

Managing Technology in Organizations

Chartered Accountancy Business Level 2 Digital Business Strategy (DBS)

Susantha Weerakoon
B.Sc. (MIS), MBA (ISM), PHD (Business Psychology)



JMC Jayasekera Management Centre (Pvt) Ltd
Pioneers in Professional Education

65/2A, Sir Chittampalam A Gardiner Mawatha, Colombo 02 | T: +94 112 430451 | E: info@jmc.lk | F: +94 115 377917

BL -8 Digital Business Strategy

CA Business Level 2

Managing Technology in Organizations



Dr. Susantha Bandara Weerakoon
(BSc (MIS), MBA (ISM), PhD (Business Psychology))

Significance of managing technology

Like most other business functions, the finance function and the role of those who work in it have been transformed in recent years by technology and other changes in the business environment. This has led to the development of new models for organising the finance function, as well other functions within the business.

Types of Technology Infrastructures

As the environments in which organizations operate become more competitive the ability to create a sustainable competitive advantage becomes considerably more difficult. As a result, strategic managers are increasingly embracing emerging technologies as a way to innovate, improve performance and ultimately get ahead of the competition. Technologies with such potential include cloud and mobile computing, big data and data analytics.

There are a number of reasons why organizations may choose to embrace new technologies. Reasons for adopting this approach may include the following, as shown below:

- Early adopters to get ahead of competitors
- Improve performance
- Quantity of data available
- Good for stakeholders

Impact of technology on finance functions and professionals

Big data – modern technology gives the ability to analyze large amounts of data very quickly and deliver results in real time. This may include financial and non-financial data. Organizations are increasingly requiring this from their finance functions.

Big data 'Is a popular term used to describe the exponential growth and availability of data, both structured and unstructured.' (SAS, 2016)

Big Data 5 Vs

SAS (2016) cite the work of Laney (2000), who suggested that big data can be defined by considering the three Vs: volume, velocity and variety. The three Vs have now been extended to include veracity. It is important to note that other authors may refer to other terms when discussing big data;

Volume – The vast volume of data generated is a key feature of big data

Variety – Variety is defined as the different types of data we can now use. Data today looks very different than data from the past.

Veracity – This concerns the quality or truthfulness of captured data

Velocity – This refers to the speed at which 'real time' data is being streamed into the organization and with which it is processed within the organization

(Adapted from: SAS, 2016)

V – value – Value refers to the worth of the data being extracted.

New developments and Innovations

Innovation: Involves the conversion of new knowledge into a new product, process or service and the putting of this new product, process or service into actual use (Johnson et al, 2017).

Innovation and competitive advantage

Johnson et al (2017) highlight that for many organizations, product innovation and being the first mover may be a major source of competitive advantage.

- (a) First movers can establish scale ahead of competitors, and thereby gain economies of scale.
- (b) Customers may find they are locked into innovative suppliers by unacceptable costs of switching to competitors, particularly if the first mover can establish technological standards.
- (c) The learning (or experience) curve effect may bring cost advantages.
- (d) A first mover may gain easier access to scarce resources than followers, such as raw materials or skilled labor.
- (e) It can lead to an enhanced reputation, particularly if a dominant brand can be established.

Disruptive innovation

Describes a process by which a product or service takes root initially in simple applications at the bottom of a market and then relentlessly moves up market, eventually displacing established competitors. The term disruptive innovation was coined by Christensen (1997).

Based on a detailed study of the computer disk drive industry, he argued that most innovation was sustaining innovation, improvements to existing products or services which companies could sell to their existing customers. Well-run companies are good at exploiting these innovations, and the established industry leaders tend to be the first to exploit them.

Disruptive innovation

Blockchain is a type of incorruptible distributed ledger that allows information to be recorded and shared with a network of individuals. It is a public form of bookkeeping which makes use of internet technologies to instantly verify and record the transactions that take place between individuals.

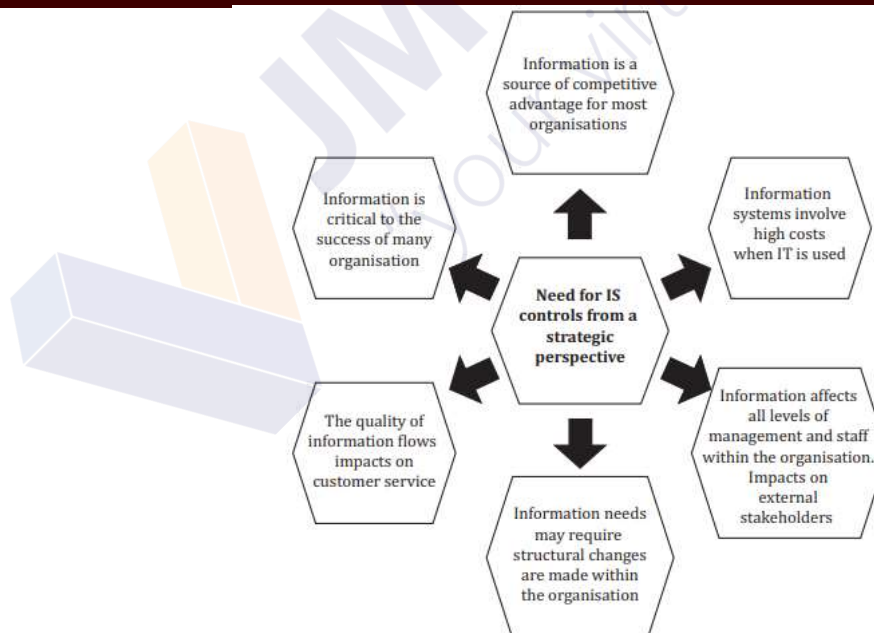
Cryptocurrencies are forms of digital currency that do not exist in physical form. **Bitcoin and Ethereum** are two of the best known cryptocurrencies. There are more than 1600 different cryptocurrencies that exist (as at June 2018) and new types of cryptocurrencies are currently evolving.

Process of managing technology

Information system controls from Strategic perspective

An information system: Consists of the systems, processes and procedures involved in collecting, storing, processing and distributing information. The information systems (IS) strategy: Is the long-term plan for systems to exploit information in order to support organizational strategies or create new strategic options.

Need for Information Systems controls



Process of managing technology

When assessing the adequacy of existing IT/IS controls, an organization should compare them against four types of control. The four types of control can be classified as being either **general** or **application** controls.

General controls are those that control the design, security, and use of computer programs and the security of data files in general throughout the organization.

Application controls are specific controls unique to each computerized application, such as payroll, accounts receivable, and order processing.

Process of managing technology

Controls over physical access are predominantly directed towards preventing unauthorized individuals gaining access to an organization's IT and IS assets. Controls are also aimed at stopping damage to the IT infrastructure that may occur as a result of natural hazards, eg a fire. Controls can be simple or advanced. Simple controls might include ensuring that doors leading to an organization's IT systems remain locked when not in use. Locks can be combined with keypad systems or card entry systems. Other controls may focus on the use of personnel. Ensuring that receptionists and security guards are on duty outside of working hours may help to control human access. This can be supplemented by the use of intruder alarms. Advanced controls are those that recognize individuals immediately, without the need for personnel or cards. However, biometric machines that can identify a person's fingerprints or scan the pattern of a retina and facial recognition are expensive, so are used only in highly sensitive industries, like defense.

Process of managing technology

Operational controls are aimed at ensuring that an organization's day-to-day activities run effectively. Most organizations establish operational controls aimed at influencing an individual's behavior. Segregation of duties Strong internal company policies often stop situations arising which lead to one individual having too much power over a particular function. This is often achieved through ensuring a **segregation of duties**. For example, the person dealing with processing the monthly payroll should not have responsibility for adding new employees to the payroll or authorizing the monthly payment of salaries from the organization's bank. **Audit trail** In the context of IT systems and controls, an audit trail is a record showing who has accessed a computer system and what operations that individual has performed.

Process of managing technology

Logical access controls are aimed at ensuring that only authorized users of IT systems are provided with access to those systems. Such measures are directed towards identifying and confirming the authenticity of the user. A common mechanism in protecting computerized data is through the use of **passwords**. Keeping track of failed attempts can alert managers to repeated efforts to break into the system. In these cases, the culprits might be caught, particularly if there is an apparent pattern to their efforts. This is called **Auditing**, and is a system feature, as opposed to business auditing, as specified under Operational controls.

Process of managing technology

Input controls

Data verification: This involves ensuring data entered matches source documents.

Data validation: This involves ensuring that data entered is not incomplete, unreasonable or duplicated.

Check digits: A digit calculated by the program and added to the code being checked to validate it.

Control totals: For example, a batch total totaling the entries in the batch.

Range checks: Used to check the value entered against a sensible range

Limit checks: Similar to a range check, but usually based on an upper limit.

Compatibility checks: Ensure that two entries to the system are compatible. The value of a sales invoice posting should be compatible with the sales tax posting.

Format check: Only accepts postings to the system which are in the correct format; otherwise they will be rejected. For example, dates must be posted in a particular format, dd/mm/yy.

Promoting Cyber security

Cybersecurity: Is concerned with the protection of systems, networks and data in cyberspace.

Cyberspace: Is the term used to describe the environment in which communication over IT networks takes place.

cybersecurity measures increasingly need to take account of the external threats:

- Threats now emerge from different parts of the world, and often involve criminal groups, corporate espionage and hackers.
- The heavy dependence on IT systems in modern business has proliferated the need for organizations to link their IT systems together throughout their supply chains and hackers can gain access to data.
- Security failures can have far wider implications than only affecting the organization's IT systems, and may include reputation damage, loss of intellectual property and disruption to operations.

Promoting Cyber security

- Making cybersecurity issues easier to understand for those not working in the organization's IT department.
- Employing a Chief Information Security Officer (CISO) to help communicate the threats posed by cyber risks
- Reorganizing roles and responsibilities to ensure that there is accountability for cybersecurity matters within the organization.
- Determining accountability for cyber risks at the strategic apex. A member of the board should be assigned responsibility for heading up cybersecurity matters.
- Learning from past security breaches.
- Determining the organization's tolerance to the cyber risks is an important step in designing management strategies.
- Ensuring that non-executive board members play an active role in promoting cybersecurity during their interactions with the board.

Improving IT / IS Controls

Practical measures might include:

Continuity planning. Organizations should have in place measures to address failures of IT/IS infrastructures to ensure the organization can continue to function. This may consist of a plan which details the contact details for crisis management staff, customers, suppliers and the location of offsite data back-up storage media.

Systems development and maintenance. Organizations need security controls to protect the data held in IT/IS infrastructures. This requires regular updating of software and hardware to ensure that the controls remain fit for purpose.

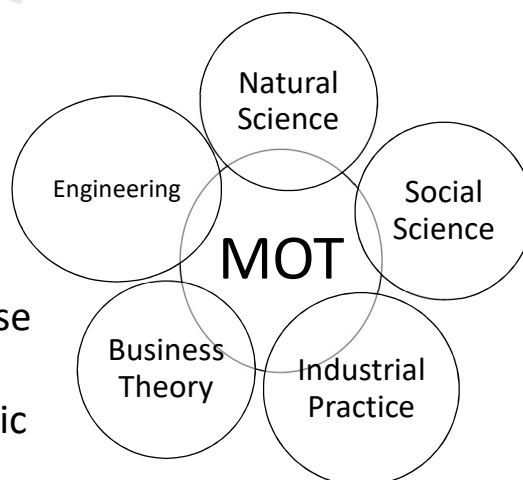
Personnel security measures. Organizations need suitable processes for ensuring that only trustworthy employees are recruited to use IT/IS infrastructures. All employees should receive adequate training on using the organization's IT/IS infrastructures. Training should be undertaken as regularly as needed to keep skills up to date.

Role of MOT in a Business

Improving IT / IS Controls

MOT is an interdisciplinary field that integrates science, engineering and management knowledge and practice. [MOT, Tarek M. Khalil p.7]

Management of Technology (MOT) refers to the design and use of the means needed within organizations to achieve economic and social objectives through technological innovation.

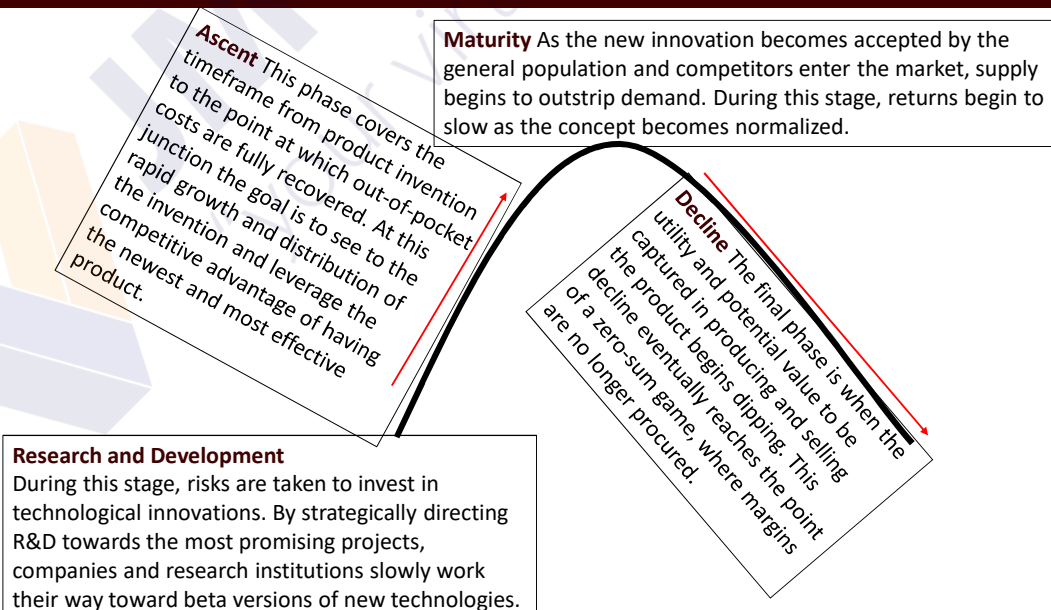


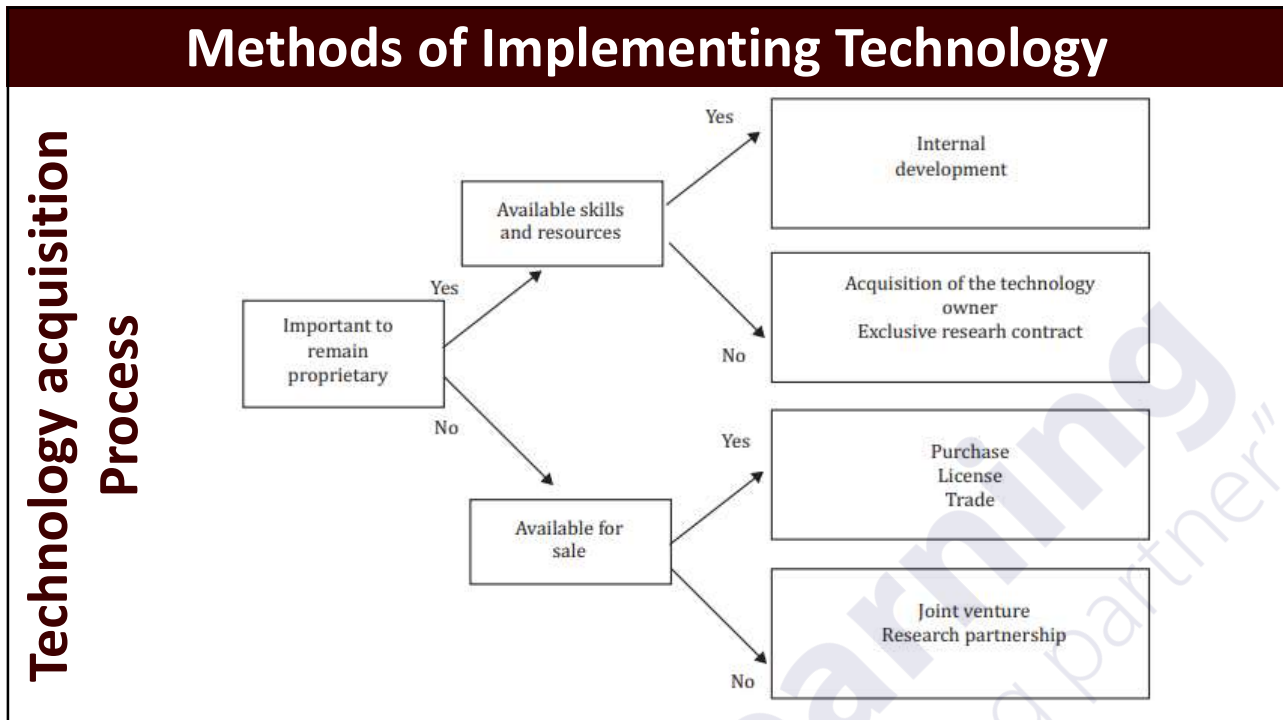
Integrating Technology to create Business Strategy

Technology cannot be isolated within the organization. For this reason, a cross functional approach is taken by organizations to ensure technology is integrated across the business. This concept is now known as a MOT, which can be considered an independent area, responsible for managing the strategy required to create the cross functional approach. This can be seen clearly when organizations implement new technology such as an ERP (Enterprise Resource Planning) system, which crosses all areas of the organization.

Methods of Implementing Technology

Technology Life Cycle





Why organization require New technology

- An old system – Legacy or management information system that lacks functionality
- Slow or out of memory on premise systems with no method for increased disk space
- Difficulties in Up scaling, again to due to old or out of date hardware
- Poor data management, in particular non-compliance with relevant laws. i.e.: General Data Protection Regulation (GDPR) in Europe
- Poor security management, with a lack of controls, including internal user controls and business partner controls, ie authentication methods
- No integration or availability to link to external cloud-based systems
- A lack of analytical and reporting capability
- New products or services requiring new technology,

Digitization and Business value

When considering the potential impact of digitization on business, it is also important to acknowledge the point highlighted in McKinsey's report: Finding your digital sweet spot (2014). The report argues that 'while online sales, social networking and mobile applications have received most of the buzz when it comes to digital', the greatest bottom-line impact may come from cost savings and changes beyond the interface between company and customer. As such, McKinsey's report suggests that technology (and digital transformation) can drive business value in four different ways:

1. Enhanced connectivity
2. Automation of manual tasks
3. Improved decision making
4. Product or service innovation

Different types of acquisition methods

Partnering: Is the term used to describe the types of arrangements which fall short of formal business combinations.

External partnering: Joint ventures, franchising and strategic alliances are all forms of partnering in which arrangements are established with external third parties with a view to achieving a common purpose. External partnering usually restricts formal legal arrangements between entities to specific operations.

Joint venture: Is an arrangement when two (or more) entities join forces to create a separate entity which has a purpose that is distinct from the business operations of the two entities that established it.

A strategic alliance: Is a type of external partnering that involves some form of co-operation between two or more organisations. Strategic alliances often involve the sharing of resources and activities to pursue a given strategy.

Different types of acquisition methods

Partnering: Is the term used to describe the types of arrangements which fall short of formal business combinations.

External partnering: Joint ventures, franchising and strategic alliances are all forms of partnering in which arrangements are established with external third parties with a view to achieving a common purpose. External partnering usually restricts formal legal arrangements between entities to specific operations.

Joint venture: Is an arrangement when two (or more) entities join forces to create a separate entity which has a purpose that is distinct from the business operations of the two entities that established it.

A strategic alliance: Is a type of external partnering that involves some form of co-operation between two or more organisations. Strategic alliances often involve the sharing of resources and activities to pursue a given strategy.



JMC vLearning
"your virtual learning partner"