Information technology (IT) is integral to the operation of any organisation. As the mechanism supporting payment systems, accounting, business processes, information storage, communication and more, it presents significant opportunities for, and risks to, the achievement of goals and strategies. Advances in IT have driven business efficiencies, better communication, innovation and other technologies, and spawned new industries and large corporations. But IT has also been blamed for high-profile problems, from disrupted industries and compromised privacy to bungled pay packets, airline delays and undelivered efficiency promises. The alluring benefits and high risks of IT have led to significant research into its management and the development of standards for its governance.

Not surprisingly, IT is increasing in importance on board and audit committee agendas, and the governance of information technology (also referred to as IT governance) is now an integral part of an organisation’s overall governance requirements and director responsibilities.

The following questions have been designed as a guide to assist directors to understand this important strategic issue and discharge their responsibilities in relation to their company’s information assets and technology.

**What is IT governance?**

The Australian Standard for Corporate Governance of Information and Communication Technology, AS8015, defines Information and Communication Technology (ICT) governance as:

“The system by which the current and future use of ICT is directed and controlled. It involves evaluating and directing the plans for the use of ICT to support the organisation and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organisation.”

There are many definitions but they all have two key components

**Information** – some emphasise the importance of the ‘information assets’, some the communication of information and others the technology depending on their perspective. For boards, information technology, should be considered in the broadest terms, including the integrity, accessibility, currency, security and reliability of the information generated and communicated, and the technology which supports it.

**Governance** – processes, systems or frameworks for the evaluation, direction or monitoring of the function (or organisation) to achieve objectives and/or strategic alignment.
Good IT governance, like good financial governance, involves implementing the processes, procedures and standards necessary to provide the board and other stakeholders with confidence in the information it provides. Good IT governance, like the governance of other plant and equipment assets, also includes assessing the effectiveness, integrity and robustness of the technology used.

At board level, IT governance is concerned with the framework of systems and processes that support informed decision-making in the usage, investment and security of IT assets.

Despite the increasing importance of IT to all aspects of business, and the expectations on directors to be diligent in all areas of governance, research by Deakin University indicates that even Australian corporations with good governance of IT at management level, fail to implement it well at board level.

Most organisations appear to adopt IT governance policies but these are not well understood by their executives. Effective IT governance requires communication between governance policy decision-makers and those who execute it through the frequent use of mechanisms known to be effective within an organisation.

Examples can include senior management announcements, committees, or intranets with documented policies and procedures that communicate the respective roles and responsibilities of various business and IT functions.

Consulting firm, PwC, attributes a poor understanding of IT governance among boards globally to an IT confidence gap – a combination of a lack of knowledge about IT and a lack of processes to assist them.

Why is IT governance important to directors and boards?

The collection, processing, accessing, communication, reporting and security of information is essential to every organisation; information technology is essential in performing these functions in any business. Therefore, the oversight of information technology is essential to good corporate governance.

How does a board fulfil its role in IT governance?

The time and focus a board devotes to IT governance will depend on many things including organisation size, maturity, industry and strategic direction. The basic steps, however, are the same

1. **Understand the role of IT in your business** – how does IT currently support and enhance your business? How is IT managed and who are the stakeholders (and who manages them)? Is it integrated and efficient? Is it secure?

2. **Understand the opportunities and risks** – How is IT used by others in the industry? How would users like it improved? What opportunities does IT present? Does IT promote or stifle innovation or communication? What are the risks and how can they be mitigated?

3. **Fit IT to strategy and strategy to IT** – Does IT, including technology and human resources, have the capability required for your objectives and strategy? Do strategy execution plans and budgets include appropriate time frames and costs for IT?

4. **Governance and monitoring** – How does the board perform its oversight of IT? What are the controls and reporting? What are the performance indicators?
How can a director assess the effectiveness of IT governance?

A good starting point is for directors and boards to self-assess their IT governance practices by asking questions such as:

- Is the board regularly briefed on the IT risks to which their organisation is exposed?
- Is IT a regular item on the agenda of the board and is it addressed in a structured manner?
- Does the board articulate and communicate the business objectives for IT alignment?
- Does the board have a clear view on the major IT investments from a risk and return perspective?
- Does the board obtain regular progress reports on major IT projects?
- Is the board getting independent assurance on the achievement of IT objectives and the containment of IT risks?
- How does the board perform its oversight of IT? What are the controls and reporting?
- What are the performance indicators?

Are our IT investments cost effective and reducing risk?

No matter the size of the organisation, or the complexity of its information systems requirements, investment in IT systems is likely to be significant enough to require board approval. Investment in IT systems is not cost effective, and presents significant risks, unless it meets the four criteria below.

Consider the following aspects in evaluating cost effectiveness and risk mitigation:

1. **Are investments aligned with and supporting the board’s strategy?** Operations, marketing, accounting, in fact, almost every function of an organisation, can be enhanced or constrained by IT. Consequently, a board’s strategy can be enhanced or constrained by IT. IT can also be integral to strategy, for example by providing competitive advantage, monitoring trends or supporting innovation. IT is also the means by which a company’s competitors may disrupt established markets; a threat which boards need to be ever vigilant of, and guarding against, through encouraging their own ongoing innovation. Importantly, IT provides much of the information from which boards develop and monitor strategy, it underlies the integrity of that information and therefore the strategy overall.

2. **Do investments in IT enable risk management and compliance requirements to be met?** Collecting, collating and reporting of information is required for compliance with numerous regulatory requirements, and for management and oversight. This information must be accurate and timely, therefore IT systems must not only produce the required output but also provide the assurance as to its accuracy and completeness. IT systems can be used to manage risk in many areas of business.

3. **Do investments in IT support business continuity?** Loss of information or failure of information technology, can be damaging to profits and/or the long term viability of an organisation. IT governance processes should enable the organisation to protect itself not only from accidental loss but also the accidental or improper dissemination of information.

4. **Will investments provide or enable appropriate security and management of information?** Hackers and viruses are also significant and real risks for many organisations, IT systems should provide sufficient protection for information assets. Equally IT must provide efficient storage and dissemination of information to those that need to use it.

Do boards and directors need to be IT literate to fulfil their duties? Boards use various resources to fulfil all their corporate governance duties including advisors, committees, auditors and the skills of the directors. However, in the Centro case, Middleton J found that “Directors cannot substitute reliance upon the advice of management for their own attention and examination of an important matter that falls specifically within the Board’s responsibilities as with the reporting obligations”.

As such, if IT has the potential to have a significant impact on an organisation, it is wise for boards and directors to have sufficient IT literacy to critically examine information about IT and, if needed, know what further information should be requested. The level of knowledge required is dependent on the level of strategic importance to the organisation and other IT governance measures in place.

Some questions that may uncover IT issues are:

- How often do projects fail to deliver what they promised?
- Are end users satisfied with the quality of IT-related services?
- Are sufficient resources, infrastructure and competencies available to meet strategic objectives?
- What has been the average overrun of operational budgets? How often and how much do projects go over budget?
- How much of the IT effort goes to ‘fire-fighting’, rather than enabling business improvements?

Like all the other specialist areas of an organisation that a board has oversight for, a detailed knowledge is not required to exercise good corporate governance, and the basics can be explained in plain English, when directors have a broad understanding of the key concepts to further question and probe as required. In most organisations, good IT governance does not require high levels of IT literacy. Instead, it requires sufficient understanding to ask the right questions of management and advisors, although the expectations of IT literacy may increase in the future as technology continues to evolve at a rapid rate.

As part of their strategy formulation, boards may seek briefings, either from internal staff or external advisors on:

- Existing and emerging technologies relevant to the organisation
- IT capabilities (technology and human resources) of the organisation
- Industry and competitor use of IT
- Emerging IT trends and capabilities
- Risks related to the organisation’s information assets
- Risks related to the organisation’s information technology.

How can directors improve their IT governance?

The first step to improving IT governance is a review of existing competencies and capabilities within the organisation and at board level. Steps that can be taken to improve IT governance include:

- Improving director competency through appointment of new directors or education of the existing ones with the appropriate IT skills and expertise
- Extending or making more explicit the responsibilities of existing board committees (eg. audit and risk)
- Establishing an additional committee or advisory group with particular focus in this area (a strategy adopted by boards with high reliance on IT capabilities)
- Reviewing audit arrangements, including the role and scope of internal/external audit arrangements
- Reviewing the range of delegations established by the board and formalising responsibility and accountability for IT management.