

# BoardMatters Quarterly

Insights for boards and  
audit committees

Volume 5 | July 2015

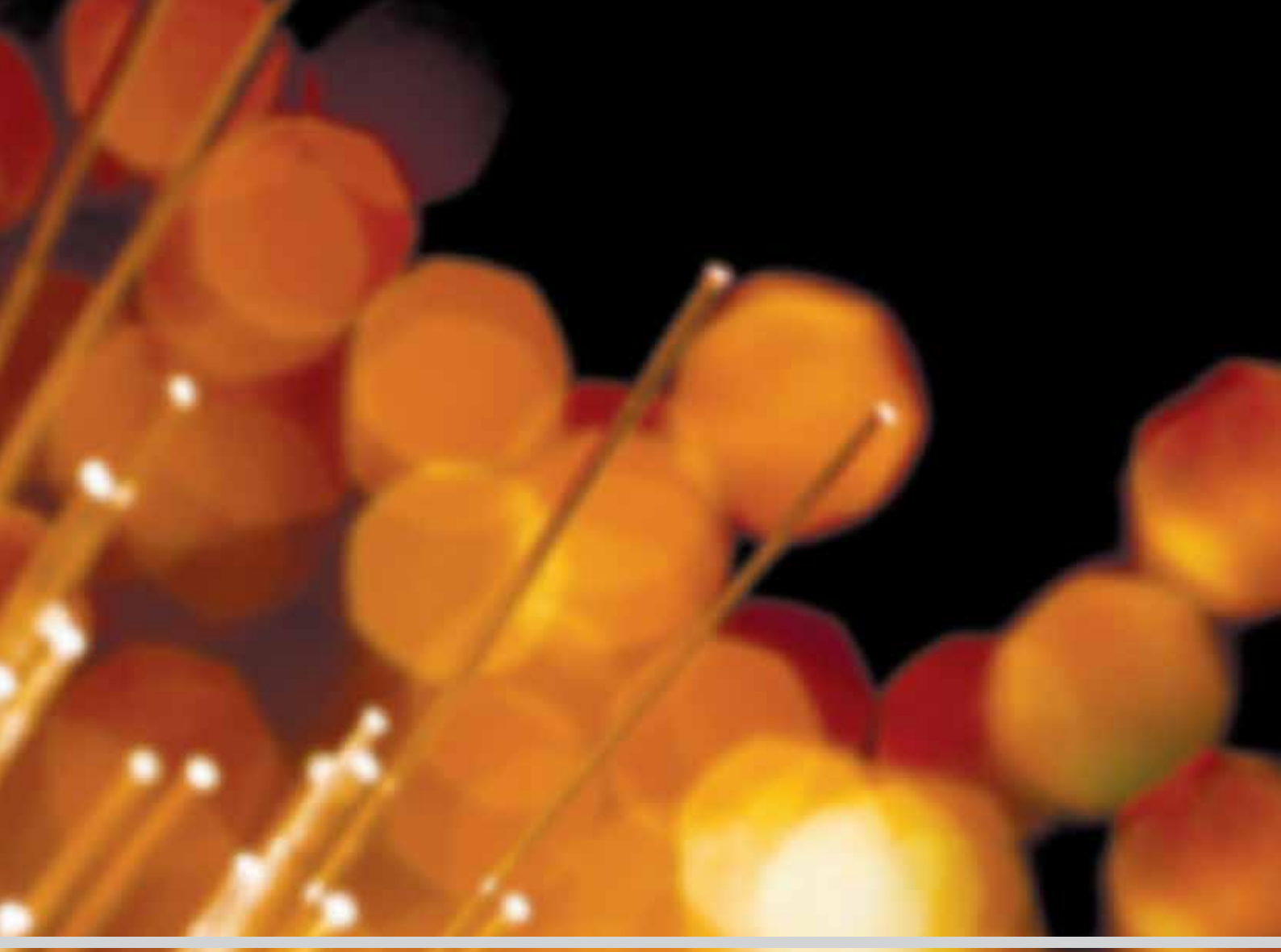


# In this **issue**

| 4

## **Cybersecurity: An emerging risk on the board agenda**

The article highlights how cybersecurity has emerged as a serious risk given the pervasiveness of technology across organisations. It makes a case for cybersecurity to be elevated to the board agenda, spelling out aspects that Boards need to be engaged with to proactively mitigate this risk



| 8

### **Digital: Shaping the future of business**

With all pervasiveness of technology which is disrupting business models, no longer can organizations be assured of business models of an enduring nature. With Boards' oversight on business strategy, it has become imperative for Boards' to be tech savvy and ensure they are guiding managements to treat such disruption brought about by technology as a major risk. Using illustrative examples, the article makes a compelling case for how enterprises that can seize the opportunities stand to gain significantly while those who cannot may lose everything

| 12

### **Putting your trust in the cloud**

Cloud computing has caught the imagination of organizations that are assessing how best to effectively harness technology while driving business efficiency. While cloud computing offers many benefits, there can be risks. These concerns are valid and venturing into the cloud without understanding the security, privacy and regulatory considerations will put the company at risk, says the article

| 14

### **Companies Act 2013: An update**

The Companies Act, 2013 and the guidance around it has been a very dynamic process. The article provides an update on key aspects relating to the reporting by auditors with regards to fraud, internal financial controls and propriety audit. The changes and clarifications significantly impact not only the auditors but also the companies they audit, the board and audit committees



# Cybersecurity: An emerging risk on the board agenda



As technology becomes all pervasive across organizations, it brings with it the risk of falling victim to cyberattacks – a potent risk that has attracted attention like never before. Are organizations across the corporate landscape alert to this emerging risk that is real? As and when a cybersecurity breach occurs, the severity of its impact will depend on how prepared and proactively engaged the board is with this challenge, **says Burgess Cooper**

Cyberattack has emerged as the next big challenge, a risk that can severely impact a company's competitive advantage and shareholder value and damage its reputation. In today's world of "always on" technology and negligible awareness around security among users, cyber-attacks are no longer a matter of "if" but "when." The wave of security breaches that have affected leading organizations across domains including ecommerce, financial services, media and entertainment, telecommunications and technology, have made it clear that no organization is immune to this threat.

Consider two instances of Cyberattacks and how these affected the organizations that fell victim to it:

## Case Study I

A leading entertainment organization was hacked and it lost more than 100 terabytes of data to unauthorized users, which compromised the confidentiality of business sensitive and personal data. The data breach included unreleased movies, personal data, employee confidential information (such as Social Security Numbers and medical information) etc.

As a result the senior management and C-level suite had to tender an embarrassing public apology to all customers and shareholders.


While this is a good example of company leadership and board taking ownership and responsibility it would take years to regain the customer trust and brand erosion caused by breach of customer privacy.

## Cast Study II

A financial services organization was attacked as a result of negligence regarding two-factor authentication. The attackers were able to move around the network and ultimately access more than 80 + servers. While no financial data was affected, the attackers were able to access customer records revealing email addresses, home phone numbers and mailing addresses for more than 60 million household customers, potentially affecting the customer trust and creating potential data privacy issues.

The resulting public disclosure brought about embarrassment and potential loss of customer trust, which would take several years to rectify, given the very nature of the financial services business.

Given the severity of its impact and graduating much beyond being treated just as a technology issue, cyberattacks have acquired the stature of a business risk that requires an enterprise-wide response. Boards need to take it out of the silo of the IT department and lead the change in mindset across the organization so that it is viewed as a risk that is managed and integrated into the overall business strategy and operations. The major hacking exploits are indicating a new trend, which has recently emerged, i.e., a company may not only be attacked for who it is, but more importantly "to whom it can give access to" thereby requiring a complete change in its cyber defence strategy. Accordingly, many businesses, which service large organizations, may be at increasing risk given that they may often be the conduit to a more sophisticated cyber-attack.



## Cyber security and Cyber governance

With the proliferation of digital media and an increasing number of people engaging in technological and social media experiences, significant amounts of information is accessible to a large number of people, with a potential to damage corporate reputation.

Given the pervasive impact that cybersecurity can have across the length and breadth of company operations, the full board should govern cybersecurity. However, more than just ensuring its put on the board agenda, it is important to ensure that cyber risk considerations are interwoven into all major discussions and decisions at the board level – whether they are about changes in the business environment or in business strategy and operations (e.g., a merger, acquisition, introduction of a new product, entrance to new markets, implementation of new technologies or software).

For example, during an acquisition, if cyber risks are not considered when diligence is carried on the acquiree to understand associated business risks, a company and its board will not fully understand associated vulnerabilities and hazards they are likely to inherit once the transaction is complete. As organizations adapt to changes in the external business environment and their business strategy and operations, boards need to ensure that related cybersecurity measures and related risks are adapted to accordingly.

A solid foundation in cybersecurity, stemming from cybersecurity knowledge from an enterprise standpoint, has become imperative for the management and the board. Putting this foundation in place is not an easy task, but boards should call upon management to “activate” its resources and bridge any human capital and knowledge gaps. With cybersecurity acquiring a sense of urgency in the boardroom, the quantum of resources that address this challenge continue to be of concern.

According to a EY’s 2014 Global Information Security Survey, 43% of survey respondents stated that their organization’s total information security budget will stay around the same in the coming year. It is the board’s responsibility to challenge management so that management is appropriately allocating resources to address cyber risks that are commensurate with risk levels. Given that technology transcends and affects all departments and corporate structures, boards should address whether management’s cybersecurity plan has a cross-functional team involving business leaders of all key departments, such as human resources. This will ensure that the management is taking a holistic and comprehensive approach toward managing cybersecurity.

### Anticipating and addressing risks proactively

Strong cyber governance will enable organizations to proactively articulate

their strategies to address advanced persistent threats. Organizations change and so do threats. Therefore, the foundation of cybersecurity must adapt to keep pace, and boards will need to adapt to these changes as they commit to incorporating cybersecurity as part of their governance responsibilities. As the economy becomes more digitized and the degree of interconnectedness with other parties (such as suppliers, vendors and customers) increases, so does the risk to the company. Therefore, when performing and re-evaluating its risk assessment, boards will need to continuously evaluate, balance and adapt to all risks (both internal and external) posed to the company, including those that are associated with the company’s broader network or ecosystem.

A key ask from boards, for them to effectively address cyber attacks, in addition to an improved understanding of such risks, is to ensure that their directors’ skills and experiences are commensurate and adequate. Otherwise they should consider adding someone with IT experience, which could help the board mitigate its cybersecurity “knowledge gap”. In some instances, boards are hiring their own experts to educate directors. Others are leveraging independent advisors (e.g., external counsel and external auditors) who can provide perspectives and insights on trends related to cyber risk present in the industry.

## Regulators speak about cyber security

Regulators across various sectors, such as telecom, insurance and banking, are taking steps to increase the oversight and highlighting the need for public companies to make disclosures related to these risks. Earlier, many private organizations did not believe in disclosing information about such attacks but recently more organizations are increasingly becoming vocal about such incidents.

Cyber threats and attacks expose organizations to legal liability. Individuals whose personally identifiable information is compromised as a result of a data breach may bring civil privacy claims under specific country legislations. Shareholders affected as result of cyberattacks could file derivative claims mentioning that officers and directors breached their fiduciary duty of care by failing to implement appropriate security control and oversight.

## Network to keep the networks safe

The ferocious dynamism of technology and the cyber threats that come with it are accelerating rapidly. Organizations need to invest not only in right security technologies but in better understanding of their ecosystem and working with trusted partners to further protect their cyber sphere together. Leading boards motivate their organizations to proactively foster relationships and increase the level of collaboration rather

than just monitoring of their own systems, working more closely with others in the industry, competitors and governments to combat threats that face them as a team.

## Deploying metrics to determine preparedness to address cybersecurity concerns

Leading practices suggest a focus on metrics, which will help the board determine whether management is appropriately adapting to potential cyber threats and responding to them swiftly.

Companies often engage in cyber security war games to assess their level of preparedness by engaging in actual real life cyber hacking, potential data loss type of scenarios and gauging the level of preparedness of the same.

The metrics should focus on the total number of breach attempts detected, time taken to respond and the effectiveness of the entire cyber security incident response procedure.

Determining benchmarks will allow boards to assess whether responses were swift and successful and also whether to consider hiring external experts to review the company's cybersecurity plans and benchmark those plans against comparable companies.

However, apart from metrics, it is important that the board is challenging the management on the need to create

an incident response plan that helps in promptly addressing any cybersecurity breach that occurs so that the damage resulting from it is minimal or altogether mitigated. Viewing cybersecurity as an enterprise wide risk will provide boards the true context of beginning to put in place a robust cybersecurity governance framework.

## Board oversight on committees to address cybersecurity framework

Boards need to set the tone to enhance security as it should be deeply rooted in the organization's strategy and culture. Board should determine whether the full board or a committee should have oversight responsibility. In some cases, a risk committee, executive/operating committee or the audit committee will be given the oversight charge. At times, audit committees may need detailed information about the organizations' cyber security practices and they often leverage the information to understand the oversight. They should understand if the team handling cybersecurity is sufficiently equipped and skilled to handle this responsibility.

The audit committee's action plan will depend on the company's level of maturity in managing security risks, and it may require more attention and time in sectors where these risks and the potential for damages are highest, such as telecommunications and financial services institutions.

## Six commandments for the board to consider



Ensure that sufficient resources are allocated to cater to cyber security issues



Understand management's preparedness in terms of an incident response plan, to respond to cybersecurity breaches



Consider the addition of new skills that could help in a better understanding of cybersecurity issues



Appointment of independent directors with knowledge of information technology systems and associated threats



Ensure metrics that test effectiveness of an incident response plan are put in place



Consider cybersecurity specific insurance

# Digital: Shaping the future of business



With technology disrupting and shaping the future of business, it is forcing organizations to rethink and realign business models lest they become irrelevant and outpaced. With boards guiding the business strategy, their perspective on how management is embracing "digital" will be a key determinant behind how enduring the business is, **says Samiron Ghoshal**

Digital is fundamentally changing how companies do business. Enabled by data and technology, digital is a continuous form of disruption to business models, products, services and experiences. It has radically changed the way people consume content, communicate, and access products and services.

New outfits, which utilize digital tools, are popping up overnight threatening to put decades-old veterans out of business even as existing companies work to gain the required agility to compete in today's increasingly complex market landscape. What began as a trickle in a select group of industries is now mainstream with brick and mortar industries such as automotive, airlines and real estate being right in the centre of this wave.

While the Sloan Management review estimates that 25% of the Fortune 500 have become bankrupt, been acquired or ceased to exist, since 2000 due to digital disruption, a report by Gartner estimates that 25% of all businesses will lose their competitive ranking by 2017.



---

## Digital is now firmly on the board agenda.

The main opportunities around Digital are centered around three distinct areas – better ecosystem connectivity, improved data based decision making, enabling new business or operating models.

Digital channels provide for better interactions with customers, suppliers, stakeholders. It enables tailoring of messages for context, adding social connectivity and making the content universally available by mixing media makes for transparency and reduced cost of operations.

Within the digital domain, social media has redefined the customer relationship dynamics. The goal is less about “selling” and more about “engaging”. One of the exceptional displays of a business’ connect with their customers is reflected during times of distress – a leading flag carrier airline presented itself as a leader in social customer service field during a tragic volcano eruption. While passengers were stranded and flights were cancelled they turned to popular social networking sites for help. The airline was prepared

for such a scenario and delivered with prompt replies to queries and assistance in arranging other means of travel. It was a perfect example of a catastrophe averted with social media and triggered a fundamental change in the way airlines handle customer service today.

Algorithms crunching information from disparate data sources provide better insights into different parts of the organization – combining data for sensors tracking wear and tear on equipment, for instance, to inventory-level data to sales data from a third system to make better decisions on when to schedule preventive maintenance.

A global cosmetics maker, for example, now operates more than 500 of its IT applications in a private cloud built and operated by its IT team. When a fire destroyed its data center in Venezuela, they were able to move all their operations to the New Jersey center within two hours – saving US\$70 million. Steps like these demonstrate the flexibility and reliability of cloud computing in preventing major mishaps and helping organizations mitigate risks.

Processes from product innovation to customer service can speed up using digital tools. Both can now be crowdsourced in part using social media tools leaving the enterprises to focus on the core and essential processes within.

In the last decade, digital technology advances have changed photography dramatically, and a former heavyweight in the analog photography business has lost its competitive edge over new tech-savvy companies. Besides not adapting to digital cameras it helped create, it also did not evolve itself with the new ways in which consumers wanted to interact with their photos and the market forces surrounding them. The recent economic downturn was the final nail in its coffin, though other companies managed to deal with it without going bankrupt. The truth is that by the time the company had both feet fully in the digital game, it had been outclassed by more nimble competitors with better products.

Several governments are following suit and improving public services and amenities. India launched the world’s largest biometric-identity program



Aadhaar, where around 370 million people have already been enrolled, and 600 million in all will be registered by the end of the first phase. India plans to use the system to make over US\$50 billion in cash transfers to poor citizens, saving US\$6 billion in fraudulent payments. The Government of Bangladesh and China are also adopting digital initiatives to augment the level of health services in their countries. Bangladesh has implemented a mobile notification system in rural regions to inform nurses and mid-wives of birth alerts helping increase infant mortality rate. Currently 89% births in these regions receive medical supervision as compared with 90% unassisted births in the past.

### Considerations for the board that define the digital agenda:

There are six major decisions that the Board needs to take:

**Digital Leader or Follower:** Enterprises have to decide whether they will lead the digital space in their industry or be laggards based on their sector, markets they service and competitive pressures. For example a motor insurance provider has more to lose from digital competition than a mining giant.

Digital forays often result in cannibalization of market share from the original business; however, it may also provide for an effective response to digital competition.

Many businesses elect diversified risk by entering small digital initiatives across businesses and then manage them using a portfolio approach investing in the successful ones and choking off funding to the not so successful ones. Others bet the bank on one or two big areas of core business.

**Co-operate or Compete:** For most large businesses the threat from digital is all across its value chain. Banks may be competing with crowdfunding start-ups on the lending side, with digital payments compete in the payments space and with other reduced digitally oriented banks all at the same time. The board has to decide what the appropriate response to each kind of threat will be.


**Business Portfolio assessment:** As the digital world produces new winners and losers, the growth and profitability of some businesses needs to be re-assessed through a digital magnifying glass. Media companies have a print v. digital assets decision to make just like the retail chains have to assess investments in warehouses (to facilitate the back-end supply chain for on-line sales) v. launching new stores.

### **Integrate or Diversify Digital Business:**

Digital businesses can be integrated in the existing brick and mortar operations or can be hived out into a new entity in view of the cultural issues that may arise due to the combining of old and new economy talent under one roof.

**Delegate or own Digital agenda:** The digital agenda needs to be driven at an appropriate level keeping in mind the structure of the enterprise, the size of the transformation, and the cultural milieu among other factors. Whether or not this is to be driven from the CEO's office or driven through a chief digital officer or the CIO is central to some of these discussions.

A recent boardroom concern has been the lack of digital expertise -- the need to have a "digital director" on the board. In 2012, a leading global financial services firm did not have any directors with risk expertise on the board's risk committee. The deficiency was corrected only after Bruno Eskil "the London Whale" caused US\$6 billion worth of trading losses through what was famously called a "risk 101 Mistake". Will the Boards wait for a "digital 101 mistake" to happen to embrace digital?



**Board Matters Forum - India is now on the Flipboard app**

Access today!




Stay abreast with the latest international and domestic news, views and EY insights for audit committees and boards. Available anytime, anywhere on tablets and smartphones

**To access Board Matters Forum - India on Flipboard, follow the steps below:**

**1.** Download Flipboard  
If you have an iPhone or iPad, download from the app store icon on your device. If you have an Android phone or tablet, download from the Google Play icon on your device.

**2.** Create your Flipboard account  
Once you download Flipboard on your device, click on the icon and sign up to create an account. Create and verify your username and password.

**3.** Finding *Board Matters Forum - India* on Flipboard  
Once you login to Flipboard, type '*Board Matters Forum - India*' in the search box on top right corner. Search result will show *Board Matters Forum - India* App, select it to open.

**4.** Subscribing to *Board Matters Forum - India*  
Tap the  tab once you are on the main page of *Board Matters Forum - India*. The *Board Matters Forum - India* icon will appear on the interface of your Flipboard page. You are ready to now use the app.

# Putting your trust in the cloud

## Building a secure environment

Cloud computing is fundamentally different from traditional enterprise computing. It is technology on demand: you use only what you need, when you need it and how you need it delivered.

While cloud computing offers many benefits, there can be risks.

---

“The IT department, management and board members are shifting their focus from saying “no” to cloud computing to saying “yes,” but in a way that adds value to the business and protects it from mounting cybersecurity risks”.

---

Some fear that communicating data over a shared network will increase their vulnerability to cyberattacks, or that cloud service providers offering the same infrastructure to multiple clients in multiple locations will not be able to maintain confidentiality of all the data.

Still others express concern that data may be transported across borders and may expose them to legal and regulatory requirements in jurisdictions with which they're unfamiliar.

These concerns are valid and venturing into the cloud without understanding the security, privacy and regulatory considerations will put the company at risk.

There is a tendency with cloud solutions to rely on the vendor (or cloud service provider) to ensure that these concerns are addressed. But boards must realize that it is management's responsibility to address the risks of moving to a cloud environment.

Boards should be thinking “cloud first” when contemplating their IT solutions but they must do it with eyes wide open and consider the risk implications.

### Understanding the issues

Some employees may already be using cloud computing, without consulting the IT department. This phenomenon, called “cloud creep,” is blurring the boundaries of corporate networks and potentially making them less secure. Business units

that want to use cloud computing may defy the IT department and procure the service themselves.

The IT department, management and board members are shifting their focus from saying “no” to cloud computing to saying “yes,” but in a way that adds value to the business and protects it from mounting cybersecurity risks.

### Reaching for STAR

Because banning cloud services may not be a viable option, developing a cloud framework that results in a secure, trusted and audit-ready (STAR) environment may make you more confident about your decision to say “yes.”





## The components of a STAR environment are as follows:

**Secure:** A secure cloud environment has the appropriate controls to protect the confidentiality, availability and integrity of the data that resides in the cloud. Appropriate controls exist to properly protect data at rest, in transit and in use.

**Trusted:** A trusted cloud environment is designed to stand the test of time. It should provide high availability and must be resilient to adverse events.

**Audit-ready:** An audit-ready cloud environment has continuous compliance and is certified to meet specific industry regulations. Appropriate procedural and technical protection is in place, documented and can be verified for compliance and regulatory purposes.

Widespread consumption of cloud services isn't on its way; it's here. Early adopters of cloud services have already gained competitive advantages.

Organizations that can think "cloud first," while managing risks using a clear and well-understood model, will benefit from the efficiencies, cost savings and additional capabilities that the cloud can deliver.

Boards and audit committees should understand the company's approach to addressing the opportunities and the challenges related to cloud computing, and they should be familiar with the framework for addressing the potential risks.

## Questions for the board to consider

- ▶ Does the board understand what data is currently stored in the cloud and has management discussed with the board what controls are in place to protect the most sensitive data?
- ▶ Has the company defined and implemented standards so its systems integrate with cloud technologies in a secure manner and have these standards been communicated throughout the company and to the board?
- ▶ What happens if something goes wrong in the cloud? Does the company have a backup and restoration strategy, and has it been reviewed with the board?
- ▶ How does the board know that what the cloud provider is telling the company is reliable? When was the last time a quality control audit of the cloud provider was performed and/or the controls were independently verified?

# Companies Act 2013: An update

**Dolphy D'Souza** provides an update on key aspects relating to the reporting by auditors with regards to fraud, internal financial controls and propriety audit. The changes and clarifications significantly impact not only the auditors but also the companies they audit, the board and audit committees

## Fraud reporting by auditors

Section 143(12) of the Companies Act, 2013 (2013 Act) required that if auditors, in the course of performing their duties, have reasons to believe that a fraud is being or has been committed against the company by its officers or employees, they will immediately report the matter to the Central Government within the prescribed time and manner. The Companies (Audit and Auditors) Rules, 2014 prescribe specific procedures to be followed and lays down a 60-day limit for fraud reporting. These provisions also apply, mutatis mutandis, to a cost auditor and a secretarial auditor.

The 2013 Act and the rules, as originally notified, did not prescribe any materiality threshold for fraud reporting by auditors. Consequently, an auditor was required to report even trivial matters of fraud/ potential fraud to the Central Government. There was a concern that this may lead to significant additional cost and burden on the company (including its board/Audit Committee), auditor and the Central Government without a commensurate benefit.

The Companies (Amendment) Act, 2015, notified on 26 May 2015, addresses the above concern. The Amendment Act envisages that materiality limits will be prescribed for fraud reporting to the Central Government. The Amendment Act also states that for fraud involving lower than the specified amount, the auditor will report the matter to the audit committee/board. Furthermore in such cases the company will disclose the

details about such frauds in the board's report. Materiality limits for reporting of frauds to the Central Government are still not prescribed.

We believe that recognition of materiality concept in the Amendment Act is a step in the right direction. It will ensure that trivial matters of fraud/ potential fraud are not reported to the Central Government. Rather, the same are looked into by the audit committee/board of the company. We recommend that while prescribing a materiality threshold, the Ministry of Corporate Affairs (MCA) should not fix a low threshold; otherwise, the objective of Amendment Act may be defeated.

The Institute of Chartered Accountants of India (ICAI) has issued the Guidance Note on Reporting on Fraud under Section 143(12) of the Companies Act, 2013. The Guidance Note, among other matters, states that section 143(12) requires an auditor to report to the government only those offences involving fraud/suspected fraud in the company by its officers or employees, if the auditor is the first person to identify or notice such an instance. In case a fraud has already been reported or has been identified or detected by the management and such a case is informed to the auditor, the auditor is not required to report the same to the Central Government. However this does not appear consistent with a plain reading of the 2013 Act and the rules.

A high level committee has been set up by the Government to look into the 2013 Act and the rules thereunder, and to

make appropriate amendments. This is a welcome step, and we hope it will bring about more ease of doing business. We would recommend that either the rules or the ICAI Guidance Note should be amended to make them consistent with each other.

## Auditors' reporting on matters that adversely affect company's functioning

In accordance with section 143(3) (f) of the 2013 Act, auditors' report should, among other comments, include observations or comments on financial transactions or matters, which have adverse effect on the functioning of the company.

Since the 2013 Act did not specify the meaning of the phrase "adverse effect on the functioning of the company", the nature of auditors' responsibilities was not clear. One possible view was that the auditor is required to report whether any of the financial transaction or other matters had any adverse impact on the functioning of the company. Under this view, the auditor will have to challenge the propriety of transactions, for example, the propriety of a business or an asset acquisition. This is not in sync with the global practice and goes much beyond the scope of a financial statements audit. Hence, there was a need for more clarity.

The ICAI has issued the Guidance Note on Reporting under Section 143 (3) (f) and (h) of the Companies Act, 2013. In accordance with the Guidance



Note, section 143(3)(f) should not be interpreted to mean that the auditor conducts a propriety audit. Such an interpretation will not only be beyond the scope of the audit of financial statements but will also not be in accordance with the objective and concept of audit stipulated under the 2013 Act.

The Guidance Note also clarifies that the scope of the audit and auditor's role remains the same as contemplated under the Standards on Auditing (SAs) and other relevant pronouncements issued by the ICAI as well as laid down in the 2013 Act. This objective is achieved by the expression of an opinion by the auditor on whether financial statements are prepared, in all material respects, in accordance with an applicable financial reporting framework.

To comply with the reporting requirements of section 143(3)(f), the auditor will need to evaluate subject matters leading to modification or emphasis of matter in the auditor's

report made in the normal course of his audit. The auditor will have to make judgements regarding which of the audit qualifications or emphasis of matter has an adverse effect on the functioning of the company within the overall context of audit of financial statements of the company. Only such matters, which in the opinion of the auditor, have an adverse effect on the functioning of the company, should be reported under this clause.

Ordinarily matters that are pervasive in nature such as going concern or matters that will significantly impact operations of the company due to its size and nature will need to be reported. Examples of emphasis of matter, which may have an adverse effect on the functioning of the company include situations where:

- ▶ Going concern assumption is appropriate but there are several factors leading to a material uncertainty that may cast a significant doubt about the company's ability to continue as a going concern, or

- ▶ A material uncertainty regarding the outcome of a litigation wherein an unfavorable decision could result in a significant outflow of resources for the company.

Examples of emphasis of matter, which may not have an adverse effect on the functioning of the company include a situation where there is an emphasis of matter:

- ▶ On managerial remuneration, which is subject to the approval of the Central Government
- ▶ Relating to accrual of a contractually receivable claim based on management estimate where the ultimate realization could be different from the amount accrued
- ▶ On frauds that have been dealt with in the financial statements of the company and will not have any continuing effect on financial statements.



### **Internal financial control (IFC) reporting at consolidated financial statement (CFS) level**

The 2013 Act contains specific requirements concerning reporting on the internal financial control (IFC). The 2013 Act requires the board report to state whether directors have laid down IFCs, and if those are adequate and were operating effectively. The 2013 Act also requires that auditor's report should state whether the company has adequate IFC system in place and the operating effectiveness of such controls.

Neither the 2013 Act nor the rules require that the provisions concerning preparation of the board report of a parent company should be applied, *mutatis mutandis*, to the consolidated board report. In fact, the 2013 Act does not contain any concept of a consolidated board report. Rather, sub-rule 8 in the Companies (Accounts) Rules 2014 clarifies that a board report needs to be prepared based on standalone financial

statements of a company. Considering this, we believe that directors of a parent company are not required to comment regarding adequacy, existence and operating effectiveness of IFCs for the group as a whole.

In the case of auditors' report, section 129(4) requires that provisions of the 2013 Act, applicable to the preparation, adoption and audit of the financial statements of a holding company will, *mutatis mutandis*, apply to the CFS. Consequently, there is an argument that auditors' report on CFS should include comments regarding existence and operations of IFCs at a group level. However, this means IFCs will need to be imposed on foreign subsidiaries, associates and joint ventures, which in their respective jurisdictions may not be required to comply with these provisions.

The ICAI has issued the Guidance Note on Audit of Internal Financial Controls Over Financial Reporting. The Guidance Note stated that requirements relating to reporting on IFC are not intended to apply

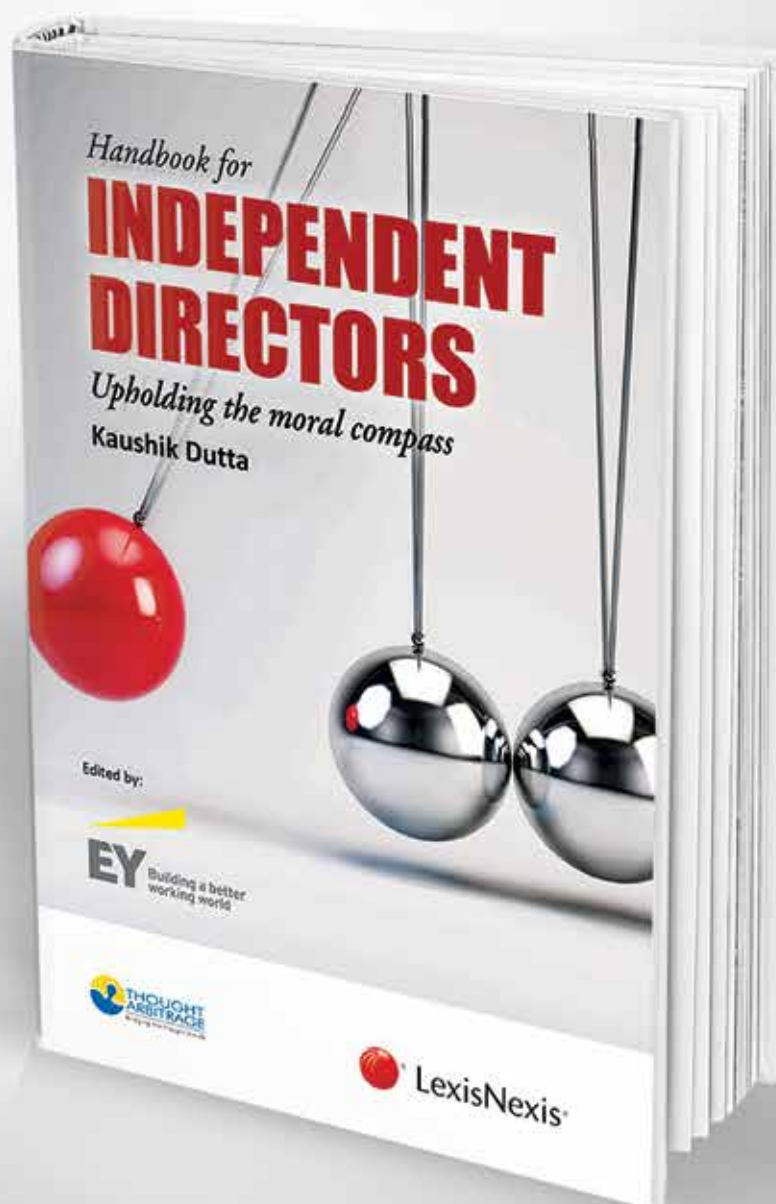
in the case of CFS. However, the said Guidance Note was withdrawn. Recently, the ICAI has prescribed the format of auditors' report on the CFS. Under this format, auditors' report on CFS should include comments on matters stated in the 2013 Act including IFCs, to the extent applicable. For matters prescribed under the Companies (Auditor's Report) Order, 2015, the Guidance Note states that auditors' reports should include comments for holding, subsidiary, associate and jointly controlled companies incorporated in India (including Indian subsidiaries, associates or joint ventures that are private companies). It appears that the same principle will be followed for reporting on IFCs. In other words, IFC reporting will not be required for foreign subsidiaries, associates or joint ventures.



# Helping you walk the tightrope

As regulators enhance their oversight and stakeholder expectations build up, are independent directors ready to walk the tightrope? Introducing the *Handbook for Independent Directors*, an extensively researched publication discussing regulatory requirements arising from the Companies Act 2013, SEBI's Clause 49 and more. The handbook, edited by EY, contains analytical reviews of case law, academic studies and global and India best practices.

To know more, write to [anil.nim@in.ey.com](mailto:anil.nim@in.ey.com)



# Offices

## Ahmedabad

2nd floor, Shivalik Ishaan  
Near. C.N Vidhyalaya  
Ambawadi, Ahmedabad-380015  
Tel: +91 79 6608 3800  
Fax: +91 79 6608 3900

## Bengaluru

12th & 13th floor  
"U B City" Canberra Block  
No.24, Vittal Mallya Road  
Bengaluru-560 001  
Tel: +91 80 4027 5000  
+91 80 6727 5000  
Fax: +91 80 2210 6000 (12th floor)  
Fax: +91 80 2224 0695 (13th floor)

1st Floor, Prestige Emerald  
No.4, Madras Bank Road  
Lavelle Road Junction  
Bengaluru-560 001  
Tel: +91 80 6727 5000  
Fax: +91 80 2222 4112

## Chandigarh

1st Floor, SCO: 166-167  
Sector 9-C, Madhya Marg  
Chandigarh-160 009  
Tel: +91 172 671 7800  
Fax: +91 172 671 7888

## Chennai

Tidel Park  
6th & 7th Floor  
A Block, No.4, Rajiv Gandhi Salai  
Taramani, Chennai-600113  
Tel: +91 44 6654 8100  
Fax: +91 44 2254 0120

## Hyderabad

Oval Office, 18, iLabs Centre  
Hitech City, Madhapur  
Hyderabad - 500081  
Tel: +91 40 6736 2000  
Fax: +91 40 6736 2200

## Kochi

9th Floor "ABAD Nucleus"  
NH-49, Maradu PO  
Kochi - 682 304  
Tel: +91 484 304 4000  
Fax: +91 484 270 5393

## Kolkata

22, Camac Street  
3rd Floor, Block C"  
Kolkata-700 016  
Tel: +91 33 6615 3400  
Fax: +91 33 2281 7750

## Mumbai

14th Floor, The Ruby  
29 Senapati Bapat Marg  
Dadar (west)  
Mumbai-400 028, India  
Tel: +91 22 6192 0000  
Fax: +91 22 6192 1000

5th Floor Block B-2  
Nirlon Knowledge Park  
Off. Western Express Highway  
Goregaon (E)  
Mumbai-400 063, India  
Tel: +91 22 6192 0000  
Fax: +91 22 6192 3000

## NCR

Golf View Corporate  
Tower - B, Near DLF Golf Course  
Sector 42  
Gurgaon-122 002  
Tel: +91 124 464 4000  
Fax: +91 124 464 4050

6th floor, HT House  
18-20 Kasturba Gandhi Marg  
New Delhi-110 001  
Tel: +91 11 4363 3000  
Fax: +91 11 4363 3200

4th & 5th Floor, Plot No 2B  
Tower 2, Sector 126  
NOIDA-201 304  
Gautam Budh Nagar, U.P. India  
Tel: +91 120 671 7000  
Fax: +91 120 671 7171

## Pune

C-401, 4th floor  
Panchshil Tech Park  
Yerwada (Near Don Bosco School)  
Pune-411 006  
Tel: +91 20 6603 6000  
Fax: +91 20 6601 5900



Ernst & Young LLP

EY | Assurance | Tax | Transactions | Advisory

**About EY**

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit [ey.com](http://ey.com).

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit [www.ey.com/in](http://www.ey.com/in).

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

© 2015 Ernst & Young LLP. Published in India.  
All Rights Reserved.

EYIN1507-075  
ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute

for detailed research or the exercise of professional judgment. Neither Ernst & Young LLP nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

DK



EY refers to the global organization, and/or one or more of the independent member firms of Ernst & Young Global Limited

---

If you have feedback or ideas for future topics, please write to [farokh.balsara@in.ey.com](mailto:farokh.balsara@in.ey.com) and / or [anil.nim@in.ey.com](mailto:anil.nim@in.ey.com)

---