UNIT-9 Technological Risk Management

Learning Outcomes

By the end of this unit the learner will be able to:

- ✓ Understand what is technology risk management
- ✓ Outline the benefits of technology risk management
- ✓ Prepare a technology risk management plan for a business.

Unit 9

Technological Risk Management

The pervasive technologies in today's world are information, communication, and controls. These technologies can reduce costs, boost growth, and increase productivity. Airlines, banks, insurers, and hotels rely heavily on internet technology. Initially, the purpose of IT was to reduce administrative and bureaucratic work load, so that the staff would have more time to do their *proper jobs*. Now, IT is an enabler of the business plan and growth targets. The efficient use of technology can transform companies and contribute towards improved and sustainable stakeholder value. This increase in value is generally driven by investment in technology, resource optimisation and diligent maintenance to sustain reliability. Rapid changes in technology and the merging of technologies, like computers and telecommunications, are continually recreating *industrial boundaries* so that *old* industrial sectors are almost non-existent.

Even Microsoft is often placed under pressure, illustrated by Bill Gates' statement *'in three years, every product we make will be obsolete. The only question is whether we'll make them obsolete or somebody else will'* (Gates 1999).

Technological development is thus both an opportunity and a threat, in terms of market growth and market share. Furthermore, the introduction of technology within a company can also expose it to a series of debilitating risks that may severely affect profitability and competitive advantage or even lead to business failure. Therefore, direction and supervision by the CEO and board are very important. This requires technology governance systems with the correct level of executive commitment and participation, clear understanding of the company's risk appetite and clearly-defined levels of responsibility for risk management including, at least, identification, monitoring, and control measurements.

Technology is a comprehensive term. Out of the various kinds of technology available, the ones considered necessary for businesses and discussed here are information, communication and control. This unit endeavours to provide a definition of technology risk management and review the primary types of technology for businesses, sources of risk and possible responses.

What is Technology Risk?

Before technology risk can be defined, we need to understand what technology in a business context really is. Economists categorise technology as an element of capital goods, one of the factors of production used by companies to produce goods consumed by society. Technology is thus a subset of production being the process that changes inputs into outputs. Traditionally, this means taking raw materials and components and converting them into finished goods. Examples of this type of transformation processes are car assembly plants, electrical appliances and computer production lines. While technology is central to the production process, it has far greater applications.

The *Oxford Everyday Dictionary* offers the following definition, *'technology is the scientific study of mechanical arts and applied sciences'*. Mechanical arts and sciences are constantly used for product design. Commodities produced by the manufacturing process exhibit incremental advances in technology and their functionality, quality and reliability that influence market creation, market share and market growth.

Therefore, technology risk can be defined as those events that would lead to insufficient, inappropriate or mismanagement of investment in technology, in terms of the manufacturing processes, product design and/or information management. Mismanagement would include poor protection of intellectual property, business continuity planning or security. The most important consequence of this risk would be a decrease in market share.

Scope of Technology Risk

The list of possible sources of technology risk is considerable. Any study of the sources of risk must be geared towards the particular activities of a company.

A sample of the sources of risk within the term *technology risk* is recorded below:

- Reduced ability to compete due to a lack of investment in technology;
- Poor technology governance, specifically IT governance;
- Ineffective protection against hacking and viruses, and a resultant loss of information confidentiality;
- Inadequate control of outsourcing;
- Inflexibility of production to be able to produce small production runs economically; and
- IT is not being aligned to the business objectives.

Benefits of Technology Risk Management

Businesses benefit from technology risk management in the following ways:

- Identifies potential market share loss due to a competitor's improvement in product design;
- Provides a higher quality of information for decision making purposes. Enables a proactive approach towards managing technology projects and maps the risks to investment in technology. In order to succeed, business leaders will need to take advantage of the new way of conducting business, based on the ever growing speed of information and create processes and products faster than competitors;
- Identifies the threats to current business practices from emerging business-to-customer relationships. Gates claims that 'Today US businesses are ahead of businesses in other countries in the adoption of digital technologies. The many reasons include openness to risk taking, individual empowerment and labour mobility' (Gates 1999);

- Offers insights into the drawbacks of not aligning technology to strategy and business operations; and
- Establishes a system of on-going assessment of the latest technological developments in the manufacturing processes (advances in technology improve productivity).

Business leaders will have to modernise and streamline their company and its processes to be able to gain full advantage of technology. The goal is to make business reflexes almost instantaneous and to make strategic thought an on-going, iterative process, not something done every 12- to - 18 months, separate from the everyday tasks of the business (Gates 1999).

Implementation of Technology Risk Management

The following issues will need to be attended to in order to create an effective system of technology risk management:

- Implement information security;
- Manage technology investment to secure business objectives and optimise investment advantages;
- Embrace new e-commerce developments;
- Monitor rivals in order to avoid being out manoeuvred by new technologies being introduced that can shift industrial boundaries;
- Ensure that the correct information reaches the correct people at the correct time by means of e-mail, intranet and management information systems; and
- Understand the risks of outsourcing and how to control them.

Main Technology Types

Information Technology

Information technology is the collection, storage, processing, and communication of information by electronic means.

Some information technology *tools* are:

- Software applications including word processing, presentation packages, graphic/drawing packages, spreadsheet s, databases, desktop publishing, and other expert systems. Using spread sheets saves inordinate amounts of time, allows staff to set up mathematical models, simplifies repeated calculations, improves accuracy, and enables asking what-if questions to see the effects of different strategies and provide several analysis tools. For example, they offer graph and chart facilities and calculate compound interest and depreciation;
- Databases are a means for organising sets of files and allow convenient access to their content. Expert systems deal with specific areas of expertise, draw conclusions from knowledge obtained from specialists with domain knowledge, and computers stored information. Their objective is to

capture the expertise and knowledge of key people, and make this knowledge available to program users;

- Management Information Systems (MIS) are special systems designed to collect and report on organisational project information. They are also programs which help executives to plan, monitor, and evaluate their performance;
- Intranets are computer networks quite like the internet, but are designed for use within a single company. Intranets are less expensive and easier to install than networks. Organisations are using them more and more to circulate internal information, such as job openings, phone directories, marketing, publicity, and training materials;
- Information assets and increasingly becoming the lifeblood of any company, and include product design, IT development, customer contacts, and manufacturing process innovation; and
- Telematics is technology that provides remote access to vehicle data via a wireless network.

Software Applications

Software application risk deals with the failure of IT applications. Applications are generally proprietary off-the-shelf software packages, software developed in-house, customised proprietary software, and bespoke software commissioned from a vendor. Some software applications, specifically those that are *job specific* and used for accounting, marketing, project management, and human resources will be under the control of the departments of the same name.

Other packages, like word processing and spreadsheets will be used throughout the company. The failure of any of these applications to perform correctly can vary from a minor irritation to massive downtime, causing employees to be idle or unable to complete priority jobs. The seriousness of the effect will depend on whether the application is used throughout the business or is department specific, and whether the application is hosted on individual PCs or on a central server.

Customised bespoke software developed in-house can cause the most problems. For example, applications that are adapted over time to meet changing needs become difficult to maintain and could form a constraint, restricting further changes from being made. If applications are inadequately documented or badly structured, they may be difficult to fault-rectify and maintain. In addition, serious defects can be unwittingly introduced by software developers when only small updates are made, as they do not understand the application's structure since they were not the original developers.

Software engineers are required to maintain, enhance, integrate, test, and release applications. Additionally, they provide system administration, monitoring, problem management, and subsequent change management.

Management Information Systems

Management Information Systems (MIS) are valuable for handling projects including risk management, organisational breakdown structures, change control, scope definition, programming, work breakdown structures, budgeting, contingency planning, value management, and earned value analysis. The risk with

these systems arises from weak implementation or inadequate execution in terms of the lack of forming a baseline from which to measure progress, accuracy of the data they contain, the completeness, currency or extent of being up to date or revision control.

Intranets

The technology which is touching everyone's lives is intranets from school children in Reading (England), who remotely access the school intranet, to the US Marine Corps who use a situation awareness application, to doctors in southern Virginia and North Carolina who access patients' records remotely over the web. Intranets save adequate time for companies provided that the information they contain is easily accessed by the majority of the employees. However, there is a risk that if the intranet is down for long periods of time, the same employees will be unable to do their work, even their routine jobs.

Telematics

Telematics are used for convenience, safety, and monitoring. Operators of a telematics system will be notified when an airbag deploys or when the *check engine light* goes on. When a safety measure is sensed in the car, an operator can call the driver to ensure they are okay, and if they are not, the operator sends help. The operator knows where to send the police and ambulance service due to GPS (Global Positioning Satellite) units in vehicles.

Telematics is believed to be a huge business opportunity area, and rather than posing a risk, it has a considerable market potential. Similarly, a Department of Transport (DoT) initiative to place chips on car number plates to monitor movement of vehicles is considered to be another business opportunity. A government trial of the devices was planned. Special cameras and hand-held readers will be able to identify 200 vehicles per second in all weathers. The DoT has claimed that the chips will record car thefts to reduce car crime because over 500,000 vehicles are stolen every year (Higginson 2005).

Information Assets

Information is the energy of companies, enabling innovative ways of working and generating the emergence new products and services. Business resources of the past were money, men, machines and materials (the four Ms). In today's world, a fifth resource has been added, which is information. As described by Earl (1997), businesses have to be able to manage information as an asset, both as a lever for business development and as a process for managing organisations.

Examples of information assets can be found in the airline and retail industries. Competition in commercial airlines is based substantially on commanding electronic channels of distribution by way of reservation systems and on aggressive sales and yield management by analysing customer databases. Within the retail sector, loyalty cards offered by organisations such as Tesco and Boots, not only provide frequent and volume purchasing discounts to customers, but also capture individual customer behaviour, allowing offerings to be customised and the development of newly targeted services.

Information strategies are no longer seen as just a means to support business strategy, they are interwoven. IT strategy and business strategy are one and it is now recognised that a business strategy is

incomplete if the information resource is not an integral part of it. Information and IT can make or break a company.

With information being a vital element of business strategy, its protection is imperative. Information risk involves damage, loss or exploitation of information assets within the IT systems. For many companies, this risk starts with not realising that the information they possess is an asset. Information asset risk can vary. For example, customer credit card details may be copied and used for fraudulent purposes and if the *theft* is made known publically, then the company suffers reputation damage as well. A competitor could get hold of important information, thus destroying competitor advantage. Core business processes which rely heavily on critical information could be seriously degraded if for example, an account enquiry function that contains out of date or inaccurate information, thus becoming ineffective.

Communications Technology Benefits

- The fastest data communication channel is available through broadband. Employees are able to work from home as efficiently as in the office, which reduces company costs;
- Video conferencing enables people to meet without leaving their offices and cuts down on travel costs and time;
- Conference calls allow a group of people to share a single telephone conversation;
- E-commerce is the fastest growing business sector. Through the internet, websites are used to advertise company products or services and offer the facility to make purchases directly over the net;
- E-mail allows prompt communication and the ability to exchange text, drawings, spread sheets, and diagrams in a format that is usable by the recipient through the use of attachments; and
- Sharing software or files is possible through network systems in which computers are linked to one another over a network.

Broadband

Broadband is a term used to describe any high-speed connection to the internet. There are actually many different types of broadband connections available through different ISPs (Internet Service Providers) in the UK.

However, companies need to reduce this risk exposure by taking some basic steps, such as installing anti-virus software to filter destructive data; activating firewall applications to prevent outsiders from getting into their systems; ensuring that operating systems, firewalls, virus protection and other software is up to date; evaluating the causes of system failures, turning off unnecessary permissions and applications such as FTP (File Transfer Protocol), mail servers, and file and print sharing; making sure technical support is available through in-house or specialist support contractors; and ensuring that the staff realise the importance of security by making IT security a part of employees' contracts, and creating and enforcing policies for the use of the internet and e-mail. In addition, information should not be kept on

individual computers as this creates a security risk. Set up regular partial and complete backup procedures. Backups should be kept away from heat, moisture and magnetism, and stored offsite.

Video Conferencing

Video Conferencing opens up a whole new series of risks which are related to technology rather than the human interactions themselves. Systems that need to communicate with each other must be compatible. For instance, without proper-planning systems used may not be compatible if they do not conform to the telecommunications standards set by the International Telecommunications Union (ITU), a United Nations agency, and the Internet Engineering Task Force (IETF). User expectations are not attuned to what is realistically possible from the available system. The company bandwidths may become out of date with current video conferencing technology.

E-Commerce

E-commerce (Electronic Commerce) is the ability to buy and sell merchandise on the internet and doing business electronically. Other applicable terms for e-commerce are B2B, business-to-business where companies do business with each other, and B2C, business-to-customer where companies do business with customers over the internet. These are the main types of e-commerce, with B2B making up the largest contingent of trade on the internet. Among the first technology organisations to move their sales and buying to the web were Cisco and Oracle.

E-mail

E-mail is now taken for granted, just as PCs are. It has become a central tool in our everyday lives, providing instantaneous communication. Coca Cola established worldwide communication with its own custom e-mail system in the 1980s and was one of the first organisations to do so.

E-mail is now ever-present and also flattens the hierarchical structure of an organisation, where everyone has access to everyone else, regardless of corporate rank, as senior managers have become more reachable. People are able to communicate and express their opinions conveniently. Telephonic communication and e-mail facilities are enabling telecommuting which means employees no longer have to live close to work. The advent of integrated phone and PC enable people to see who they were talking to and overcomes the solitary nature of working at home. E-mail makes remote interaction with colleagues and customers possible.

Attaching links to pages on the company intranet to e-mails sent to staff also makes internal communication easier. However, this total dependence on e-mails causes massive problems when it is not available temporarily. The same backup and support services that are used for the other major IT systems must be put in place for an e-mail server. The company e-mail system must be protected from unsolicited e-mails such as *spam* or *junk mail*, and virus as discussed under the heading *Broadband*.

Control Technology

Computer-based production control applications include:

- Computer Aided Design (CAD) is the means to produce designs, drawings, and data using computers. These systems increase flexibility and speed;
- Computer Aided Manufacture (CAM) is the use of computers to manage manufacturing processes and improves the quality and speed, while reducing costs;
- Computer Integrated Manufacture (CIM) uses IT to incorporate sections of the manufacturing process, e.g. design and production (CAD and CAM);
- Manufacturing Resource Planning (MRP) is an inventory management model and computerised planning system;
- Flexible Manufacturing Systems (FMS) are an important capability in a wide variety of strategic industries enabled by numerically controlled machines, affecting the integration of manufacturing, productivity, and quality;
- Mechatronics are the combination of computer technology with microelectronics and mechanical engineering; and
- Operations Research (OR), also known as Management Science (OR/MS), looks at a company's operations and through analytical approaches, such as mathematical or computer models, discovers better methods to run the operations. Analytical tools are used by operational research consultants to assist with decision making, like decision theory, theory of games, critical path analysis, replacement production, dynamic programming, scheduling, Marko chains, queuing theory, simulation, and stock control.

CAD

Computer Aided Design (CAD) has conventionally been a computer aided system for designing and communicating 2D designs or 3D models, for artefacts or components of artefacts. This system is used in the electronics, mechanical engineering and construction industries. CAD aids in visualising a design concept before manufacturing the products. The design can be tested and evaluated for aspects such as physical shape, material suitability, size, aesthetic attributes and volume, fluid dynamics, and conductivity before being manufactured.

The key concept of CAD is there presentation of an idea or concept using the most appropriate ICT tools for the product that is being designed. The risks associated with use of CAD software are caused by the way the software is used rather than by the software itself. The more well-known products can be considered reliable as they have been around for years and have been updated and improved.

However, the hardware used to run CAD applications must have sufficient processor speed and sufficient memory. The biggest risk faced with using CAD is that the benefits that should be delivered are not achieved. There are a number of reasons for this, from the way the users work together, poor user training, or using the wrong software product for the task at hand.

CAM

CAM or Computer Aided Manufacturing is the computerised management of manufacturing production machines and range from computer numerical control (CNC)11 machines to high- performance programmable industrial robots, which can perform diverse industrial tasks. CAM is generally linked with CAD systems. The integrated CAD/CAM system converts the computer-generated design drawings into guidelines for the production machines, thus optimising uniformity between the designs and the finished products. Initially, due to the difference between the capabilities and file formats used by drawing and machining programs, CAD only had a small effect on CNC. However, the creation of CAD applications like AutoCad and SoliWorks which incorporates CAM intelligence, and as CAM applications such as Master CAM started using sophisticated CAD tools, design, and manufacture became more unified.

Engineering processes like those used in car manufacturing are often the most frequently used example of CAM. The biggest advantage of CAM is its ability to enable mass customisation where small batches of products can be customised to customer specifications. Without CAM/CAD, customisation would be a very expensive time-consuming manual process. Thus, using CAD applications enables customisation and quick design changes. On the other hand, the automatic controls of the CAM system enable the machinery to be adjusted automatically for different orders.

The key risks associated with CAM and CAD/CAM are too little investment in research and development; the lack of full integration with CAD; not keeping up with CAD/CAM developments and how they could increase productivity and/or create competitive advantage; not benchmarking output against rivals and not meeting customer preferences in product lines. Overarching these risks are the usual operational risks of protecting intellectual property, business continuity, outsourcing, maintenance programmes, maintenance contracts, and security.

MRP

MRP is in actual fact a spreadsheet tool that converts sales forecasts into purchasing requirements for materials and components and also, plans the actual production. MRP methodologies are used in the manufacturing of goods which is based on several stages in the production process. The stock levels of raw materials, single components and sub-assemblies, and finished goods are analysed in the MRP application.

Essentially, much of the demand can be forecasted accurately when the demand for the finished product is known. For example, when an order for a particular customised model of a BMW sports car is received, the exact quantity of sub-assembled components, like body panels, is known. This, in turn, determines what raw material, like steel and types of paint are needed. MRP can assist with the control of stock where the need for one item depends on a higher order item and all relevant components. To meet the demand of finished goods, the system would automatically generate orders for the given items.

Managing Technology Risk

IT Governance

According to Thomas (2005), the idea of IT governance has come about as a way of imposing order on chaos. While chaos may be too strong a word, there have been a number of spectacular IT failures, particularly in the public sector. There is a conviction that careful management of risk has a direct relationship with the success of any business, as expressed by Paul Beach, the head of corporate banking at Atos Consulting: "If shareholder value is coming out of your IT, then good corporate governance of that is absolutely vital because a risk poorly managed could drive that value away" (Thomas 2005).

With the unavoidable use of IT within companies, a critical dependency for business operations has been created. More and more organisations rely on IT to provide a competitive edge or need to use IT successfully to achieve advantage over competitors. Therefore, company boards must include IT in their good governance programme. Corporate IT governance is about their boards being responsible and using methods to ensure that risk is reduced and assigned suitably as follows:

- Allocating clear risk accountability tasks i.e. realising that final responsibility for risk management rests with the board. Although, the board may delegate responsibility for certain aspects of risk management; they bear the responsibility of ensuring its successful implementation. The board's responsibilities cannot be renounced;
- Establishing the company's IT risk appetite, which will then guide decisions like outsourcing, business continuity, system integration, insurance, and security;
- Updating the risk register, proactively controlling risk response actions and frequently reviewing high-level risks at board level;
- Ensuring that risk management is ingrained within the management structure to enable managers to respond quickly to changes in risk profiles. They should know in advance how to escalate risk information throughout the company, i.e. what to report, when to report, in what format, in how much detail, and to whom;
- Understanding that a transparent and proactive approach to risk management ensures competitive advantage;
- Enabling comprehensive two-way communication. IT managers must become good communicators by sharpening their language and presentation skills to make sure the full implications of IT issues are communicated as IT practitioner language can become an obstacle to effective communication. The decision making ability of the board is dependent on the quality of the information that is provided as is the board's capability to make judgements. The board needs to know how much IT risk the organisation is taking;
- Making sure that IT is in line with business objectives and can understand that IT is critical to developing the company;

- Realise the IT fit. No company can survive while standing still. IT systems must adapt to reflect and be aligned to organisational change;
- Understanding the opportunities and risks related to new technology like e-commerce, outsourcing, adopting of new business models and the integration of legacy IT systems within acquired companies with existing IT systems is vital;
- Keep track of where IT projects overrun, exceed their budgets, require expensive on-going maintenance, or failure to satisfy the needs of the end-users;
- Understanding how important robust return-on-investment studies have been for IT expenditure'
- Conducting lessons learnt workshops on all completed IT projects and insist that managers of successive projects study these lessons learnt reports;
- Make certain the board is aware of the newest IT developments and that a lack of investment would reduce market share of the company;
- Analyse the IT industry to identify alternative suppliers to avoid overdependence on a single vendor; and
- Ensuring that IT risk is accumulated so that the risk control tasks can be prioritised and that everyone understands the consequences of risk mitigation action, which means that the reduction in one risk does not increase risk exposure elsewhere in the company, to the extent that the overall IT risk is enlarged.

Investment

A general consensus is that IT projects are not delivering against targets. Recent research by Accenture, based on interviews with 300 executives in the UK and Ireland, identified two main concerns over IT development projects. Andrew Morlet, head of the strategic IT effectiveness group at Accenture, explains "First there was a strong consensus that IT spending is going up and the alignment between business and IT is improving. But now, there is still a belief that IT is not delivering against investment" (Manchester 2005).

Time and cost are the most important features of investment decisions, irrespective of who makes them. Investment is when an outlay of something of economic value, usually cash, is made at one point in time which is expected to yield economic benefits for the investor at some other point in time. Generally the benefits follow outlay. Furthermore the outlay is normally a large single amount while the benefits are seen in a stream of smaller amounts over a long period of time. However, a chief executive is often expected to produce improvements in bottom-line within a specified timeframe. Thus, there is pressure on a project to produce quick improvements in performance and/or costs right from the start.

The Investment Decision-Making Process

Determine investment funds available

↓

Identify profitable project opportunities

↓

Define and classify proposed project(s)

↓

Evaluate proposed project(s)

↓

Approve project(s)

↓

Monitor and Control Project(S)

Generally, IT projects are appraised from a benefit and risk viewpoint; where risk is linked to the degree of certainty about reaching the time, cost and quality parameters specified. The investor wants to see the returns in terms of the business benefits and the life expectancy and maintenance costs of the asset during its useful lifespan.

The investment process can be seen as a sequence of six key stages, each of which must be given due consideration by managers. Many risks are inherent in any investment processes. Common risks include insufficient input from IT specialists, lack of stakeholder involvement, lack of satisfactory end-user consultation, inadequate project definition, poor assessment benchmarks, inadequate time devoted to the selection process, and insufficient assessment of the implementation and in-use risks.

Determine the Investment Funds Available

The board usually determines the funds available for business IT investment. The limit on available capital for any one period could mean that the available funds will not be enough to finance all of the identified projects. When this occurs, some form of *capital rationing* has to be undertaken. This means that managers are faced with the responsibility of deciding what the best use of the available investment funds would be. The plans may consist of projects to replace existing hardware and software to reduce operating costs and improve overall business performance or new IT projects to support new processes.

Identify Profitable Project Opportunities

Identifying profitable investment opportunities is an important part of the investment process. However, management may have submitted so many proposals and is clamouring for funding that this task is executed too quickly and may simply end up being a gathering process.

Defining and Classifying Proposed Project(s)

At this stage, the aim of the process is to convert promising ideas into full-blown proposals. This will require further detailed information. The first stage will involve gathering enough information to facilitate a preliminary screening. Many proposals fall at this step as it soon becomes clear that they are unprofitable or unacceptable for other reasons. Proposals that are deemed worthy of further investigation continue to the next stage.

Evaluate Proposed Projects

Usually a detailed evaluation is done on projects that have passed the preliminary screening stage and have been fully developed.

To do this, answers to a number of key questions must be provided, including the following:

- What is the scope and goal of the project?
- What are the expected benefits and how were they ascertained?
- Does the project support the overall business objectives?
- What is the cost and are funds available? If no specific amount is available, what is the most likely figure?
- What is the expected return on investment?
- What other resources are required to successfully complete the project, e.g. number of employees or external vendors?
- What is the project timescale, what are the key milestones of the project and does the time scale meet the CEO's expectations?
- What is the expected pattern of cash flow/expenditure?
- Are there any interfaces with existing or other planned projects?
- What are the key aspects for implementation?
- Were risk issues taken into account in the appraisal process and what was the outcome?
- How soon will the benefits be felt?
- Will they be felt immediately once the new system is implemented or will they accumulate over time?

Return on Investment (ROI) is a key evaluation method. In an IT context, ROI calculations provide a company with an estimate of the percentage return that it will make over a specified period, as the result of investing in a new computer system.

The ROI is calculated as:

$$\%ROI = benefits/costs \times 100$$

The current annual costs take the following aspects into account: employee costs, existing software licence costs, software support, hardware support, overheads (rent and/or building running costs), and

any other maintenance costs. The investment costs include the consultancy fees, hardware and software purchased costs, costs of installation and the costs to remove any redundant hardware/software. The new estimated annual costs consist of the software licence costs, software and hardware vendor support, and employee operators and overheads, such as rent and building running costs.

Jordan and Silcock (2005) describe what they call "Investment traps whereby projects do not live up to expectations and the business benefits envisaged at the outset of a project are not realised":

- Project overspend increases the initial outlay;
- Project runs late and the achievement of business benefits is delayed;
- Business take-up and usage is less than planned, diminishing business benefits;
- A merger or acquisition requires significant redevelopment effort to accommodate the unforeseen needs;
- System is more costly to support, maintain and enhance than planned increasing costs and lowering net benefits; and
- Business requirements change or system requires replacement sooner than planned, reducing the asset's useful life.

Approve Projects

Formal approval will be given once the manager(s) responsible for authorising the investments are content that the projects should be conducted. However, if more information is needed from those proposing the project or if revisions to the proposal are required, then, the final approval for a project maybe postponed. In some cases, if the project does not provide a return on investment, then the project may be rejected.

Monitor and Control Projects

Electing to invest in a new IT project does not guarantee that it will progress and be implemented without problems. Managers will have to actively control the project through to completion.

Managers should insist on seeing regular project progress reports that provide information like actual vs. planned expenditure, actual vs. Planned progress, any changes to the brief and the effectiveness of risk management actions. In extreme cases, if circumstances have changed dramatically for the worse, managers may abandon the project.

Projects

There is abundant evidence that IT projects have a poor track record in delivering against their objectives. The delivery objectives, as with projects across other industries, are typically time, cost, and quality (including functionality) (Jordan and Silcock 2005).When late projects slip, the company is deprived of the planned benefits for a longer period. On the other hand, projects which are slipping but are being forced to reach their completion date, stand the risk of poor functionality, operability and

maintainability since they will not deliver all that they were meant to deliver and there are operational problems that require rectification. A functionality and quality gap will create a loss of benefits.

When the project is only for internal use, operational problems reduce effectiveness. Depending on the scale of the project, this shortfall may cause a minor performance issue or significant cost implications when for example, a loss of automation results in a far lower reduction in headcount than desired. Poor performance on a project can totally damage a business's reputation when projects are outward facing and are at the interface with the general public, business partners or suppliers.

More project funds are often requested when projects are late or struggling from lack of the right mix of personnel. When these funds are provided, the initial benefits become diluted. The cost of slippage is the sum of the direct costs of in-house resources retained longer, the costs of consultancy support if the reason for delay lay with the sponsor, the indirect costs of lost business benefits for the period of the slippage and the impact on any dependent projects.

When a large proportion of the original budget has already been spent, which may already amount to several millions, and more funding is requested which pushes the project over the limit of acceptability and there is still no certainty on the final costs, the decision to abandon the project is extremely difficult. There is a school of thought that says *big and ugly* projects should be abandoned for interlinked *small and beautiful* projects to overcome poor project experiences.

However, this introduces a different problem that of managing a programme of interdependent projects, which is a significant challenge to manage as each has a different set of risks. When a project fails there is *a lost opportunity risk* where the original objectives of the project have not been met and the previously identified shortcomings have not been addressed, especially considering that if the money invested in the project had been invested in a bank it would have earned interest or the money could have been invested in another project. Jordan and Silcock (2005) describe a further negative outcome of failed projects as *collateral damage* risk. This risk they describe refers to project team members who suffer a crisis of confidence and lose the trust of the planned recipients of the project.

Further Reading:

- ✓ ***Information Technology Risk Management and Compliance in Modern Organisations (Advance in Information Security, Privacy and Ethics) 1st Edition, (2017), By Manish Gupta, Raj Sharman, John Walp, Pavankumar Mulgund***
- ✓ ***Technology Risk A Complete Guide – 2021 Edition, By The Art of Science – Technology Risk Publishing***

