting duties, and in doing so, ensure they are equipped with the necessary capabilities to discharge their duties effectively.

[3] One suitable training course will be the Director Financial Reporting Essentials Course organised by the SID in collaboration with the ISCA. The first 3,000 directors who voluntarily attend this course before 31 March 2016 will be entitled to subsidies of $300 per individual (about 50% of the course fees) funded by ACRA. Please also look out for other training seminars conducted by us which are made available throughout the year.

[4] Mainboard Listing Rules (610(5) for prospectus and 1207(10) for annual reports) and Catalist Listing Rules (407(4)(b) for offer document and 1204(10) for annual reports).

Budget 2015: Many happy (tax) returns

By Daniel Ho, Director of Taxes & Yap Hsien Yew, Tax Senior Manager

The Deputy Prime Minister and Minister for Finance (the Minister) delivered his 2015 Budget Statement on 23 February 2015. Also known as the "Jubilee Budget" on account of Singapore's 50th year of independence, Budget 2015 focuses on Singapore's need to build for the future and to cater for inclusive growth.

The Minister reported that Singapore's economy grew by 2.9% in 2014. For 2015, the Minister expects Singapore's GDP growth to be between 2% to 4% and the global economic outlook to be uncertain. Against this backdrop, one key focus of Budget 2015 is to sharpen the support to businesses that are making significant effort to raise productivity, especially by innovating and internationalising. This article talks about some of the measures announced in Budget 2015 to support companies in internationalisation and raising scale.

Enhancing the Double Tax Deduction (DTD) for Internationalisation scheme

To provide greater support to businesses venturing overseas, by co-sharing their risks and initial costs of expanding overseas, as well as creating skilled jobs and opportunities for Singaporeans to work overseas, the Minister has proposed that the scope of expenditure qualifying for double tax deductions (DTD) be expanded to include manpower costs incurred for Singaporeans posted to new overseas entities. The amount of such qualifying manpower expenses to be allowed DTD under the scheme will be capped at $1 million per approved entity per year, subject to conditions. Businesses will have to apply to International Enterprise Singapore (IE Singapore) to enjoy the DTD on qualifying manpower expenses. This will apply to qualifying manpower expenses incurred from 1 July 2015 to 31 March 2020.

The introduction of the 200% tax deduction for qualifying manpower expenses incurred from 1 July 2015 to 31 March 2020 is intended to encourage businesses in Singapore to continue to venture outside Singapore. Companies should ensure that they apply for this scheme to the extent that they meet the conditions to be laid out by IE Singapore, which will be released by IE Singapore by end May 2015.

International Growth Scheme (IGS)

The Minister has proposed a new tax incentive scheme (the IGS) in Budget 2015 to provide greater and more targeted support for larger Singapore companies in their internationalisation efforts. The IGS provides for a concessionary tax rate of 10% for a period not exceeding five years on their incremental income from qualifying activities.

The IGS will empower larger Singapore companies to establish themselves as globally competitive companies and enable them to create higher value jobs for their employees, while they continue to anchor their key functions in Singapore. This can also help ensure Singapore's economic sustainability in today's uncertain global climate.

This new scheme will be administered by IE Singapore and details will be announced by IE Singapore by May 2015. For the IGS to be helpful to potential investors, it is hoped that there will be more guidelines available in terms of the requirements in order to be considered for the IGS. This would enable potential investors to do a self-assessment before approaching IE Singapore to discuss the possibility of tax incentives.

Mergers and acquisitions (M&A) tax allowance scheme

To further encourage Singapore-headquartered enterprises to grow and build critical mass via acquisitions, the Minister has announced that the M&A tax allowance scheme will be extended beyond 31 March 2015 for 5 years till 31 March 2020.

Additionally, qualifying M&A executed from 1 April 2015 will enjoy these (revised) tax benefits:

1. an M&A allowance rate of 25% (up from 5%) of up to $20 million (reduced from $100 million) of the acquisition value of all qualifying M&A per YA;
2. stamp duty relief on the transfer of unlisted ordinary shares for qualifying M&A that will be capped at $20 million (reduced from $100 million) on the value of qualifying M&A deals: essentially reduced to $40,000 of stamp duty relief per financial year; and
3. 200% (no change) one-year tax allowance write-down on transaction costs incurred on qualifying M&A, subject to an expenditure cap of $100,000 per YA.

The shareholding eligibility criteria for the M&A tax allowance scheme have also been relaxed to 20%/50% from 50%/75% respectively. This means that instead of having to acquire shares which exceed the 50% or meet the 75% ordinary shareholding thresholds in order to qualify for M&A tax allowances, this threshold has been revised downwards to at least 20% or more than 50%. However, where the more than 50% threshold is met, any further acquisition of ordinary shares will not be eligible for M&A tax allowance.

The revisions to the M&A tax allowance scheme should be a boon for many Singapore companies, especially SMEs that are contemplating to restructure, acquire, merge or consolidate so as to be more competitive, achieve economies of scale or gain a greater market share in these challenging times. This is a big helping hand assisting Singapore companies to be scalable for the future especially with the regional economic integration in the ASEAN Economic Community. The relaxation of the shareholding eligibility criteria would also enable Singapore companies to expand via entering into alliances with other companies without necessarily obtaining a controlling stake in the other party, which are often more difficult to execute.

What it means for companies

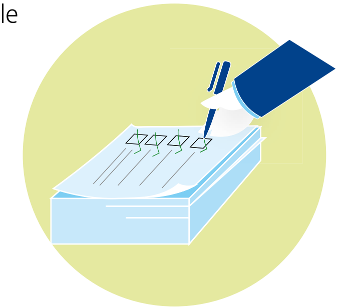
In this environment of ongoing change, companies, their management and board of directors must respond quickly and adeptly if they are to effectively address the disruptive changes that surround and affect them. In particular, as businesses expand operations into new markets, the complexity of ensuring tax efficient profit repatriation, managing tax risks and complying with tax reporting requirements multiplies. For boards of directors, this often requires greater oversight on their part.

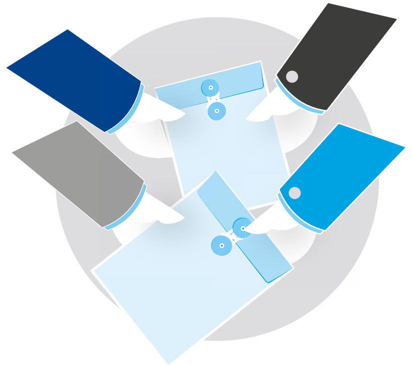
With that in mind, boards of directors should consider asking the following critical questions when evaluating the tax aspects of an internationalisation strategy:

Do we understand our company's legal structure, tax position, tax risks as well as the potential reporting requirements both in our home jurisdiction (Singapore) and in other countries in which we operate?

Are we comfortable that the organization has adequately addressed the potential tax costs or outcomes arising from the internationalisation strategy or expansion plans, built these into the financial projections and has the ability to manage the tax risks arising from implementation?

Have we examined what are the incentives and grants available and the requirements for qualification in order to obtain operational and fiscal benefits from our internationalisation strategy?





Have we addressed the transfer pricing aspects in respect of inter-company transactions with and support provided to the overseas entities?

Anticipating tomorrow's complex issues and new strategies can be challenging. With the increasing scrutiny from tax authorities and the regulatory, financial and reputational costs if tax risks or issues are not addressed adequately, Boards may find themselves having to play a more active role in understanding and addressing tax risks.

Analytics: Crunchy questions for boards

While Boards may benefit greatly from insights gleaned from data, few have seen the practice of business analytics as a worthy place to invest their time. That is not surprising, given the competing demands for their attention.

As the issue of risk increasingly becomes a core strategic concern for many businesses, organisations are facing increasing pressure to identify a wider range of risks and better understand the impact of differing economic environment on business risk and performance. As a result, there is a need for better ways to secure consistent and reliable data to drive smarter insights.

In many organisations, two types of analytics are being practiced at any given moment. On one end of the spectrum is pulling together numbers and generating some supporting visualisations. On the other end is the ability to identify complex, non-linear relationship between different domains of the business while using differing types of data. It is the latter end of the curve that boards should be concerned with because the insights can help organisations plan better for the future and standardise decision making to align with organisational risk management goals.

Put simply, risk-focused business analytics is an important ingredient in developing and sustaining a competitive edge at a time when risk issues affect business strategy more than ever. And analytics itself is rising as a strategic issue as data becomes increasingly more plentiful and more valuable. In some cases, it has even changed the makeup of the executive suite as chief analytics officers join the rank and collaborate with their peers who are accustomed to making more qualitative decisions.

As board begin to embrace analytics, it is important to be able to zero in on what we call "crunchy questions" that will pave the way for action by the management.

Risk portfolio

- What is our risk profile – and how does it match up with our risk appetite?
- What specific exposures should the firm worry about?
- How is our financial performance affected by risk in terms of impairment or Value at Risk?
- What are our capital requirements, in lights of our risk profile?
- If we suddenly faced a stressed risk environment, how would we likely perform?

Strategy

- What exactly is our organisation's risk appetite misaligned with our business strategy?
- Which early warning signs may help us avoid strategic missteps in the future?
- How should we adjust compensation to reward risk-intelligent behaviour?
- What is the specific impact of the shifting regulatory environment on our business?
- How strong or weak is our risk culture today?

Analytics connections with other roles

Digital Directors: The board's role in the cyber world

By Thio Tse Gan, SEA Cyber Security Leader

Cyber security threats are not just for information technology specialists anymore. Today, cyber security is drawing attention from the very top, and it has become a huge concern for corporate boards. The reasons for this board level concern are not hard to understand – a number of organisations have been badly shaken by cyber security breaches and their boards are being held accountable. It is estimated that 1 billion records was compromised in 2014[1] and the average loss for each breach ranges between USD52 to USD87[2].

[1] Gemalto's 2014 Breach level index

[2] Verizon's 2015 Data Breach Investigations Report

So how can directors best conduct oversight and ensure their companies are adequately protected against cyber threats?

Boards, traditionally used to focusing on strategic and governance risks, now find themselves involved in the oversight of technology because the use of technology is critical in determining the success of business. Yet, the benefit that technology has brought to organisations also poses risks that need to be understood and managed.

This advancement of computing power in tandem with that of Moore's law[3], coupled by the level of sophistication of cyber criminals has resulted in exponential growth in the level of cyber threats. These threats are no longer random in nature.

Hence, to effectively provide oversight and governance, the board first need to understand the different types of actors that exist, their level of sophistication and their determination as shown in diagram 1. Cybercriminals strategises and targets organisations that maximises their return on investment, and the most demanding perpetrators are those where the end goal is monetisation of the records that they are able to compromise.

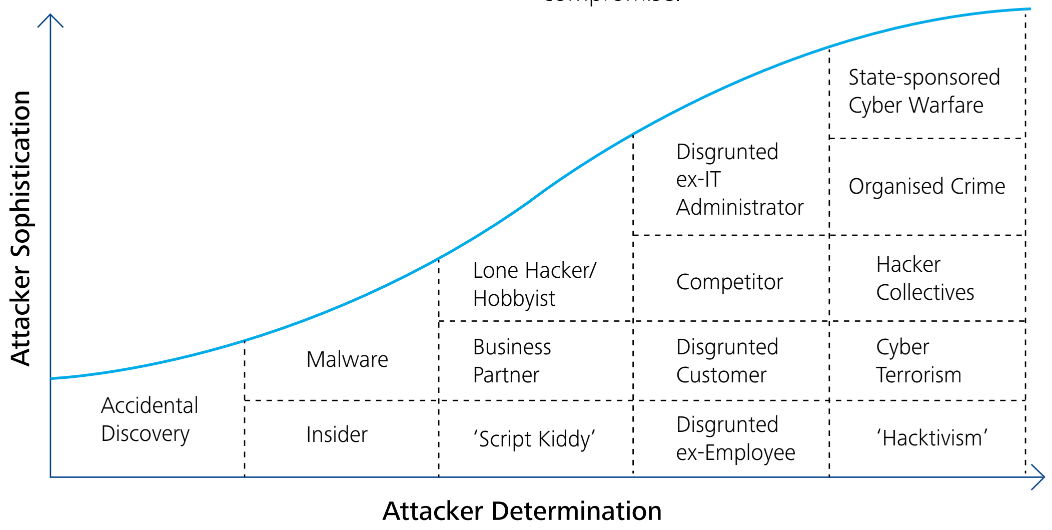


Diagram 1

[3] Moore's law states that processor speeds, or overall processing power for computers will double every two years. http://www.mooreslaw.org/

Then as a next step, directors must recognise and understand the importance of their organisation's digital assets such as data, information, applications, and networks that exist within the organisation's walls. This also extends to their suppliers, vendors and other partners, and to data and information that reside in employees' mobile devices.

To gauge the vulnerabilities of these assets, directors might want to ask:

- What information is leaving the organisation, and how?
- What are the "crown jewels" that we must protect?
- What are the cyber threats that our organisation faces?
- How do we know our controls are operating effectively and have they been validated?

The answers to these questions will help set the tone for transparency and a two-way conversation between management and the board, setting up a "ladder" approach in which threats are categorised and managed according to their associated risk with the appropriate priority and resources.

Guarding against cyber threats is a mind-set change across the entire organisation and it should be devoted to achieving three things: Secure.Vigilant.Resilient™

- **Security** of data and systems centers on risk-prioritised policies, procedures, and controls, such as those for devices, e-mail, home-based data, and third-party data use which is important because of the increased number of vendor and outsourcing arrangements.
- **Vigilance** means rapidly flagging violations and suspicious occurrences, and responding appropriately. It also includes being adaptive - absorbing new threat information and adjusting to changes in the business and technology environment to keep eyes on what matters most.
- **Resilience** focuses on damage control and repair, and ensuring that post-attack recovery will be swift.

The balance of investment in secure, vigilant, and resilient capabilities will vary between organisations, and will need to be applied differently to the various areas within an organisation but that said cyber security programs have some common characteristics:

- **They are executive-led.** Executive leaders must set the stage by defining cyber risk management priorities, appetite, and mechanisms of accountability. Support from the top is essential in ensuring that diverse groups and departments collaborate. The Board Risk Committee's charter should also be expanded to include the mandate of how the organisation should be allocating resources to managing cyber risks. Directors can also lead by creating a board cyber chair to oversee management activities on cyber; and ensuring that the appropriate senior management is focused on cyber.
- **They involve everyone.** Although specific roles need to be defined, the program is not the sole responsibility of a single part of the organisation. It requires broad horizontal and vertical participation, and behavioural change throughout the organisation to ensure success.

- **They are programs, not projects.** Although it usually requires a series of projects to get off the ground, such programs require continuous review and improvement cycles to adapt to changes in the business risk and threat landscapes.
- **They are comprehensive and integrated.** The secure, vigilant, and resilient elements are not distinct silos of activity; they are a set of lenses through which every essential business process and growth initiative should be evaluated or planned. Each involves people, process and technology components. And done well, each will improve the others.
- **They reach beyond your walls.** Your ecosystem includes various partners, suppliers, and vendors; significant cyber incidents directly impacting them may also substantially affect you.

Becoming secure, vigilant, and resilient requires that the organisation embrace a fundamentally different view of what we have previously called "security." Yesterday's security program was often perceived as a burden – an externally-imposed set of restrictions, rules, and procedural hurdles that impeded business initiatives. In the pace of today's climate, organisations cannot afford to be slow simply because it cannot be perfectly secured. You cannot secure everything equally. Being secure means focusing protection around the risk-sensitive assets at the heart of your organisation's mission.

Essential truths

1. No industry is immune. Every company's information network will be compromised. It is not a question of if you will be at risk but when and how you manage.
2. Cyber damages go beyond dollars. The long term effects on reputation, brand and morale, are significant and take their toll on organisations.
3. Speed of attack is increasing and response times are shrinking. Small highly skilled groups exact disproportionate damage and threat rate is increasing while response window shrinking.
4. Everything cannot be protected equally. Understanding the need to define 'crown jewels' allow you to make better risk decisions without getting caught up in noise.
5. Traditional controls are necessary but not adequate. Your protection networks and firewalls are probably high enough but it is always important to look at detective controls and new technologies.
6. Regulators and government are important stakeholders. Various privacy rules, guidelines, executive orders, consumer protection are increasing and it is important to keep updated.

Many boards hear from the chief information officer, chief technology officer, chief information security officers or others who are tasked with monitoring the cyber risk. Some company boards engage cyber security experts to speak with them about the risk, how to mitigate it, and signs that may signal a breach. However, Boards should also consider seeking feedback from key partners and customers.

Either way, boards should proactively ask questions of management, champion education and awareness programs company-wide, and treat risk as a priority, because the financial, operational, legal, security, and reputational risks posed by cyber threats are far too serious to ignore. The peril of cyber threat will continue to be present and the first step to averting it lies with the board and their commitment towards managing cyber risk.