MCI (P) 119/12/2015

SID
SINGAPORE INSTITUTE OF DIRECTORS

DIRECTORS' BULLETIN

Quarter 2, 2016

MANAGING RISKS

Taking risks

By **WILLIE CHENG**
Chairman, SID

DIRECTIONS

We are taking a risk in theming this issue of the *Bulletin* on risks.

Naysayers say, "Most boards already go overboard on conformance and risk management. We thought SID has, rightly, been pushing the notion that corporate governance is about performance, rather than just conformance. Focusing a *Bulletin* issue on risk management would be regressing."

There are some misunderstandings in this reasoning.

For one thing, though the reality is that we live in a world already fraught with risks, there are two sides to the risk equation: danger and opportunity.

For example, cyberattacks spell danger for most companies today. Yet, many technology companies have found business opportunities in helping organisations deal with the problem. Even non-tech companies can claim a competitive advantage of greater security if they are able to successfully rebuff these attacks while their competitors get hacked.

As a country, Singapore is in the risk business. Andrew Crilly and Jane Johnson drive the point home when they describe how Singapore has successfully seized opportunities while avoiding dangers to be where it is today as a successful financial and business hub (see page 6, "Changing fortunes").

Secondly, risk management is about both conformance and performance.

Yes, boards need to ensure the company performs. This is why, at SID, we emphasise the need for boards to modernise their companies' business models, set the right strategic directions and foster innovation to drive value creation. All these actions, however, must be done in the context of each company's risk environment and appetite.

Of course, regulations do exist to ensure boards and companies take an appropriate level of risk; but, quite frankly, they exist mainly because far too many companies have taken excessive risks at the expense of their stakeholders. Conformance to regulations should therefore help companies stay safe whilst preserving the opportunity to perform.

A key reason for making risk the theme of this issue is the launch of the *Board Risk Committee (BRC) Guide* on 31 March 2016. This is the third in a series of corporate governance guides for boards in Singapore.

The BRC is a relatively new phenomenon in boardrooms. While it is mentioned in the Code of Corporate Governance, it is not specifically "required" unlike the audit, nominating and remuneration committees, which have specific guidance on committee composition, duties and processes.

As a result, a board could discharge its responsibility for risk governance using a variety of governance structures and approaches. The new *BRC Guide* seeks to shed light on these matters, so do get your copy.

Meanwhile, as misunderstood as "risk" may be, we hope you will enjoy this issue, which aims to provide a contemporary and timely review of this critical topic. ■

PUBLISHER

Singapore Institute of Directors

168 Robinson Road #09-06/07
Capital Tower
Singapore 068912
Tel: +65 6422 1188
Fax: +65 6422 1199
Email: secretariat@sid.org.sg
Website: www.sid.org.sg

EDITOR

Adlena Wong

EDITORIAL COORDINATORS

Joyce Koh
Chia Yi Hui

DESIGN

Epiphany Design

PRINTER

Entraco Printing Pte Ltd

CONTENTS

FEATURES

COLUMNS

INDUSTRY NEWS

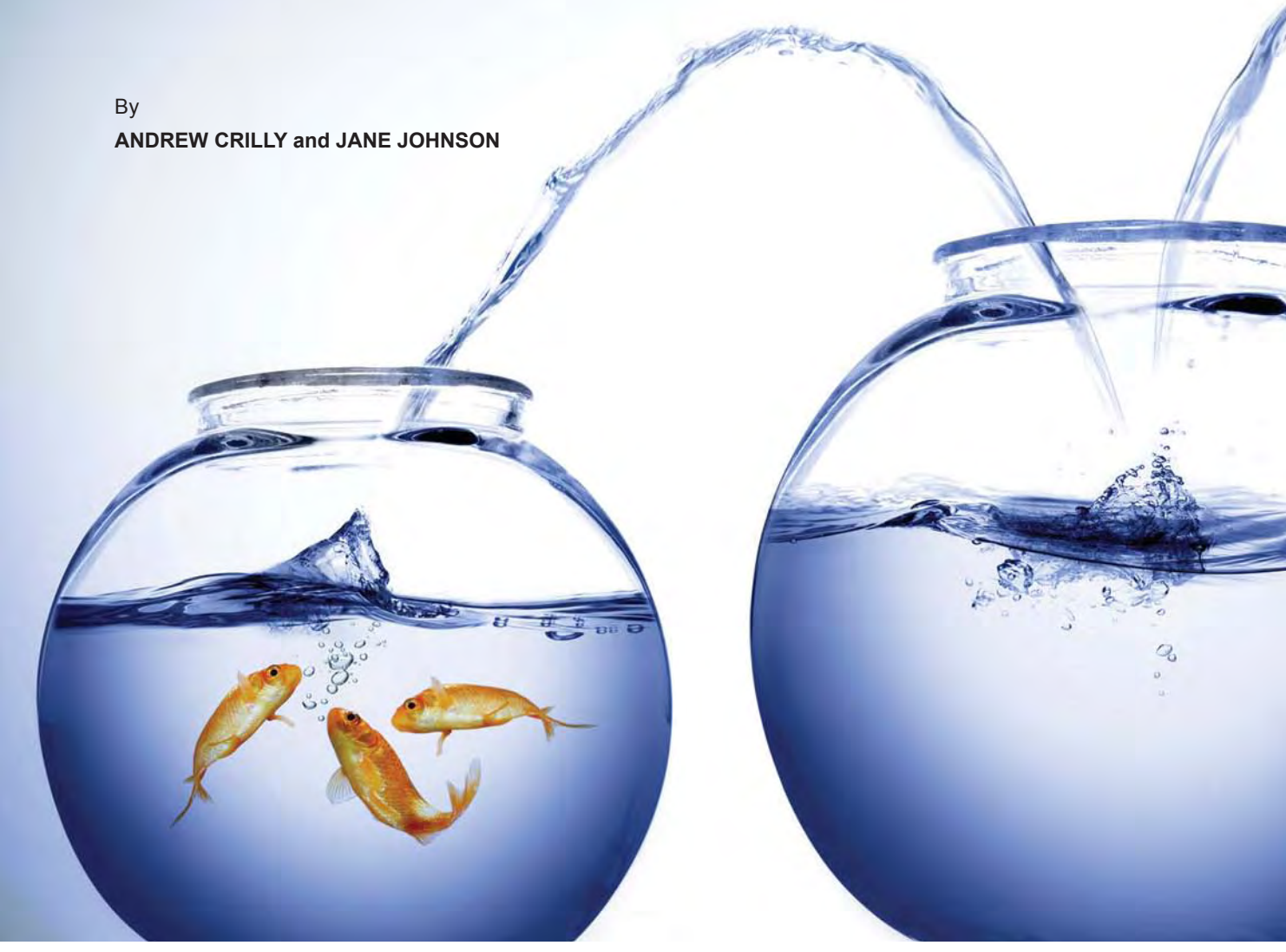
SID NEWS

SID CALENDAR

CHANGING FORTUNES:

Singapore and the risk business

By
ANDREW CRILLY and JANE JOHNSON



Singapore took a lot of risks to get to where it is today as a financial and business hub. What new risks must Singapore take to keep its hub status in a fiercely competitive world?

Singapore's Central Business District, home of the Singapore Exchange (SGX).

During the 1970s, Singapore evolved from its manufacturing base towards a value-added service economy.

In 1973, the Stock Exchange of Singapore (SES) opened its doors. Around Boat Quay it was the traders, dressed in their distinctive yellow and black tailored jackets that became the symbol of prosperity and the changing fortunes of Singapore.

Through them, Singapore secured its future as a financial hub. They were the front line of a new class of bold risk-takers who glimpsed how financial fortunes would be made in the time ahead.

The emerging hub, which was renamed Singapore Exchange Ltd (SGX) in 1999, rapidly became an active node of a worldwide network of similar financial hubs that are currently managing the risks and rewards of trillions of global transactions.

Risky Business and Singapore

Modern Singapore has always been in the risk business.

In the 1960s, the island's political leaders bet that a container revolution would happen and established the Port of Singapore as a transportation hub. They took a critical risk because at that time it was not known whether containers – standardised steel boxes that were developed during the 1950s – would take off and become the modus operandi of all the transportation industries, and especially shipping.

The uncertainties and risks involved would have evoked questions like *"What would the future*

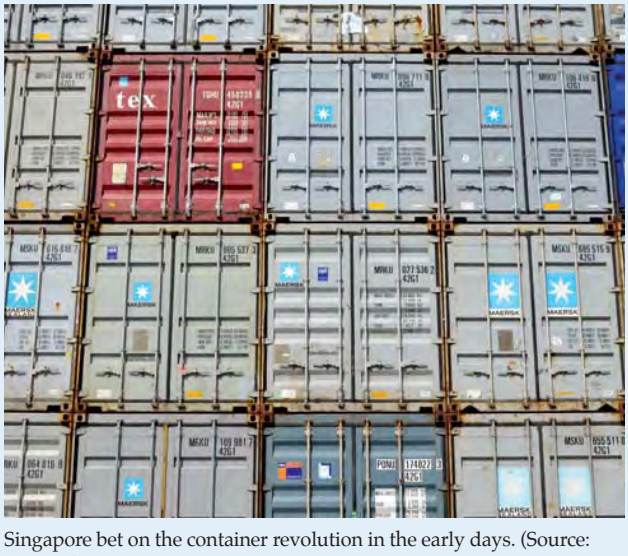
demand for the containers be?", "How well would the innovative operating base of specialist cranes function?", and *"Would the workforce be able to adjust to the revolutionary changes in cargo handling when using the cranes?"*

These amounted to massive risks of monetary and human capital. But, they all paid off.

By turning around fleets of container ships at great speed, the Port Authority of Singapore (PSA) was ahead of the game, and established what is now the largest transshipment hub in the world.

The real reward for taking those risks in the early days was that Singapore gained confidence in its nation-building programme, an achievement that at the time far outstripped the monetary gains.

This national risk was embraced in equal measure when Singapore Airlines soared above all others to make it the top destination for tourism and commerce. Singapore's facilities at Changi continue to set world standards as an air hub that leaves everybody else playing catch up. More risk, more reward.



Singapore bet on the container revolution in the early days. (Source: Pixabay)

Singapore Airlines: More risk, more reward. (Source: Pixabay)

Innovation, Risk and Changing Fortunes

Both these nation-building services ran the gauntlet of risk to reach their reward. Because of their success, we can easily take Singapore's world-class sea and air hubs for granted.

They were risky enterprises that required vision and belief. Their success led to confidence and an appetite for risk in both domestic and international markets.

Returning to the present, for Singapore to retain preeminence in the world it will have to grow a steady stream of innovation in all of its service industries. It is the only way to keep its hub status in a fiercely competitive world.

Innovation is the change that unlocks new value. This applies in many different ways and across all kinds of industries. Put succinctly, innovation leads to changing fortunes.

Taking risks established Singapore as a transport hub for South East Asia, but where are today's risks to be found?

Opportunities are Everywhere

Risk induced by innovation and change is very apparent in the financial world. Fortunes might appear to be made by chance but it is the use of

new instruments of finance that underlie success in this extremely complex world.

In truth, innovative risk should be part and parcel of every business in Singapore. To avoid risk is a risk in itself in today's world. Singapore needs to live on the edge if it is to succeed in its work. It is an imperative that applies to every Singaporean company – without exception.

We need only look at the performances of powerful city-states of the past to realise that the inspired brilliance of their citizens spearheaded their changing fortunes. The citizens with the smarts lived and breathed their innovations – they created wealth for sponsors who were also committed and took chances.

This kind of personal risk-induced success that plays such a crucial role in growing the wealth of Singapore can be readily found – one example is Creative Technology.

The Creative Story

Ngee Ann Polytechnic's most famous student, Sim Wong Hoo, fulfilled his vision of turning computers into multimedia tools for education and entertainment when he started Creative Technology.

In 1989, his trademark Sound Blaster card scooped the highly competitive world of consumer technology in bringing digital audio and music to the world via computers, an innovative move that others would follow.

The serial entrepreneur soon became Singapore's first technology billionaire, and he continues to add more innovation to the market. In 2012 his HanZpad was launched with Chinese partners as an educational innovation for upwards of 200 million Chinese students.

Creative Technology is now investing in the new round of disruptive technologies to leverage what is known as "the sharing economy".

The Sharing Economy

Companies like Uber and Airbnb are pioneering this new style of economy. These innovators have developed novel ways of providing digital services that deliver greater value by improving on the legacy value offered by traditional service providers. Once again, innovation is unlocking value that is shared among the risk-taking partners.

Uber threatens established, trusted cab companies in many countries, and Airbnb provides devastating competition for hoteliers worldwide. Their incredible success at the expense of others has raised the spectre of income inequality – that is a growing issue that will have to be addressed before too long.

Creative Technology joined the sharing economy by investing in a small Singaporean start-up that is aiming to disrupt the telecommunications industry by abolishing all telephone calling charges.

Gentay Communications developed an innovative application for mobile phones that not only provides free calls but also improves voice quality by a clever use of the internet. Its inventors, the father-and-son duo of Martin and Daniel Nygate, originally developed their application called "nanu" to add value to maritime communications and the shipping industry.

Their secret sauce is the proprietary use of lower frequencies of bandwidth to improve voice clarity – an innovation that provides a competitive advantage over the global frontrunners Skype and Viber who are among the giants of the sharing economy.

The network of innovative hubs creates wealth using digital and often disruptive technology oin a global scale. (Source: Pixabay)

The greatest risk for Gentay is poor customer numbers. This abated when it signed an agreement with India's largest smartphone provider, Intex. As nanu works for all classes of connectivity from 2G upwards it is particularly suitable for the vast Indian market.

Although the rewards may be in sight for Gentay, it is worth pointing out that risky startups have a high attrition rate. Entrepreneurial initiatives have a downside risk too.

Risk and Reward

Singapore's development as a hub city follows the traditions of the great hub cities of the past. Places like Athens, Rome, Venice, Amsterdam and London established physical hubs that allowed them to expand world trade, and they all took risks to gain the rewards that led to the domination of world trade in their times.

In the past, there was a migration of wealth from city to city. This has become a network of several innovative hubs whose wealth creation is due to digital and often disruptive technology on a global scale. As always, increases in wealth spring from opportunities that are selectively developed by clever risk-takers.

As Singapore's track record has shown, it is only the most positive risk-takers who can maintain and improve Singapore's standing as a world hub.

Singapore is punching above its weight and the business world endorses that view. The *Bloomberg Innovation Index* published in January 2016 rated Singapore 10th in the world, ahead of formidable competitors like the United Kingdom, Canada, Australia and Russia.

Singapore has always embraced risk both nationally and internationally. Its good fortune is the result of its professional commitment to the competitive, connected and sharing economy of the modern world. ■

Andrew Crilly and Jane Johnson are directors of Mach One London Ltd. This article is based on an upcoming three-book series, Risk: Journey of Discovery, by the two authors, which describes the evolution of risk from ancient times to the complex financial markets of today.


COMPETITION
FRAUD
BUSINESS DISRUPTION
CYBERATTACKS
WORKPLACE SAFETY
DISREPUTE
LIQUIDITY

GOVERNING RISK AND ALIGNING STRATEGIES

An agile and robust Enterprise Risk Management framework can contribute to the success of an organisation's strategy.

By
DAVID TOH and GREG UNSWORTH

Accomplishing business imperatives has become increasingly challenging due to technological change, globalisation and increased regulations. More often than not, businesses find themselves making regular and larger-than-usual pivots in strategy.

Given the volatile and complex environment, a continued focus on risk governance is required to safeguard an organisation's future and to help it navigate through rough seas.

The board is ultimately responsible for providing strategy oversight for the organisation, which by extension then includes the governance of risk. To protect stakeholders' interests and to avoid unacceptable levels of risk, the board needs to set the tone and direction for how an organisation approaches risks in the course of its business.

Aligning strategy and risk

Boards do this by making certain that management adopt and implement an Enterprise Risk Management (ERM) framework that ensures risks are identified, evaluated, treated and monitored in accordance with its overall risk strategy, policy and appetite.

However, a company's strategic priorities are constantly changing to address external issues (such as trends and events) and whether internal capabilities are capable of responding to business challenges. Therefore, risk information, including risk appetites and tolerances, can quickly become misaligned and outdated unless routinely updated to reflect both current and future business climates.

A good starting point for better alignment would be to ask: "What are the strategic objectives?" and "What are the strategic initiatives?". The answers can help organisations better understand their current risk processes and if these are able to support the company's growth.

In many companies, risks are usually seen as a separate entity to strategic initiatives. Thus, gaps are created between risk plans and strategic objectives resulting in a perceived limited risk reduction. This suggests an insufficient understanding of risk, where organisations do not recognise that risk is an organic component of business strategies. Business owners are unaware of existing ERM programmes or planned development of risk management capabilities.

A new paradigm is therefore required whereby risk is assumed to be part of the business environment; with its effects felt in the catalysis, implementation, and eventual success or failure of business plans.

Thus, coordination and communication between ERM teams and other business functions such as the senior management teams and planning groups must be improved. A greater risk expertise of ERM teams can then be woven into the decision-making process, through increasing the collective information pool. ERM teams would also create better designs of risk management activities aligned to both short-term and long-term strategies.

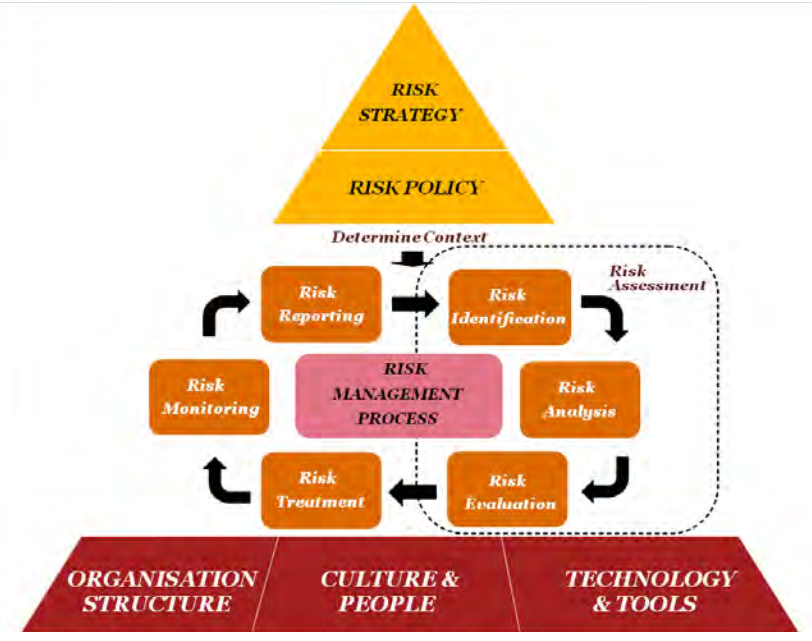
Critically, business units would be more familiar with existing and future risk capability resources. The desired aim should lead to better integration of risk management plans and enhanced organisational performance, rather than an additional hindrance.

ERM basics are still important

Beyond embedding strategy and strategic thinking into risk management, an effective ERM is important for sustainable risk management.

The key elements of an ERM includes a risk management process that starts with the identification of the risk strategy, risk policy and risk universe, through to risk mitigation and reporting. The process is governed by an

An Enterprise Risk Management Framework



- Starting at the top, the risk management strategy and policy for managing risk articulates the organisation's commitment to risk management and what it seeks to achieve through the adoption of sustainable and practical risk management disciplines.
- At the core lies the risk management process. This process provides a consistent approach for considering risk that can be built into the way the organisation determines its strategy and other key decisions, and how it designs and executes its core business activities. This step-by-step process helps to integrate the assessment, treatment, monitoring and communication of risk into the way the organisation goes about its business.
- How the organisation is structured to ensure that information on its risks and how they are managed forms one of the three key pillars supporting the framework. Risk intelligence is communicated to those that need to be aware of the information to make informed and timely decisions.
- The second pillar focuses on Culture and People, and is required to ensure that the organisation has appropriate resources and skill sets to manage enterprise risks. It also articulates the organisation's culture and core values towards risk management.
- Finally, the Technology and Tools pillar provides the mechanisms the organisation uses to sustain the risk management process in an effective manner.

organisation construct, facilitated by a culture and people equipped with the appropriate risk management tools and technologies. (See box on the elements of a risk management framework).

Integrating risk and strategic decision-making

Yet, whichever ERM framework a company adopts, it is important that risk management is tightly integrated with strategic decision making. There are many ways and places in the risk management framework where this can be done. The case studies following this article illustrates how three exemplary organisations from telecommunications, banking and healthcare industries align their risk management and strategic priorities. ■

Greg Unsworth is the Digital Business and Risk Assurance Leader of PwC Singapore and David Toh is the Internal Audit Practice Leader of PwC Singapore.

Risk Management Case Study 1

Focus on risk culture, structure and process to achieve accountability

Singtel, one of the region's largest telecommunications provider, seeks to promote a risk-centric culture, create a strong corporate governance structure, and establish proactive risk management processes.

By
TAY KIM LEE
Head Group Risk Management, Singtel

Risks can come to light in many ways and forms and impact a company's ability in achieving its objectives. Risk also has the potential to impact the reputation, regulatory, operational, human resources and financial performance of a company.

At Singtel, we have a risk philosophy (see figure 1) and risk management approach that are underpinned by three key principles: Culture, Structure and Process.

Based on these principles, the Group has put in place a risk management framework that provides oversight and accountability at the board and management levels.

The risk management framework outlines the risk governance process, as well as systematic process of responding to risks, i.e. identifying, assessing, monitoring, managing and reporting of risks. The framework also outlines the risk appetite and provides guidance on the risk tolerance levels across strategic, operational, financial and reputational aspects for the Group.

With the enhanced risk governance structure (see figure 2), board-level reporting and communications, there is emphasis on transparency, accountability and visibility of risk management within the Group.

The Group's risk management is aligned with the ISO 31000:2009 Risk Management framework. The identification and management of risks are delegated to management, who assumes ownership and day-to-day management of these risks. Management is responsible for the effective implementation of risk management strategies, policies and processes to facilitate the achievement of business plans and goals within the risk tolerance levels established by the board.

The key business risks are proactively identified, addressed and reviewed on an ongoing basis.

Figure 1: Risk Philosophy

Risk Centric Culture
- Set the appropriate tone at the top
- Promote awareness, ownership and proactive management of key risks
- Promote accountability

Strong Corporate Governance Structure
- Promote good corporate governance
- Provide proper segregation of duties
- Clearly define risk-taking responsibility and authority
- Promote ownership and accountability for risk taking

Proactive Risk Management Process
- Robust processes and systems to identify, quantify, monitor, mitigate and manage risks
- Benchmark against global best practices

Figure 2: Risk Governing Structure

The Board
- Instills culture and approach for risk goverance
- Provides oversight of risk management systems and internal controls
- Reviews key risk and mitigation plans
- Determines risk appetite and tolerance
- Monitors exposure

Audit Committee
- Reviews adequacy and effectiveness of the Group's internal control framework
- Oversees financial reporting risk for the Group
- Oversees internal and external audit processes

Risk Committee
- Reviews and recommends risk strategy and policies
- Oversees design, implementation and monitoring of internal controls
- Reviews adequacy and effectiveness of the Group's risk framework
- Monitors the implementation of risk mitigation plans

Management Committee
- Implements risk management practices within all business units and functions

Risk Management Committee
- Supports the Board and Risk Committee in terms of risk governance and oversight
- Sets the direction and strategies to align corporate risk management with the Group's risk appetite and risk tolerance
- Reviews the risk assessments carried out by the Business Units
- Reviews and assesses risk management systems and tools
- Reviews efficiency and effectiveness of mitigations and coverage of risk exposures

The principal risk categories identified are:
- Economic Risks
- Political Risks
- Regulatory and Litigation Risks
- Competitive Risks
- Regional Expansion Risks
- Project Risks
- New Business Risks
- Technology Risks
- Vendor Risks
- Information Technology Risks
- Breach of Privacy Risks
- Financial Risks
- Electromagnetic Energy Risks
- Network Failure and Catastrophic Risks
- Talent Management Risks

These risks are mitigated by the Group by continuously updating our organisational structure, talent management and development, reviewing our policies and processes, and investing in new technologies to meet changing needs. Close monitoring and control processes, including the establishment of appropriate key risk indicators and key performance indicators, are also put in place to ensure that risk profiles are managed effectively.

As the Group is also transforming and venturing into new growth areas, such as premium video, cybersecurity, digital marketing and advanced analytics to create new revenue streams, the risks associated with these new businesses are closely studied so that appropriate counter measures can be put in place.

Overall, the Group aims to continually improve the understanding and management of risks amid the evolving and dynamic environment we operate in. ■

Risk Management Case Study 2

Banking on risk management

By
ELBERT PATTIJN
Chief Risk Officer, DBS

As a leading financial services group in Asia, DBS considers risk management a core part of its business, which is now established across 18 markets.

At DBS, we manage risks on behalf of our clients who want to make deposits, payments or hedge their exposures. On the other hand, we take risk on clients that borrow from or hedge with us. In addition, we run market risk, liquidity risk, operational risk and other business risks.

Given that risk management is so much at the heart of our business, DBS has an elaborate framework for identification, assessment, measurement, control and reporting of risks. We also emphasise that every employee is responsible for and has a role to play in risk management.

We divide these responsibilities into three lines of defence, namely, the business, the control units and, lastly, the internal auditors. This becomes part of our Risk Culture, enshrining the practice that every employee of the bank is accountable for these risks in their domain, irrespective of whether they are in the front line or support and control units. The assessment of how individuals in the bank manages these risk forms an important part of their key performance indicators, appraisal, promotion and remuneration.

In order to ensure we give consideration only to risks we actively seek, DBS has in place a clear strategy that details in which markets we want to be active and with what type of clients and products. This strategy is augmented by Target Market and Risk Acceptance Criteria for each country and industry. These documents articulate the industries and geographic areas we want to be active in and under what criteria we want to engage the business, so that we have a clear, documented and shared understanding of the nature of the risks we are prepared to consider.

This understanding is further quantified by our Risk Appetite Statement. This Board-approved statement details how much risk we can take and what an acceptable risk mix is, for example, client vs. proprietary and retail vs. wholesale.

The Risk Appetite Statement considers items like our capital, rating, liquidity and profitability requirements that get translated to limits and other control measures for our credit, market, liquidity and operational risk activities. The bank's senior management is responsible for cascading these limits and control measures to the business unit to ensure adherence and report resulting exposures to the Board.

For example, we have maximum amounts we can lend in certain countries, industries, down to maximum allowable exposures to any given client. Similarly, we have an overall Value-At-Risk (VAR) limit for our market risk taking activities. We also set granular limits for currencies, interest rates, commodities and equities and these get even more granular when it comes to individual traders. Further, when managing liquidity risk,

we apply strict standards for the amount and constitution of liquid assets we need to hold to buffer potential cash outflows out of the bank.

All these risk measures are governed by a set of individual or committee authorities, policies, IT-systems and reports to ensure total risk appetite as well as the more granular limits are adhered to.

Invariably there is a growing requirement for models to be able to quantify these limits and exposures in isolation as well as in combination with one another. Prior to using these models and submitting them for approval to the regulatory authorities, we have a prudent process of developing, validating and auditing these models – all to ensure sufficient and effective challenge of the models so that business is robust enough to operate regardless of conditions.

As part of our ongoing portfolio monitoring, we observe macro or micro economic trends and constantly apply diverse scenario analyses (such as low oil prices, higher interest rates and so on) to relevant parts of the portfolio. On top of that, we apply full stress tests to the whole portfolio. All these allow us to gauge the impact of events that are outside the range of expectation and to ensure that the bank can withstand very severe headwinds.

DBS has a detailed and documented Recovery Plan that outlines the steps to be taken to recover from a stress situation. We even run "reverse stress tests" that are designed to "break the bank" so we are able to identify what catastrophic events could give rise to such an occurrence.

Outside of looking at the traditional risks, we proactively identify and monitor top and emerging risks which, should they materialise, may have a significant impact on our business activities, financial results and reputation and affect our ability to deliver against our strategic priorities. ■

Risk Management Case Study 3

Driving strategic alignment through a risk appetite framework

As the shared IT service provider to public healthcare in Singapore, IHiS manages IT investments and resources strategically in accordance with the risk appetite of its key stakeholders.

By
CHONG YOKE SIN
Chief Executive Officer,
Integrated Health Information Systems

Information technology (IT) plays a critical role in the delivery of healthcare services for our Public Healthcare Institutions (PHIs). IT provides the foundation for the integrity and privacy of healthcare records that are critical for the right decisions for the patient to be made.

As part of the healthcare family, Integrated Health Information System (IHiS) creates value by collaborating with PHIs to transform care through strategic IT planning, cost effective implementation of IT systems, efficient IT operations, and leadership in innovative IT solutions.

IT investments and resources must be directed strategically to deliver the right outcomes and in accordance to the risk appetite of the healthcare landscape. This does not in any way curtail innovation. Rather, a risk appetite approach to strategic planning and execution enables our organisation to realise its strategy with a practical approach that ensures success.

The IHiS risk appetite framework provides a useful tool in communicating the rationale for the strategy and execution path for the board, PHI stakeholders and staff. It articulates what the bets are for the organisation, why these decisions were taken and how we intend to get to the destination while considering the risks and mitigating strategies along the trajectory.

The risk appetite approach is a living one where the level of risk is continuously adjusted based on the state of the foundation and landscape achieved. This approach in communicating strategies with staff engenders trust and commitment within the organisation, necessary for success in any execution.

IHiS established a risk appetite framework that divides its acceptable and undesirable risks into strategic, financial and operational parameters within which the company's business model is executed.

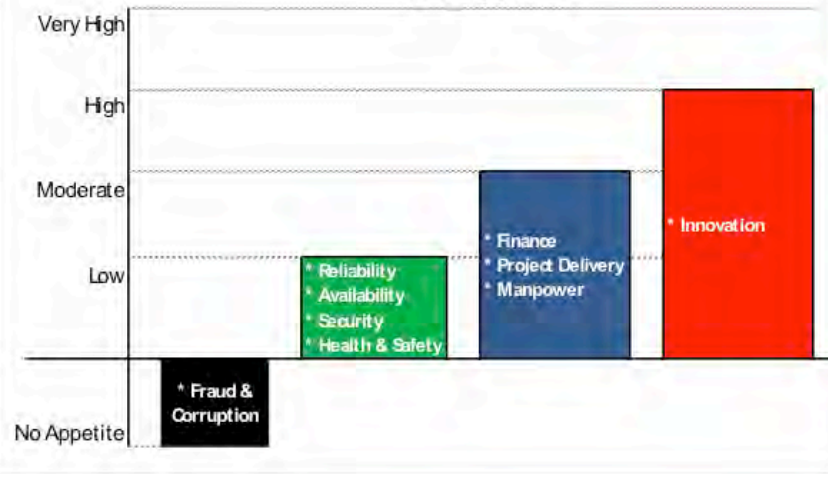
A corresponding risk appetite definition process draws implied risk appetite statements from historical risk-taking decisions (e.g. investments in technology), incidences (e.g. cyber incidences, frauds), strategic objectives (e.g. innovations to develop enterprise architecture components), risk profiles (i.e. current risks that are being managed), and organisational limits (e.g. financial authorisation limits).

Using the implied risk appetite, IHiS formulated its risk appetite statement (see box) around business drivers to communicate the tone and expectations from its leadership to its stakeholders expressing what and how much risk it is willing to take.

IHiS Risk Appetite Statement

Systems Reliability, Availability and Security

We recognise PHI's ever growing reliance on IT and the increasing security issues due to cyber threats. As the reputation of public healthcare is tethered to the reliability, availability and security of the IT systems we manage, our risk appetite is very low. For the same consideration on integrity, we have zero tolerance against corruption and fraud perpetuated by our staff, vendors and other stakeholders.



Project Delivery Services and Manpower

We take a moderate risk appetite to project delivery services and manpower as we deliver a wide of range of IT systems of varying size, criticality and complexity that require careful balancing of time, limited resources and risks. IHiS recognises that our staff could be exposed to health hazards when they discharge their duties in the healthcare environment. Thus we have a low risk appetite for health and safety risks, and will take robust measures to protect our staff, consistent with the health and safety policies of the healthcare institutions we serve.

Financials

Our risk appetite for financial outcomes is moderate to support the risk appetite in project delivery services, manpower and innovation, for as long as we are operating with a healthy operating cash flow. This posture to finance will enable us to support the growth in healthcare IT and keep us in line with public healthcare concerns to contain and keep its costs manageable.

IT Innovation

Our risk posture in innovation is high, in order to provide leadership in the adoption of technologies for the pursuit of excellence in healthcare. We will lead in the exploration of IT technologies, validate its efficacy and set the pace for adoption in order to minimise the IT risk exposure to the PHIs, but we will maintain congruence with risk appetites related to reliability, availability, security, manpower and financials.

IHiS risk appetite statement reflects its risk management philosophy to develop a culture which manages risks holistically across the organisation that is aligned to strategy and consistent with the public healthcare stakeholders it serves. It is, however, not cast in stone and changes in accordance to the dynamic and ever growing public healthcare environment. The framework and definition process enables future risk appetite dialogues with stakeholders so that IHiS can better weather the changes while supporting the fulfilment of the Singapore Healthcare 2020 vision. ■

The importance of defining risk appetite

By **IRVING LOW**
Council member, SID

COUNTING BEANS

Under Singapore's Code of Corporate Governance, the Board should determine the company's level of risk tolerance, specifically the nature and extent of the significant risks it is willing to take to achieve strategic objectives (Principle 11). In practice, this task is often delegated to either the Audit Committee or the Board Risk Committee.

With the increased importance of operational risks today, the scope of this task has grown substantially. So has the audit committee's workload. A recent KPMG global survey of audit committees found that over half of audit committees in Singapore now spend significantly more time fulfilling their responsibilities.

Risk oversight is critical to any company. Good risk oversight reduces the odds that a company will experience going-concern issues. However, risk oversight now constitutes a very large proportion of the audit committee's workload.

To some extent, this increased workload may be attributed to an insufficient understanding of the board's risk appetite. For example, if a board has not adequately defined the amount of risk it is willing to accept, the audit committee may end up simply adding every new issue to its agenda - even those that do not warrant the board's attention.

To better balance the workload, boards should attempt to gain a better understanding of their risk appetite.

Difficulties with Understanding Risk Appetite

Several issues may impede the board's understanding of risk appetite.

The first is the "check-box" approach that many boards take to defining their risk appetite or risk tolerance. However, the "check-box" approach may not be the most effective as it may be too generic in nature. It may even add to the burden of the audit committee by being too conservative resulting in a larger volume of risks/decisions being escalated or by being poorly defined leading to inconsistencies in the company's risk management policies. Boards need to consider whether their definition is appropriate to the company's situation.

In other cases, the board may not have a sufficiently good understanding of the company's strategy and risks. Hence, they are unable to determine the specific levels of risks that are acceptable for the company's current position.

Another possible obstacle is that the audit committee may not have received sufficient or quality information about key risk areas. For example, the KPMG survey discovered that 40 per cent of audit committees in Singapore felt they did not receive quality information on critical risk areas such as supply chain risk, cyber security, and systemic risk. Such lack of information may prompt the audit committee to take a conservative position regarding risk appetite.

Attaining a Clearer Definition

The most basic method of defining risk appetite is to consider the company's current stage of growth. The faster the company wishes to grow, the higher its risk appetite should be. Then when the company reaches or wishes to maintain a stable state, the board should moderate its risk appetite.

The company's industry will also significantly affect its risk appetite and tolerance. In the fast-moving high technology industries, for example, companies may have a much higher tolerance for risk. But in regulated industries such as the financial industry where compliance is of great importance, the risk appetite should be very low.

To minimise the possibility of "mission creep" – the addition of more items to the audit committee's agenda regardless of relevance or necessity – boards and audit committees need to ensure that they have a solid understanding of the business strategy and risks.

To better balance the workload, boards may also wish to reallocate their risk oversight responsibilities. This may involve creating new committees to focus on specific categories of risks such as Health and Safety. Several boards in Singapore are already moving in this direction.

Boards may also consider bringing in additional expertise, depending on the company's direction. For example, if a company is in a phase of inorganic growth, the audit committee might wish to include M&A expertise.

At the same time, boards and audit committees need to communicate more closely with management, especially key functional personnel such as financial controllers or information officers. This would help to improve the information they receive about key risk areas, and contribute to their understanding of the business.

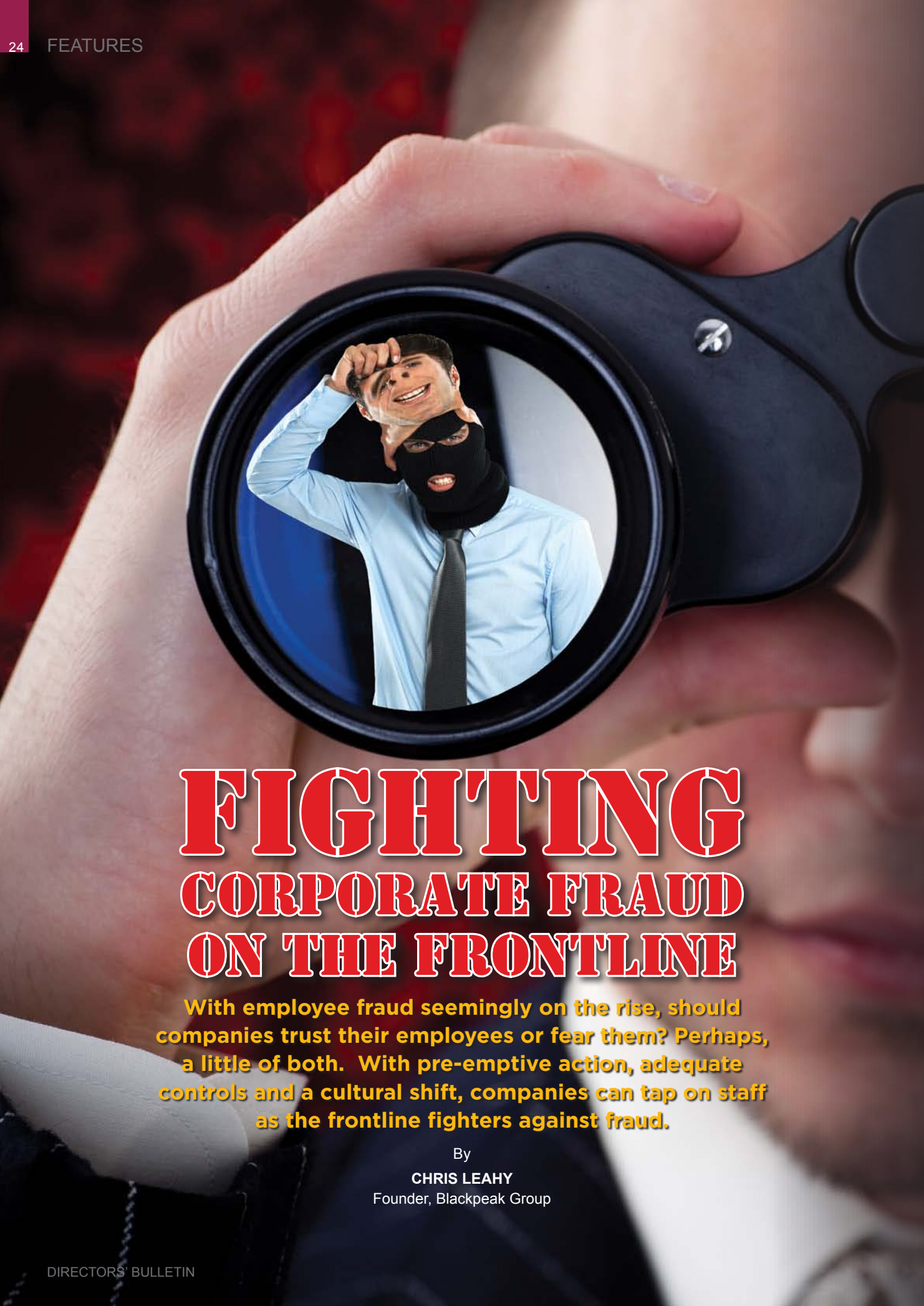
A Tool to Enhance Performance

In today's operating environment, it often appears difficult to attain both effective risk management and a balanced workload for the audit committee. Risk appetite can act as a tool to achieve and enhance the company's performance.

A well-defined risk appetite acts as a tool to regulate the audit committee's workload by streamlining its agenda. The potential benefits of this include more time for quality discussions, a deeper understanding of the business, and better understanding of the board's risk oversight responsibilities.

Risk appetite also acts as a guideline for the board to set clearly defined limits on what the company can do and what it should avoid. This may extend to various aspects of the company's operations, including investment strategy, growth plans and even talent recruitment.

At the end of the day, risk appetite regulates many other large and small decisions that have significant impact on a company's performance. The better articulated the board's risk appetite is, the more useful it will be. ■



FIGHTING CORPORATE FRAUD ON THE FRONTLINE

With employee fraud seemingly on the rise, should companies trust their employees or fear them? Perhaps, a little of both. With pre-emptive action, adequate controls and a cultural shift, companies can tap on staff as the frontline fighters against fraud.

By
CHRIS LEAHY
Founder, Blackpeak Group

Employee fraud is always there. It does not increase with or during recession. It may be that it just becomes more visible and less easy to hide. However careful a company, if a rogue employee is determined to steal, chances are he or she will do so, and quite possibly get away with it.

Rogue employees are of course the exception and not the rule. But it is often the company that creates the environment that breeds such employees. To illustrate the point, let us consider two separate significant internal fraud investigations.

The first involved the Singapore office of a global commodities trading company. Following the exit of a trader under controversial circumstances, allegations emerged of non-arm's length deals between firm clients and certain senior traders. An investigation revealed the allegations to be true and also uncovered other questionable transactions undertaken by staff, including some senior management. These included transaction skimming, front running trades and questionable business expenses.

The second case concerned the systematic theft of raw material over several years from a Singapore manufacturer by a single employee. After an anonymous tip-off via the firm's whistleblower system, investigators uncovered the extent of the theft, which ran into millions of dollars, after an exhaustive and costly inquiry.

Lessons

While the cases were quite different, they shared two key similarities that explain how the frauds occurred and how they were discovered. They offer important lessons for companies keen to combat internal fraud.

First, the frauds occurred due to weak internal controls. This created an environment that allowed employees to commit fraud. This is not an excuse for the crimes of course, but it is a difficult truth for many boards to accept that weak internal controls, poor oversight and a lack of accountability are present in any significant fraud case that is being investigated.

Second, on a more positive note, both frauds were uncovered through the same means: a whistleblower, in one case anonymous (but almost certainly an employee) and in the other, a recently departed staffer. Why is this significant? Because invariably when internal fraud is committed, somebody inside knows, or at least knows something.

In the case of the global trading firm, several staff interviewed onsite during the investigation held valuable information that helped proved the case. Why did none of them blow the whistle to head office? Reasons vary, but often staff are fearful of local management and losing their job, or just helpless in general. In this instance, the eventual whistleblower approached head office after the Singapore management fired her.

Unchecked, fraud in an organisation can become cancerous and spread rapidly. Staff at the global trading firm watched as traders acted dishonestly while some decided to join in defrauding the company. Opportunity and means gave rise to rationalisation – the classic employee fraud triangle.

The "lone wolf" employee at the manufacturing company was able to act with impunity for years due to the absence of adequate checks and balances, such as separation of duties, adequate reporting and accountability. He had unfettered access to areas his job had no right to and enjoyed de facto signing authorities that could not be justified by his rank in the firm. Why did he commit the crime? The opportunity was there, the need was fuelled by a taste for gambling and high living and he was able to rationalise his actions (at least in his mind) by explaining with conviction that he had served the company faithfully for years and was sick of seeing senior management paid so much.

Spot the Fraud

Detecting fraud inside a company is not easy. There are many potential "red flags" (see the table for a non-exhaustive list) but identifying such signs is not conclusive; rather, it indicates the need for further investigation.

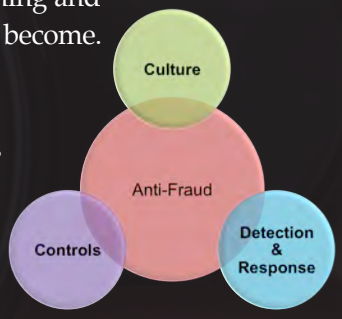
In the two investigations, there were red flags everywhere. Local management of the trading firm was able to onboard new clients with no background checks and no head office approval. The same executives that placed trades also approved settlement of such trades, including the movement of funds. Expense accounts to entertain firm customers were overly generous and some expense items were suspect.

The rogue manufacturing company employee behaved erratically and roamed the factory at will. His authorising signature appeared on control forms that he compiled, while the simplest of checks revealed a lifestyle that could not be supported by his salary nor his background.

Company, Heal Thyself

When it comes to internal fraud, prevention is always better than cure. While no anti-fraud system can ever be completely fraud-proof, installing a robust system is always cheaper than dealing with internal fraud post facto. Yet many boards seem to believe that fraud is something that happens to other companies and eschew preventive measures on cost grounds. This is penny wise and pound foolish: ask the directors of any company hit by internal fraud how costly, time-consuming and stressful such events can become.

A comprehensive anti-fraud system comprises three inter-related components of culture, controls, and detection and response.



Red Flags: A Selected List of Warning Signs

WHERE	WHAT
Purchasing	Sudden change of vendor(s) and/or changes in purchase behavior and/or timing of purchases
	Unusual purchase volumes and/or concentration
	Strange or unclear invoice descriptions
	Invoice slicing (large invoices split into multiples below approval thresholds)
	Unexplained agency/consultancy agreements
	Unusual RFP/tender processes/timings
Accounts receivable	Unusual/sudden changes in collection patterns
	High level of customer complaints
	Unexplained differences between sales, inventories and cash receipts
	High level of transaction amendments/overrides
	Frequent changes of customer details/processes
Accounts payable	Frequent cost over runs on budget
	Incomplete/improper procurement and/or payment approvals (missing documentation, account changes)
	Unusual payee details (name, address, bank account)
	Incomplete vendor files (information, approvals)
Staff	Never take leave/refuse to share duties or delegate
	Sudden changes in behaviour/demeanour
	Lifestyle issues: gambling, unexplained wealth, addiction
	Unexplained or unjustifiable expenses
	Unusually close relationship with vendors/customers

It begins in the boardroom, with a fundamental governance decision to establish, inculcate and enforce a zero tolerance policy towards fraud. Without buy-in at the board level, any anti-fraud policy is doomed from the start. The "tone at the top" needs to cascade to management and staff through socialisation and training. Explaining why as well as how the system is being implemented, emphasising its democratic nature — that it will apply to all staff, irrespective of rank — helps generate ownership among employees.

The company should establish clear policies, controls and procedures and follow them without exception. The detailed requirements are too numerous to state here, but entail a clear separation of duties, accurate reporting and careful monitoring and follow up. Diligence begins early, with adequate background screening of all prospective employees, integrity checks on vendors and counterparties and investigative and reputation due diligence on all material transactions.

Finally, the company should implement a clear and consistent system of detection and response, leveraging both internal resources, such as internal audit, as well as external help, including auditors, lawyers and investigators. Establishing a clear and unambiguous independent reporting line for this system, typically reporting into the Audit Committee, is vital.

Adopting a formal whistleblowing system, including a hotline for staff and other stakeholders to report suspicions, can help enormously to eradicate fraud within an organisation and enforce the "zero tolerance" policy. Surveys of multinational companies show that hotlines are consistently the best source of information of fraud within a company, with most information coming from staff.

Call to Action

Sadly, even the best anti-fraud systems may not exempt a company from employee malfeasance.

When a fraud hits...

Do:

- Respond to any fraud incident swiftly.
- Establish a crisis management team of appropriate internal and external resources.
- Develop a logical and cogent plan of action with clear responsibilities and communication channels.
- Identify actual or potential evidence (e.g.: email/IT, files) and secure it.
- Devise a communications plan – internally and externally – and agree when and how information is disseminated.

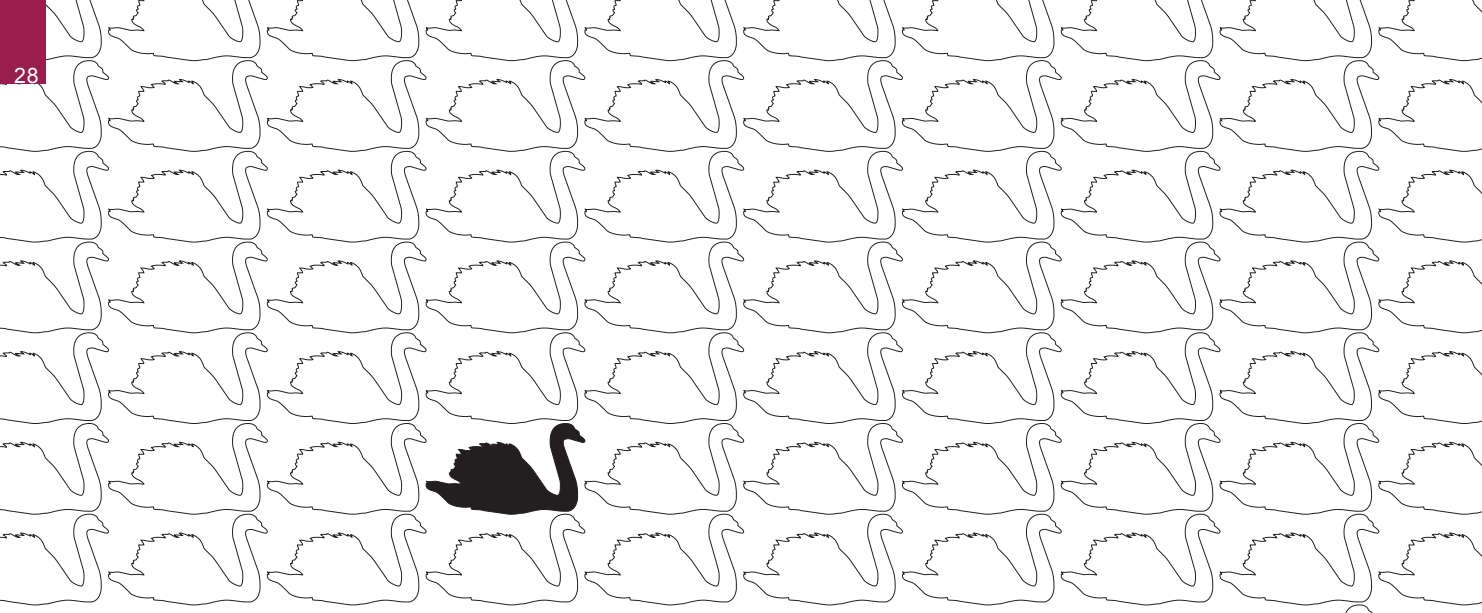
Don't:

- Pretend the problem doesn't exist: inaction is the worst response.
- Try to manage the process internally: separating directors and management from any investigation provides an important buffer.
- Form precipitate conclusions or theories: let the facts of the case emerge.
- Start interviewing suspects or witnesses without facts and before it is established who is complicit.
- Interfere with potential evidence for whatever reason.

So what should companies do if they find "red flags" or when someone blows the whistle?

The first rule is to act decisively and promptly in a planned and coherent way. The box "When a fraud hits" provides a list of "dos" and "don'ts" for effective action.

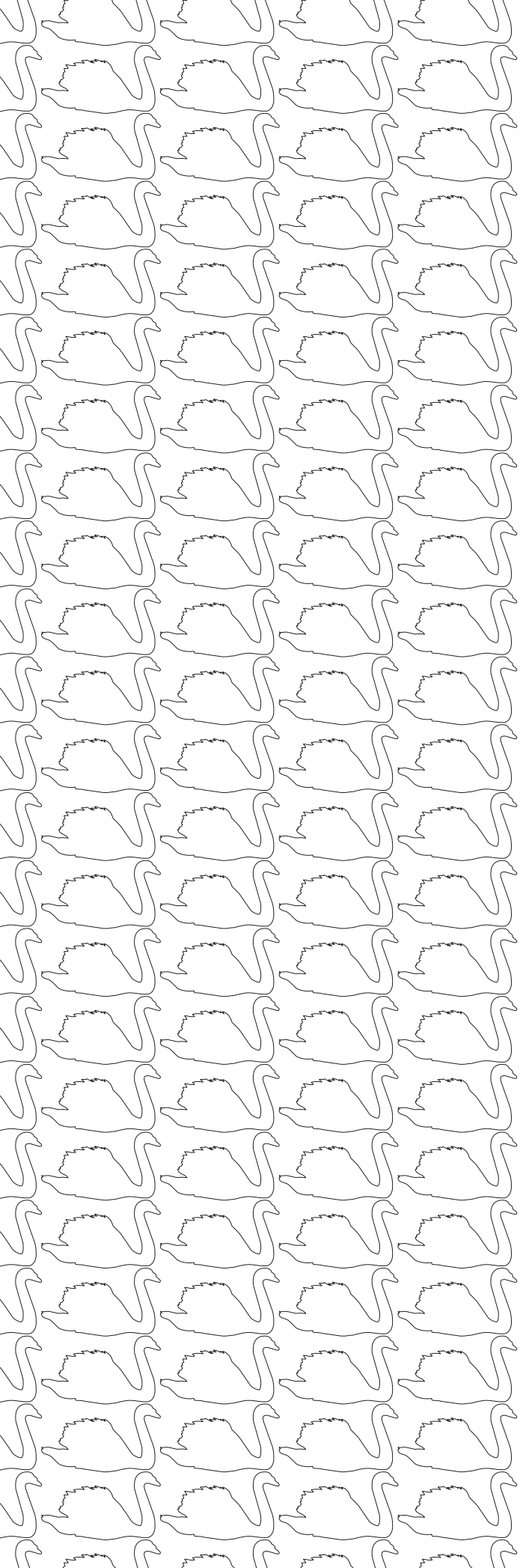
While internal company fraud by definition entails employee malfeasance, the truth is that a company's staff remains its first and most effective line of defence against fraud. Helping employees help the company combat fraud through anti-fraud and whistleblowing systems vests trust in staff and empowers them. And this will save the company time, money and angst in the long run. ■



Anticipating black swans

"Black swans" are monumental and highly surprising events. Yet, they are often rationalised on hindsight as possibly predictable. Can the "unknown unknowns" be predicted?

By
DAVID CHEW
Executive Director, Risk Consulting, Deloitte Southeast Asia



What do the rise of the Internet, September 11 attacks and the Arab Spring have in common? Observers have called them "black swan" events – unprecedented and unexpected, just like how amazing it is to find a black swan in a flock of regular white ones.

Nassim Taleb who developed the theory of black swan events in his book, *The Black Swan: The Impact of the Highly Improbable*, characterises a black swan event as:

1. One that is a total surprise; an outlier that lies outside the realm of regular expectations, because nothing in the past can convincingly point to its possibility.
2. One that has a major, or even, catastrophic impact.
3. When done and dusted, it is rationalised, on hindsight, as something that could have been expected.

While once extremely rare, black swan events now seem to be uncommonly common. Today's upheaval of the market place by digital disruptors the likes of Uber and Airbnb have the hallmarks of a black swan.

A recent report, *Patterns of Disruption: Anticipating Disruptive Strategies in a World of Unicorns, Black Swans, and Exponentials* by Deloitte, noted that disruption tend to go undetected until it is too late; it is also a lot easier to identify them in retrospect, as in the case of a black swan event.

Top Five Risks to Businesses

Top Five Global Risks By Impact	Top Five Global Risks By Likelihood	Top Five Risks for Singapore
1. Failure of climate change mitigation and adaptation	1. Large scale involuntary migration	1. Cyber attacks
2. Weapons of mass destruction	2. Extreme weather events	2. Asset bubble
3. Water crises	3. Failure of climate change mitigation and adaptation	3. Energy price shock
4. Large scale involuntary migration	4. Interstate conflict with regional consequences	4. Terrorist attacks
5. Severe energy price shock	5. Major natural catastrophes	5. Spread of infectious diseases

Source: The Top Five Global Risks (By Impact and Likelihood) are based on the *Eleventh Global Risk Report* (World Economic Forum, 2016). The Top Five Risks for Singapore are based on responses to the *Executive Opinion Survey (World Economic Forum, 2014)*.

Searching for the Black Swan

To respond effectively to the disruption requires the incumbent to first and foremost concede that the threat as it is, is happening. Such concession is hard to come by. This is usually due to cognitive biases that are made up of confirmation biases (favouring outcomes which more aligned to a particular view), herd mentality (following competitor or market actions, often based on imperfect information), and ambiguity bias (preference for outcomes with greater certainty).

If one could rise above these biases, there are patterns and trends preceding catastrophic events that may be extrapolated to predict black swans.

For example, the World Economic Forum has tabled the top risks to businesses (see box on "Top Five Risks to Businesses"). These risk factors are the "known unknowns" whereas black swan events are usually associated with the "unknown unknowns" (see box on the "Basic Sources of Risk and Uncertainty").

Basic Sources of Risk and Uncertainty

	Knowns	Unknowns
Known	Things we are aware of and understand	Things we are aware of but don't understand
Unknown	Things we understand but are not aware of	Things we are neither aware of nor understand

Note: Former US Secretary of Defense Donald Rumsfeld was quoted as saying in 2002: "... as we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns – the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones." His remark has led to much discussion and adaptation of approaches to risk management.

However, if a few of the "known unknowns" that have been trending as the top risks in the last few years were to converge, it is possible to see glimmers of black swans or disruptions to the Singapore economy as follows:

Large scale involuntary migration + Profound social instability → Refugees at our borders?

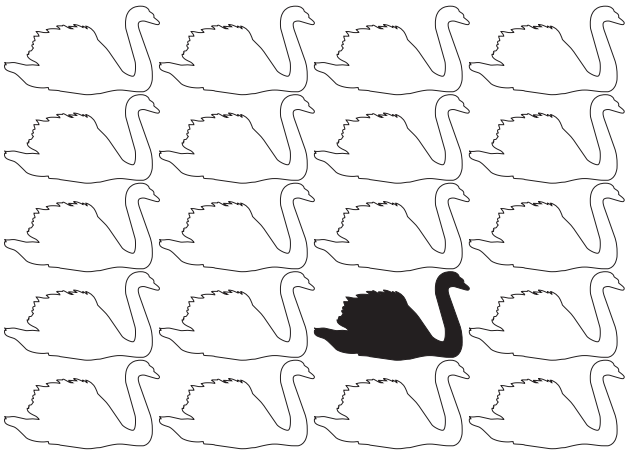
Major natural catastrophes + Extreme weather events → Destruction of key infrastructure?

Severe energy price shock + Interstate conflict with regional consequences → Fiscal crises

On their own, the global risk factors are seemingly remote to Singapore. However, a confluence of two (or more) of these "known unknowns" could well turn into black swan events in Singapore. The confluence of the risk factors identified above has been limited to two for illustration purposes. In reality, this is closer to infinity, and comes in various permutations and weightage.

Go Beyond Traditional Risk Management

Traditional approaches for managing risk tend to focus on monitoring available financial, economic or event operational indicators as well as qualitative (and subjective) assessments. However, because these approaches are generally based on (limited) facts and experience and clouded by judgment and perception, the resulting mitigation strategies and hedges are not capable of detecting future catastrophic risks or predicting future performance.



This relegates a strategic risk management plan to a mere incident response plan. Instead, there should be thought given to, and preparation made for the eventuality of such critical risks.

To make up for limited knowledge and experience and to cope with the endless permutations of risk factors, we should look outside of traditional structures and methods, develop new ways of gathering data and insights, and appreciate other perspectives. The last, seeing things from other points of view, is particularly important as cognitive biases is reduced through introduction of diverse perspectives.

Lastly, in an era when risk can become reality in the blink of an eye, we should re-examine the very assumptions we hold dear and the decision-making process that has worked (thus far). As philosopher Bertrand Russell advised: "In all affairs, it's a healthy thing now and then to hang a question mark on the things you have long taken for granted."

It is only through constant challenge of our assumptions, no matter how fundamental, that we will be able to keep complacency at bay and react at the first sign of trouble.

If black swan events are truly unpredictable, the one who detects it faster than the others will have an overwhelming competitive advantage. ■

The rise and rise of unicorns

By **ROBERT CHEW**
Council Member, SID

INNOVATION

Unicorn. To the layperson, it is a mystical creature that exists in the realm of fantasy. However it is also a trending term for a privately-held startup that has achieved a billion (US) dollar valuation.

Back when the word "unicorn" was conjured in 2015, only 39 companies were deemed to have gained this legendary status. The number crept up to 81 in the same year, according to VentureBeat. By the first month of 2016, we are looking at 229 unicorns, with a combined worth of US$1.3 trillion.

Among the 229 unicorns are now-household names – Uber (worth US$51b) and Airbnb (US$25.5b). While US-based companies dominate the list, those from China such as mobile device maker Xiaomi (US$45b) and ride sharing company Didi Kuaidi (US$15b), as well as India's e-commerce tour de force, Flikart (US$15b), are proving to be more than storied successes. Singapore too has its share of unicorns, including GrabTaxi (US$1.5b) and gaming device manufacturer Razer (US$1b).

Beyond your Imagination

With that much moolah exchanging hands, it begs the billion-dollar question: "Are these unicorns really the fabulous moneymakers they are made out to be?" And with 10 per cent of them emerging as "deacons" (read: startups with valuation above US$10b), are they really worth that much?

Consider WhatsApp. It is a messaging application that has a billion users globally. On 19 February 2014, when Facebook announced its plan to acquire it for US$19b, WhatsApp had 417 million users. It more than doubled its user base in two years. Yet, it has accomplished this growth and scale with a small engineering team of no more than 50. WhatsApp is the exemplar of young, nimble unicorns operating in a time of fast moving, exponential change driven by technology. It is disrupting the communications landscape and forging new markets.

Now let us look at Facebook – the company that acquired WhatsApp. Many (myself included), had considerable doubts about the potential of Facebook in its early pre-IPO days. It was not the first social media startup. It was not generating revenue, let alone profits. But it became a unicorn when Russian investment group Digital Sky Technologies invested US$200m for a 1.96 per cent stake in the company, giving Facebook a US$10b valuation.

So what sets the deacons apart from the unicorns? What makes them worth their billions? Like Google, they were not necessarily the first in the market. Google was not the first to provide internet search and advertising. Neither was WhatsApp trailblazing the online messaging system, nor Facebook a first-mover in social networking.

Simple. These companies are what they are because they fulfilled a demand – at a scale and at unprecedented speed.

Google found a better way to provide search results using the founders' Page Rank algorithm.

WhatsApp delivered messaging functionality using a minimalist approach to large scale infrastructure deployment with an open source operating system and a computer language designed for concurrency. Facebook started off as a platform for college students, meeting their dire need for an identity and relationships using a simple user interface, then innovated with their BigPipe system that served dynamic web pages much faster.

In short, they disrupted – in a way they knew how and knew best. Their brand of disruption leverages the exponentially improving capabilities of digital technologies. To do this, however, requires smart geeks, people with the depth of technical skills and knowledge, matched with people who profoundly understand what users and consumers want and need. When done right, unicorns are no longer mythical organisations, they become giants that incumbent businesses must reckon with.

Walking among Giants

The tech giants of today – Apple, Facebook and Google – were once not very dissimilar to today's unicorns. They were disrupters and understand the risk of being disrupted. To mitigate this risk, these tech giants scan, track and assess startups much like allowing the latter to test new products and markets. Just as these startups are becoming successful, these giants would acquire them.

Over the last decade, Google has been one of the biggest and most successful acquirers in the tech industry. It purchased YouTube for US$1.65b in 2006, DoubleClick for US$3.1b in 2007, Waze for US$0.97b in 2013, and Nest for US$3.25b in 2014. Probably one of Google's most deployed acquisitions was Android, the dominant operating system for mobile devices, which it acquired for US$50 million, a drop in the bucket, compared to the value of a unicorn.

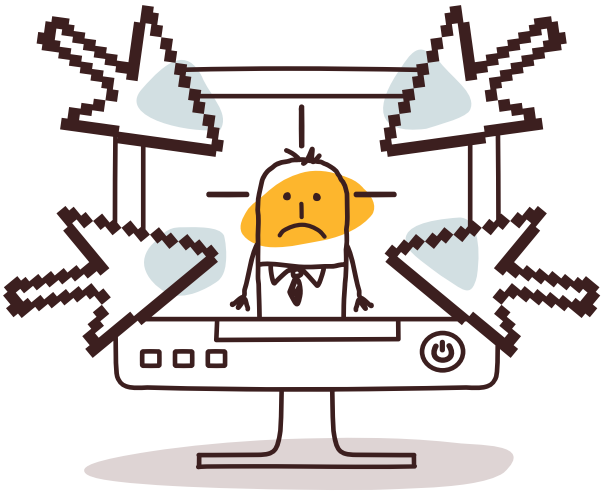
Traditional non-tech companies have also been trying to mitigate the risk of being disrupted by sending their corporate development staff to look for possible acquisitions in Silicon Valley and beyond. Walmart was among the earliest to do this, acquiring Kosmix (a web guide) in 2011, renaming it @WalmartLab and locating it in Silicon Valley, miles away from the retailer's Arkansas headquarters. The retailer has steadily acquired more companies and technologies in its fight to compete with Amazon.

Other examples span a variety of industries. In 2013, Monsanto, a multinational chemical and agricultural biotechnology corporation, bought big data weather company Climate Corporation for US$1.1b. Insurer UnitedHealth Group bought health data analytics company Humedica for a reported "hundreds of millions of dollars". Fitness clothing retailer Under Armour bought fitness tracking app developer MapMyFitness for US$150m.

The rise of the unicorns not only reinforces the view that digital technology is indeed disrupting businesses and industries but also signal the need to keep scouting new technologies and talent – through acquisition – has to persist in order to survive and prosper in the process.

It is unwise – even in the backdrop of a volatile 2016 – to think that the unicorns, akin to its fabled creature counterpart, are not going to live on and leave their legacies. ■

MANAGING REPUTATIONAL RISK IN THE DIGITAL AGE



A company's reputation is a measure of relative public trust and growing it is every organisation's end goal. But the digital age signals a more cautious approach.

By
KATE HOLGATE AND SIOBHAN GORMAN

It is safe to say companies with a strong reputation are trusted more than their competitors, which lowers their operating costs and increases their license to operate.

As a business grows and interacts with a larger and more diverse group of stakeholders, its reputation becomes more broad-based. Historically, this growth has tended to make a company's reputation more resilient. In the digital age, however, this broader exposure increases a company's vulnerability to catastrophic reputational risk.

Directors of companies, whether privately owned start-ups or publicly listed blue chips, are increasingly focused on their role as guardians of corporate reputation.

While the old favourites of scandal and business failure will always be on the "worry list", increasingly, data breaches are taking the top spot with boards and management teams around the world, who are justifiably concerned about the reputational risks from mishandling a breach.

See box for a check list of agenda items that directors can go through to see if their corporate reputational risk can be safeguarded.

In the wake of a string of high-profile breaches across a range of sectors in recent years, it is clear that poorly-managed cyber crises can result in enduring, profound damage.

The Worst that Can Happen

One of the takeaways these crises is that the biggest mistake companies can make is to say too much, too soon, and too confidently.

In the days immediately following a breach, no company can fully know the scope and effects of the incident. Providing too much detail early on is the first step down a road of repeated, and uncomfortable, corrections of your own story, which effectively is a "spin-cycle" erosion of your company's credibility.

Target Corp., for example, initially said 40 million customer records were affected by a breach that occurred on December 2013. A month later however, it revised that figure up to 110 million.

Similarly, Home Depot Corp. in September 2014 said 56 million customer credit card records were affected, and a month-and-a-half later, the total customer records affected came to be 109 million.

U.S. officials said in June 2015 that a hack of the Office of Personnel Management affected four million current and former federal employees, and a month later, said there were two breaches that affected nearly 22 million.

Lines of Defence

When a data breach does unfold, what rules should leadership live by?

First and foremost, focus on authenticity and customer needs. Using overly legalistic and technical language in external statements can be off-putting – especially for customers.

Show stakeholders – employees, business partners, investors, and the public – that you are investigating and managing a breach competently and confidently will help preserve your company's reputation.

That said, the best response to a reputation breach reflects thorough planning and practice. This is prudent as corporate boards are increasingly asking what management is doing to prepare for violations, even as many companies continue to punt on preparedness. At a recent computer security conference in Dallas, only a few hands – of hundreds – went up when attendees were asked if they had ever participated in a company-wide cyber security drill.

Scenario-based planning is one of the most useful actions a company can take in advance of a breach. Developing relevant and usable preparedness materials allows companies to resolve internal frictions before a crisis, address business continuity concerns, and clarify who will speak for the company.

That plan can be tested with a company-wide drill or "war game." Planning should also take into account new cybersecurity threats. Take into reference the latest risks; recent examples include the Big Data Breach, with the theft of troves of data from healthcare companies, the US Office of Personnel Management, and others.

After the deluge ends, the best next step a company can take is to immediately begin preparing for next incident. Assess strengths and weaknesses and incorporate them into your future response plan.

Corporate Reputation: A Director's Check List

In today's hyper-transparent and super-connected world, here are questions for a director to ponder over:

1. **Stakeholders:** How does the company track and engage leading representatives of the groups who can impact the company's future? Do they have what they need to act as ambassadors for the company?
2. **External profile:** How do the company's website and other traditional and digital media assets stack up against its peers? Does it proactively manage its external profile?
3. **Monitoring:** Does the company know what people think about its business, investment case and employee proposition?
4. **Business in society:** Does the business help meet a societal need and how does it demonstrate that aspect of its value?
5. **Thought leadership:** How do you help observers understand your markets and the trends you are seeing?
6. **Big risks:** Has the Board played them out and is there an effective plan in place?

Because hackers often infiltrate corporate computer systems by tricking an employee into unknowingly providing access, another sensible approach is to ingrain cybersecurity into corporate culture through a sustained, internal education campaign. The goal is to both reduce the risk of cyberattacks and ensure that employees understand the importance of the role they play protecting company computer networks. ■

Kate Holgate is the Head of Brunswick Group Singapore and Siobhan Gorman is Director of Brunswick Group Washington DC.

CRISIS SITUATION

How to communicate during a crisis

When a crisis hits, the reputational and long term damage can be greater than the immediate economic and other costs of the event. However, a crisis that is well-managed can actually enhance the reputation of the company.

By
JASON NISSE
Partner, Newgate Communications

On 4 November 2010, a Qantas Airbus A380 took off from Singapore Changi Airport. Shortly after, when the plane was cruising above the Indonesia island of Batam, one of its Rolls-Royce Trent 900 engines failed. According to an official report by the Australian Transport Safety Bureau (ATSB), the incident sent debris into the aircraft's left wing and fuselage and some landed on Batam. ATSB also reported that "there was significant damage to the aircraft's electrical, hydraulic and other systems."

Fortunately the pilot was able to steady the plane and land it safely. Qantas then proceeded to ground its entire fleet of A380s while it investigated what happened. Simultaneously, Qantas communications team went into full swing, reassuring passengers on its safety protocols, effectively laying the blame on Rolls-Royce.

While the British engine maker immediately said it was investigating, in depth communications about the incident was too little too late. In June 2011, six months after the mishap, Colin Smith, Rolls-Royce's Director of Engineering and Technology, admitted the company had "fallen short" of "the high standards of safety, quality and reliability that our customers and their passengers are entitled to expect".

What Difference a Crisis Response Makes

Qantas, in common with most airlines, has a finely honed crisis communications process structured around the understanding that the maintenance of its business model relies on convincing the public that it is the safe way to fly.

Airlines control very few of the levers – from the way their aircraft and engines are built; how they are likely owned, and quite often maintained by other companies; they fly in and out of airports owned by other organisations and usually rely on air traffic control run by national governments. That is why when there is any air crash or near miss, the airline almost always toots their own horns, praising responsiveness of air crew or their well-oiled emergency procedures, both of which are two of very few areas airlines control.

Rolls-Royce, on the other hand, is an engineering company and, as such, has a culture where people want to be sure of the facts before they say anything. The company's delay in communicating effectively with the media and its customers (the airlines, and you and me) has been characterised as a poor response to the crisis.

The contrast between Qantas' communications reaction to this crisis and that of Rolls-Royce shows the challenges companies face when they are thrown into this sort of maelstrom. The damage caused to Rolls-Royce's reputation is hard to measure, but since then it has issued five profits warnings and changed its chief executive. Question is: could Rolls-Royce have communicated better?

Expect the Unexpected

So what can companies do to ensure their communications are not flat-footed by a crisis?

The next two pages set out the preparation that a company should make way before such a crisis happens, and the practical actions that a board can take to avoid the common mistakes in communications when a crisis does hit.

As Prussian Field Marshall Helmuth Graf von Moltke famously said, "no plan survives contact with the enemy". No one can legislate for Tony Hayward, then CEO of BP, telling journalists, "I want my life back". However, preparation, planning and understanding how you communicate – and why – will enable you to adjust your plans when events come to blow you off course.

A well-managed crisis can actually enhance the reputation of a company. A crisis is not all gloom and doom.

Crisis Communications

PREPARING FOR A CRISIS

1. Prepare and update a risk register

The process starts many weeks, months or even years before a crisis hits. The risk register details the potential risks to the business, be they operational, financial, regulatory or reputational, and is usually maintained by a team led by the chief risk officer or the CFO. What enlightened companies do is involve their communications team in the risk assessment and mitigation process – giving views on what the reputational impacts of any issues are, spotting additional risks and offering mitigation strategies.

2. Identify and monitor all communication channels

This will involve working out what channels are being monitored, and who should be monitoring them. This should cover conventional and digital media, including social media. With many journalists, non-governmental organisations and other opinion formers using Twitter in particular, social media monitoring is critical so you know what is being said. This does not mean you have to engage on social media – often the best strategy is to take the conversation "offline" by contacting the journalist or opinion former directly.

3. Map relevant social media influencers

Often social media is the "canary in the coalmine", telling you of issues before the phone call comes from the media, or alerting you of developments in a crisis as they occur. In a crisis you need to know who is influential on social media, and who your friends are. You need to make your friends influential and the influencers, your friends. Trying to do this in a fast moving crisis is extremely difficult so trying to map influencers ahead of time is an extremely worthwhile exercise.

4. Confirm escalation procedures

Escalation procedures need to be sorted out so that communications can be quickly signed off. Here, businesses can learn from large pressure groups such as Greenpeace and Friends of the Earth, which despite having thousands of staff in scores of locations, have a developed and devolved communications structure which allows them to respond rapidly to any events.

COMMUNICATING IN A CRISIS

1. Brief your employees

If you have consumer-facing employees – say in call centres – they need a script for what to say to the media when a crisis strikes. Simply referring to corporate communications may suffice, but sometimes, especially when there are fatalities involved, they may need to show empathy without opening up the company to any liability. This is why tone is important in a crisis communications situation. Apologies are essential – but increasingly, they are not enough. They have to be sincerely and swiftly given and the organisation has to give an indication of how it will fix the problem.

2. Know your media engagement guidelines

In a crisis, it is crucial to take control of communications. You need to decide who your spokesperson or people will be. This has to be someone who is senior enough to affect change – I call it the "responsible adult". If the spokesperson is too junior – say a press officer – then the media simply will push for a more senior person and, in a consumer-facing situation, the public simply will not feel it is being dealt with at a high enough level.

3. Empower your crisis team

The crisis team needs to include operational management, government relations, media relations, investor relations, internal communications and legal. All communications to all channels need to be consistent. The legal team needs to feel they have enough control over what is said

without taking control of communications. This is a tricky balance and if you get it wrong you could end up like BP was during the Deepwater Horizon disaster – so concerned about the legal issues that the communications came across as bland and lacking empathy. The communications team needs to be the internal journalist in the team. They have to ask the difficult questions and dig out the truth. It is a natural inclination of managers in a business to try to cover up their mistakes, but if they do not give the crisis team all the relevant information, the potential for greater disaster increases.

4. Determine the desired outcome

One of the most important things to do at the beginning of a crisis is to assess "what good looks like". It is almost impossible to get back to where you started – the data has already been lost, the dam has already been breached, the senior executive has already resigned – but you need to work out what is a reasonable place for you to be when the dust settles. This desired outcome determines your strategy and enables you to keep focused on what you need to do and how you need to do it. ■

The COSO Frameworks:

A common language for combined assurance

Combined assurance brings together all the stakeholders of an organisation in managing its risks. The COSO Frameworks is an effective way of implementing combined assurance.

By
UANTCHERN LOH and SIDNEY LIM

Combined assurance is the latest thinking in managing an increasingly complex and risky world.

The *2009 King II Report* defines combined assurance as "integrating and aligning assurance processes in a company to maximise risk and governance oversight and control efficiencies, and optimise overall assurance to the audit and risk committee, considering the company's risk appetite". In practical terms, it is about optimally bringing together the assurance providers – both internal and external – of the enterprise.

The case for organisations to adopt combined assurance has long been made (see "The ins and outs of Combined Assurance", *SID Directors' Bulletin Q2, 2015*). It is fully understanding and implementing the concept that is challenging.

Thus far, the COSO Frameworks, which comprise the Enterprise Risk Management (ERM) Integrated Framework and the Internal Control Integrated Framework (see box), is a good common language for achieving combined assurance.

The COSO Frameworks are rigorous methodologies for implementing integrated risk management. Implementing them can itself be a challenge. In a recent COSO Academy roundtable discussing the matter, participants suggested that organisations could begin with the following steps in adapting COSO for implementation:

Step 1: Produce a board risk guide that highlights the need for COSO.

Step 2: Draw on the experience of directors who have implemented enterprise risk management and seen the benefits first-hand, as well as those who did not implement it and had bad experiences as a result.

Step 3: Put in place a national incentive for implementation or adoption, to help offset the associated costs.

Step 4: Get internal audit to frame COSO adoption as a control self-assessment, so that other departments are more willing to try it out.

The COSO Frameworks

The ERM Integrated Framework

ERM is a process, effected by an entity's board of directors, management and other personnel, applied in a strategy setting and across the enterprise and designed to identify potential events that may affect the entity with risk managed to be within that of the entity's risk appetite, to provide reasonable assurance regarding the achievement of the entity's objectives.

The COSO ERM Integrated Framework:

- Provides sound principles and guidance for ERM to help organisations deal with risk and achieve their objectives.
- Clearly describes the key elements of a robust ERM process and how risks are managed within an organisation's risk appetite.
- Demonstrates that ERM can add value to an organisation by helping management achieve organisational performance and profitability targets and prevent loss of resources.
- Enables management to better assess how much risk the organisation accepts relative to stated objectives.
- Provides clear and practical direction and guidance for the implementation of ERM.

The Internal Control Integrated Framework

Internal control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the areas of effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

The COSO Internal Control Integrated Framework provides:

- A means to apply internal control to any type of entity, regardless of industry, legal structure, at the levels of entity, operating unit, or function.
- A principles-based approach that provides flexibility and allows for judgment in designing, implementing and evaluating internal control.
- The requirements for an effective system of internal control by considering how components and principles are present and functioning and how components operate together.
- A means to identify and analyse risks, and to develop and manage appropriate responses to risks within acceptable levels and with a greater focus on anti-fraud measures.
- An opportunity to expand the application of internal control beyond financial reporting to other forms of reporting, operations, and compliance objectives.

Companies can now be more systematic in how they look at internal control with regards to risk management. The COSO Internal Control Integrated Framework sets forth the requirements for an organisation to have an effective system for internal control and reduce risks to an acceptable level. The COSO Enterprise Risk Management Integrated Framework expands on internal control to incorporate a fuller risk management process, evaluate and manage risks more effectively and efficiently. ■

Uantchern Loh is the Chief Executive of Singapore Accountancy Commission and Sidney Lim is the Managing Director of Protiviti Southeast Asia.

The GRC professional

By **PHILIP FORREST**
Council member, SID

EXPANDING HORIZONS

There is a new acronym in town: GRC which stands for Governance, Risk Management and Compliance.

In a sense, GRC is not new. It is what many see boards and management already do:

- Governance: The oversight role of boards in directing the company, including the governance of risks.
- Risk management: The set of processes by which the board and management identify, assess, manage and monitor risks.
- Compliance: Ensuring that the organisation conforms to regulations and other stated requirements.

What is clear is that the amount of risk management and compliance activity in organisations have grown over the years. This is due to pressures from increasing regulations, higher business complexity, and an increased focus on accountability.

Along with this, the number of personnel involved in a company in these activities have increased. They go by different labels: internal auditor, compliance officers, risk officer, legal compliance officer, IT control officer, etc.

More significantly, these functions are managed independently. They each do their own things – which could either lead to a great deal of overlap or lapses in the company's controls. This has led to the need to view these functions more holistically and in an integrated manner.

GRC has thus emerged as a term that refers to the "co-ordination and integration of governance, risk management and compliance to meet the business objectives of the organisation".

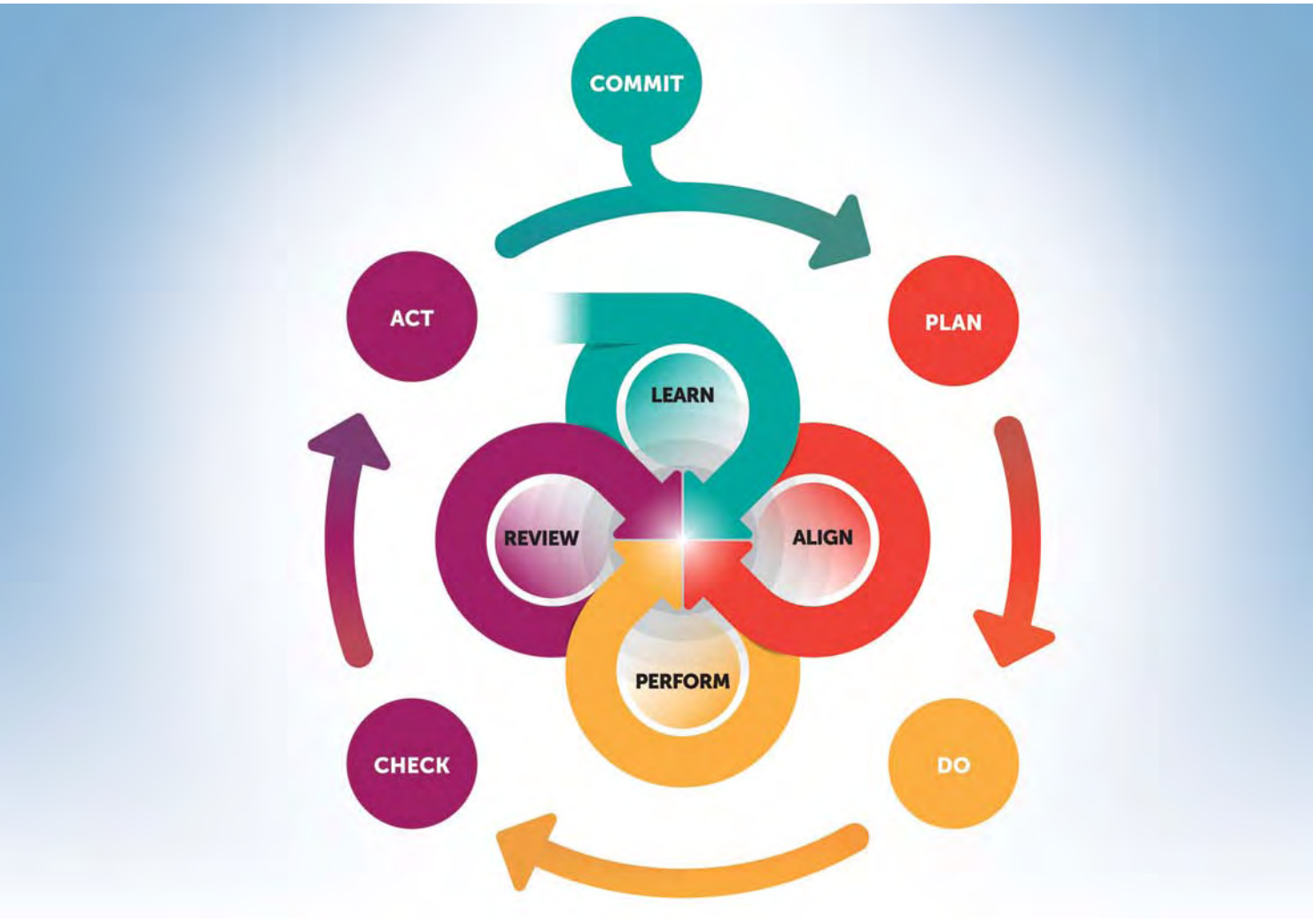
There are several elements to a sound GRC framework:

- An active governance model and structure that drives day-to-day accountability.
- A sound system for risk profiling and reporting.
- A technology platform and tools to automate and make efficient much of the compliance work.
- Capable professionals in the different risk and compliance areas.

Capable professionals to implement an organisational-wide GRC framework can be a challenge. Whether these professionals work in internal audit, compliance, IT, legal, or risk, they need to understand the big picture and details of integrated risk management and compliance, and their own functional areas. Given the importance of this field, standards, training and certification programmes have been developed by industry bodies and organisations to build up career professionals working in GRC fields.

One of the leading organisations is OCEG (formerly known as the Open Compliance and Ethics Group), a global, nonprofit think tank headquartered in the US. It currently informs, trains and empowers more than 50,000 members on GRC.

OCEG has developed a GRC Capability Model for Principled Performance, the only international



GRC Capability Model for Principled Performance

standard that provides comprehensive and detailedpractices for building and implementing an integrated GRC capability. In addition, OCEG provides courses and two related GRC certification programmes – the GRC Professional and the GRC Audit.

And here's the good news: SID is partnering Straits Interactive to introduce the GRC Professional Programme in Q2 2016. Straits Interactive is a Singapore-based consulting and training company, focused on the Personal Data and Protection Act and compliance. It is licensed by OCEG to deliver the training for the certification programme.

The three-day GRC Professional Programme will provide attendees with the knowledge necessary to effectively design and enhance integrated GRC activities across an organisation.

As a part of the course, participants will work on a project to design an integrated GRC roadmap for their organisations. They will be provided with a user-friendly software, the GRC toolkit for the development throughout the three days, and will be allowed to retain the software for their own use for the next twelve months.

Participants will receive a Certificate of Attendance. In addition, they may choose to sit for an online test to achieve the internationally recognised GRC Professional Certification. The course will fully prepare participants for a passing grade. ■

Mitigating business risks through strategic conflict resolution

By
LOONG SENG ONN
Executive Director, Singapore Mediation Centre

Business deals can sometimes go awry, potentially putting an organisation in jeopardy and its reputation and finances at risk. However, these can be circumvented when the appropriate dispute resolution mechanisms and conflict resolution clauses are in place.

Receiving a letter of demand or a writ of summons could severely impact one's psychological well-being. A writ marks the start of court proceedings which, too often, is responded to by a company's engagement of legal help, where discussions to settle are stalled, swords are drawn and financial blood is spilt.

In today's world, what is public is subject to greater scrutiny and spreads faster. Taking a legal battle public is a surefire way of putting a company's reputation up for target practice. A single episode of negative publicity can fritter away all the goodwill and brand equity that a company may have taken decades to build. Such publicity can result in loss of perceived value and impact future business relations.

For instance, Marco Polo Marine's recent scuffle with Sembcorp Marine over the termination of a S$306-million rig contract caused Sembcorp Marine's shares to plummet to a six-year low, after the legal action was made public.

This is where mediation can play a vital role.

Mediation is a method of resolving disputes that uses a skilled neutral third party – a mediator – to manage the negotiation process confidentially and steer those involved in the dispute towards settlement. Put simply, a mediator helps parties find win-win solutions for all. Fault-finding is parked aside as parties focus on finding solutions that will meet their interests.

Making a Case for Mediation

In some cases, a mere whiff of a public spat can already prove to be damaging to one's reputation. In managing reputational risks, mediation offers a private and confidential environment where parties can engage in closed-door discussions and explore options without generating negative publicity. When a settlement is reached, the details might also be kept confidential.

Because mediation is "without prejudice" (read: discussions and documentation resulting from mediation cannot be used against any party if no settlement is reached), parties can still go on to enforce their rights, which remain intact post-mediation, if an amicable end is not possible.

Mediation reduces financial risks for organisations, helping them lower their legal spending and hence, save costs. In the 2015 *Litigation Trends Annual Survey* commissioned by Norton Rose Fulbright, 14 per cent of survey respondents in Asia reported an annual litigation expenditure (excluding costs of settlement and judgement) of over US$10m; seven per cent spent between US$5m and US$10m; and 64 per cent spent less than US$500,000.

Mr Kevin Kwek, Director at Legal Solution LLC who was involved in a banking dispute of S$5.3m commented, "The matter which was initially fixed for a 13-day trial in the High Court, was resolved by mediation at the Singapore Mediation Centre (SMC). By going through mediation, my client saved at least S$400,000 in legal and court fees, along with a lot of time and mental stress that is usually associated with trials."

Cost and Effect

Mediation at SMC is kept relatively affordable; the mediation fee for sums in dispute over S$60,000 starts from S$963 per party, per day.

SMC has mediated over 2,700 matters, with a 75 per cent success rate. Of the cases that settled, more than 90 per cent were mediated within a day.

In mediation, parties also have control over the proceedings and the outcome. Parties going through an adjudicatory process like litigation or arbitration will always run the risk of the neutral deciding against them. A skilled mediator is trained to guide parties through complex issues and help them leave their entrenched positions and attain solutions that work for both parties. At SMC, parties have a choice of mediators from over 10 specialisations to meet business needs.

Business leaders today cannot ignore the opportunity costs, time and resources consumed in a legal battle. Each hour spent in a dispute can be more productively used to seek new business ventures. A long drawn dispute drains management time and other business resources. If legal fees can be reduced, these expenses can then be channelled to drive the business, which in turn increases companies' profits. By first mediating, companies can reduce their financial and reputational risks when faced with a dispute. ■

Directors' indemnities and insurance: How covered are you, really?

By **VICTOR YEO**
Brand and Communications committee member, SID

SID SINGAPORE INSTITUTE OF DIRECTORS | BOARDROOM MATTERS

Imagine the following scenario.

A director is prosecuted for allegedly being in criminal breach of his duties. The case goes through the courts and the director is found innocent. He is landed with a huge legal bill for which he tries to seek an indemnity from the company or the insurers under the directors' and officers' (D&O) liability insurance policy that the company had purchased. Lo and behold, he finds the company is not legally obliged to indemnify him under either the terms of his appointment or its constitution. Nor does the policy cover legal expenses for criminal prosecution or regulatory actions. The director, though blameless, is out of pocket for tens, if not hundreds, of thousands of dollars in legal fees.

Most directors will have some inkling of the directors' liability insurance coverage the company has taken out, but probe further and chances are they will be unaware of the extent and details of that coverage. Given the scenario above, it is crucial that they step up their understanding of the legal exposure they face when serving on corporate boards and, more importantly, what protection they have.

What Does the Law Permit?

The recent changes to the Companies Act have clarified the extent to which a company can provide legal protection for its officers (including directors) against liability.

For starters, section 172 voids any arrangement whereby a company purports to exempt or indemnify its directors from liability in connection with any negligence or breach of duty in relation to the company.

Companies are, however, allowed to indemnify their directors in respect of liabilities incurred to third parties. The only exceptions to this are arrangements of indemnity for the payment of fines or liabilities incurred in defending civil suits, criminal prosecutions or regulatory actions taken against the director where he is convicted or judgment is given against him. Such arrangements are void. This is fair as directors should not be reimbursed by the company where he has breached his duties to it.

In other words, indemnities may be given for legal costs and other expenses incurred in successfully defending against any action. They can extend to costs associated with mediation or arbitration proceedings as well as expenses incurred in trying to reach an amicable settlement. They can also cover liability in respect of third party suits against directors in performing their duties properly for the company and associated legal costs. The indemnity can be provided for in the company's constitution or the director's contract. It can even be agreed upon after the expenses or liabilities have been incurred (provided the director is found not guilty).

Instead of, or in addition to providing an indemnity, companies may arrange for appropriate D&O insurance coverage. The law explicitly allows companies to purchase and maintain insurance, for the benefit of its officers, against liability incurred for negligence or breach of other duties. The extent of the coverage depends very much on its terms and the premium the company is willing to pay. Coverage can extend to matters for which an indemnity is not permitted by law.

Time for a Review

The implementation of the new provisions of the Companies Act dealing with indemnities and insurance against liability for officers presents an opportunity for directors to review their indemnity and insurance coverage vis-à-vis their respective companies.

The first thing directors should do is to review the scope and monetary limits of the company's existing D&O liability insurance policy to see if the coverage provided is adequate. Consideration should be given to whether their coverage extends to matters for which an indemnity by the company is void under the law. If it does not, directors should seriously look into arranging for such coverage personally. In this regard, the SID has an arrangement whereby its members can have personal D&O insurance coverage for up to $1m for up to three separate directorships at a reasonable cost.

There should also be a discussion about whether the company should provide any indemnity to its directors against liability to third parties, and if so, the extent of such indemnity. This indemnity could be expressly incorporated into the directors' terms of appointment.

In recent years, the potential for directors to face legal suits or prosecution as a result of performing their duties has increased significantly. This may be attributed to various factors including the higher standards of care and diligence that the

modern corporate community expects of directors, the increasing complexity and sophistication of businesses and regulations, and the increasingly litigious society in which we live.

An adequate insurance framework for directors would very much help give directors some peace of mind. What is often not realised is that companies also stand to benefit from these arrangements as they can help ensure the company does not lose out in cases where the directors who are found liable to the company are unable to fully compensate the company from their personal assets. ■

Boardroom Matters is a weekly column by SID for The Business Times and its online financial portal, BT Invest, where this article was first and recently published.

D&O insurance market in Singapore

There is a very active director and officer liability (D&O) insurance market in Singapore with several hundred million dollars of capacity and numerous insurance companies underwriting the risks.

By
TONY MITCHELL
Finex Leader, Asia Pacific, Willis Towers Watson

With the efforts made to encourage Lloyd's and other insurers to establish in Singapore, there is today a significant oversupply of D&O capacity. This means that insurers are prepared to be incredibly competitive in pricing and scope of coverage. While this is very much to the advantage of directors, the latter need to ensure that directors actually review the insurance coverage together with their exposures, and not just feast on the premium discounts.

The quality and suitability of coverage is at risk of being inadequate as the continuing reduction in commissions to brokers means that they are often not able to spend the quality time needed to structure insurance coverage to suit a client's exposures. As premiums have fallen, there is the danger that D&O policies become increasingly commoditised. Although on the surface the policies have become wider, there is an increased chance that serious flaws in cover, and other technical issues and inconsistencies only rear their ugly heads when it is time for a claim to be made.

All leading D&O insurers have their own policy wordings that grant cover to directors and companies in the way that the insurers wish to provide capacity. A summary of the key Insurers and their Singapore capacity and appetite is shown in the table.

SINGAPORE INSURERS' CAPACITY

SINGAPORE INSURERS	PRIMARY CAPACITY	SELECTIVE RISKS
ACE Insurance Ltd	US$25million	US-listed companies and Australian risks will be carefully reviewed
AIG Asia Pacific Insurance Pte Ltd	US$20million	US-listed – US$5million max. limit
Allianz Global Corporate & Specialty SE Singapore Branch	US$30million	None specifically but review each risk on its merits
Allied World Assurance Company Ltd	US$25million	None specifically. Depends on risk quality
Argo	US$20million	Banks, Stock Exchanges, US-listed
AXA Insurance Singapore Pte Ltd	€15million (Singapore/ Malaysia/ China)	SEC-regulated, Financial Institutions, companies with claims activity
AXIS Specialty Limited (Singapore Branch)	US$25million	China-listed businesses
Berkshire Hathaway Specialty Insurance Company	US$100million	China-listed companies and US IPO
Catlin XL Insurance Company Ltd	US$25million - US$50million	Individually reviewed
DUAL Underwriting Agency through MSIG Insurance (Singapore) Pte Ltd	US$20million	US-listed or HO in US; ADR Level 2 and above
Federal Insurance Company (Chubb)	US$50million	
HDI Global	Not a primary insurer	No FI D&O or entities with ADR level 3 and above
Liberty International Pte Ltd	US$20million	Not for Profits; Mining Exploration; airlines; US-listed
Newline Asia Services	US$15million	US-listed
QBE Insurance (Singapore) Pte Ltd	US$50million	US-listed
Starr International Insurance (Singapore) Pte Ltd	US$25million	
Tokio Marine	US$25million	None specifically
Zurich Insurance Company Limited (Singapore Branch)	US$20million	Adoption/ Foster Care, Auto-related, Aviation, Biotech, Mining, Oil and Gas, Pharmaceutical, US-listed

*Ace Insurance recently acquired Chubb and will go forward under the Chubb brand.

Current Claims Trends

The Singapore claims environment is still fairly benign but there has been an up tick in claims involving regulatory enquiries and employment-related disputes. Directors need to be particularly careful in reviewing the availability of legal representation costs before "official enquiries". Often regulators "enquire" about potential breaches before launching official investigations, and the costs of hiring external auditor and legal advice in the enquiry stage can run into the millions. Also there is the question of whether the costs incurred at this stage benefit the company or the insured persons.

With more Singapore companies operating overseas, it is essential that directors understand the implications of this and the change in risk exposure that results. Overseas courts have often proven to be less than impartial when it comes to

10 Questions Directors Should Ask Their D&O Insurance Providers

1. How much available cover do I really have – how is my available limit of cover diluted?
   a) Within which categories of employee and at what level of seniority do I share the D&O limit purchased by the company on my behalf?
   b) Does the limit provide cover for the company as well?
2. Do I enjoy the benefit of any cover for fines and penalties awarded against me personally, including those from the recently-introduced SGX listing committees which are empowered to impose fines on companies and directors for breach of listing rules?
3. Do insurers unequivocally commit to waive their right to rescind the policy save as against any individual directors being guilty of fraudulent misrepresentation or non-disclosure?
4. Does the policy provide a mechanism under which insurers will advance all defence costs and legal representation expenses to me pending resolution of any dispute between the company and the insurers as to the extent of such costs being ultimately covered under the policy?
5. Am I covered for the costs of an investigation following death or bodily injury occurring as a result of corporate activity?
6. What provision is there in the policy for my protection in case of an actual or potential conflict of interest between the company and myself as a result of which I may require separate legal representation?
7. How will my policy respond in the event that there is an extradition order made against me?
8. What protection does the policy provide against future claims against me if I retire or resign during the policy period, or if during such period the company is the subject or object of mergers and acquisitions activity?
9. Am I aware of any circumstances that could give rise to a claim against me? Have I told my insurers about this and do I really understand what this means and the implications of failing to do so?
10. With regard to my external directorship positions, do I have proper cover for liability from these under my company's insurance arrangements?

claims involving national interests and involving foreign corporations and directors operating in their countries. Also many countries insist that local policies are put in place rather than paying claims to local directors and corporations using overseas policies. A failure to do this can result in serious frustrations, delays and additional tax payments.

Challenge the Cover

Directors are usually not involved in the negotiation of this fundamental protection of what is after all a personal liability. Then they become surprised and frustrated when a claim situation arises.

Directors should arrange for briefings from their insurance providers at which they have to ask pertinent questions and really engage in the details of the cover and how it will respond in certain claim scenarios (See box "10 Questions Directors Should Ask Their D&O Insurance Providers").

All too often, directors rely on benchmarking policy limits against similar organisations rather than arranging cover on a risk-based basis that truly reflects their risk profile. For example, DBS and a large European bank may have similar market capitalisations but their risk profiles will be totally different. Benchmarking can be a useful guide but it is a long way short of the complete answer.

Remember, when it is time to make a claim, it will be too late if you discover there is no or inadequate cover. ■

Criminality and technology top risks for Singapore's banking industry

By
FANG EU-LIN
Partner, PwC Singapore

The Centre for Study of Financial Innovation in association with PwC released the 2015 edition of its annual *Banking Banana Skins survey* recently. The survey reveals that yesterday's risks may no longer be today's and tomorrow's. Whilst some of the risks are unsurprising, some of the results are curious and one could agree or disagree. Having such discourse would not save the world from a financial crisis, but could offer different perspectives and perhaps better decisions and calibrations.

Key Findings

- New and old risks continue to challenge the banking industry. Respondents from around the world and in Singapore identified the same top four risks as per 2014, though the order is different. "Criminality" and "technology" are the top two concerns in Singapore.
- Macro-economic environment uncertainties are at the top of everyone's mind. Despite prudential reforms, banks remain vulnerable to high debt levels, future interest rates, weakness in China and other emerging markets, and softening commodity prices. Lower growth rates, together with regulatory reforms will put pressure on banks to manage returns.
- Criminality, including the risks to banks in areas such as money laundering, tax evasion and cyberattack rose the highest among the concerns in the last year. One Singapore-based respondent was quoted: "Cyber theft will grow and at least one bank will fail in the next 10 years as a result."
- Technology is giving rise to "fintech" competitors that are challenging traditional ways of doing things and are operating using more nimble systems and lower overheads. Traditional bank earnings models are threatened. To improve margins, banks are experimenting with new industry models that leverage technology and are more customer than product-centric. However, this could expose them to even higher risks such as cybercrime and financial terrorism.
- Regulation continues to be a concern. Banks recognise the need for tougher controls; many question their cost and effectiveness. Banks are not only bearing the direct costs of regulation – new capital and liquidity requirements, restructuring costs, higher costs of compliance, and higher costs of customer acquisition – but also the cost of greater management time to re-engineer processes, change culture and increase compliance efficiency. Industry margins are being impacted. ■

Top 10 Business Risks For Banking Industry in 2015

World Rank	Banana Skin (Risk)	Singapore Rank
1	Macro-economic environment	3
2	Criminality	1
3	Regulation	4
4	Technology risk	2
5	Political interference	-
6	Quality of risk management	10
7	Credit risk	-
8	Conduct practices	8
9	Pricing of risk	-
10	Business model	-
-	Social media	5
-	Reliance on third parties	6
-	Capital availability	7
-	Liquidity	9

The Audit Committee Seminar

Raising the bar

A record of more than 450 audit committee (AC) members and directors thronged the Regional English Language Centre auditorium on 5 January 2016 for the second annual Audit Committee Seminar jointly organised by ACRA, SGX and SID.

The seminar's theme was "Raising the bar on financial reporting". Clearly the bar is being raised not just for ACs, but also auditors and chief financial officers (CFOs), and, arguably, the regulators as they seek to respond to a more demanding and complex business and investment environment.

The seminar covered several new developments, including:

- The audit quality indicators (AQIs) disclosure framework by ACRA;
- The new auditor reporting standards;
- Sustainability reporting for listed companies on a "comply or explain" basis;
- SGX regulatory initiatives including independent Listing Committees, Compliance Bulletin and "comply or explain" compliance review.

ACRA also provided an update of the first phase of its enhanced Financial Reporting Surveillance Programme (FRSP) and what it will be focusing on in the next round, while SGX reviewed recent case studies where it detected areas of concerns.

We summarise the key takeaways from the event in the following pages.

For those who need more information on the content covered in the seminar, do get your copy of the *2016 Mini-Guide for Audit Committees: Hot topics that ACs and directors need to know* which was launched at the event. The four hot topics in the mini-guide that was jointly produced by ACRA, PwC and SID are: FRSP, Enhanced Auditor Reporting, AQI Disclosure Framework, and New/Revised Singapore Financial Reporting Standards.

SGX Regulations

New SGX Developments

- Three independent Listing Committees (Advisory, Disciplinary and Appeals) were established in October 2015 to strengthen the listing regulatory process.
- SGX Listing Compliance Bulletin launched in December 2015 shares recommended practices, guidelines and case studies of compliances.
- Consultation paper on sustainability reporting being introduced on a "comply or explain" basis; launched in January 2016.
- SGX hired KPMG in October 2015 to review listed companies' compliance with the "comply or explain" requirements.

Case Studies of Areas of Concern

- Issuance of convertible securities must comply with rules such as the maximum number of shares to be issued and any material alteration to securities' terms after issue must be approved by the shareholders.
- Bonus issues should not result in shares to be less than $0.50 based on the daily weighted average price.
- Distinction between a bonus and a rights issue is a matter of substance and not name. The rules and disclosure requirements for both are different.
- If a company's ability to operate as a going concern is contingent on fundraising exercise, the company must monitor the progress of the fund raising and ensure that trading suspension is requested should fund raising be unsuccessful.
- Suitability of new auditors to be justified.
- SGXNet is not to be used for promotional purposes.

Powers of the listing committees

"The Listings Disciplinary and Appeals Committees have all the enforcement powers of the Exchange which include private warning, requiring issuers to appoint independent advisors and reviewers of internal controls and processes, and objecting to appointment of directors and/or executive officers. On top of these, the Committees can publicly reprimand issuers, directors and executive officers, require resignation of directors and executive officers, impose fine against issuers and prohibit issuers' access to market facilities – what is commonly termed as the "cold shoulder rule".

Ms June Sim
Head, Listing Compliance, SGX

Why sustainability reporting

"Sustainability reporting complements financial reporting by covering the non-financial aspects, including the environmental, social and governance aspects of the company's business and strategy. This gives investors better insight into the companies they invest in by enabling them to assess a company's prospects and quality of management more holistically. It is widely recognised that the disclosure of material information beyond the financial numbers enhances transparency and builds greater understanding and trust among investors over time."

Mr Loh Boon Chye
CEO, SGX

Is SGX toughening up regulation?

"Although my background [in Commercial Affairs Department] is in enforcement, the regulations and our focus at SGX are aimed at prevention and containment. Enforcement is not our first response, and it shouldn't be… [Hence for our review of companies' compliance with the CG Code] we are not naming and shaming right away. Rather we are going to highlight areas of concern and, for example, point out boiler plate responses in the "comply or explain"' statements that are not adequate...

We highlighted the disclosure concerns related to the China-linked companies (in November 2015) to give fair warning… The hardest part about being a regulator is finding the right touch… Transparency is about being clear and giving fair warning, ensuring due process, including the right to be heard. There should be no unwritten rules."

Mr Tan Boon Gin
Chief Regulatory Officer, SGX

Audit Quality

Enhanced Auditor Reporting

- The UK has been the front runner of the new auditor reporting standard. In Singapore, ISCA has issued the new and revised standard to be effective for audits of financial statements ending on or after 15 December 2016.
- The major change in the new audit report is a new section on "key audit matters" (KAM) for listed entities. These are matters deemed by the auditor to be most significant in the audits of financial statements.
- Other changes in the new audit report include the greater visibility for a going concern, and the restructuring of the audit report for readability.

Audit Quality Indicators (AQIs)

- ACRA has introduced a voluntary AQI Disclosure Framework for implementation from 1 January 2016 onwards. Whilst not the sole determinant, AQIs can provide additional data points to help ACs evaluate auditors based on quality during new appointments or re-appointments.
- The Framework comprises eight AQIs:
  1. Audit Hours – Time Spent by Senior Audit Team Members
  2. Experience – Years of Audit Experience and Industry Specialisation
  3. Training – Average Training Hours and Industry Specific Training
  4. Inspection – Results of External and Internal Inspections
  5. Independence – Compliance with Independence Requirements
  6. Quality Control – Headcount in Quality Control Functions
  7. Staff Oversight – Staff per Partner/ Manager Ratio
  8. Attrition Rate – Degree of Personnel Losses
- Big 4 audit firms have committed to provide the AQIs data to the Audit Committee in a standardised format to facilitate comparison.

Will any auditor do?

"While an AQI is not a single definitive measure of audit quality, each AQI is an objective and measurable data-point that indicates the level of audit quality. Therefore, Audit Committees would benefit by having access to such data points in helping them choose the right auditor based on quality."

Ms Julia Tay
Deputy Chief Executive, ACRA

Why the new audit report?

"The Global Financial Crisis highlighted the need for change. Commentators argued if the crisis did not mean individual auditors failed, did this mean that the audit failed. In other words, did the audit meet the legitimate expectations of users? As a result, the UK's Financial Reporting Council implemented a package of measures including those to enhance the relevance and transparency of the audit. Hence, the new auditor report. When it was first introduced in the UK, it met with some resistance, but the experience to date has been overwhelmingly positive. Auditors surpassed expectations, the differences between and within firms emerged, and investors now read the audit reports."

Mr Paul George
Executive Director, Conduct Division, UK Financial Reporting Council

How do these new requirements by regulators reflect on auditors?

"The audit profession has always been focused on being relevant and we need to do a better job at communicating this. As an illustration, the new auditors' report which sets out key audit matters was very much an initiative of the audit profession – led by the International Auditing and Assurance Standards Board. Ensuring relevance and upping the quality of the financial reporting ecosystem and supply chain is fundamental to ensuring trust in the capital markets.

The development of the AQI disclosure framework (which ACRA has taken a practical approach to) is an example of collaboration with the profession. Having eight quality indicators across a broad range of metrics sets us up for a continuing journey towards audit quality. However, AQIs should be an enabler, not an algorithm or formula which one should blindly apply."

Mr Max Loh
Managing Partner, EY ASEAN and Singapore

Financial Reporting Surveillance

Latest Developments on ACRA's FRSP

- The Financial Reporting Surveillance Programme (FRSP) reviews financial statements for compliance with the accounting standards.
- It was enhanced in 2014 to cover financial statements where auditors have issued "clean" audit opinions.
- Findings indicated that the state of financial reporting by Singapore-incorporated listed companies is generally healthy. However, there is still room for improvement as a number of instances of non-compliance with the Accounting Standards were identified.
- Out of 49 financial statements of listed companies reviewed in the first review cycle, there were four instances of severe non-compliance, 54 instances of other non-compliances, and 74 areas for improvement. Four companies received warning letters and 29 companies received advisory letters.
- ACRA will focus on the following areas in their review of the FY2015 financial statements:
  - Control over investees
  - Call or put option over shares of investee
  - Business acquisitions
  - Long-life assets value and impairment testing
  - Breaches of borrowing covenants
  - Sale-and-leaseback transactions
  - Statement of cash flow
  - Impact from the currency environment
  - Fair value measurement
  - Earnings per share

How hot are the CFO and AC seats?

"There is definitely more work for the CFO and the finance team resulting from the additional scrutiny and requirements. However, we should put things into perspective – the additional information required is, in the long term, good for us. The business we are in is a capital-intensive one and capital flows freely across borders. If investors are not comfortable with our level of transparency, they can take their money and move elsewhere. Sometimes, rumour and speculation can become reality so transparency and the appropriate level of governance are key. We also receive complaints from investors about the thickness of our annual reports which can go up to 300 pages. Data and information are not the same thing, so we need to summarise some of the data in a succinct way to provide the information for our investors to make the right decisions."

Mr Arthur Lang
Group CFO, CapitaLand

"The hot seat of the AC Chair is a function of today's environment of volatility and risks. The AC's responsibility can be thought of in terms of three "I"s. The first is "integrity", ensuring the integrity of the financial statement and organisation. The second is "institution", giving due attention and diligence and not think that it is all about the data. The third is "information", providing information that are useful and assuring to investors. The basic responsibility has not changed but the demands of the investors and the public have increased. So, we have to respond."

Ms Euleen Goh
Audit Committee Chair of CapitaLand, SATS and Royal Dutch Shell

Causes of non-compliance to accounting standards

"The three root causes of non-compliance are insufficient scrutiny of the financial statements, aggressive judgements, and an over-reliance on a weak accounting team. ACs need to review financial statements carefully and with rigour, be alert to management's motivations and challenge their judgements when appropriate, and ensure the competent and well-resourced finance team are in place."

Ms Bong Yap Kim
Director, Financial Reporting Surveillance Department, ACRA

Why the focus on directors?

"Many directors would like to know why the enhanced FRSP programme is targeted at ACs and directors, when it is the CFO who prepared the financial statements which are passed by the auditors."

Mr Willie Cheng
Chairman, SID

"The FRSP exercise is not meant to be punitive but to raise directors' awareness of their responsibilities with regards to financial reporting. Section 201 of the Companies Act places the responsibility on directors to ensure that the financial statements are true and fair and in accordance with the accounting standards. In fairness, directors can rely on information and advice by competent third parties. However, such reliance must be diligently (and not blindly) exercised."

Mr Kenneth Yap
Chief Executive, ACRA

"We talk about the responsibility and liabilities of directors. Should not the liability also lie with the auditors? After all, the board is relying on the opinion provided by the auditors. A Singapore Court of Appeal judgement ruled that directors can rely on professional advice which include auditors."

Mr Kevin Scully
Executive Chairman, NRA Capital

"To say that auditors get away with things is far from the truth. Like all other professionals, auditors are subject to immense penalties if they have been negligent. ACRA supervises the accounting/auditing profession in a very stringent manner and holds the profession to the highest quality and standards. Not all actions taken may be highly publicised but as members of ACRA's Public Accountants Oversight Committee, I can assure you that audit professionals have clear accountability and face severe consequences when standards are not met.

Mr Max Loh
Managing Partner, EY ASEAN and Singapore

Remuneration Committee Guide launched

More than 300 directors came together to witness the launch of the *Remuneration Committee (RC) Guide* at the Marina Mandarin Hotel on 15 January 2016.

The guidebook is the second volume in a series of Corporate Governance Guides for Boards in Singapore developed by SID with the support of ACRA, MAS and SGX. The first guidebook, the *Nominating Committee Guide* was launched in August 2015. In his welcome address, SID Chairman Willie Cheng shared that the remaining guides – the *Board Risk Committee Guide*, a revamped *Audit Committee Guide*, the *Board Guide* and an *eGuide to the Code of Corporate Governance* will be released progressively by the first quarter of 2017.

The guest-of-honour for the event was Mr Loh Boon Chye, CEO of SGX. He spoke of the need for "robust and considered deliberations by boards" on remuneration matters, especially with shareholders increasingly questioning the remuneration and reward system used by boards.

Mr Shai Ganu, Asia Business Leader for Mercer's Talent business presented highlights on the structure and contents of the guidebook. Mercer provided the resources for the writing of the *RC Guide*. He noted that while the guidebook provides several perspectives and best practices that can be referenced by RCs, the context and strategy of every company is unique and therefore, it is more important to focus on "best fit" rather than "best practice".

Mr Ganu went on to underscore the importance of adequate executive remuneration-related disclosures as a measure to allay shareholder concerns. "It is imperative that companies in Singapore stay ahead in adopting best practices with regards to remuneration-related disclosures, else investors will prompt regulators to adopt measures such as 'say on pay'."

Mr Loh in his address said that "say on pay" (the right of shareholders to vote on executive remuneration) has gained momentum in the US and other markets, but has yet to take root in Singapore. Noting that there are arguments for and against "say on pay", he invited directors to actively contribute their thoughts and concerns to the debate.

A spirited debate did indeed take place at the panel that followed. The panel comprised

members drawn from the RC Guide Review Panel and was chaired by Ms Wong Su Yen, Chairman of Nera Communications and the Review Panel.

Ms Rachel Eng, Joint Managing Partner, WongPartnership provided a legal perspective on the best practices framework for RCs and the need to link board pay to the company's strategy and value creation.

Concurring with Ms Eng, Mr Simon Israel, Chairman of Singtel spoke of the need for the reward instruments to be simple while being tightly linked to underlying business performance, taking into account business cycles and the organisational culture. He said that it is important for RCs to ensure that there is no inherent disincentive for doing the right thing on the part of directors and executives.

Mr Liew Mun Leong of Changi Airport Group shared why as a leader he has always been very passionate about developing talent from within the organisation. He also said that too often companies do not realise how non-executive directors are the best internal consultants; they have a multitude of outside-in perspectives and can be great sounding boards to executives.

Professor Jean-Francois, the Shell Chaired Professor of Human Resources and Organisational Development at INSEAD, then introduced yardsticks to consider when boards are choosing measures of company performance. He felt that while Total Shareholder Return (TSR) is important, boards need to be cognisant of whether the different measures used are "complete or controllable" and whether they are "lead or lag" metrics. He added that qualitative aspects of performance should also be taken into account.

Summing up the day, Mr Kenneth Yap, CEO of ACRA, thanked those present for the lively and stimulating debate, observing that clearly "pay is a lightning rod" and yet an essential element of talent retention. He urged everyone to read and understand the principles expounded in the guidebook as part of their duty as stewards of the enterprise. ■

Feedback on Sustainability Reporting

On 5 January 2016, SGX issued a Consultation Paper on Sustainability Reporting on a "Comply or Explain" basis (see box).

SID organised a small group feedback session for members on the Consultation Paper on 29 January 2016. 27 directors and experts in sustainability reporting attended the session. There was a good mix of mostly directors from small to mid and large cap listcos present. In addition, a handful of experts – from consulting firms and NGOs – in sustainability reporting also contributed their views.

The group reviewed the questions set forth in the Consultation Paper and more. The various response and options were vigorously debated. A summary response paper on the feedback from the group was submitted to SGX on 5 February 2016. ■

SGX Consultation Paper

Proposed Features of Sustainability Reporting

Mandatory Reporting

- SGX-ST Listing Rules for Mainboard and Catalist companies (Rule 711A) amended to mandate a sustainability report for financial year within five months of year-end for all mainboard and catalist companies.
- The 2011 *Guide to Sustainability Reporting for Listed Companies* will be implemented as a Practice Note.

"Comply or Explain"

- Sustainable reporting requirements to be on "comply or explain" basis.
- Primary components in report:
  - o Material ESG factors
  - o Policies, practices and performances
  - o Targets
  - o Sustainability reporting framework
  - o Board statement
- Components under consideration:
  - o Anti-corruption
  - o Diversity
- Stakeholders to be engaged for the "verification" of material ESG factors.
- Working guideline on materiality provided.

Board Responsibility

- Board must approve material ESG factors which are reported.
- Board must approve the annual sustainability report.
- Board must make statement on compliance with primary components or otherwise.
- Board must address questions on sustainability report.

Implementation

- Rules take effect for financial year ending on or after 31 December 2017.
- Phased implementation on adoption of key ESG factors.
- Independent assurance encouraged but optional.

Remuneration practices in Singapore

More than 50 corporate directors and management turned up at the 2015 Hay Group Survey on Director and Executive Pay forum held on 28 January 2016, to learn about the latest trends for Singapore non-executive director (NED) remuneration and top executive remuneration.

Based on Hay Group's studies, Mr Kevin Goh, Director of Hay Group Singapore, shared that the median average directors' fee remained flat at S$60,000 per annum. Both medium and small-sized companies had no increase in the average directors' fees whereas the larger companies had a marginal four per cent increase.

As for executive compensation, the total CEO pay had an average increase of 0.4 per cent with the median at S$937,000 per annum. Leading all other sectors is the property sector, with the highest median CEO compensation of S$3.38 million per annum.

Mr Goh also covered both short-term and long-term incentives, elaborating on the various frameworks and schemes used by Singapore companies. He also touched on the pay for performance practices in Singapore and shared that the four common financial indications of performance for remuneration purposes were:

1. One-year Earnings Per Share (EPS) growth
2. One-year Total Shareholder Return (TSR)
3. Return on Common Equity (ROE)
4. Return on Invested Capital (ROIC)

For 2016, Hay Group expects that there will be more pressure from SGX and the public where guidelines may turn into "rules". ■

SGX revisions to Directors' & EOs' undertakings

In October 2015, SGX established three independent Listing Committees to strengthen the listing policy and review process as well as enhance enforcement of listing rules. In the consultation for the formation of these committees conducted a year earlier, SGX had proposed amending Listing Rule 720 (1) to require all issuers to procure Letters of Undertaking (LOU) to comply with the Listing Rules from their directors and executive officers.

Following further feedback (after the consultation paper) from stakeholders, including SID, SGX is amending the form of the LOU. Briefly, these include:

- Change of wording from "the best of my ability" to "use my best endeavours" for compliance with the requirements of the Listing Manual.

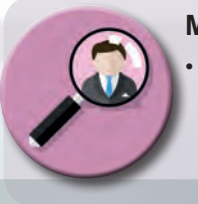
- Removal of reference to compliance with the Securities and Futures Act, The Singapore Code on Takeovers and Mergers, Companies Act (Chapter 50) and other securities laws.
- Removal of requirement to provide information/documents and to co-operate in any investigation conducted by SGX.

Directors and executive officers can execute the LOU by 30 April 2016. ■

Coming soon: SID's new website

SID's revamped website will be integrated with an engagement backend system to provide you with on-the-go seamless service – anytime, anywhere, on any device. The focus is to enhance your engagement experiences with SID.

Here's a peek of some of the services that will appear in your personalised dashboards…

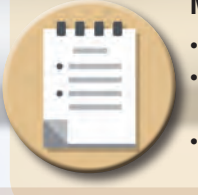


My Site

- Snapshot of details on your SID membership, directorships, professional development courses and events.

Registration

- Simply select the event you plan to join. As all your personal data are already stored, you need not key them in again.



My Professional Development

- Past and present pictorial showcase of courses
- Your CPD hours and duration will be automatically tracked
- You can plan your training ahead with SID's Professional Development schedule for the year.

Board Appointment Services

- Your interest in joining new boards, and current directorship experiences will be captured in SID's system. This will enable SID to match you with the opportunities when they arise.

Keep your eyes peeled for SID's new website in the second half of this year.

SID's Q1 Events (January 2016 – March 2016)

DATE	TYPE	EVENT DETAILS
12 Jan 2016	PD	ACRA-SGX-SID Audit Committee Seminar – Raising the Bar for Financial Reporting and Audit
14 Jan 2016	PD	LCD Module 1: Listed Company Director Essentials
15 Jan 2016	PD	Launch of *Remuneration Committee Guide*
20 Jan 2016	PD	Board and Director Fundamentals
27 Jan 2016	PD	Director Financial Reporting Essentials
28 Jan 2016	PD	2015 Hay Group Survey on Director and Executive Pay: Re-evaluating Rewards
29 Jan 2016	Advocacy	Dialogue Session on the SGX Consultation Paper, *Sustainability Reporting: Comply or Explain*
2 Feb 2016	PD	Directors Compliance Programme
18 Feb 2016	PD	Directors Compliance Programme
19 Feb 2016	Event	SID Lo Hei Lunch
24 Feb 2016	PD	Improving Board Risk Oversight Effectiveness
3 Mar 2016	PD	SID-INSEAD International Directors Programme Tea/Cocktail Talk
10 Mar 2016	PD	Dealing with Damn Difficult Directors
10 Mar 2016	PD	NPD Module 5: Financial Management and Accountability
17 Mar 2016	PD	So, You Want to Be a Nonprofit Director?
22 Mar 2016	PD	Director Financial Reporting Essentials
23 Mar 2016	PD	Confronting The Hot Spots – Redefining Business Success and Managing Geopolitical Risks in a Changing World
29 Mar 2016	PD	LCD Module 2: Audit Committee Essentials
30 Mar 2016	PD	LCD Module 3: Risk Management Essentials
31 Mar 2016	PD	Launch of *Board Risk Committee Guide* and ASEAN Corporate Governance Scorecard

A life of adventure on wheels

By **GERARD TAN**
Treasurer, SID

AFTER HOURS

My love affair with road biking began on Valentine's Day 2009 when I bought my first road bike, a Specialised Roubaix. I was 54 then.

The experience was exhilarating. Within months, I found I could ride faster but I was also getting leg cramps, back, neck and shoulder aches, as the rides got more frequent and longer. Normal, it seems, for newbies as road bikes need to be fitted fairly precisely to one's built for ergonomics and performance.

What started as a hobby became a passion, and the years that followed became an adventure on two wheels.

My cycling kakis and I got bored cruising Changi Coastal Road week after week. We decided to form a team to take part in the 2010 OCBC 40 km Cycle Challenge, our first competitive cycling event – something to train for!

In 2011, I signed up for the Nanyang Technological University Bike Rally, a round-the-island event that covered about 150 km. The ride took me to all four corners of Singapore – that's when you realise just how tiny the country is. That experience bolstered my confidence and I decided that I should put my pedal to the metal, but overseas. Singapore was simply too flat! This was the start of my series of overseas biking holidays.

That same year, I took part in the inaugural Tan Tock Seng Hospital (TTSH) Charity Ride. My first overseas cycling trip was a ride from Malacca to Singapore. With TTSH, we subsequently rode in Bintan and Thailand.

The Tour de Bintan (TdB) is a two-day three-stage event. That November I completed the first of three TdBs. For one who had only "suffered" Mt Faber, Bintan was a shock to my system. Never had I suffered so much climbing hill after hill for over 270 km in two days.

However, it was Cameron Highlands that proved to be my first true mountain climb. It was not only leg-breaking but also lung-splitting. I trudged for a good 50 km straight up from the base to Tanah Rata at the top. The downward journey was a different ball game altogether. I was clinging on to the bike's brakes so tight – I had to, for it was a good two hours spent freewheeling down a twisty mountain rife with several blind corners and S-bends.

The one that took the cake was a six-day Vars cycling trip in the French Alps. It was a retirement

present I gave myself in July 2012. It was, without a doubt, the most wonderful and visually stunning cycling experience of my life. Awe-inspiring mountains – other than the cycling itself – took my breath away. The highlight of the trip was riding up one of the mountains to the town of Albertville la Troussuire (2,356m above sea level) where I saw the Tour de France riders come through and witnessed the finishing stage!

In 2013, I decided to mix my love for fine food and wine with cycling and headed to Tuscany and did a gourmet tour on bike. For five days, we traversed the wine region, lunched in beautiful medieval towns and stayed in wineries where we enjoyed top-notch Italian wines and food.

In January 2014, I participated in the 150 km Mt Tanaraki challenge in New Plymouth, New Zealand. Even though it was in the prime of summer, it was so windy at some points that some of us were nearly blown off our bikes by 30 km per hour gusts that were biting cold!

Cycling has been good fun and recreation for me but it certainly comes with its share of dangers. Unfriendly and inconsiderate vehicle drivers is one of them.

A road bike is light with skinny tires, which makes it quite twitchy at times. It does not ride well over portholes and unevenly paved roads. Crashing is a matter of when – and how bad – for a road biker.

This may sound morbid but my most memorable crashes included being knocked down by a motorbike in 2011, a scooter in 2012 (both happened in Bintan), and fracturing my right collar bone after losing control over a poorly-finished road works patch along Tanjong Rhu Road a couple of years ago.

Two operations and seven months later though, I was back on my bike. I have since added jogging and weight training in the gym to build bone and core muscle strength to reduce the risk of fractures in future crashes.

As Albert Einstein once said: "Life is like a bicycle. In order to keep your balance, you must keep moving."

I hope to keep on pedalling for many years to come. ■

Upcoming events

Core Professional Development Programmes

PROGRAMME	DATE	TIME	VENUE
So, You Want to Be a Nonprofit Director?	17 Mar 2016	1730 – 2030	Capital Tower
Director Financial Reporting Essentials	22 Mar 2016	0900 – 1700	Capital Tower
LCD Module 2: Audit Committee Essentials	29 Mar 2016	0900 – 1230	Marina Mandarin Singapore
LCD Module 3: Risk Management Essentials	30 Mar 2016	0900 – 1230	Marina Mandarin Singapore
Launch of Board Risk Committee Guide and ASEAN Corporate Governance Scorecard	31 Mar 2016	0900 – 1115	Marina Mandarin Singapore
SID-SMU Directorship Programme Module 1: The Role of Directors	4 – 6 April 2016	0900 – 1700	SMU Campus
LCD Module 4: Nominating Committee Essentials	5 Apr 2016	0900 – 1230	Marina Mandarin Singapore
LCD Module 5: Remuneration Committee Essentials	7 Apr 2016	0900 – 1230	Marina Mandarin Singapore
Directors Compliance Programme	9 Apr 2016	0900 – 1330	Capital Tower
LCD Module 6: Investor and Media Relations Essentials	12 Apr 2016	0900 – 1230	Marina Mandarin Singapore
GVG Module 1: Effective Board for Growth Companies	14 Apr 2016	0900 – 1230	Marina Mandarin Singapore
NPD Module 6: Fundraising and Outreach	14 Apr 2016	1700 – 2030	Children Cancer Foundation
GVG Module 2: Fund Raising for Growth Companies	20 Apr 2016	0900 – 1230	Marina Mandarin Singapore
Directors Compliance Programme	25 Apr 2016	1300 – 1730	Capital Tower
GVG Module 3: The Paradox of Risk for Growth Companies	27 Apr 2016	0900 – 1230	Marina Mandarin Singapore
Directors Compliance Programme	5 May 2016	1300 – 1730	Capital Tower
LCD Module 1: Listed Company Directors Essentials	5 May 2016	0900 – 1730	Marina Mandarin Singapore
Masterclass for Directors Module 1: Board-Management Interactions	6 May 2016	0900 – 1700	TBA
SID-SMU Directorship Programme Module 3: Finance for Directors	9 – 11 May 2016	0900 – 1700	SMU Campus
NPD Module 7: Social Trends	12 May 2016	1700 – 2030	Crossings Cafe
Directors Compliance Programme	17 May 2016	1300 – 1730	Capital Tower
Directors Financial Reporting Essentials	18 May 2016	0900 – 1700	Capital Tower
GVG Module 5: Family Business Governance and Succession	19 May 2016	0900 – 1230	Marina Mandarin Singapore
GVG Module 4: Improving Financial Savviness for Directors	20 May 2016	0900 – 1230	Marina Mandarin Singapore
Board and Director Fundamentals	24 May 2016	0900 – 1700	Marina Mandarin Singapore
SID-SMU Directorship Programme Module 5: Strategic CSR and Investor Relations	26 – 27 May 2016	0900 – 1700	SMU Campus
IDP Module 1: Board Effectiveness and Dynamics	19 – 22 Jun 2016	0900 – 1700	INSEAD Campus
Masterclass for Directors Module 3: Fair Process Leadership in the Boardroom	23 Jun 2016	0900 – 1700	TBA
SID-SMU Directorship Programme Module 2: Assessing Strategic Performance	27 – 29 Jun 2016	0900 – 1700	SMU Campus
LCD Module 1: Listed Company Directors Essentials	12 Jul 2016	0900 – 1730	Marina Mandarin Singapore
LCD Module 2: Audit Committee Essentials	13 Jul 2016	0900 – 1230	Marina Mandarin Singapore
LCD Module 3: Risk Management Essentials	13 Jul 2016	1400 – 1730	Marina Mandarin Singapore
LCD Module 4: Nominating Committee Essentials	14 Jul 2016	0900 – 1230	Marina Mandarin Singapore
LCD Module 6: Investor and Media Relations Essentials	14 Jul 2016	1400 – 1730	Marina Mandarin Singapore
LCD Module 5: Remuneration Committee Essentials	15 Jul 2016	0900 – 1230	Marina Mandarin Singapore
Directors Financial Reporting Essentials	20 Jul 2016	0900 – 1700	Capital Tower

Core Professional Development Programmes

PROGRAMME	DATE	TIME	VENUE
So, You Want to be a Director?	4 Aug 2016	1030 – 1230	Capital Tower
SID-SMU Directorship Programme Module 4: Risk and Crisis Management	11 – 12 Aug 2016	0900 – 1700	SMU Campus
Masterclass for Directors Module 2: Boardroom Dynamics	23 Aug 2016	0900 – 1700	TBA
SID-SMU Directorship Programme Module 6: Effective Succession Planning and Compensation Decisions	6 – 7 Sep 2016	0900 – 1700	SMU Campus
Masterclass for Directors Module 4: Board Evaluation	7 Sep 2016	0900 – 1700	TBA
GVG Module 1: Effective Board for Growth Companies	21 Sep 2016	0900 – 1230	Marina Mandarin Singapore
GVG Module 2: Fund Raising for Growth Companies	21 Sep 2016	1400 – 1730	Marina Mandarin Singapore
GVG Module 3: The Paradox of Risk for Growth Companies	22 Sep 2016	0900 – 1230	Marina Mandarin Singapore
GVG Module 4: Improving Financial Savviness for Directors	22 Sep 2016	1400 – 1730	Marina Mandarin Singapore
GVG Module 5: Family Business Governance and Succession	23 Sep 2016	0900 – 1230	Marina Mandarin Singapore
IDP Module 2: Board Decision Making and Oversight	26 – 28 Sep 2016	0900 – 1700	Fontainebleau
Board and Director Fundamentals	28 Sep 2016	0900 – 1700	Marina Mandarin Singapore
Directors Financial Reporting Essentials	30 Sep 2016	0900 – 1700	Capital Tower

Other Professional Development Programmes

PROGRAMME	DATE	TIME	VENUE
Board Risk Committee Chairmen's Conversation	8 Apr 2016	0900 – 1100	Four Seasons Hotel Singapore
Intellectual Property – Leveraging IP for Growth	28 Apr 2016	0900 – 1100	Marina Mandarin Singapore
Board Chairmen's Conversation	10 May 2016	1100 – 1300	TBA
China – What's the New Normal?	31 May 2016	0900 – 1100	Marina Mandarin Singapore
Risk Management – Black Swans	24 Jun 2016	0900 – 1100	Marina Mandarin Singapore
Remuneration Committee Chairmen's Conversation	15 Jul 2016	1100 – 1300	TBA
Cyber Security: Building Resilience	29 Jul 2016	0900 – 1100	TBA
Fraud, Bribery and Corruption: What You Didn't Know	5 Aug 2016	0900 – 1100	Marina Mandarin Singapore
Audit Committee Chairmen's Conversation	18 Aug 2016	1100 – 1300	TBA

Major Events

EVENT	DATE	TIME	VENUE
Corporate Governance Chinese Forum	2 Aug 2016	1000 – 1400	TBA
Launch of Singapore Governance and Transparency Index	3 Aug 2016	0900 – 1100	TBA
SID Directors' Conference	5 Sep 2016	0900 – 1630	Suntec Singapore Convention & Exhibition Centre

Socials

EVENT	DATE	TIME	VENUE
Rid Your Back Pain Using Traditional Chinese Medicine	12 Apr 2016	1730 – 1930	Singtel ComCentre
SID Golf Tournament	8 May 2016	1100 – 2030	Tanah Merah Country Club

Course dates are subject to change. Please refer to www.sid.org.sg for the latest updates.

Welcome to the family

December 2015

Arumugam Ravinthran
Bowden Alwyn
Chiang Fock Pong
Chockalingam Ramasamy
Chong Kek Sing
Choo Peng Leong, Phillip
Fungkong Victor
Ganesan Venkataraman
Goh Gabriel De En (Roy)
Gough Julia
Harsh Saluja
Koh Chai Ping, Michelle
Koh Lavinia
Lau Chin Huat
Liew Sam
Lim Heng Lin
Lim Ming Yan
Long Keith
Loy York Ying
Mahamunkar Maneesha
Mason David
McNulty Stephen
Nguyen Ha Lan Jamie
Saye Christopher Dale
Scully Peter
Tan Lay Hong
Teo Swee Lian
Vohra Vineet
Wee Meng Seng, Aloysius
Wildblood Andrew
Wong Kim Yin
Wu Longbao
Yeo Boon Keong
Yeo Yeow Hwee

January 2016

Alan Zeller
Chi Ping Huey
Chia Boon Kuah
Chow Yin Nei, Angeline
Cooper Lindsay William Ernest
Ellenbogen Nir
Goh Sia
Grier Nigel Robert Davies
Hawkins Nicholas
How Meng Hock
Jumabhoy Iqbal
Kerner Clive
Klingensmith David
Koh Ngin Joo, Julie
Koh Soon Chua
Krishnan Nanda Kumar
Lee Tiong Seng
Liak Teng Lit
Low Yee Khim
Mei Ming Zhi
Nagakawa Kiyoshi
Ng Yong Hwee
Quah Kung Yang
Ramanathan Subramanian Arun Kumar
Seah Royce
See Jaacky C C
Seek Ngee Huat
Sella Itzhak
Sin Chee Mei
Smart-Gill Dickon
Tan Yew Meng
Yoo Loo Ping

SID Governing Council 2016

CHAIRMAN
Willie Cheng

FIRST VICE-CHAIRMAN
Daniel Ee

SECOND VICE-CHAIRMAN
Soh Gim Teik

TREASURER
Gerard Tan

COUNCIL MEMBERS
Ramlee Buang
Robert Chew
Wilson Chew
Junie Foo
Philip Forrest
Kevin Kwok
Lee Kim Shin
Elaine Lim
Irving Low
Ng Wai King
Poh Mui Hoon
Andy Tan Chye Guan
Tan Boon Gin
Tan Yen Yen
Eugene Wong
Wong Su Yen