UNIT 1 PORTFOLIO MANAGEMENT AND *IT* APPLICATIONS

Structure **Page Nos.**

1.0 INTRODUCTION

A process can be used gainfully only when it is understood well, in this unit you will be made familiar with the objectives, steps, methods and gains of the portfolio management. This unit takes you through the first, and ultimately the most empowering, phase in portfolio management implementation. You will learn why establishing a portfolio management team with well-defined roles and responsibilities is critical. You will also gain an understanding of why it is crucial to carefully define the portfolio management process and choreograph its interrelationship with the budgeting process, the project proposal process, and other existing business processes.

You will learn how to apply these concepts in an operational organisation. This unit provides an understanding of the value of a portfolio management solution and offers insight into the types of functionality that must be inherent in such an application.

The world is getting increasingly interconnected and information is now centralised and we see businesses being pushed to the edge of the networks. In order to race to the market, security, and controls over such critical information tend to get overlooked.

This translates into issues related to confidentiality, integrity and availability of information — key controls in the information economy. Effective information risk management therefore assumes critical importance. Not only risk needs to be minimized but there is strong need for readiness for the disaster recovery. In this unit you will gain an insight for meeting these challenges.

1.1 OBJECTIVES

After going through this unit, you should be able to:

- define the portfolio management;
- explain the portfolio management methods and implement it;
- define the risk management and will be able to plan to alleviate it;
- explain disasters management;
- appreciate the challenges and issues of the portfolio management;
- select the tools of the portfolio management suiting the requirement, and
- Appreciate the emerging technologies.

1.2 WHAT IS PORTFOLIO MANAGEMENT

Portfolio Management is a process which facilitates determining the right (project) investments mix, i.e., deploying limited resources to maximize business performance, which is a key management challenge. Most capital investment activities take the form of projects that need to be managed as part of a portfolio. Project portfolio management entails balancing resources, business needs, business risks and changing parameters, while at the same time maximizing the return on (project) investment.

Portfolio Management was originally coined in the financial and investment community, and the term was used for the process of managing the assets of a mutual fund; including choosing and monitoring appropriate investments and allocating funds accordingly.

The adoption of the terminology into other industries such as real estate resulted in a modification of the term to reflect industry specific purposes. Similarly, within the technology sector, the term now applies to a set of projects or programs grouped collectively and monitored. We can define portfolio management as the expression of the alignment of the corporate and IT strategic plans, viewing the portfolio as a suite of complementary investments that collectively provide the best possible allocation of resources to meet the business needs of the corporation.

Portfolio Management (PM) applications integrate all project-related informations within a single, web-based enterprise solution. Organisations use PM solutions to better align and manage their projects, people, and partners so that they can achieve greater return on their portfolio of investments.

Basically, Portfolio Management is a discipline used to ensure that a correct mix of investment activity is initiated, grouped, funded and managed. Technology assets are categorised as an investment portfolio allowing for:

- Investment bundling
- Prioritisation
- Evaluation
- Decision insight and support
- Balance between timing, current needs, and future requirements

Considering the complexities, the problem of managing the technology portfolio is broken into set of smaller problems to facilitate analysis. Among the issues to be considered when discussing the technology portfolio are:

- Technology / business alignment
- Investment balance
- Resource management
- Negotiation between competing projects or goals
- Risk mitigation and management
- Technology performance and reporting

Considered as part of the whole, each contributes to the overall portfolio. Considered independently, each is both a manageable problem and a powerful tool.

Portfolio Management Objectives allow the organisation to be focused, fast, and agile. Achieving these high level objectives necessitates a variety of inter-related steps. These include the following:

- **Grouping:** Synergies between technology spending plans with business strategy;

- **Investment Focus:** Viewing expenditures (human, asset, capital) as investments. This also includes a process to track performance;
- **Governance:** Process for making IT investment decisions;
- **Cost Control:** Understanding the main drivers of IT costs for restraint purposes, and
- **Efficiency:** Use of financial resources efficiently, leveraging wherever possible.

Various methods are used to create and balance the portfolio, ranging from highly strategic to tactical:

Financial portfolio analysis: Balance and risk mitigation is achieved by spreading investments over a number of different initiatives. Projects are balanced across a number of categories that can include strategic or business objectives, compliance or required maintenance and research and development. Depending on the organisation's objectives, this allows steering committees to incur the least risk and take advantage of market dynamics.

Top down / bottom up: Companies either apply the big picture of top-down thinking that looks at growth, or how dual projects or business unit objectives provide benefits in bottom-up planning. Both exercises are popular with immature project organisations. However, if conducted separately in a vacuum, it provides a restricted view of the inter-relationships of projects to the organisation. A combined top down/bottom-up approach is the desired solution for such an endeavor.

A variety of **Portfolio Management Benefits** are possible for the organisation successfully executing a PM initiative. Chief among these is the expression of value in business terms.

Other key benefits include:

- Insight into schedule / budget variance
- Return on investment calculations
- Increased resource utilisation and reduced headcount
- Extrapolating financial benefits of a project
- Project interventions and results
- Discontinued projects or corrective measures as necessary

Ultimately, a portfolio management for technology organisations will offer IT management and a sense of symmetry with business objectives; like, a project selection approach based on hard data and the metrics, costs, budgets, and other objective criterias.

It should be noted, however, that as long as IT continues to plan at the individual initiative level, the tactical and reactive nature of most IT organisations would remain. Effective portfolio planning and management bridges the gap towards flexibility and risk mitigation.

There are five primary **value addition** propositions that can be achieved with the implementation of a PM solution. These include:

- **Align Business Strategy and Execution:** Integrate executive guidance (portfolio and financial plans), line sponsorship and project-level execution so that you do the right work;

- **Plan and Execute effectively and efficiently:** Standardise workflows and automate business processes so that you can do the right work faster;

- **Leverage Resources (People, Partners, Money and Assets):** Manage resources across the enterprise and around the world so that you use the right resources;

- **Make global teams more productive:** Share and reuse information, work products and templates so that you do the work right, and

- **Improve visibility and control:** Gain organisational transparency so that you can identify and solve problems early.

The market for Portfolio Management solutions is full of competitive offerings. It is important that PM software evaluations base evaluation criteria on value versus just features and functions. Traditional feature / function evaluation approaches can mislead an organisation to select an application that does not deliver a return on investment, or worse yet, provide a stopgap solution to only part of the problem.

Portfolio Management Requirements that must be available in the offered / selected PM solution can be judged based on recognising the importance of achieving value and measurable return on investment and variety of features and functions which must be present in the PM solution.

These can be broadly categorized into four functional areas:

- Budget and Financial Management;
- Business Planning and Portfolio Management;
- Project and Resource Management;
- Collaboration and Knowledge Management.

The **budget and financial management** functionality of a PM solution should integrate with existing financial and Enterprise Resource Planning (ERP) applications to provide the organisation with real-time project-based budget and financial management capabilities. Easy access to accurate project-based financial information is mandatory so that the organisation can make better and faster business decisions and invest money for maximum return. Functionality should also be provided to automate traditionally manual processes so that resources previously wasted on redundant data entry, manual analysis of project cost estimates, actual time and expenses can be redeployed.

Benefits that should be enabled by the application include the ability to:

- Align spend with projects of greatest return;
- Utilise project-based budgets to make better decisions;
- Manage project budgets against financial objectives, and
- Make project budgets transparent to sponsor organisations.

Functionality required while delivering the above value and benefits include:

- Project and Resource-driven Budget and Approval Process;
- Budget by project, initiative and organisation;
- Budget billable and non-billable projects;
- Budget revenue and expense;
- Configure budget rules;

- Define multi-year and rolling budgets;
  - **Comprehensive Rate Management:**
    - Define flexible rates for budget;
    - Establish multiple rate hierarchies;
    - Use the same or different rates for actual;
  - **Integration:**
    - Integrate with third-party general ledger systems, including providing and sponsoring cost center transactions;
    - Perform prior period adjustments;
    - Align budget management with project management;
  - **Chargeback:**
    - Budget project chargeback to sponsoring organisations;
    - Incurred vs. budgeted cost chargeback;
  - **OLAP Reports:**
    - General ledger cost analysis;
    - Actual vs. total budget;
    - Project detail cost analysis;
  - **Additional Financial Management Functionality:**
    - Inclusion of capital expenditures in non-labour expenses;
    - Incremental project funding;
    - Major expenditure requests;
    - Real-time data vs. historical data views;
    - View-based (resource, cost center, or organisation) breakdown of labour components salary, fringe, etc.

As an example, budgeting is a relatively mature process within the majority of organisations. However, the corporate requirement to ensure alignment with changing business and economic condition necessitates a continuous re-budgeting in order to remain competitive. As a result, thousands of hours of time, effort and paper are required to keep budget data current and aligned.

In the 'bottom-up' and 'top-down' budgeting method, an easy way to understand look and feel can be provided. Top-down budget amounts are provided by the sponsoring organisation, and subsequently, the budget layers are built up project-by-project, program-by-program. It is vital to note that budgeting is conducted at the work level, not the cost-center level, thereby ensuring accuracy. The system also feeds the corporate budgeting system, thus allowing management of both the provider side and the consumer side.

Another critical feature facing the financial severity is funding. This notion provides the benefit of releasing the total money associated with a project. Thus, a project with a large budget may only receive a portion of the allocated funding in the initial stages, with the balance released upon completion of defined milestones. This allows project sponsors to effectively govern the distribution of funds and re-allocate funds midstream if necessary. Funds can be allocated in stages and even from other projects.

The **business planning and portfolio management** aspects of a PM application should enable the organisation to define, evaluate, and monitor their portfolio of projects for maximum return on investment. Organisations should be able to use this functionality to establish the definition, scope, risks and expected return for their portfolio of projects. In addition, they should be able to model new and existing projects to determine the optimum portfolio mix that maximizes their investment return.

Once portfolios are defined and prioritised against corporate objectives, organisations should be able to monitor project portfolios through customisable views. With real-time access into performed project work and planned project resources, organisations should be able to use the PM application to ensure their portfolio of projects, remains aligned with corporate objectives, identify and resolve project risks and resource bottlenecks, and proactively make decisions to maximise return on investment and minimize time to market.

Benefits that should be enabled by the application include the ability to:

- Select the most important projects;
- Establish the right definitions of project success;
- Monitor project performance against objectives;
- Re-align projects when market conditions change, and
- Cancel low priority and failing projects quickly.

Functionality required delivering the above value and benefits include:

- **"What if" scenario modeling / Sensitivity Analysis:**
  - Compare portfolio plans against current operating plans
  - Analyse the impact of new projects on the portfolio
  - Drag and drop schedules
  - Create multiple versions of project portfolio to compare against supply
- **User-defined views:**
  - By project (past, in progress, or planned)
  - By resources (staff, skills or budget)
  - By schedule (past, current, or projected)
- **Multiple criteria based views:**
  - Actual vs. planned
  - Actual vs. budget
  - Actual vs. schedule
- **OLAP Reporting:**
  - Project work by project type
  - Planned vs. actual work
  - Project work by project priority
  - Track initiative status
  - View initiative projects at a glance
  - View initiatives in Gantt charts
- **Simulating projects:**

The **project and resource management** component of a PM application should provide a single record of all project-related activity so that project stakeholders at all levels are equipped with relevant and actionable information to make better and faster decisions throughout the project management lifecycle. It should enable an organisation to build project plan with speed and precision while utilizing fewer and lower cost resources.

Benefits that should be enabled by the application include the ability to:

- Manage project plans to objectives;
- Communicate and monitor work for better results;
- Identify and resolve problems early;

- Manage dependences across projects;
- Assign the right people to the right projects;
- Fully utilize FTEs and reduce contractor costs;
- Leverage resource talent across your global enterprise, and
- Take advantage of resources in lower cost geographies.

Functionality required delivering the above value and benefits include:

- **Initiative Management:**
  - Set up unlimited hierarchical relationships initiatives, programs and projects
  - Monitor initiative home pages and configurable dashboards
  - Define initiative charters and goals
  - Track initiative risks and issues
  - Run initiative reports
  - Track initiative status
  - View initiative projects at a glance
  - View initiatives in Gantt charts
- **Project Management:**
  - Establish customizable project home pages
  - Define project charters and goals
  - Define project team members and stakeholders
  - Plan, assign and monitor tasks, deliverables, and milestones
  - Plan and monitor dependencies within and across projects
  - Define project impacts and drivers
- **Risk and Issue Management:**
  - Define and monitor risks and issues
  - Assign issue and risk actions
  - Status issues and risks
  - Identify common risk and issues across projects
- **Resource Management:**
  - Define hierarchical skills profiles for resources
  - Request and allocate resources
  - Allocate resources based on weighted proficiencies
- **Time and Expense:**
  - Record time and expenses for project tasks
  - Route time and expense approvals
  - Lock approved timesheet data
  - Capture and report non-billable time and expenses
  - Establish user-defined billable hour maximums
  - Report on missing timesheets
  - Configure alerts for timesheets that are overdue or await
  - Define timesheet periods
  - Billable vs. non-billable time tracking
- **Microsoft Project and Project Server Integration:**
  - Synchronized project, task and resource management
  - Integrated OLAP reporting
  - Shared configuration and security administration
  - Configurable field mappinging.

Collaboration and Knowledge Management capabilities that span the processes of portfolio, budget, project, resource, and external relationship management must be available in the Portfolio Management Software selected. A Web-based user interface

is necessary to enable organisations to seamlessly collaborate and share project-related information across internal and external project teams.

Benefits that should be enabled by the application include the ability to:

- Establish a single source for all project-related information,
- Empower project teams with relevant and actionable information,
- Collaborate seamlessly across geographies and business partners.

Functionality required to deliver the above value and benefits include:

- **Customized Home Pages:**
  - Organisational, initiative, project, and individual views
- **Knowledge Sharing across the Extended Enterprise:**
  - Document management including check-in/check-out and version history
  - Templates of standard documents, plans, and budgets
  - Forums for threaded discussions
  - User-configurable views
  - Email documents
- **Role-based User Support:**
  - IT, R&D, financial and line of business executives
  - Project managers
  - Global project team members
  - Customers
  - Partners
  - Contractors and service providers
- **Comprehensive Reporting:**
  - OLAP reports
  - Standard reports
  - Crystal reports
  - Adhoc reports
  - PowerPoint charts
- **Security Administration:**
  - Password composition and frequency restrictions
  - Exportable login audit log

The Role of Services is critical in the successful implementation of a PM solution. Issues including integration with ERP applications, backend databases, as well as the skill and expertise required to deliver the above, are crucial aspects of a PM vendor's strength.

Each step in the implementation process must be designed to deliver incremental benefits, even those before the sales commitment. This allows for the enterprise to achieve more value sooner, however a traditional "big bang" that takes longer to implement, reduces total value, and has a higher risk.

The software must provide tools to enable services team to develop and provide detailed work plans, monitoring progress via weekly status reports, maintaining logs of issues and risks, and ensuring oversight of bug and enhancement requests. As part of the transition management strategy, the team should conduct extensive executive workshops and interviews, executes upon a comprehensive communications plan, and delivers upon a value assessment.

Another key ingredient in any successful software implementation is end user acceptance and usage. In a nutshell, **Transition Management** is the process of deliberately influencing the human, organisational and workflow aspects associated with a change or introduction of technology to achieve the desired results. This notion must be integrated into the overall implementation process. By ensuring that the enterprise quickly and effectively adopts its new technology, productivity as an organisation and more competitiveness in their industry is within reach.

Enterprises should look to realize the following benefits from a transition management effort:

- Broadened ownership of implementation success across organisations by creating goal alignment through early, end-user involvement;
- Minimized organisational barriers to success by identifying and mitigating organisational issues that will either lengthen the implementation or jeoparadize its success;
- Improved organisational knowledge and skills for the new environment, as well as increased organisational effectiveness during implementation;
- Accelerated attainment of projected benefits by focusing on post-implementation issues like user acceptance, productivity, and human performance support, and
- Pass on ownership feeling to the end-user at the early stage of the project.

1.3 DESIGN AND IMPLEMENTATION OF PORTFOLIO MANAGEMENT

Before we get into the Design and Implementation of Portfolio Management, let us look once again at the benefits expected from the implementation of the Portfolio Management. These are:

- Maximize value of IT investments while minimizing the risk;
- Improve communication and alignment between Information System group and business leaders;
- Encourage business leaders to think “team,” not “me,” and to take responsibility for projects;
- Allow planners to schedule resources more efficiently;
- Reduce the number of redundant projects.

There’s no single right way to do IT portfolio management. Vendors, consulting companies and academics offer many models, and often companies develop their own methodologies. Off-the-shelf software is available from a variety of vendors but there are plenty of hurdles to doing it well. There are, however, best practices and key logical steps that can be learned from the organisations which have integrated portfolio management into the fabric of IT management.

Here are the key steps in creating and managing the IT investment portfolio based on the experience of gained from several companies.

Step 1 Assemble: Project Inventory

Portfolio management begins with gathering a detailed inventory of all the projects in the company, ideally in a single database, including name, length, estimated cost,

business objective, ROI and business benefits. There are MNC's who maintain a global database of all its IT projects using software from established IT vendors.

In addition to project plan information, all company users—which may be in thousands from various regions and countries—will have to add weekly updates on how much time they spend working on projects. This is used to gather information on resources.

Creating a project portfolio inventory can be painstaking but is well worth the effort. For many companies, it may be their first holistic view of the entire IT portfolio and any redundancies. A good inventory is the foundation for developing the projects that best meet strategic objectives.

Step 2 Evaluate: Identify Projects that Match Strategic Objectives

A logical starting point creates a product strategy — markets, customers, products, strategy approach, competitive emphasis, etc

The next step involves establishing a portfolio process. The heads of business units, in conjunction with the senior IT leaders in each of those units, compile a list of projects during the annual planning cycle and support them with good business cases that show estimated costs, ROI, business benefit and risk assessment. The leadership team vets those projects and shifts out the ones with questionable business value.

Next, a senior-level IT steering committee made up of business unit heads, IT leaders and perhaps other senior executives meets to review the project proposals; a good governance structure is central to make this work. Portfolio management without governance is an empty concept conversely; putting portfolio management in place can force companies with weak governance structures to improve them.

One of the core criterion for which projects get funded is how closely a project meets a company's strategic objectives for the upcoming year. For this purpose an executive leadership team, which may include the CEO, may create strategic initiatives, such as CRM or organisational excellence. The IT governance council, made up of business leaders and senior IT leaders, then may evaluate projects based on how well they map against those initiatives. It is worthwhile to assess risk from a technology point of view, a change-management point of view, the number of people that a project will impact and whether it will involve huge reengineering. Using methodology borrowed from the product development group (modified for IS, but keeping terminology that business executives are familiar with), projects are may be placed "above the line"— those that should be funded, or "below the line"— those that shouldn't.

A project portfolio review board (comprising of senior officers / departmental heads) may further evaluate the project opportunity assessment for every proposal.

A good evaluation process can help companies detect overlapping project proposals up front, cut off projects with poor business cases earlier, and strengthen alignment between IS and business executives.

Step 3 Prioritize: Score and Categorise Projects

After evaluating projects, most companies will still have more than they can actually fund. The beauty of portfolio management is that ultimately, the prioritisation process will allow you to fund the projects that most closely align with your company's strategic objectives.

Next, the projects are required to be placed into portfolios—multiple portfolios may be a good idea in many companies because they allow alike projects to be pooled together.

In case of the large technology portfolio, its management team—made up of project sponsors, function managers (for example, representatives from engineering, financial services and operations, and CEO himself) and product portfolio managers (people with long-term project leadership responsibilities in areas such as services or data management)—may vet projects and come up with a list for the portfolio team to score.

They then prioritised them using a model that has four key tenets:

a) **Identify four to seven strategies:** For example, limiting technology risk and increasing the reliability of the infrastructure.

b) **Decide on one criterion per strategy:** For example, the team decided the criterion for limiting technology risk would be whether the technology had been implemented in a comparable organisation and the benefits could be translated to the company easily.

c) **Weigh the criteria:** Allocate the weight to each criteria.

d) **Keep the scoring scale simple:** Many companies use a scale of one to five. For the technology risk strategy, five might mean that it has been used in a comparable organisation and the benefits could be transferred easily; three could mean it's hard to do because it would require changing processes; one might mean they haven't seen it work anywhere else.

Following the scoring, the team may draw a line based on how many projects it could do with existing resources. In the case of the large technology portfolio, the line may be calculated where demand (the list of projects) meet supply (resources—in this case, the cumulative money value of available application engineers plus overhead); the line may be a little less than halfway down the list. Those projects above the line could be taken up immediately.

There is no one method to categorise IT investment portfolio. One approach is to categorise it as you would do with your own financial portfolio, balancing riskier, higher reward strategic investments with safer categories, such as infrastructure. Some companies recommend a portfolio divided into three investment categories: running (keeping the lights on), growing (supporting organic growth) and transforming the business (finding new ways of doing business using technology). Those categories can then be cross-tabulated with four to five value-focused categories, such as how those investments support revenue growth, reduce costs or grow market share.

In another model, based on their the previous experience, companies view their IT portfolios on multiple levels and at different stages, by visualising their investments in aggregate and placing them in four categories, with the per cent of IT expenditures apportioned across each. For example they may have 5 per cent [of the projects] in strategic areas, 15 per cent to 20 per cent in the informational category, and the remaining percentage split between the infrastructure and transaction modules,

The payoffs that come from a thorough evaluation and prioritisation process is the primary reason portfolio management is so effective. Firstly communication between IS and business leaders improves, and portfolio management gives business leaders a valuable, newfound skill—the ability to understand how IT initiatives impact their companies.

Secondly, business leaders think "team," not "me," and take responsibility for projects. One tried-and-true method for how a business leader got money for his unit's projects was to scream louder than everyone else. Portfolio management throws that practice out the corner office window; decisions are made based on the best interests of the company.

Thirdly, portfolio management gives business leaders responsibility for IT projects. No longer the IT persons had to sell these IT projects to the business. For example a project for marketing, it's the marketing executive who has to sell the project to the rest of the team. In the changed scenario, (instead of the technology people who were earlier proposing the projects) now the businesspeople propose the projects and [take responsibility] for risk profiling, ongoing operational costs and timeliness of delivery.

Finally, everybody knows where the money is flowing and why, which is especially important to CEOs and CFOs who are increasingly demanding that technology investments deliver value and support strategic objectives.

Step 4 Review: Actively Manage the Portfolio

A top-notch evaluation and prioritisation process is ineffectual rather quickly if the portfolio is not actively managed following approval of the project list. Doing that involves monitoring projects at frequent intervals, at least quarterly (preferably it should be monthly), the project management office is required to get financial and work progress perspective updated from project leaders. This information is required to go into a database, from where the project inventory and its status is circulated to all concerned. Some of the companies assign project status—green (good), yellow (caution) or red (help!)—and include an explanation of the key driver causing a yellow or red condition. The IT steering committee meets once a month to make decisions to continue or stop initiatives, assess funding levels and resolve resource issues.

Monitoring project portfolios regularly also means projects that have run off the rails can be killed more easily. "People have an aversion to stopping projects, but the majority of projects which are canceled are done because there's a change in company strategy—a change in priority or direction. For example, if there's a strategy decision to focus on SAP, then it makes sense to cancel a new system that interfaces with PeopleSoft.

Portfolio management is a good thing. But getting to nirvana requires a serious commitment from both the business and IS sides, as well as a whole lot of sweat equity. Here are some of the pitfalls and ways to overcome them.

- **Democracy is not easy:** Taking power away from business leaders accustomed to calling the shots will not always go smoothly.
- **Group decision:** Business leaders who didn't have decisions scrutinized previously now are [having] decisions decided by group consensus, people realize it does work and that group of people can make better decisions than one or two making unilateral decisions.
- **There's no single software that does everything:** "There are really good budget packages, resource management packages and fairly good portfolio management packages, but no package that ties it all together,"
- **Getting good information isn't easy:** Take, for example, the transparency of the cost structure. There has to be good information around all technology costs and investments
- In addition, **database must be updated regularly**, so that there continuous flow of status of each project to the concerned persons to enable them to react quickly to market changes.
- **It's still hard to make tough decisions on whether to undertake—or cancel—projects:** as an organisation has a tendency to say, we shall figure out a way to make those work."
- **It's an additional time constraint on busy executives:** Good portfolio management means good IT governance means regular IT governance committee meetings. Just about every company today has its people stretched.

1.4 PORTFOLIO MANAGEMENT METHODS

We have gone through the implementation of portfolio management at Para 5.3 above. The basic steps for implementation are:

1) Collect / identify all ongoing and proposed projects / opportunities.
2) Out of the list compiled at a) above, identify/evaluate projects/opportunities which meet strategic requirement of the company.
3) Prioritize as per the score & categorize these projects/opportunities.
4) Review the projects/opportunities for adoption plan and monitor their implementation.

Each of the above steps can be carried out by different methods. In fact Portfolio Management vendors, not only present their own variant of methods in their packages, but these packages have some minor variations in sequence of these steps also. We will be discussing some of the common methods for each of these steps.

Step 1: Collect information on all projects (on-going and planned): In this step goal is to collect all relevant information on the projects like, status of the project, resources used and required for completion of the project, project schedule and the risk factor involved. Methods used for this are:

- **Central repository** based present day systems which collect data in formats generated (based on initial key information / data entered) by the system and stored in the data base.

- **Conventional procedures** of project management, wherein data is entered for each project and stored in a common database.

Step 2: Evaluate for Strategic Compliance: A logical starting point for this step is to create a product strategy — markets, customers, products, strategy approach, competitive emphasis etc. Some companies define these strategies in terms of Key Performance Indicators (KPIs). Once strategy is defined then each identified project / opportunity is evaluated against strategy to determine if those opportunities are in line with the corporate strategic direction. In a sense, this may be the identification and initial screening of projects before more in-depth analysis is conducted. The questions asked are: What is the project? Does the project fit within the focus of the organisation and the business strategy and goals? This evaluation is done in two manners: (a) Tactical Evaluation, and (b) Financial Evaluation.

a) Tactical Evaluation

- **Top-down, strategic buckets:** Begin at the top with your business's strategy and from that, the *product innovation strategy* for your business – its goals, and where and how to focus your new project efforts. Next, make splits in resources: 'given your strategy, where should you spend your money?'. These splits can be by project types, product lines, markets or industry sectors, and so on. Thus, you establish *strategic buckets* or envelopes of resources. Then, within each bucket or envelope, list all the projects – active, on-hold and new – and rank these until you run out of resources in that bucket. The result is multiple portfolios, one portfolio per bucket. Another result is that your spending at year-end will truly reflect the strategic priorities of your business.

- **Top-down, product roadmap:** Once again, begin at the top, namely with your business and product innovation strategy But here the question is: 'given that you have selected several areas of strategic focus – markets, technologies or product types – what major initiatives must you undertake in

order to be successful here?'. It's analogous to the military general asking: given that I wish to succeed in this strategic arena, what major initiatives and assaults must I undertake in order to win here? The end result is a mapping of these major initiatives along a timeline – the project roadmap. The selected projects are 100% strategically driven.

- **Bottom-up:** "Make good decisions on individual projects, and the portfolio will take care of itself" is a commonly accepted philosophy. That is, make sure that your project gating system is working well – that gates are accepting good projects, and killing the poor ones – and the resulting portfolio will be a solid one. Even better, to ensure strategic alignment, use a scoring model at your project reviews and gates, and include a number of strategic questions in this model. Strategic alignment is all but assured: your portfolio will indeed consist of all "on strategy" projects (although spending splits may not coincide with strategic priorities).

b) Financial Evaluation

It is to further define the project (if needed) and to analyze the details surrounding its utility. The utility of a project captures the usefulness of the project, its value, and is typically defined by costs, benefits, and associated risks. The questions to ask are: Why should this project be pursued? What is the usefulness and value of the project? Several things are to be considered. Establish criteria and develop a model to support decision making; Make sure accurate data is available to make decisions. Establish a process to analyze the project information; uniformly apply the methodology across the organisation. The different methods for valuation are:

- **Net Present Value (NPV):** In this method for each project NPV is determined which is divided by the key or constraining resource. For example for the Project A NPV will be divided by X where X is costs still left to be spent on the project A.; that is, Portfolio Index of this project will be NPV/X. Some of the companies multiply this factor by probability (say P) of completion of the project. Then Portfolio Index will be NPV * P / X. Projects are rank-ordered according to this index until out of resources, thus maximizing the value of the portfolio (the sum of the NPVs across all projects) for a given or limited resource expenditure.

- **ECV:** The Expected Commercial Value method uses decision-tree analysis, breaking the project into decision stages – e.g., Development and Commercialisation (*Figure 1*), define the various possible outcomes of the project along with probabilities of each occurring (for example probabilities of technical and commercial success). The resulting ECV is then divided by the constraining resource (as in the NPV method), and projects are rank-ordered according to this index in order to maximize the portfolio index. The method also approximates *real options theory*, and thus is appropriate for handling higher risk projects.

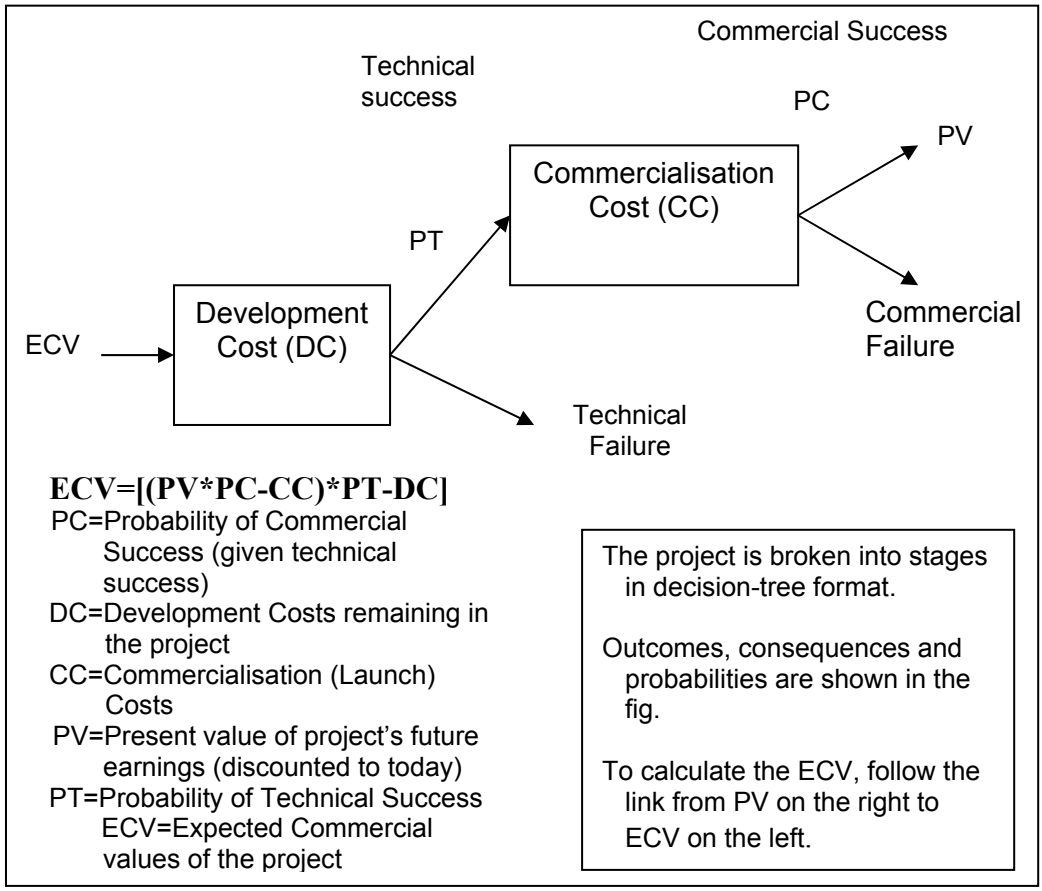


Figure 1: Calculation of expected commercial value of project

Step 3. Prioritizing and Balancing: The third major area of portfolio management is the development and selection of the project portfolio. The questions to ask are: Which projects should be selected? How does the project relate to the entire portfolio, and how can the project mix be optimized? Several things need to be considered: Establish a process that will help optimize the portfolio not just the individual projects. Establish port- folio decision meetings to make decisions.

Seek Balance in Your Portfolio: Here, the goal is to achieve a desired balance of projects in terms of a number of parameters; for example, long term projects versus short ones; or high risk versus lower risk projects; and across various markets, technologies, product categories, and project types (e.g., new products, improvements, cost reductions, maintenance and fixes, and fundamental research). Pictures portray balance much better than do numbers and lists, and so the techniques used here are largely graphical in nature. These include:

- *Scoring model:* Decision-makers rate projects on a number of questions that distinguish superior projects, typically on 1-5 or 0-10 scales. Add up these ratings to yield a quantified project usefulness score, which must clear a minimum hurdle. This Score is a proxy for the "value of the project" but incorporates strategic, leverage and other considerations beyond just financial measures. Projects are then rank-ordered according to this score until resources run out. A typical scoring scheme is shown in *Figure 2*.

IGNOU	SCORING TABLE							
Criteria	Scores weight	Partition	Rapid part	Growth	Sequence	Average Score	Weight	Weight age
Strategic alignment								
Production business limit	7	8	6	8	8	7.5	5%	12.4
Product manufacturing	7	9	7	6	7	7.6	6%	5.6
Product support	7	8	6	7	6	7.3	7%	6.3
Product Knowledge								
Customer needs	8	7	7	5	7	7.6	12%	5.6
Product preparation	8	7	8	5	5	7.4	8%	5.3
Market Effectiveness								
Market criteria	9	8	8	4	8	7.6	7%	3.7
Market policy	8	6	6	7	8	7.2	5%	6.2
Risk								
Types of risks	8	8	5	7	8	7.6	6%	9.1
Affect of risk	6	6	4	6	9	7.3	9%	5.8
						Total	100%	75.7

Figure 2: Scoring Table: The worksheet computes the average scores and applies the weighting factors to compute the overall score

- *Bubble diagrams:* Display your projects on a two-dimensional grid as bubbles as in *Figure 3*. The axes vary but the most popular chart is the risk-reward bubble diagram, where NPV is plotted versus probability of technical success. Then seek an appropriate balance in numbers of projects.

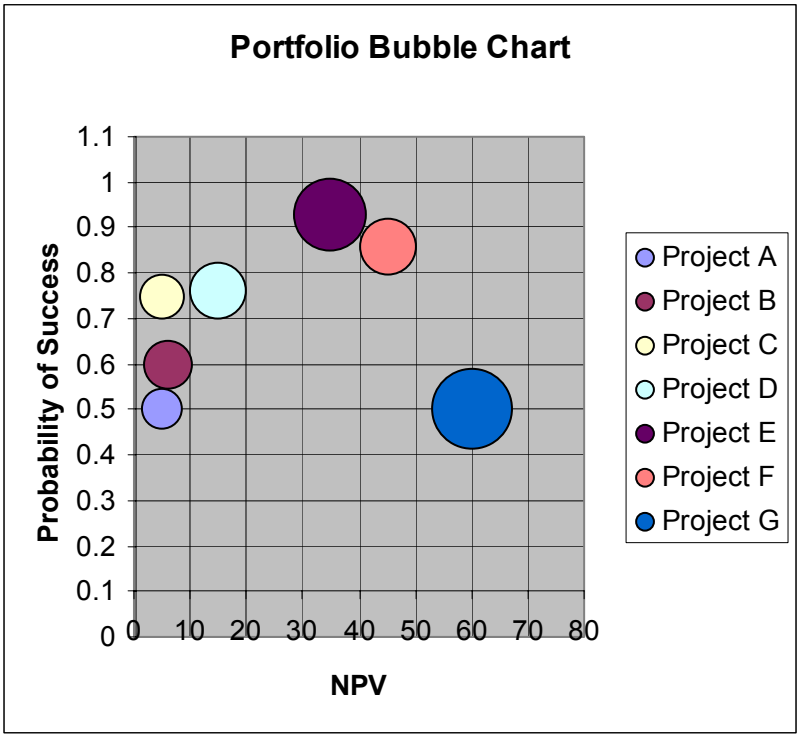


Figure 3: Bubble diagram

The bubble diagram provides a graphical view of the project portfolio risk-reward balance. It is used to assure balance in the portfolio of projects — neither too risky nor conservative and appropriate levels of reward for the risk involved. The horizontal axis is Net Present Value, the vertical axis is Probability of Success. The size of the bubble

is proportional to the total revenue generated over the lifetime sales of the product (for working out cost impact, the size of the bubble is made proportional to the cost of the project).

• *Pie charts: Figure 4* shows spending breakdowns as slices of pies in a pie chart. Popular pie charts include a breakdown by project types, by market or segment, and by product line or product category.

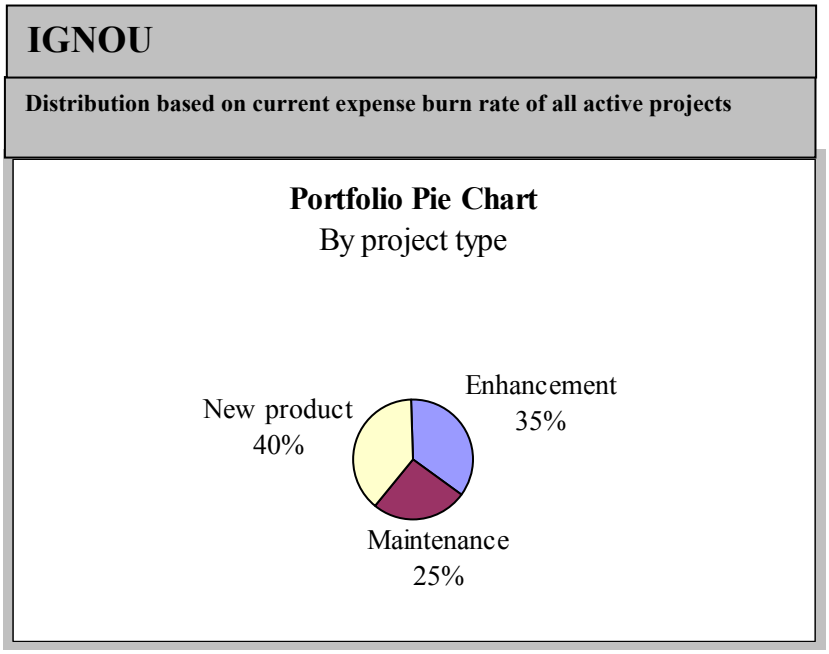


Figure 4: Pie chart for spending breakup

While this visual presentation is useful, it can't prioritize projects. Therefore, some mix of these techniques like, bubble chat along with pie chart etc. is appropriate to support the Portfolio Management Process. This mix is often dependent upon the priority of the goals.

Both bubble diagrams and pie charts, unlike the maximisation tools outlined above, are not decision-models, but rather *information display*: they depict the current portfolio and where the resources are going – the 'what is'. These charts provide a useful beginning for the discussion of 'what should be' – how should your resources be allocated.

A final check is to analyse product and technology roadmaps for project relationships. For example, if a lower priority platform project was omitted from the portfolio priority list, the subsequent higher priority projects that depend on that platform or platform technology would be impossible to execute unless that platform project were included in the portfolio priority list.

Balancing

It is very important that the Right Number of Projects are picked. Most companies have too many projects underway for the limited resources available. The result is pipeline gridlock: projects end up in a queue, they take too long to reach the market, and key activities – for example, doing the up-front homework – are omitted because of a lack of people and time. Thus, an over-riding goal is to ensure a balance between resources required for the active projects and resources available. Here are the ways:

- **Resource limits:** The value maximization methods build in a resource limitation – rank your projects until out of resources. The same is true of bubble diagrams the

sum of the areas of the bubbles – the resources devoted to each project – should be a constant, and adding one more project to the diagram requires that another be deleted.

- **Resource capacity analysis:** Determine your resource demand, prioritise your projects (best to worst) and add up the resources required by department for all active projects (usually expressed in person-days per month). Project management software, such as MS-Project, enables this roll-up of resource requirements. Then determine the available resources (the supply) per department – how much time people have to work on these projects. A department-by-department and month-by-month assessment usually reveals that there are too many projects; it suggests a project limit (the point beyond which projects in the prioritized list should be put on hold); and it identifies which departments are the bottlenecks.

Decision Gates Process

Right from the first stage, the elimination of projects which do not meet the requirements of that step are required to be eliminated. This process of removal or delaying of projects is carried out by decision gates (*Figure 5*). The process chain for decision-based monitoring and reporting includes the following **decision points or gateways**, each of which requires associated reports.

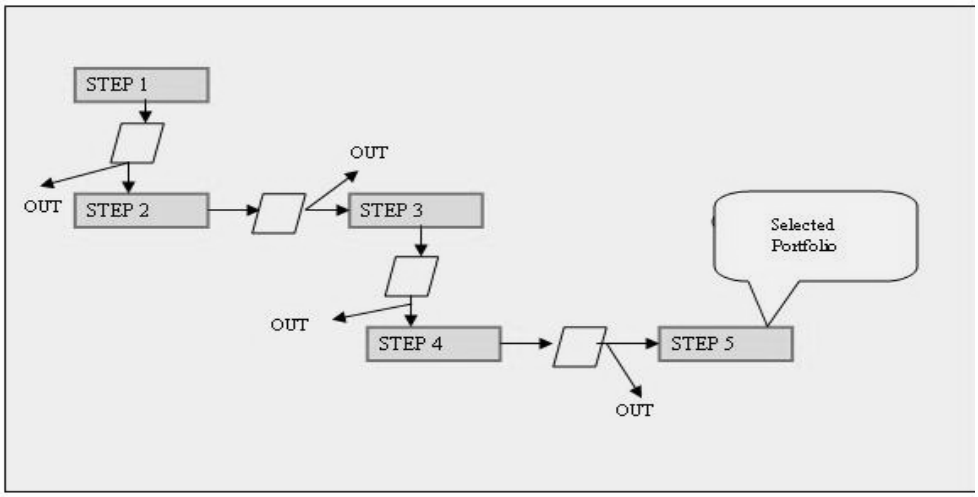


Figure 5: Decision step gates

1) **At the Data Gathering stage:** After **pre-screening** has taken place, project ideas are subjected to a selection process designed to filter out ideas with little potential. The remaining project ideas are only then evaluated as to their cost-effectiveness and classified as must-do or can-do projects. In the next step, high-potential ideas are developed into business cases and fleshed out. Ideas that seem unattractive at this point fail to pass the gateway and are rejected. The project ideas are presented in an overview showing how they fulfill the above criteria; this helps decide which ideas pass the gateway and which should be rejected.

2) **At the Evaluation stage: Project dependencies** must be evaluated to pinpoint dependencies within and between strategic buckets. (Defined top-down, strategic buckets represent areas of strategic focus and spending splits, and each project is assigned to just one bucket). This helps to pinpoint potential synergy. Any redundancies must then be eliminated by reconfiguring projects and by creating programs of projects. For this purpose, dependencies must be evaluated and presented in visual form to assist with decision-making.

3) Company-internal billing is based on rates set by the organisational units involved. Due to differing cost structures and fluctuating demand, **internal billing rates** must be reviewed regularly. Once capital constraints have been determined, supply and demand for specific resources must also be determined. Internal billing rates between organisational units can be recalculated on the basis of actual resource costs. This requires information on resource supply and demand as well as the underlying costs of the resources.

4) **Prioritisation:** Projects should be assigned priorities based on their perceived value, and a project ranking system must be developed. Project value can be either quantitative such as net present value, expected commercial value, return on investment, etc or qualitative such as strategic contribution, operational urgency, strategic alignment, risk, etc. Project value information is presented in the form of a score table or graphical chart, enabling decision-makers to evaluate the project portfolio using a wide variety of criteria. This leads to a more balanced assessment.

5) **At the Approval stage:** Following prioritization, the **project portfolio** is finalized. Based on the comparison and evaluation of quantitative and qualitative criteria relating to strategic importance, value and risk, a concrete scenario is selected for implementation. Decisions must be made as to which projects to execute, continue or cancel. To this end, alternative scenarios are compared using the above criteria. A change list must also be drafted, stating which projects are to be started, continued, postponed, brought forward, or abandoned.

6) Once a portfolio has been selected for implementation, the **allocation of resources** must be determined. The selected scenario dictates how resources need to be allocated to organisational units, and determines whether and what additional capacity (in-house and external) is required. An evaluation of how the selected portfolio affects resource availability and allocation is provided as decision-support.

7) The project portfolio selected also drives the **allocation of capital**. The scenario selected determines the investment required and the capital allocated to each organisational unit in the form of funding for in-house effort, outsourced effort, and investment. In addition, the budgets of the strategic buckets are reviewed and adjusted, providing baseline information for subsequent investment control/monitoring. An analysis of capital distribution is used as decision-support for approving the allocation of funds.

8) **At the Control stage: Analysis of deviations** is performed regularly while the projects in the portfolio are underway. Deviations are identified by comparing target and actual values; this method also provides information on their scale and severity. The project portfolio may require adjustment as a result. Decision-making on corrective action is facilitated by reports showing qualitative and quantitative parameters for the entire portfolio, and highlighting the impact of serious deviations from plans or targets.

Step 4 'WHAT IF' analysis and project adoption: Once the organisation has its prioritised list of projects, it then needs to determine where the cutoff is based on the business plan and the planned level of investment of the resources available. This subset of the high priority projects then needs to be further analyzed and checked. The first step is to check that the prioritized list reflects the planned breakdown of projects based on the strategic allocation of the business plan.

The *Figure 6* shows the portfolio adopter designed to let executives or project managers conduct 'what if' scenario modeling and analysis. This view shows a portfolio of projects (top left) and the dates the projects are scheduled to start and end

(top right). The bottom half of the screen shows the impact on overall capacity of the firm to do them (bottom right). Users can adjust any portion to show the impact of delaying or canceling projects in the portfolio on capacity, money, marketing value.

IGNOU

File Edit Portfolio Format Display Spread Flow Help

Projects Portfolio Period Data Units Spread

	A	B	C	Project Name	Project ID	Description	Manager
1				Database Update	A/P Screen Add		
2				Development	Gen Mod Bill Info		
3				E-Commerce	Gen Mod Market		
4		√		Online Trading	GL Field Addition		
5	√	√		Bank Card Program	Marketing Info		
6				CRM Roll Out	LAN Install		

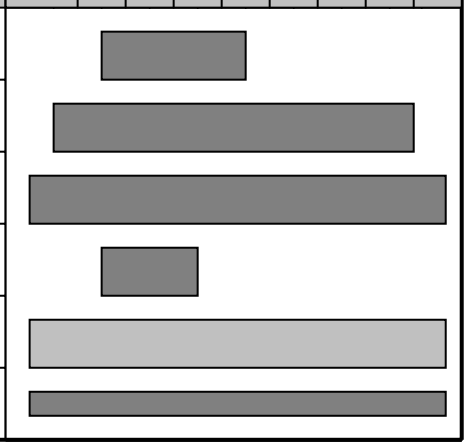
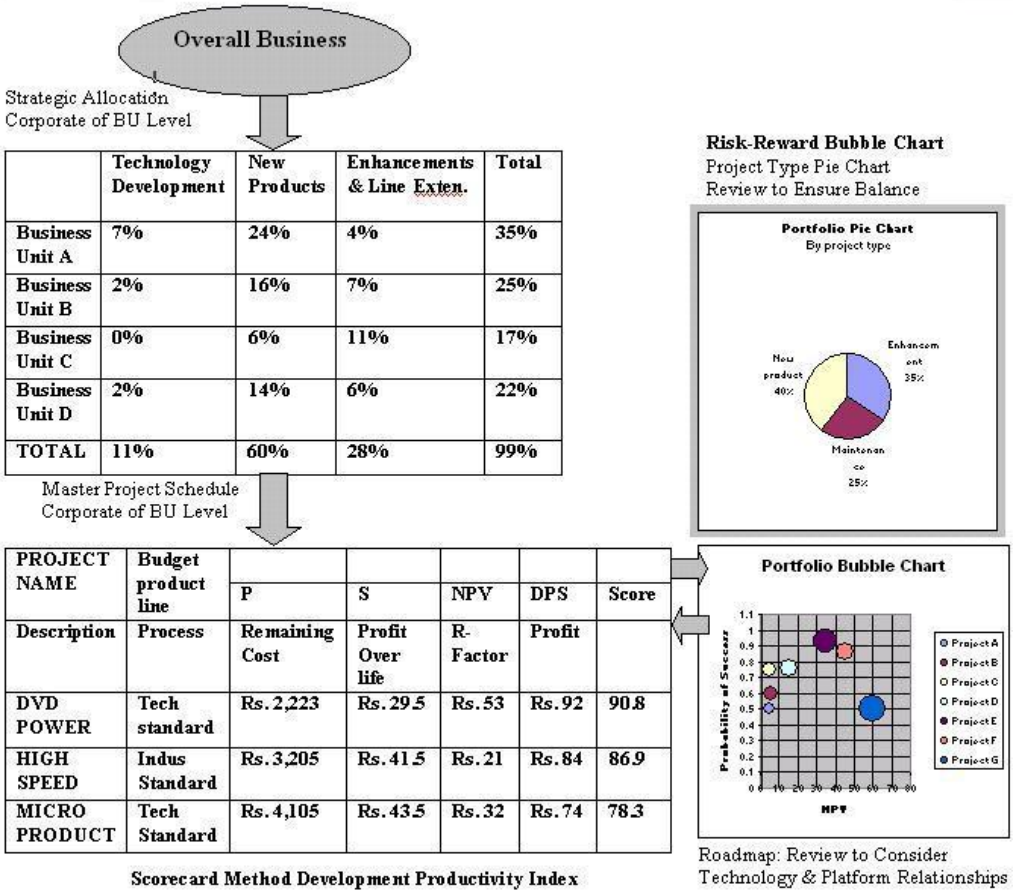


Figure 6: Portfolio adopter

The selected portfolio projects are taken up for implementation / continuation. However, the monitoring process has to continue. For this purpose most of the vendors are offering a dashboard as part of their software package. This dashboard presents an overall view as shown in *Figure 7*.



	Technology Development	New Products	Enhancements & Line Exten.	Total
Business Unit A	7%	24%	4%	35%
Business Unit B	2%	16%	7%	25%
Business Unit C	0%	6%	11%	17%
Business Unit D	2%	14%	6%	22%
TOTAL	11%	60%	28%	99%

PROJECT NAME	Budget product line	P	S	NPV	DPS	Score
Description	Process	Remaining Cost	Profit Over life	R-Factor	Profit	
DVD POWER	Tech standard	Rs. 2,223	Rs. 29.5	Rs. 53	Rs. 92	90.8
HIGH SPEED	Indus Standard	Rs. 3,205	Rs. 41.5	Rs. 21	Rs. 84	86.9
MICRO PRODUCT	Tech Standard	Rs. 4,105	Rs. 43.5	Rs. 32	Rs. 74	78.3

Figure 7: Overall view of portfalio management process

Check Your Progress 1

1) State True or False:
   a) The portfolio management process eliminates need for Investment bundling, Prioritization, Evaluation and Decision insight and support. True ☐ False ☐
   b) The portfolio management makes possible, grouping of technology, Investment Focus and cost control. True ☐ False ☐
   c) **ECV = [(PV * PC - CC) * PT - DC]**
      Where PC = Probability of Commercial Success,
      DC = Direct Cost, CC = Commercialization (Launch) Costs,
      PV = Present Value of project's future earnings (discounted to today),
      PT = Probability of Technical Success and ECV = Expected Commercial Value of the project. True ☐ False ☐
   d) Scoring Tables are used for prioritizing the portfolios. True ☐ False ☐
   e) Bubble diagrams are used for prioritizing the portfolios. True ☐ False ☐

2) Answer the Following Questions:
   i) What are the key functional requirements which must be available in the Portfolio Management Solution?
   ……
   ……
   …….

   ii) What are the steps for portfolio management implementation?
   ……
   ……
   ……

1.5 RISK MANAGEMENT

With the Information Technology, although management needs to be aware of all potential risks, *operational risk* is the primary risk associated with it. Operational risk (also referred to as transaction risk) is the risk of loss resulting from inadequate or failed processes, people, or systems. The root cause can be either internal or external events. Operational risk is present across all business lines.

Operational risk may arise from fraud or error. Management's inability to maintain a competitive position, to manage information, or to deliver products and services can also create and compound operational risk. Weak operational risk management can result in substantial losses from a number of IT threats including business disruptions or improper business practices.

All organisations should properly identify, measure, monitor, and control operational risk. Management should distinguish the operational risk component from other risks to enable a stronger focus on operational risk mitigation. The board should ensure that a program exists to manage and monitor this risk. The program should address the institution's tolerance for risk, the effectiveness of internal controls, management's accountability in regards to risk mitigation, and the processes needed to manage IT effectively.

Operational risk includes not only back office operations and transaction processing, but also areas such as customer service, systems development and support, internal controls and processes, and capacity planning. Operational risk from IT also affects credit, compliance, strategic, reputation, and market risks. Management should be aware of the implications of operational risk including:

- **Liquidity, interest, and price risks:** Credit and market risks can materialize from external changes in markets, industries, or specific customers. Internal controls that rely heavily on the availability and performance of technology create additional operational risk exposure. For example, a failure to properly implement changes to underwriting, account management, or collection systems can lead to significant losses, and higher loan servicing and collection costs
- **Reputation risk:** Reputation risk stems from errors, delays, or omissions in information technology that become public knowledge or directly affect business partners, customers and consumers resulting in a loss of confidential information and potential customer withdrawal of funds. Two activities that can lead to reputation risk are the unauthorised disclosure of confidential customer information and the hacking/modifying of an institution's website
- **Strategic risk:** Strategic risk can stem from inaccurate information or analysis that causes management to make poor strategic decisions. For example, IT management could decide to save money by delaying an infrastructure upgrade to increase network bandwidth, which could result in a business line losing market share due to an inability to compete.
- **Compliance (legal) risk:** Compliance risk results from the institution's inability to meet the regulatory and legal requirements associated with its IT products and services. Legal risk may lead to civil or criminal liability if, for example, an institution discloses confidential information or provides inaccurate or untimely consumer compliance disclosures.

IT management should have a corporate-wide view of technology. It should maintain an active role in corporate strategic planning to align technology with established business goals and strategies. It also should ensure effective technology controls exist throughout the organisation either through direct oversight or by holding business

lines accountable for IT-related controls. From a control standpoint, management should assess risks and determine how to control and mitigate the risks. Management should continually compare its risk exposure to the value of its business activities to determine acceptable risk levels.

IT Risk Management Process

IT controls result from an effective risk assessment process. Therefore, the ability to mitigate IT risks is dependent upon risk assessments. Senior management should identify, measure, control, and monitor technology to avoid risks that threaten the safety and soundness of an institution. The institution should

1) *plan* for use of technology,
2) *assess* the risk associated with technology,
3) decide how to *implement* the technology, and
4) establish a process to *measure and monitor* risk that is taken on. All organisations should have:
    - An effective planning process that aligns IT and business objectives;
    - An ongoing risk assessment process that evaluates the environment and potential changes;
    - Technology implementation procedures that include appropriate controls, and
    - Measurement and monitoring efforts that effectively identify ways to manage risk exposure.

This process will typically require a higher level of formality in more complex institutions with major technology-related initiatives.

The risk identification and management process for technology-related risks is not complete without consideration of the overall IT environment in which the technology resides. Management may need to consider risks associated with IT environments from two different perspectives:

- If the IT function is decentralized, and business units manage the risk, then management should coordinate risk management efforts through common organisation-wide expectations.
- If the IT department is a centralised function that supports business lines across shared infrastructure, management should centralize their IT risk management efforts.

Planning IT Operations and Investment

Planning involves preparing for future activities by defining goals and the strategies used to achieve them. Information technology is an integral part of large number of companies like financial institution operations. Therefore, such companies like, financial institutions should integrate IT resources and investments into the overall business planning process. Major investments in IT resources have long-term implications on both the delivery and performance of the institution's products and services.

Plans may vary significantly depending on the size and structure of the organisation. Every organisation should strive to achieve a planning process that constantly adjusts for new risks or opportunities and maximizes the value of IT to the organisation. Management should always document plans; however a written plan does not guarantee an effective planning process. Management should measure specific plans by whether they meet the organisation's business needs. For all plans, the examiner should evaluate the process as well as the written product. A sound plan requires the board of directors, senior management, and user involvement in the planning process.

The board of directors should review and approve the plan. Senior management participates in formulating and implementing the plan. The individual departments and functional areas identify specific business needs and, ultimately, implement the plans.

Risk Identification and Assessment

Operational IT planning should identify and assess risk exposure to ensure policies, procedures, and controls to remain effective. Information security risk assessments are essential. The assessments should identify the location of all confidential customers and corporate information, any foreseeable internal and external threats to the information, the likelihood of the threats, and the sufficiency of policies and procedures to mitigate the threats. Management needs to consider the results of these assessments when overseeing IT operations.

The risk assessments should cover all IT risk management functions including security, outsourcing, and business continuity. Senior management should ensure IT-related risk identification and assessment efforts at the enterprise-wide level are coordinated and consistent throughout the organisation. A strong, high-level, risk assessment process provides the foundation for more detailed assessments within the functional risk management areas. An effective IT risk assessment process will improve policy and internal controls decisions across the organisation.

Senior management can use risk assessment data to make informed risk management decisions based on a full understanding of the operational risks. Small institutions with less complex systems may have a more simplified risk assessment process. Regardless of the complexity, the process should be formal and should adapt to changes in the IT environment. Examiners should measure the effectiveness of the process by evaluating management's understanding and awareness of risk, the adequacy of formal risk assessments, and the effectiveness of the resulting policies and internal controls.

Ongoing Data Collection

Understanding the institution's environment is the first step in any risk assessment process. Senior management should incorporate information on IT issues such as resource limitations, threats, priorities, and key controls from several sources. In developing a formal risk assessment, management should collect and compile information regarding the organisation's information technology environment from several locations including:

- IT systems inventories are critical to understanding and monitoring the tactical operations of the institution's information technology as well as to identifying the access and storage points for confidential customer and corporate information.
- IT strategic plans provide insight into the organisation's planning process. Review and analysis of the strategic plans as part of the risk assessment process may spotlight developing risk exposures or other deficiencies that limit the institution's ability to implement strategic priorities.
- Business recovery and continuity plans prioritise the availability of various business lines to the institution and often encompass restoration and provision of control, customer service, and support. The plans can offer insight into the organisation's critical operating systems and the control environment.
- Due diligence and monitoring of service providers can present valuable information on the servicer control environment. The information is necessary for a complete risk assessment of institution's information technology environment.

- Call center issue tracking reports can often indicate potential performance or control issues if the problem reports are aggregated and analysed for repetitive or common issues.

- Department self-assessments on IT-related controls can provide early identification of policy noncompliance or weaknesses in controls.

- IT audit findings provide insight into the veracity and responsiveness of the institution's staff and management, commitment to policy compliance and internal controls.

Risk Analysis

Management should use the data collected on IT assets and risks to analyze the potential impact of the risks on the institution. The analysis should identify various events or threats that could negatively affect the institution strategically or operationally. Management should evaluate the likelihood of various events and rank the possible impact. Some examples of events that could affect the institution include the following:

- **Security breaches:** Security breaches that can affect the institution include external and internal security breaches, programming fraud, computer viruses, or denial of service attacks

- **System failures:** Common causes of system failures include network failure, interdependency risk, interface failure, hardware failure, software failure, or internal telecommunication failure

- **External events:** Institutions are also exposed to external threats including weather-related events, earthquakes, terrorism, cyber attacks, cut utility lines or wide spread power outages that bring about system or facility failures.

- **Technology investment mistakes:** Mistakes in technology investment including strategic platform or supplier risk, inappropriate definition of business requirements, incompatibility with existing systems, or obsolescence of software may constrain profitability or growth.

- **Systems development and implementation problems:** Common system development and implementation problems include inadequate project management, cost/time overruns, programming errors (internal/external), failure to integrate and/or migrate successfully from existing systems, or failure of system to meet business requirements.

- **Capacity shortages:** Shortages in capacity result from lack of adequate capacity planning, including the lack of accurate forecasts of growth.

Once the institution has identified the universe of risks, management should estimate the probability of occurrence as well as the financial, reputation, or other impact to the organisation. Organisational impacts are highly variable and not always easy to quantify, but include such considerations as lost revenue, flawed business decisions, data recovery and reconstruction expense, costs of litigation and potential judgments, loss of market share, and increases to premiums or denials of insurance coverage. Typically, risk analysis ranks the results based on the relationship between cost and probability.

Prioritisation

Once management understands the institution's technology environment and analyzes the risk, it should rank the risks and prioritize its response. The probability of

occurrence and the magnitude of impact provide the foundation for reducing risk exposures or establishing mitigating controls for safe, sound, and efficient IT operations appropriate to the complexity of the organisation. The overall risk assessment results should be a major factor in decision making in most IT management responsibility areas including:

- Technology budgeting, investment, and deployment decisions
- Contingency planning
- Policies and procedures
- Internal controls
- Staffing and expertise
- Insurance
- IT performance benchmarks
- Service levels for internal and outsourced IT services and
- Policy enforcement and compliance

Monitoring

Management and the board should monitor risk mitigation activities to ensure if identified objectives are complete or are in process. Monitoring should be ongoing, and departments should provide progress reports to management on a periodic basis. Ongoing monitoring further ensures that the risk assessment process is continuous instead of a one-time or annual event. Key elements of an effective monitoring program include:

- Mitigation or corrective action plans;
- Clear assignment of responsibilities and accountability, and
- Management report.

IT Controls Implementation
These guidelines are applicable to both in-house and external provider situations.

Policies, Standards, and Procedures

Management should adopt and enforce appropriate policies and procedures to manage technology risk. The effectiveness of these policies and procedures depends largely on whether they are used by internal staff and vendors. Testing compliance with these policies and procedures often helps to identify and correct problems before they become serious. Clearly written and frequently communicated policies can establish clear assignments of duties, help employees to coordinate and perform their tasks effectively and consistently, and aid in the training of new employees. Senior management should that ensure policies, procedures, and systems are current and well documented

Internal Controls

The institution should adopt adequate controls based on the degree of exposure and the potential risk of loss arising from the use of technology. Controls should include clear and measurable performance goals, the allocation of specific responsibilities for key project implementation, and independent mechanisms that will both measure risks and minimize excessive risk-taking. Management should re-evaluate these controls periodically.

Management practices associated with general controls include:

- Reporting effectiveness to the Board of Directors;
- Periodic review and updating of policies, standards, and practices;
- Regular review of internal and third party audit results;
- Review of service level agreements, and

- Review of control metrics including issues and corrective action plans.

Adequate internal controls should be structured to assure senior management that:

- Personnel create, transmit, and store records and transactions in a safe and sound manner;
- Adequate segregation of duties exists;
- MIS data are reliable and the reporting cycle is adequate;
- Necessary Quality Checks have been implemented;
- Operating procedures are efficient and effective;
- Procedures are in effect to assure continuity of business;
- The institution identifies and monitors high-risk conditions, functions, and activities, and
- There is proper adherence to management standards and policies, applicable laws and regulations, regulatory statements of policy, and other guidelines.

Independent audits can verify that these controls exist and are functioning effectively.

Personnel

All organisations should mitigate the risks posed by IT staff by performing appropriate background checks and screening of new employees. In addition to staff, the controls in this section are relevant for vendor personnel, consultants, and temporary staff that support the IT function. Typically, the minimum verification considerations include:

- Character references;
- Background checks including confirmations of prior experience, academic credentials, professional qualifications, or criminal records, and
- Confirmation of identity from government issued identification.

Insurance

In establishing an insurance program, management should recognise its exposure to loss, the extent to which insurance is available to cover potential losses, and the cost of such insurance. Insurance programs should be commensurate with the complexity and risk of each institution. Management should weigh these factors to determine how much risk the organisation will assume directly. In assessing the extent of that risk, institutions should analyse the effect of an uninsured loss on themselves and any affiliates or parent companies. Management should also review a company's financial condition and/or credit rating reviews when deciding on an insurance company. Once management has acquired appropriate insurance coverage, it should establish procedures to review and ensure its adequacy. These procedures should include, at a minimum, an annual program review by the board of directors

1.6 DISASTER MANAGEMENT

A disaster is defined as a sudden misfortune that is ruinous to an undertaking. This means that there is little time to react at the time of the misfortune. Preparations are required to have been made in advance. The focus should, therefore, be on disaster planning.

The first step in disaster planning is to **assess risk.** A computer or network disaster typically involves loss of or damage to data, the inability of programs to function, or the loss of data communication. Risk assessment answers the question, what is the probability a particular disaster to occur and how serious will be the effect likely to be if it does occur. Among the disasters that should be assessed are natural disasters such as floods, fires, and earthquakes and manmade disasters such as air conditioning failures, viruses, hacking, and vandalism. The line between the two is not clear-cut

because a flood can be the result of vandalism to a water pipe and a fire can be deliberately set as an act of vandalism.

A risk assessment matrix should be created, one which puts the probability on one axis and the effect on the other, with the risk factor fixed by the combination of the two factors:

Effect may be classified as Major, Moderate, and Minor. Probability of Risk may be classified as High 5 4 3 Moderate 4 3 2 and Low 3 2 1 on a 5 point scale.

A risk factor of 5 requires much more attention and warrants a much greater outlay of resources than a risk factor of 1.

The risk factor will vary by area of the country, nature of the community, and type of organisation. In much of California, earthquakes would be rated a risk factor of 5; along the flood plains of the Mississippi River flooding would be a risk factor of 5. Viruses, while probable, usually have only a minor effect, therefore, they would have a risk factor of 3. Hacking, this rates highly probably for Fortune 500 companies; rates low for smaller organisations, but may rate a risk factor of 3 because its effect may be major. In many areas floods are likely to be the result of a broken pipe and have a low risk factor of 1 or 2 because their effect tends to be localized and, therefore, minor or moderate.

The second step in disaster planning is **risk reduction**. This is achieved by lowering the risk factor by reducing the probability, reducing the effect, or both. For example, while no disaster plan can reduce the probability of an earthquake, housing the organisation in California that is quake-resistant should reduce the effect of one. Placing a computer room where there are no overhead pipes reduces the probability of flooding; rack-mounting the computer hardware so that it is several inches above the floor reduces the effect. Installing anti-virus software reduces the probability of a disaster; regularly backing up all data reduces the effect.

The third step in disaster planning is to earmark resources. Disaster planning need resources (takes time and expertise), but it is within the means of most organisations. A small task force of staff members, given time to read the literature and contact other organisations that have done disaster planning, can develop a disaster plan in weeks or months. What is difficult for many organisations is finding separate funds to carry out the plan. Retrofitting an old building to withstand earthquakes can cost hundreds-of-thousands or millions of dollars; mirroring a database of a large organisation can cost huge amount of money. Each risk factor must, therefore, have a price tag associated with it. An organisation has to decide whether the risk reduction is worth the price and, if so, seek the funds to pursue the risk reduction.

It may not be realistic to lower the highest risk factors first because the funds may not be available. It may be necessary to focus on lowering risk factors for which the resources are available. Heat/smoke and water detectors are within the means of most organisations and should not be skipped over just because the risk factor is not a 4 or 5.

The fourth step in disaster planning is to identify Common Disaster Plan Elements. Every disaster plan should set forth both preventive measures and remedies in at least the following areas:

Servers

Every organisation with one or more servers should have a server room that is secured with a combination lock such as a Simplex and a reinforced door with a deadbolt at least 1.5 inches long. If the room is not windowless, the windows should be barred. The room should have both fire/heat detection and water detection sensors which set

off a local alarm and send a signal to an off-premises monitoring facility. At a minimum, it should have fire extinguishers suitable for electrical fires. An organisation that has hundreds-of-thousands of dollars in equipment in its server room should consider a built-in fire suppression system.

Excess heat is, by far, the most commonly reported cause of server downtime and damage. An office should, therefore, augment its building air conditioning with a room-size air conditioner that kicks-in only when its thermostat shows that the temperature in the room has risen above a office specified level, typically 68 degrees. An additional safeguard is available, a thermostat inside any cabinet which has a cooling fan. When a fan fails and the temperature rises, an alarm should be triggered.

Water damage is the second-ranking cause of server downtime and damage, although the damage is rarely greater than moderate. There should be no water pipes in the ceiling above the room, or in the walls that enclose it. The server(s) and associated peripheral equipment should be rack-mounted so that up to six inches of standing water will not affect the equipment.

Power irregularities are the third-ranking cause of server downtime and damage. An UPS (uninterruptible power supply) should be used to protect all servers against surges, spikes, brownouts, and blackouts. The UPS should have a rating which is it least twice the total KVA requirements of the devices it protects. KVA (Kilo Volt Amperes) is a rating that is calculated by multiplying the number of volts by the number of amperes and dividing by 1,000. While a office may not want to operate its servers on battery back-up for an extended period, the UPS should provide power long enough for an orderly shutdown of all servers.

The database server should be protected by its own firewall, preferably a proxy-server between it and the Web server on which the patron access catalog is mounted. A proxy server shields the database server from direct access by initiating a separate inquiry, rather than passing the external inquiry through to the database server. The firewall can be on the same hardware platform as the database server. The Web server can support not only the patron access catalog, but also other files and a gateway to electronic resources outside the organisation. It should include remote patron authentication software so that access to other than records the organisation wishes to make available to everyone is limited to those who are authorized users.
Each server should be configured with a logging tape drive--typically a 4mm or 8mm streaming tape drive-- so that all information written to disk is also written to tape. Each evening the logging tape should be removed and stored away from the server room and a new tape mounted for database back-up. Overnight, the content of the disk drives should be written to tape. The next morning, the back-up tape should be removed and stored away from the server room and a new tape mounted for logging that day's transactions. It will then be possible to restore all files using the most recent back and logging tapes. Magnetic media can become unstable with repeated use, therefore, seven logging tapes--one for each day of the week--should be used. Seven back-up tapes should also be used. All of the tapes should be replaced at least every year.

An organisation may choose to do a back-up only once a week. If so, all of the logging tapes for the week should be saved so that they and the previous week's back-up tape can be used to restore the files. The logging tapes and the previous week's back-up tape should be stored away from the server room. In a large facility than may be at the opposite end of the building, but for smaller facilities it should be off-site.

At least once per week, a current back-up tape should be sent to an off-site storage facility to protect against the loss of the on-site back-up tape.

Organisations that can afford RAID (Reduced Array of Inexpensive Disks) should configure their servers with them. RAID technology mirrors everything written to one

disk on another disk. If a disk fails, the mirroring disk provides access to the information without resorting to the rebuilding of files from the combination of back-up and logging tapes.

Network

An organisation can do a great deal to secure a LAN (local area network), but only a limited amount to secure a WAN (wide area network). The former usually is limited to a single building or part of a building; the latter usually ties two or more LANs together using a telco or other common carrier's circuits. The telco or common carrier has the responsibility for its portion of the WAN. Wan should be protected there appropriate firewalls.

The preferred LAN topology is a hybrid star, one that has several central star network points linked in a star. In other words, several desktop clients are connected to a hub, and several hubs are connected to yet another hub. The cabling from the desktop clients to the hubs can be relatively inexpensive Category 5 UTP (unshielded twisted pair); the wiring among hubs should be STP (shielded twisted pair) or fiber optic to dramatically improve performance and security.

Network hardware should be secured in locked data communications closets or cabinets. All data jacks should be capable of being de-activated when no office equipment is connected to them. The practice of distributing a large number of data jacks around a building for use by patrons with laptops should be avoided unless these jacks are on a separate LAN segment that can be isolated from the database server of the automated office system. Patrons need access only to the patron access catalog, and possibly to other servers: Web, Internet, CD-ROM, image, etc.

If a wireless LAN is implemented, it should access only a segment of the office’s LAN, one that can be isolated from the database server of the automated office system.

The most vulnerable part of a office's network is the connection to the Internet, both access from the Internet to its servers and from its servers and clients to the Internet. Fortunately, it is cost effective to protect a office's database server with its own firewall so that there is protection against in-office users, as well as external users. More vulnerable are the other servers and the clients or desktop workstations. Most offices seek to protect them only from users outside the office. This can be done by installing a network firewall. The firewall can be configured not only to restrict access to specific categories of users or specific types of queries, but can also be configured to facilitate access to office-selected resources.

Clients

PCs and Macs are the most vulnerable technology in offices because they can be compromised by staff and patrons who behave unwisely by downloading attachments or bringing in software and data disks from outside the office. Viruses are the greatest threat. An Anti-virus software is absolutely essential. Products from companies such as McAfee and Norton detect computer virus signatures and alert the user to them before they enter the client; however, anti- virus products are of little value if they are not regularly updated. Literally hundreds of new viruses are unleashed every week, therefore, anti-virus software should be updated at least weekly by downloading the latest version.

Almost all viruses travel via e-mail attachments or diskettes. Staff should, therefore, be instructed not to open an attachment if the source of the e-mail is not known or the attachment is not expected. They should be particularly suspicious of attachments with strange-sounding titles. When in doubt, the sender should be asked by return e-mail to describe the contents of the attachment. Staff should be instructed not to bring

software from home for loading on office machines, nor to carry diskettes back and forth between home and work machines.

The fifth step in disaster planning is to establish Recovery Procedures. It is important to state in the disaster plan not only what recovery procedures are to be followed if a disaster occurs, but also who has what responsibility. Who calls whom and what information should they be prepared to give? Who performs the needed diagnostics? Who restores the files? What are the instructions for packing and shipping the corrupted files?

Communication is of great importance during a disaster. It should not be assumed that regular telephone service will be available. Key personnel should have cell phones for use when regular telephone service fails or is overloaded. The cell phone in the server room should be stored in a wall-hung watertight cabinet on the wall adjacent to the entrance door. The instructions for dealing with a computer/network disaster should be stored in the same cabinet. All important telephone numbers should be stored in each cell phone. If a disaster affects more than the office, the cellular service may be swamped with calls. It is, therefore, a good idea to instruct the operator in the server room to use the redial and speaker features of the regular telephone while seeking to get through on the cell phone.

A designated operator for each hour the office is open is a good practice. This may be a member of the circulation desk's support staff ,the staff which usually is in the office all of the hours the office is open. The designated person would perform the end-of-day swap of the logging and back-up tapes as part of his/her routine duties. Otherwise, s/he would leave her/his regular duties only when there was a problem.

The designated operator on duty at the time of a disaster should have instructions to call the support desks for the servers that have been affected. The numbers should be encoded in both the server room's telephone and the cell phone that has been provided as a back-up.

Each designated operator should participate in an occasional disaster drill that simulates an actual disaster that affects one or more servers.

Designated manager to support the designated operator who may encounter a situation that overwhelms him/he should also be considered. There should always be a designated manager in the office or available by telephone 24 hours per day, seven days per week. While there may rarely be a need to decide about evacuation of the office or another major action, the capacity to do so must be in place.

An external resource is the vendor of an automated office system is an important resource in diagnosing problems that result from a disaster. When drawing the contract, make it clear that the vendor shall be liable not only for the performance of the central site and its client software, but it shall undertake remote diagnostics through the network to the desktop. In other words, it shall pinpoint a problem regardless of where it is. If coverage has not been purchased for 24 hours a day and seven days a week, there should be provision for emergency support at agreed upon hourly rates outside the normal coverage hours.

If the database server for the automated office system is affected by a disaster, the vendor's trouble desk should be called so that remote diagnostics can be performed and guidance can be obtained. If the vendor of the automated office system is not responsible for the management of hardware maintenance, hardware problems should be referred to the manufacturer's support desk.

Sources of support for all other servers should be identified and their telephone numbers must be encoded in the server room's telephone and in the cell phone that have been provided for back- up.

Most offices do not have the luxury of a network specialist. A office should, therefore, rely on the networking staff of a parent organisation or consider contracting with a network support service for remote diagnostics and recovery assistance. While these firms are found in most major cities, a regional or national firm with experience in automated office systems should be considered.

One or more data recovery firms should be identified. These firms recover data from hard drives, diskettes, or any other storage medium that has been damaged by flood, fire, physical impact, or a virus. A large national firm usually is able to accommodate a rush order better than a smaller local one.

Insurance coverage for disaster is part of the insurance plan by larger organisations. The office should carry insurance that includes coverage for its servers, network, and clients. In order to make claims, it is essential to have an absolutely current inventory of all hardware and software, including purchase data and price. A copy of this information should be stored at a remote site.

In case of damage that is visible, photographs should be taken promptly after the disaster to substantiate an insurance claim.

1.7 PORTFOLIO MANAGEMENT ISSUES AND CHALLENGES

In implementation of a portfolio management application, there are many successes associated with it, there are many lessons learned also. Issues and challenges which need to be understood are:

1) **Portfolio Management system acceptance**

Since true success of portfolio management system lies in active involvement of all concerned, it is important that the system's benefit are recognized and appreciated by them. The application champion (business side and application administrator) for this purpose may find themselves constantly 'selling the benefit' of the tool. They may need to become evangelist for portfolio management and have the stick-to-it-ness to weather the storm. Resistance may be strong and critics will most likely outnumber advocates. They will need to continually prove the value of the application and its data. This is not easy, it is not pretty, and it will become frustrating. This may also require doing some behind the scenes magic to prove that the application has value.

There will also be a significant training and learning curve. Even if the organisation is mature in its artifacts, processes, methodology, and terminology, there will be a new means of recording and reporting it.

2) **Real Time Readiness**

In the past, a project manager had control over when information about the project was shared and available for all members of the project team and for executives. The project manager could masks blemishes and possible lapses by controlling when information was shared. For example, if the project manager led a project status call every other Thursday, they could possibly wait until Wednesday night to update their issues report. If an issue was due a week before, the report might not get updated until before the review. Now with a portfolio management system, the day the issue becomes past due it can be flagged in reports. The PM might now have to do daily management of the issues.

3) **Conformity to override Flexibility**

One of the benefits of a portfolio management system is the ability to track information consistently across projects. Latest maturity models call for consistency across the organisation. A portfolio manager enforces conformity and an individual PM will loose some of the flexibility they have in tracking and reporting project status. For example using issues again, a PM might want to have a way to indicate an issue is resolved prior to being closed. This way they could have a report that shows issues 'resolved' and ready to go off the list. Another project manager may be more of the mindset that it goes straight to closed. People can refer to a closed issues report to see what's been closed in the past week. While we can not say which method is better, a portfolio management issues workflow will force the process. If a program manager wants to have consistency in reporting of all projects across the portfolio, an individual will need to sacrifice some of their individual style to conform to the portfolio work flow.

4) **System to be for the Users**

As you take project management from desktop applications and non-integrated artifacts, you have risen to the level of application management. With application management, comes the entire cycle of enhancement requests, workflow requests, and even field names. A PM might not get the feature he/she wants – or may have to compromise.

5) **Requirement of an Application Administrator**

First thing to do when implementing a portfolio management system is to appoint an application administrator and an application change control process. We need to budget a person's time into the care and feeding of this application. There is no rule of thumb regarding how many Full Time Equivalents (FTE's) are required for application administration, but it will have a direct relationship to the organisational maturity, the business process maturity, and the breadth of the audience. In one of the organisation where PM was implemented, workgroups was brought onto the Portfolio Management Application involved new people, new business model, Beta applications, and new customers. This group ended up with an application administration team that looked at the business request and two trained administrators that did the physical administration (defining views, reports, filters, adding users, creating work flows etc.) There were also two team members who looked at templates and business needs and helped set priorities with the application administrators. Application administration is a different responsibility than a system administrator or a data base administration. An application administrator needs a strong skill set balanced between knowledge of project management principles and methodologies, knowledge of the business, and technical knowledge of data bases, SQL, report writing, and trouble shooting. A system administrator focuses on making sure the operating system and the hardware work, the application administrator makes sure the application meets the business need. The organisation may head for failure if it is thought that a system administrator can provide the business needs fulfilled by an application administrator. Finally, there will be changes and churn on the application. It is going to need someone to manage those, train the users on changes, and prioritise the work. We can imagine many organisations under estimate the care and feeding needed to keep an application viable.

6) **Making it business management application requires sincere efforts by all**

Everybody has the best of intentions, but taking care of the low level minutiae that makes up a portfolio management system is cumbersome, time consuming, and some people may see it of little value. A basic premise of a portfolio application is that executive levels of information can flash from multiple projects at one time. However, to get that executive level, the lowest of details must be there and many project managers will not put it in, unless they are hounded to put it in, or they are 'punished' if they don't. Excellence is a mindset and the middle manager must

maintain vigilance to insure compliance. There's an entirely integrated thread with this thought and that involves cross-organisational compliance so the portfolio management tool transcends a project management application and becomes a business management application. The impact, both cultural and technical, aspects of this concept are way to deep to cover in this thinking

7) **Reports grow exponentially if not reasoned out**

Input is one aspect of an application, output is another and there is an exponential demand for output. The main outcome of a well organised report is that there is always tendency to request for a new report or the same report with a 'slight modification'. We feel there is a way to stop this. The requests will continue to flow in and unless and until you reason out the and bring out new report only when there is genuine need for the same. However, it is difficult task to make people agree.

8) **People will Blame the System for their Own Lapses**

It is a rule of human nature. People will blame the system to hide their own insecurities and lack of knowledge. No matter what system is created, it will have its own set of idiosyncrasies and there will be some things the application will require that make no sense at all, but the application requires it. Be thick skinned and prepared for people to blame the system for their problems.

9) **Mental block**

No matter how much you train, hand hold, and evangelize, some people just won't get the idea of project rolling up to program, rolling up to portfolio. You may encounter resistance as to why do I need to do it this way? Portfolio management is a completely different perspective and does require a certain amount of abstract visualizing (is there any other type?) – some people who are Great silo-based project managers, will just not get the inter-dependencies of projects within a portfolio management system. While work with these people, one be careful and understanding, the odds are that they want to do well, and they have a wealth of knowledge and experience, but they have a mental block.

10) **Customisation efforts increase with time**

Every salesman who pushes a portfolio management system touts its flexibility and the capability to customize the system to meet your business need. Most give you the capability to add custom fields and create your own reports, but as stated earlier the demand for various outputs never ceases. In the infancy of the system you will be able to quickly add a custom field to meet a need, but after months of customization here and there, the ripple effect can be enormous.

1.8 TOOLS AND TECHNIQUES

The portfolio management tool market is growing: There are large numbers of vendors who are offering Portfolio Management Tools. Each vendor talks about the salient features of his tools and offers a variant method for the Portfolio. However, each vendor is offering automation of Portfolio process to some degree. Coordinating information across this portfolio management domain itself dictates a number of key product features that one should look for when considering a tool to assist with automating the portfolio management process. Three key requirements include:

- **Common repository**. A single data repository that each group will access for reporting will be a requirement for an organisation moving to full IT portfolio management. Multiple groups, each using separate tools and repositories, will quickly lead to inaccuracy and conflicts as data becomes out of sync.

- **Direct data collection and interchange**. Data should enter the portfolio management tools directly and without manual input. Requiring project managers to enter information for each project will also quickly lead to data corruption or omissions. Resource utilisation and project information should be gathered directly from project management systems and spending data fed into the system directly from financial management tools.

- **Configurable data views and portals:** Each user of the tool will have different requirements. When considering a portfolio tool, make sure that the interface is configurable for each user constituency, centralising common tasks and reports, and allowing for the addition of reports and functions as the portfolio management process grows, matures, and expands.

Given below is a **list of some of the major Commercial Portfolio Management tools** along with their vendor's name. A brief writ-up on the salient features of the tools offered by them is also given.

- **Business Engine Network by Business Engine Corp:** It is strongest in professional services automation, relies heavily on Microsoft Project for project management functions, offers good support for the IT budgeting process across multiple currencies. However, it could do a better job with opportunity management, particularly in the area of time and resource management.

- **The Edge for IT Pacific Edge by Software Inc:** It is strong in cost estimating, portfolio analysis, scenario planning and resource allocation, and has good reporting capabilities with Microsoft Project. It includes its own project and resource management tools. However, weak in terms of mapping internal workflow processes with the software. But the product allows an organisation to modify its work processes as they mature with its internal IT portfolio management methodologies.

- Legadero cadence Portfolios by Legadero Software provides everything you need to get a handle on all of your projects. This includes true Portfolio Management via approval process automation, information collection, metric-building and graphical decision support analyses and dashboards. All solutions are easy to evaluate, implement and learn.

- **MaestroTec (MaestroTec, Inc.):** By Maestro-EPM is a web-based solution that helps you manage project portfolios, resources, assets, work flow, and time and expenses.

- PlanView by PlanView Portfolio Management is a rich, integrated Web-native solution that helps organisations manage portfolios, projects, and resources. It is flexible enough to support the needs of small, medium, and large organisational models.

- **PortfolioDirector by Artemis International Solutions Corp:** Strong integration with Microsoft Project client, it has excellent user interface, and good time tracking and reporting and graph-generation capabilities. However, the standard product doesn't support calculation fields, making it tough to estimate overall resource requirements, such as the people, time and money needed for a project. An optional module adds this function.

- **PMOffice (Systemcorp):** This product is an Enterprise Project Portfolio Management solution that automates all your projects, people and priorities across the entire organisation. Companies can organize all projects into portfolios, and instantly track all project deliverables, budgets, tasks, changes, risks and issues from one central location.

- **Portfolio Management Solutions (Pacific Edge Software):** Pacific Edge solutions focus on three key areas of Enterprise Portfolio Management - IT, NPD, and Business Investment Portfolio Management, and allows for a multitude of investment types to be managed within each of these portfolios, such as: assets/applications, projects, products, and resources.

- **Project Activator:** Project Activator is a completely web based portfolio and project management software solution. It tracks active, pending, on hold and completed projects, completes document management, collaboration, project scheduling, resource allocation, budgeting, time tracking with internal and external customers. It has completely secure, Java and XML architecture. The Catalogue feature allows separation of projects by discipline, division, customer, project type.

- **Project InVision (Project InVision):** Project InVision software automates the essential business processes of portfolio analysis and project management.

- **Project Office:** Pacific Edge Softwares product, Project Office, provides a simple, painless way to manage project and resource information across an organisation and provides seamless integration to Microsoft Project for detailed planning and scheduling.

- **ProSight Portfolios Posited Inc:** Interoperates with other products such as Business Engine and its professional services automation capabilities. However, ProSight is more of a portfolio analysis tool than a portfolio management tool.

- **ProSight:** Only top-down portfolio management can deliver immediate value to your organisation. Using prosight portfolio management software, you can realized rapid buy-in and participation from executives and delivered immediate, tangible results—all without replacing existing software or processes. Best of all, ProSight's unique approach guarantees that any organisation can start managing any portfolio, immediately.

- **StatFrames Software Suite United Management Technologies Corp:** Strong in IT portfolio analysis and program management arenas, UMT is moving into portfolio management. StatFrames can identify internal processes. However, lacks asset management capabilities

- **TeamHeadquarters (Entry Software):** This product is a collaborative, browser-based software application combining project portfolio management (PPM), document management and helpdesk in one seamless application. This combination enables workgroups to manage all planned and unplanned initiatives from one integrated environment.

- **UMT:** Portfolio Management Solutions (UMT)- UMT software and consulting leverage 14 years of portfolio management expertise with Global 500 companies to align IT investments with quantifiable business drivers and justify IT spend. Enterprise solutions incorporate Efficient Frontier modeling to determine the optimal mix of initiatives, budget allocation, and skilled resources, while maximizing value and ensuring IT Portfolios execute business strategy.

1.9 EMERGING TECHNOLOGIES

In the Emerging Technologies three key technology themes (as per Gartner) are expected to be having significant growth and need to be watched: (a) Technologies that will enable the development of Collaboration, (b) Next Generation Architecture, and, (c) Real World Web.

a) **Collaboration**

A number of key collaboration technologies designed to improve productivity and ultimately transform business practices are:

- **Podcasting:** Podcasting offers a way to 'subscribe' to radio programmes and have them delivered to your PC. It is predicted that podcasting subscriptions will grow increasingly important as the market for content continues to fragment, which will lead to a massive shift in radio, and ultimately TV content delivery. Podcasting is an extremely efficient method for delivering audio and spoken-word content to niche audiences and as such could become an important corporate communications tool.

- **Peer to Peer (P2P) voice over IP (VoIP):** Vendor-proprietary P2P VoIP applications are under development although security concerns still need to be addressed. Services like Skype currently enjoy significant consumer adoption and are beginning to make inroads into the business landscape. It is predicted that the technology will be important for collaborative and multimedia applications as well as low-cost communications.

- **Desktop Search:** Also known as personal knowledge search, this is an individual productivity application, residing on the desktop and using local processing power to provide search-and-retrieve functionality for the desktop resident's local e-mail, data store and documents. Google, Microsoft and Yahoo are competing for customer attention, adding to the hype but customers not exhibiting much interest in buying solutions. However desktop search will become a standard feature in Microsoft Longhorn, currently planned for 2006 and should reduce content recreation, increase content reuse whilst raising productivity.

- **Really Simple Syndication (RSS):** RSS is a simple data format that enables web sites to inform subscribers of new content and distribute content more efficiently by bypassing the browser via RSS reader software. RSS is widely used for syndicating weblog content but its corporate use is only starting to be tapped for activities such as corporate messaging. Its simplicity makes it easy to implement and add to established software systems. It is predicted that RSS will be most useful for content that is 'nice to know' rather than 'need to know'.

- **Corporate Blogging:** This involves the use of online personal journals by corporate employees, either individually or in a group, to further company goals. It reached the peak of hype in 2004 although mainstream firms have not yet got involved. Its impact will be on projecting corporate marketing messages primarily and secondarily in competitive intelligence, customer support and recruiting.

- **Wikis:** A simple, text-based collaborative system for managing hyperlinked collections of web pages; it usually enables users to change pages or comments created by other users. Wikis are becoming available from commercial vendors, in addition to many open-sourced products, but not yet from established enterprise vendors. However, they are widely used as

collaborative, distributed authoring systems for online communities, especially those using open-source projects. It is predicted that Wikis will impact ad hoc collaboration, group authoring, content management, web site management, innovation, project execution and research and development.

b) **Next Generation Architecture**

Next generation architecture will constitute the third big era in the IT industry's history (the first having been the hardware era and second belonging to software). These emerging technologies will form key pillars of the new architecture:

- **Service Oriented Architecture (SOA):** SOA uses interactive business components designed to be meaningful, usable and useful across application or enterprise boundaries. Despite the current disillusionment with SOA, it is expected support for SOA to grow and for it to mature as a technology within ten years although many changes in user and vendor organisations and technologies are required before SOA reaches its full potential. However, in the longer term, it is believed that SOA has the potential to be transformational to a business.

- **Web Services-Enabled Business Models:** These productivity-boosting models represent a new approach to doing business among enterprises and consumers that would not have been possible without the benefits of web-services. However enterprises are still wrestling with what web services will do and it is expected that the potentially transformational impact of Web Services-Enabled Business Models will have to wait for more-mature standards and clearer examples.

- **Extensible Business Reporting Language (XBRL):** This is an Extensible-Markup-Language-defined standard for analyzing, exchanging and reporting financial information. XBRL helps organisations meet multiple financial reporting needs through a single instance of financial data. It also improves the timeliness and accuracy of financial and regulatory reporting, validation and distribution. XBRL enables integration, aggregation, validation and comparison of financial data. It also automates sourcing and the review of financial data for activities such as loan acceptances, investment portfolio management and risk reviews. Financial accounting software vendors are already incorporating XBRL while regulatory and transparency pressures increase the significance and likelihood of XBRL adoption. However, there have been setbacks in XBRL adoption in the past year; the most significant have been delays in the FDIC and FSA projects that will mandate XBRL reporting.

- **Business Process Platforms (BPP):** BBP provide business process flexibility and adaptability. They use SOA design principles and are metadata and model driven. It is believed that Business Process Platforms will enable business process fusion and move innovation from business application vendors to BPP ecosystems. Ultimately they will replace customized business applications and custom development by extending core applications platforms with composite applications.

c) **Real World Web**

It is believed that adding networking, sensing and processing to real-world objects and places is creating a 'Real-World-Web' of information that will enhance business and personal decision-making:

- **Location-aware applications:** These are mobile enterprise applications that exploit the geographical position of a mobile worker or an asset, mainly

through satellite positioning technologies like Global Positioning System (GPS) or through location technologies in the cellular network and mobile devices. Real-world examples include fleet management applications with mapping navigation and routing functionalities, government inspections and integration with geographic information system applications. Mobile workers will use either a PDA or smart phone, connected via Bluetooth to an external GPS receiver, or stand-alone positioning wireless device.

- **Radio Frequency Identification:** Otherwise known as RFID, passive Radio Frequency Identification has been somewhat over hyped in recent years although vehicle-based systems are strong. It involves the tagging of very small chips to arbitrary types of objects. These chips transform the energy of radio signals into electricity then respond by sending back information that is stored on the chip. The most conducive environments for passive RFID are chaotic or unstructured business processes where RFID's ability to read without a direct line of sight gives it the edge over traditional bar-coding methods. These might include such diverse activities as manufacturing, healthcare, logistics, animal tracking and laundry automation.

- **Mesh Networks — Sensor:** Mesh Networks are ad hoc networks formed by dynamic meshes of peer nodes, each of which includes simple networking, computing and sensing capabilities. Potential impact areas include low-cost industrial sensing and networking, low-cost zero management networking, resilient networking, military sensing, product tagging and building automation.

Check Your Progress 2

1) State True or False:

a) Risk factor is worked out by combination of (a) probability of risk and (b) effect of risk. True ☐ False ☐

b) In disaster recovery plan, communication, designated operator, designated manager and external resources likely to be needed must be listed and kept updated. True ☐ False ☐

c) Portfolio management technique is a tool in which only top management is involved. True ☐ False ☐

d) For automating the portfolio management process, the key tools to be looked for are: Common repository, Direct data collection and interchange and configurable data views and portals**.** True ☐ False ☐

e) For implementing a portfolio management system appointment of an application administrator does not help if system administrator is already in place. True ☐ False ☐

2) Answer the Following Questions:

a) What are the steps involved in IT Risk Management Process?

……
……
…….

b) What are the steps involved in planning for Disaster Management?

……
……
……

1.10 SUMMARY

In this unit, we have discussed practically all aspects of the portfolio management. We have covered starting from what is portfolio management to its techniques, methods, tools, issues relating to it and its implementation procedure. This is one of the most acceptable procedure for evaluation of software projects these days. It is suggested that this study may be further supplemented by completing case studies on this topic.

Another very important area covered in this unit is risk assessment and preparation for the disaster management as well as recovery from the disaster. With the growing dependence on information systems, preparedness for any eventuality is definitely a wise thing. It is a matter of concern that after the tragedy so many people and authorities talk about it but eventually keep on hanging on it till next tragedy happens. So let us look forward not to this mistake and prepare for it.

Emerging technologies discussed in this unit are basically for motivating all students to cultivate the habit of looking around the Internet and other places to keep abreast to the trend.

1.11 SOLUTIONS / ANSWERS

Check Your Progress 1

1) True or False

(a) False, (b) True, (c) False, (d) True, (e) True.

2) Answers / solutions

(a) The key functional requirements which must be available in the Portfolio Management Solution are:

Budget and Financial Management:

i) Business Planning and Portfolio Management,
ii) Project and Resource Management,
iii) Collaboration and Knowledge Management.

(b) The steps for portfolio management implementation are:

i) Gather all ongoing / planned Projects list with necessary details,
ii) Evaluate: Identify Projects That Match Strategic Objectives,
iii) Prioritize and Categorize Projects,
iv) Review: select the Portfolio and implement it.

Check Your Progress 2

1) True or False

(a) True, (b) True, (c) False (d) True (e) False.

2) Answers / Solutions.

(a) The steps involved in IT Risk Management Process are:
i) *plan* use of technology,
ii) *assess* the risk associated with the selected technology,
iii) decide how to *implement* the selected technology, and
iv) establish a process to *measure and monitor* risk.

(b) The steps involved in planning for Disaster Management are:
   i) assess risk,
   ii) find options which have lower risk levels / risk reduction,
   iii) identify Common Disaster Plan Elements,
   iv) establish Recovery Procedures.

1.12 FURTHER READINGS/REFERENCES

1 J. O'Brian. Management Information Systems: *Managing Information Technology in the Networked Enterprise (3rd Ed)*, Irwin, 1996.

2 Robert Schultheis & Mary Sumner, *Management Information Systems: The Manager's View*, Tata McGraw Hill

3 Sadagopan S., *Management Information Systems*, Prentice Hall of India.

4 Basandra S.K., *Management Information Systems*, Wheeler Publishing.

5 Alter S., *Information Systems: A Management Perspective*, 3/e, Addison Wesley.

6 http://www-users.cs.york.ac.uk/~kimble/teaching/mis/mis_links.html.

7 http://www.scs.leeds.ac.uk/ukais/Newsletters/vol3no4.html#Definition.

8 http://members.tripod.com/michaelgellis/tutorial.html.