Information Technology and Corporate Governance

By Sunil R Chandiramani

Corporate governance has taken centre-stage across boardrooms around the world. The term applies to all aspects of a business. Given the fact that technology is expected to play a key role in helping organisations achieve their business objectives, it is imperative to discuss the role of corporate governance over technology.

Risk management is a critical component of corporate governance. Risk management helps organisations recognise the wide spectrum of risks that they are exposed to. It aims to help them prioritise risks based on their potential impact, put mitigation plans in place, and monitor them so that they don’t become hurdles in achieving corporate objectives. Information technology is a key support function in any business, and regulation requires the board and the management to report key risks, and their assessment of how these risks are being managed. The Chief Information Officer (CIO) needs to play a significant role in supporting boards, audit committees and the management, in first understanding, and then implementing, good governance over IT.

Security and disaster recovery used to be major risk factors, but today, IT risk management covers a range of factors such as runaway projects, global sourcing, regulatory compliance, privacy, trans-border data flow, export control, financial disclosure, certifications, business continuity, fraud detection, protection of intellectual property and shortage of skilled resources. The list is endless, and promises to keep growing.

The sources proliferating risk are increasing manifold as well. Natural disasters such as fires, floods, earthquakes and cyclones have always been a risk for IT. To that list of natural calamities can be added an ever-expanding range of man-made risks—viruses, worms, Trojan horses, phishing, spyware and identity theft—making the IT risk management job more difficult every passing day. In addition, globalisation, new technology and attrition rates complicate the task of managing IT risks.

What is IT risk management? Simply put, it is the identification, assessment and mitigation of risks related to information technology. The growing importance of IT for successful execution of business goals calls for an effective risk management programme. Corporate reliance on IT raises the stakes in terms of the importance of maintaining 24x7 business continuity.

Technology not only creates new risks, but also plays an important role in mitigating risk. As such, IT executives must now work closely with business unit leaders and executive managers to adopt a formalised set of reproducible and scalable risk and compliance management technologies and techniques.

The seven key areas of risk that CIOs need to discuss, strategise and budget for include the
Business Continuity Planning/Disaster Recovery Planning (BCP/DRP)

Every organisation faces the risk of having to deal with known and unknown disasters. Organisations that use IT strategically and need to recover from significant business interruptions deploy Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) systems. BCP should not only be documented but also tested, updated and validated regularly to mitigate the threat of the non-availability of IT services disrupting automated operations and key business operations. BCP/DRP are not only about infrastructure and planning, they are also about people. People play a key role in ensuring that the organisation continues to function securely at pre-determined acceptable levels. DRP/BCP are like insurance and need to be renewed as insurance is done with premium payments.

Information security and data integrity

Security-related incidents have been on the front-burner of organisations for several years. Security breaches may occur due to the negligence of staffers, third-party access to key applications, or lack of appropriate security of information systems. It is essential that all organisations have information security policies and procedures in place as well as a formal incident response management team that can detect and escalate security breaches. Key risk areas that need to be focussed in logical access management include lack of procedures on user access rights and inadequate review of access rights on a periodic basis. Segregation of duties amongst users should be addressed to promote tighter control. Physical access risks exist on account of poor awareness levels and training. Investments made by organisations are for physical goods and not on IT assets, especially data. Physical security functions are typically not integrated with information systems security.

Data integrity risk encompasses all of the risks associated with the authorisation, completeness and accuracy of transactions as they are entered into, processed by, summarised and reported on by various application systems deployed by an organisation. These risks pervasively apply to each and every aspect of an application system used in supporting a business process. Integrity can be lost due to programming and processing errors, and poor management. Adequate preventive controls and detection need to be put in place to ensure that only valid and complete data are entered into all systems and applications.

Sourcing and outsourcing

Another complexity relates to global sourcing trends for IT services, and, more broadly, business process outsourcing. Organisations may embark on a relationship with a vendor which leads to a marked drop in service standards, and the cost savings are not as expected. Disputes between partners are common where commercial contracts have not been properly constructed according to established IT governance principles or are not applied from the start. There should be no room for ambiguity on standards, objectives and responsibilities. Today, all risk mitigation strategies must be extended to service providers.
There is a need to ensure that adequate IT risk mitigation measures and controls are adopted by all third parties and the controls need to be tested from time to time.

**Performance measurement**

With IT there’s a choice: you can drive it or be driven. In a business context, risk is not just about disasters and security attacks, but also about the business risks of costly project failures. Given the significant costs and strategic value of IT, measuring its performance is as important as any other key business function. Yet many organisations find IT performance measurement challenging, so they settle for measuring what they can rather than what they want or need to. Most organisations run several IT projects rather than an IT programme. Several of them are in fact ‘Project Failures,’ and this happens due to a number of reasons from poor planning to a weak business case, a lack of involvement from the top management, poor budgeting and inadequate quality control. With a significant amount of investment going into IT projects, failures can have adverse effects which can take months and years to recover from.

**Regulatory non-compliance**

Many regulations and laws apply to information systems—privacy, data integrity, systems availability, and delivery of accurate financial reporting. Sarbanes-Oxley and the future EU’s 8th Directive specifically demand that boards and senior executives understand IT risks. Ignorance is no defence. Violation of licence terms and conditions is common. It may happen unknowingly, but exposes the organisation to legal and reputation-related risks. Organisations can face legal implications if software licences are not upgraded and regular reviews not conducted for validity of licences.

**IT strategy and spends**

Sub-optimal spending on IT can worsen the overall risk posture of an organisation. Good IT governance includes the understanding of cost drivers and issues in IT, the nature of budgets and spending, and how spending is monitored. With IT costs increasing as a proportion of corporate expenditure, shareholders and other stakeholders expect organisations to be diligent in ensuring that these costs are justified and controlled.

IT strategy also includes planning for technology obsolescence. Technology that is inadequate for the enterprise or becomes obsolete too soon is a growing concern. This has an adverse effect on productivity, cost efficiency as well as on security. Technology is changing at a rapid pace, and unless organisations constantly upgrade their IT infrastructure, their business will suffer.

**IT management infrastructure**

IT management infrastructure plays a key role in IT governance. Often, organisations do not have an infrastructure to support the requirements of the business in an efficient, cost-effective and well-controlled manner. Infrastructure risks are associated with a series
of information technology processes used in defining, developing, maintaining and operating an information processing environment and the associated application systems. This normally stems from a lack of or weak organisational planning. The use of wireless networks, IT outsourcing, storage of customer data on electronic payment systems, online sales and service channels, remote networking and increase in automation of manual processes continue to affect a company’s IT risk exposure and can only be lessened by effective IT management infrastructure.

Given the reality of risk and its management in IT, the key question is: who is responsible for the identification, management and monitoring of IT risks?

Who should own IT risks?

Owning IT risks and giving direction for managing key risks are fundamental aspects of IT governance. An absence of top management responsibility and accountability for risk management can result in serious risks being ignored, potentially misguided actions, and wastage of capital.

The board has a responsibility for determining the strategic direction of the organisation and for creating the environment and structures for risk management to operate effectively. As IT has become more important to the operations and success of every business, some boards have recognised its role in business growth and incorporated it in the board’s agenda. In many organisations, the board has taken a hands-off approach to IT, allowing the IT department or even third parties to whom IT is outsourced to take decisions and suggest projects or programmes that might benefit the business. The impact of such misalignment can have financial consequences and lead to events which are damaging to the reputation of an organisation.

Some companies choose to delegate board-level oversight to IT steering committees in much the same way as they do with audit and compensation. But boards remain challenged by such issues as who should sit on these committees, what level of technology expertise is required, and how best to use the skills of other business leaders such as non-executive directors.

The board has a fiduciary responsibility to shareholders and the organisation, while executive management has an operational responsibility to ensure the continuation of business in the face of systems failure, threats or attacks—all of which fall within the realm of proper IT governance.

The responsibility of the CEO involves adopting a risk control and governance framework, embedding responsibilities for risk management in the organisation, and monitoring IT risks and accepting residual IT risks.

The responsibility of assessing risks and mitigating them to ensure that they are transparent to the stakeholders, implementing an IT control framework, and ensuring that roles critical for managing IT risks are appropriately defined and staffed lies with the CIO.
Since the user of IT services is the enterprise, it should set the mandate for risk management and provide the resources to support and monitor the plan designed to protect specific business interests. In today’s complex business environment, the IT service provider also needs to advise its clients to ensure that proper safeguards are in place. Internal and external auditors need to throw light on inadequate processes or risks that are not being appropriately addressed. They must assure the management that adequate measures have been adopted and implemented, or even make recommendations for improvement.

Ultimately, individuals across the organisational hierarchy need to be aware of their responsibilities towards an effective IT risk management programme. Building a fence around IT risk to separate it from the rest of your organisational activity will not work because the alignment of your IT strategy to your business strategy will underline the success and even the survival of your organisation.

*(The author is Partner-National Director Risk & Business Solutions Ernst & Young India. He may be contacted at sunil.r.chandiramani@in.ey.com)*