

CH 3: Information System Concepts

3.7.1 Top Management and Information Systems Management Controls

The controls adapted by the management of an enterprise are to ensure that the information systems function correctly and they meet the strategic business objectives. The management has the responsibility to determine whether the controls that the enterprise system has put in place are sufficient to ensure that the IT activities are adequately controlled. The scope of control here includes framing high level IT policies, procedures and standards on a holistic view and in establishing a sound internal controls framework within the organization. The high level policies establish a framework on which the controls for lower hierarchy of the enterprise. The controls flow from the top of an organization to down; the responsibility still lies with the senior management. **Top management is responsible for preparing a master plan for the information systems function.** The senior managers who take responsibility for IS function in an organization face many challenges. The major functions that a senior manager must perform are as follows:

- (a) **Planning** – This includes determining the goals of the information systems function and the means of achieving these goals.
- **Preparing the plan: This involves the following tasks:**
 - **Recognizing opportunities and problems that confront the organization in which Information technology and Information systems can be applied cost effectively;**
 - **Identifying the resources needed to provide the required information technology and information systems; and**
 - **Formulating strategies and tactics for acquiring the needed resources.**
 - **Types of Plans:** Top management must prepare two types of information systems plans for the information systems function: a **Strategic plan** and an **Operational plan**. Both the plans need to be reviewed regularly and updated as the need arises. The planning depends upon factors such as the importance of existing systems, the importance of proposed information systems, and the extent to which IT has been integrated into daily operations.
 - **Strategic Plan: The Strategic Plan is the long-run plan covering, say, the next three to five years of operations;**
 - **Operation Plan: It is the short-plan covering, say, next one to three years of operations.**
 - **Role of a Steering Committee:** The steering committee shall comprise of representatives from all areas of the business, and IT personnel. The committee would be responsible for the overall direction of IT. **The ultimate responsibility for information systems planning should be vested in an information systems steering committee. The steering committee should assume overall responsibility for the activities of the information systems function.** Here the responsibility lies beyond just the accounting and financial systems; for example,

the telecommunications system (phone lines, video-conferencing) office automation, and manufacturing processing systems.

- (b) **Organizing** – There should be a prescribed IT organizational structure with documented roles and responsibilities and agreed job descriptions. This includes gathering, allocating, and coordinating the resources needed to accomplish the goals that are established during Planning function.
- **Resourcing the Information Systems Function:** *A major responsibility of top management is to acquire the resources needed to accomplish the goals and objectives set out in the information systems plan. These resources include hardware, software, personnel, finances and facilities. Adequate funding should be provided to support the acquisition and development of resources when and where they are needed. Further, Auditors should question whether top managers have a good understanding of the role the information systems function should play in their organization.*
 - **Staffing the Information systems Function:** *Staffing the Information systems function involves three major activities - Acquisition of information systems personnel, Development of information systems personnel; and Termination of information systems personnel.*
- (c) **Leading** – This includes motivating, guiding, and communicating with personnel. **The purpose of leading is to achieve the harmony of objectives; i.e. a person's or group's objectives must not conflict with the organization's objectives. The process of leading requires managers to motivate subordinates, direct them and communicate with them.**
- **Motivating and Leading Information Systems Personnel:** *Though many theories exist, however there is no one best way of motivating and guiding all people and thus the strategies for motivating/leading people need to change depending upon particular characteristics of an individual person and his/her environment.*
 - **Communicating with IS Personnel:** *Effective communications are also essential to promoting good relationships and a sense of trust among work colleagues. For example - Due to failure in understanding the directions given by the top management, a serious error is made in the system design; the effect of which is for long-term.*
- (d) **Controlling** – This includes comparing actual performance with planned performance as a basis for taking any corrective actions that are needed. **This involves determining when the actual activities of the information system's functions deviate from the planned activities.**
- **Overall Control of IS function:** *When top managers seek to exercise overall control of the information systems function, two questions arise:*

- *How much the organization should be spending on the information systems function?*
- *Is the organization getting value for the money from its information systems function?*
- **Control of Information System Activities:** *Top managers should seek to control the activities on the basis of Policies and Procedures; where Policies provide broad, general guidelines for behavior whereas Standards provide specific guidelines for behavior. New and existing staff must be made aware of the policies and procedures that govern their work.*
- **Control over Information System Services:** *For each service level, estimates must be made of the expected benefits and resource consumption and finally the review committee must establish priorities.*

3.7.2 Systems Development Management Controls

Systems Development Management has responsibility for the functions concerned with analyzing, designing, building, implementing, and maintaining information systems. System development controls are targeted to ensure that proper documentations and authorizations are available for each phase of the system development process. It includes controls at controlling new system development activities. The six activities discussed below deal with system development controls in IT setup. These are given as follows:

- **System Authorization Activities:** All systems must be properly authorized to ensure their economic justification and feasibility. As with any transaction, system's authorization should be formal. This requires that each new system request be submitted in written form by users to systems professionals who have both the expertise and authority to evaluate and approve (or reject) the request.
- **User Specification Activities:** Users must be actively involved in the systems development process. User involvement should not be ignored because of a high degree of technical complexity in the system. Regardless of the technology involved, the user can create a detailed written description of the logical needs that must be satisfied by the system. The creation of a user specification document often involves the joint efforts of the user and systems professionals. However, it is most important that this document remains a statement of user needs. It should describe the user's view of the problem, not that of the systems professionals.
- **Technical Design Activities:** The technical design activities in the SDLC translate the user specifications into a set of detailed technical specifications of a system that meets the user's needs. The scope of these activities includes systems analysis, general systems design, feasibility analysis, and detailed systems design. The adequacy of these activities is measured by the quality of the documentation that emerges from each phase. Documentation is both a control and evidence of control and is critical to the system's long term success.

Control	<p>The Control phase has two major purposes:</p> <ul style="list-style-type: none"> • Task progress in various software life-cycle phases should be monitored against plan and corrective action should be taken in case of any deviations. • Control over software development, acquisition, and implantation tasks should be exercised to ensure software released for production use is authentic, accurate, and complete.
Design	A systematic approach to program design, such as any of the structured design approaches or object-oriented design is adopted.
Coding	Programmers must choose a module implementation and integration strategy (like Top-down, Bottom-up and Threads approach), a coding strategy (that follows the percepts of structured programming), and a documentation strategy (to ensure program code is easily readable and understandable).
Testing	<p>Three types of testing can be undertaken:</p> <ul style="list-style-type: none"> • Unit Testing – which focuses on individual program modules; • Integration Testing – Which focuses in groups of program modules; and • Whole-of-Program Testing – which focuses on whole program. <p>These tests are to ensure that a developed or acquired program achieves its specified requirements.</p>
Operation and Maintenance	<p>Management establishes formal mechanisms to monitor the status of operational programs so maintenance needs can be identified on a timely basis. Three types of maintenance can be used are as follows:</p> <ul style="list-style-type: none"> • Repair Maintenance – in which program errors are corrected; • Adaptive Maintenance – in which the program is modified to meet changing user requirements; and • Perfective Maintenance - in which the program is tuned to decrease the resource consumption.

3.7.4 Data Resource Management Controls

Many organizations now recognize that data is a critical resource that must be managed properly and therefore, accordingly, centralized planning and control are implemented. For data to be managed; better users must be able to share data; data must be available to users when it is needed, in the location where it is needed, and in the form in which it is needed. Further it must be possible to modify data fairly easily and the integrity of the data be preserved. If data repository system is used properly, it can enhance data and application system reliability. It must be controlled carefully, however, because the consequences are serious if the data definition is compromised or destroyed. Careful control should be exercised over the roles by appointing senior, trustworthy persons, separating duties to the extent possible and maintaining and monitoring logs of the data administrator's and database administrator's activities.

The control activities involved in maintaining the integrity of the database is as under:

- (a) **Definition Controls:** *These controls are placed to ensure that the database always corresponds and comply with its definition standards.*
- (b) **Existence/Backup Controls:** *These ensure the existence of the database by establishing backup and recovery procedures.* Backup refers to making copies of the data so that these additional copies may be used to restore the original data after a data loss. Backup controls ensure the availability of system in the event of data loss due to unauthorized access, equipment failure or physical disaster; the organization can retrieve its files and databases. Various backup strategies are given as follows:
- **Dual recording of data:** Under this strategy, two complete copies of the database are maintained. The databases are concurrently updated.
 - **Periodic dumping of data:** This strategy involves taking a periodic dump of all or part of the database onto some backup storage medium – magnetic tape, removable disk, Optical disk etc. The dump may be scheduled.
 - **Logging input transactions:** This involves logging the input data transactions which cause changes to the database. Normally, this works in conjunction with a periodic dump.
 - **Logging changes to the data:** This involves copying a record each time it is changed by an update action.
- (c) **Access Controls:** Access controls are designed to prevent unauthorized individual from viewing, retrieving, computing or destroying the entity's data. Controls are established in the following manner:
- User Access Controls through passwords, tokens and biometric Controls; and
 - Data Encryption: Keeping the data in database in encrypted form.
- (d) **Update Controls:** *These controls restrict update of the database to authorized users in two ways:*
- *By permitting only addition of data to the database; and*
 - *Allowing users to change or delete existing data.*
- (e) **Concurrency Controls:** *These controls provide solutions, agreed-upon schedules and strategies to overcome the data integrity problems that may arise when two update processes access the same data item at the same time.*
- (f) **Quality Controls:** *These controls ensure the accuracy, completeness, and consistency of data maintained in the database. This may include traditional measures such as program validation of input data and batch controls over data in transit through the organization.*

3.7.5 Quality Assurance Management Controls

Quality Assurance management is concerned with ensuring that the –

- *Information systems produced by the information systems function achieve certain quality goals; and*
- *Development, implementation, operation and maintenance of Information systems comply with a set of quality standards.*

The reasons for the emergence of Quality assurance in many organizations are as follows:

- *Organizations are increasingly producing safety-critical systems and users are becoming more demanding in terms of the quality of the software they employ to undertake their work.*
- *Organizations are undertaking more ambitious projects when they build software.*
- *Users are becoming more demanding in terms of their expectations about the quality of software they employ to undertake their work,*
- *Organizations are becoming more concerned about their liabilities if they produce and sell defective software.*
- *Poor quality control over the production, implementation, operation, and maintenance of software can be costly in terms of missed deadlines, dissatisfied users and customer, lower morale among IS staff, higher maintenance and strategic projects that must be abandoned.*
- *Improving the quality of Information Systems is a part of a worldwide trend among organizations to improve the quality of the goods and services they sell.*

Quality Assurance (QA) personnel should work to improve the quality of information systems produced, implemented, operated, and maintained in an organization. They perform a monitoring role for management to ensure that –

- *Quality goals are established and understood clearly by all stakeholders; and*
- *Compliance occurs with the standards that are in place to attain quality information systems.*

3.7.6 Security Management Controls

Information security administrators are responsible for ensuring that information systems assets **categorized under Personnel, Hardware, Facilities, Documentation, Supplies Data, Application Software and System Software** are secure. Assets are secure when the expected losses that will occur over some time, are at an acceptable level. **The control's classification on the basis of "Nature of Information System Resources – Environmental Controls, Physical Controls and Logical Access Controls (discussed under Section 3.6.2)" are all security measures against the possible threats.**

Threat Identification: *A threat is some action or event that can lead to a loss. During the threat-identification phase, security administrators attempt to flesh out all material threats that can eventuate and result in information systems assets being exposed, removed either temporarily or permanently, lost, damaged, destroyed or used for*

unauthorized purposes. Some of the major threats and to the security of information systems and their controls are as discussed in the Table 3.7.2:

Table 3.7.2: Major Security threats and their control measures

Threat	Controls
Fire	Well-designed, reliable fire-protection systems must be implemented.
Water	Facilities must be designed and sited to mitigate losses from water damage
Energy Variations	Voltage regulators, circuit breakers, and uninterruptible power supplies can be used.
Structural Damage	Facilities like BCP, DRP, Insurance etc. must be adapted to withstand structural damages that may occur due to earthquake, snow, wind, avalanche etc.
Pollution	Regular cleaning of facilities and equipment should occur.
Unauthorized Intrusion	Physical access controls can be used.
Viruses and Worms	Controls to prevent use of virus-infected programs and to close security loopholes that allow worms to propagate.
Misuse of software, data and services	Code of conduct to govern the actions of information systems employees.
Hackers	Strong, logical access controls to mitigate losses from the activities of hackers.

However, in spite of the controls on place, there could be a possibility that a control might fail. When disaster strikes, it still must be possible to recover operations and mitigate losses using the last resort controls - A Disaster Recovery Plan (DRP) and Insurance.

- **DRP: A comprehensive DRP comprise four parts – an Emergency Plan, a Backup Plan, a Recovery Plan and a Test Plan. The plan lays down the policies, guidelines, and procedures for all Information System personnel.** BCP (Business Continuity Planning) Controls are related to having an operational and tested IT continuity plan, which is in line with the overall business continuity plan, and its related business requirements so as to make sure IT services are available as required and to ensure a minimum impact on business in the event of a major disruption. The controls include Critical Classification, alternative procedures, Back-up and Recovery, Systematic and Regular Testing and Training, Monitoring and Escalation Processes, Internal and External Organizational Responsibilities, Business Continuity Activation, Fallback and Resumption plans, Risk Management Activities, Assessment of Single Points of Failure and Problem Management.

- **Insurance:** Adequate insurance must be able to replace Information Systems assets and to cover the extra costs associated with restoring normal operations. Policies usually can be obtained to cover the resources like – Equipment, Facilities, Storage Media, Valuable Papers and Records etc.

3.7.7 Operations Management Controls

Operations management is responsible for the daily running of hardware and software facilities. Operations management typically performs controls over the functions as below:

- (a) **Computer Operations:** The controls over computer operations govern the activities that directly support the day-to-day execution of either test or production systems on the hardware/software platform available. Three types of controls fall under this category:
- **Operation controls:** These controls prescribe the functions that either human operators or automated operations facilities must perform.
 - **Scheduling controls:** These controls prescribe how jobs are to be scheduled on a hardware/software platform.
 - **Maintenance controls:** These controls prescribe how hardware is to be maintained in good operating order.
- (b) **Network Operations:** This includes the proper functioning of network operations and monitoring the performance of network communication channels, network devices, and network programs and files. Data may be lost or corrupted through component failure. The primary components in the communication sub-systems are given as follows:
- Communication lines viz. twisted pair, coaxial cables, fiber optics, microwave and satellite etc.
 - Hardware – ports, modems, multiplexers, switches and concentrators etc.
 - Software – Packet switching software, polling software, data compression software etc.
 - Due to component failure, transmission between sender and receiver may be disrupted, destroyed or corrupted in the communication system.
- (c) **Data Preparation and Entry:** Irrespective of whether the data is obtained indirectly from source documents or directly from, say, customers, keyboard environments and facilities should be designed to promote speed and accuracy and to maintain the well being of keyboard operators.
- (d) **Production Control:** This includes the major functions like- receipt and dispatch of input and output; job scheduling; management of service-level agreements with users; transfer pricing/charge-out control; and acquisition of computer consumables.

- (e) **File Library**: This includes the management of an organization's machine-readable storage media like magnetic tapes, cartridges, and optical disks.
- (f) **Documentation and Program Library**: This involves that documentation librarians ensure that documentation is stored securely; that only authorized personnel gain access to documentation; that documentation is kept up-to-date and that adequate backup exists for documentation. The documentation may include reporting of responsibility and authority of each function; Definition of responsibilities and objectives of each functions; Reporting responsibility and authority of each function; Policies and procedures; Job descriptions and Segregation of duties.
- Each IS function must be clearly defined and documented including system software, application software, database administration etc.
 - Policies establish the rules or boundaries of authority delegated to individuals in the enterprise. Procedures establish the instructions that individuals must follow to complete their daily assigned tasks.
 - Documented policies should exist in IS for use of IS resource; Physical security; Data security; On-line security; Use of Information systems; Reviewing, evaluating, and purchasing hardware and software; system development methodology; and Application program changes.
 - Job descriptions communicate management's specific expectations for job performance. Job procedures establish instructions on how to do the job and policies define the authority of the employee.
 - Segregation of duties refers to the concept of distribution of work responsibilities such that individual employees are performing only the duties stipulated for their respective jobs and positions.
- (g) **Help Desk/Technical support**: This assists end-users to employ end-user hardware and software such as micro-computers, spreadsheet packages, database management packages etc. and also provides the technical support for production systems by assisting with problem resolution.
- (h) **Capacity Planning and Performance Monitoring**: Regular performance monitoring facilitates the capacity planning wherein the resource deficiencies must be identified well in time so that they can be made available when they are needed.
- (i) **Management of Outsourced Operations**: This has the responsibility for carrying out day-to-day monitoring of the outsourcing contract.

3.8 Application Controls and their Categories

Application system controls are undertaken to accomplish reliable information processing cycles that perform the processes across the enterprise. Applications represent the interface between the user and the business functions. For example, a counter clerk at a bank is required to perform various business activities as part of his/her job description and assigned responsibilities. S/he is able to relate to the advantages of technology when he is able to

modification. A queue is the list of documents waiting to be printed on a particular printer; this should not be subject to unauthorized modifications.

- **Controls over printing:** Outputs should be made on the correct printer and it should be ensured that unauthorized disclosure of information printed does not take place. Users must be trained to select the correct printer and access restrictions may be placed on the workstations that can be used for printing.
- **Report distribution and collection controls:** Distribution of reports should be made in a secure way to prevent unauthorized disclosure of data. It should be made immediately after printing to ensure that the time gap between generation and distribution is reduced. A log should be maintained for reports that were generated and to whom these were distributed. Where users have to collect reports the user should be responsible for timely collection of the report, especially if it is printed in a public area. A log should be maintained about reports that were printed and collected. Uncollected reports should be stored securely.
- **Retention controls:** Retention controls consider the duration for which outputs should be retained before being destroyed. Consideration should be given to the type of medium on which the output is stored. Retention control requires that a date should be determined for each output item produced. Various factors ranging from the need of the output, use of the output, to legislative requirements would affect the retention period.

3.9 Information Technology General Controls

Information Technology General Controls (ITGC) are the basic policies and procedures that ensure that an organization's information systems are properly safeguarded, that application programs and data are secure, and that computerized operations can be recovered in case of unexpected interruptions. IT General Controls are the foundation for the overall IT control environment as they provide the assurance that systems operate as intended and that output is reliable. Failure to ensure these controls are designed and operating effectively means that there will not be any assurance over the IT Application Controls.

ITGCs may also be referred to as General Computer Controls (GCC) which are defined as: Controls, other than application controls, which relate to the environment within which computer-based application systems are developed, maintained and operated, and which are therefore applicable to all applications. The objectives of general controls are to ensure the proper development and implementation of applications, the integrity of program and data files and of computer operations. Like application controls, general controls may be either manual or programmed. Examples of general controls include the development and implementation of an IS strategy and an IS security policy, the organization of IS staff to separate conflicting duties and planning for disaster prevention and recovery.

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

whole, General Controls apply to all computerized applications and consist of a combination of system software and manual procedures that create an overall control environment.

Examples of primary objectives for general controls are to safeguard data, protect application programs, and ensure continued computer operations in case of unexpected interruptions. General controls are applied at the entity-wide, system, and business process application levels. The effectiveness of general controls at the entity-wide and system levels is a significant factor in determining the effectiveness of business process controls at the application level. Without effective general controls at the entity-wide and system levels, business process controls generally can be rendered ineffective by circumvention or modification. The most common ITGCs are as follows:

- *Logical access controls over infrastructure, applications, and data.*
- *System development life cycle controls.*
- *Program change management controls.*
- *Data center physical security controls.*
- *System and data backup and recovery controls.*
- *Computer operation controls.*

These General controls have already been covered in earlier topics.

CH 4: BCP and DRP

The diagram shows a 3x3 grid representing a Business Impact Matrix. The vertical axis (Y-axis) is on the left, and the horizontal axis (X-axis) is at the bottom. The grid cells contain the following values:

3 (minor)	6 (Major)	9 (Catastrophic)
2 (Trivial)	4 (Major)	6 (Major)
1 (Trivial)	2 (Trivial)	3 (Minor)

Fig. 4.8.1: Business Impact Matrix (1)

Identify all the mission critical processes for categorizing into Vital, Essential and Desirable and looking for the probable disasters as per the list attached.

The Business Impact Analysis matrix is also used to assess Risk and is thus also referred as Risk Assessment Matrix. The interpretation of Fig. 4.8.1 can be drawn like this.

In a risk assessment matrix, risks are placed on the matrix based on two criteria:

1. **Likelihood**: the probability of a risk or the occurrence of the disaster – On Y Axis
2. **Consequences**: the severity of the impact or the extent of damage caused by the risk - On X Axis

Likelihood of Occurrence

Based on the likelihood of the occurrence of a risk, the risks can be classified under one of the following categories:

1. **Definite (scaled 3)**: A risk that is almost certain to show-up during project execution. If you're looking at percentages a risk that is more than 80% likely to cause problems will fall under this category.
2. **Likely (scaled 2)**: Risks that have 60-80% chances of occurrence can be grouped as likely.
3. **Unlikely (scaled 1)**: Rare and exceptional risks which have a less than 10% chance of occurrence.

Consequences

The consequences of a risk can again be ranked and classified into one of the following categories, based on how severe the damage can be.

1. **Trivial/Insignificant (scaled 1)**: Risks that will cause a near negligible amount of damage to the overall progress of the project.

2. **Minor (scaled 2):** If a risk will result in some damage, but the extent of damage is not too significant.
3. **Major (scaled 3):** Risks with significantly large consequences which can lead to a great amount of loss are classified as critical.
4. **Catastrophic (scaled 4):** These are the risks which can make the project completely unproductive and unfruitful, and must be a top priority during risk management.

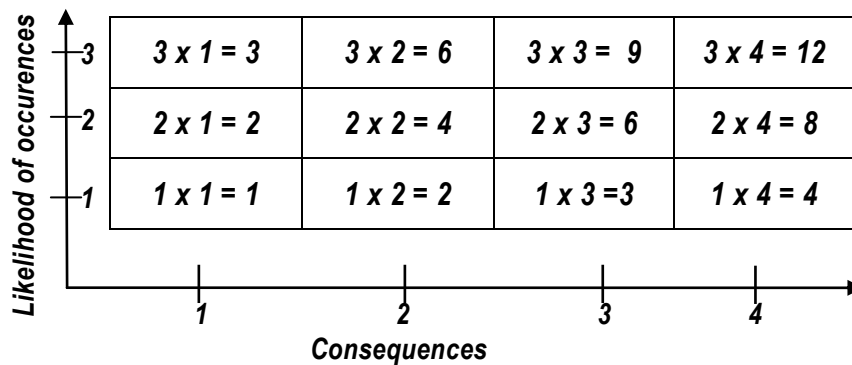


Fig. 4.8.2: Business Impact Matrix (2)

Like-wise the grid can be extended depending upon the criteria one chooses.

Depending upon the grid value, the risk can be assessed.

- Like values 8 to 12 can be categorized into Catastrophic.
- Values 4 to 6 can be denoted as Major.
- Value 3 can be given as Minor.
- Values 1 and 2 can be denoted as Trivial.

In some books, the values can be classified into High, Medium, Low, and Very Low.

4.8.3 Risk Assessment

The risk assessment is assessment of the disruption to critical activities, which are supported by resources such as people, process, technology, information, infrastructure supplies and stakeholders. The enterprise should determine the threats and vulnerabilities of each resource, and the impact that would have, in case it becomes a reality. It is the decision of the enterprise to select a risk assessment approach, but it is important that it is suitable and appropriate to address all of the enterprise's requirements.

Specific threats may be described as events or actions, which could, at some point, cause an impact to the resources, e.g. threats such as fire, flood, power failure, staff loss, staff absenteeism, computer viruses and hardware failure.

4.14 Types of Back-ups

When the back-ups are taken of the system and data together, they are called total system's back-up. Various types of back-ups are given as follows:

- (i) **Full Backup:** A Full Backup captures all files on the disk or within the folder selected for backup. With a full backup system, every backup generation contains every file in the backup set. ***At each backup run, all files designated in the backup job will be backed up again. This includes files and folders that have not changed.***

It is commonly used as an initial or first backup followed with subsequent incremental or differential backups. After several incremental or differential backups, it is common to start over with a fresh full backup again. Some also like to do full backups for all backup runs typically for smaller folders or projects that do not occupy too much storage space. The Windows operating system lets us to copy a full backup on several DVD disks. Any good backup plan has at least one full backup of a server.

For example - Suppose a full backup job or task is to be done every night from Monday to Friday. The first backup on Monday will contain the entire list of files and folders in the backup job. On Tuesday, the backup will include copying all the files and folders again, no matter the files have got changed or not. The cycle continues this way.

Advantages

- *Restores are fast and easy to manage as the entire list of files and folders are in one backup set.*
- *Easy to maintain and restore different versions.*

Disadvantages

- *Backups can take very long as each file is backed up again every time the full backup is run.*
- *Consumes the most storage space compared to incremental and differential backups. The exact same files are stored repeatedly resulting in inefficient use of storage.*

- (ii) **Incremental Backup:** An Incremental Backup captures files that were created or changed since the last backup, regardless of backup type. ***The last backup can be a full backup or simply the last incremental backup. With incremental backups, one full backup is done first and subsequent backup runs are just the changed files and new files added since the last backup.***

For example - Suppose an Incremental backup job or task is to be done every night from Monday to Friday. This first backup on Monday will be a full backup since no backups have been taken prior to this. However, on Tuesday, the incremental backup will only backup the files that have changed since Monday and the backup on Wednesday will include only the changes and new files since Tuesday's backup. The cycle continues this way.

Advantages

- *Much faster backups.*
- *Efficient use of storage space as files are not duplicated. Much less storage space used compared to running full backups and even differential backups.*

Disadvantages

- *Restores are slower than with a full backup and differential backups.*
- *Restores are a little more complicated. All backup sets (first full backup and all incremental backups) are needed to perform a restore.*

- (iii) **Differential Backup:** ***Differential backups fall in the middle between full backups and incremental backup.*** A Differential Backup stores files that have changed since the last full backup. ***With differential backups, one full backup is done first and subsequent backup runs are the changes made since the last full backup.*** Therefore, if a file is changed after the previous full backup, a differential backup takes less time to complete than a full backup. Comparing with full backup, differential backup is obviously faster and more economical in using the backup space, as only the files that have changed since the last full backup are saved.

Restoring from a differential backup is a two-step operation: Restoring from the last full backup; and then restoring the appropriate differential backup. The downside to using differential backup is that each differential backup probably includes files that were already included in earlier differential backups.

For example - Suppose a differential backup job or task is to be done every night from Monday to Friday. On Monday, the first backup will be a full backup since no prior backups have been taken. On Tuesday, the differential backup will only backup the files that have changed since Monday and any new files added to the backup folders. On Wednesday, the files changed and files added since Monday's full backup will be copied again. While Wednesday's backup does not include the files from the first full backup, it still contains the files backed up on Tuesday.

Advantages

- ***Much faster backups than full backups.***
- ***More efficient use of storage space than full backups since only files changed since the last full backup will be copied on each differential backup run.***
- ***Faster restores than incremental backups.***

Disadvantages

- ***Backups are slower than incremental backups.***
 - ***Not as efficient use of storage space as compared to incremental backups. All files added or edited after the initial full backup will be duplicated again with each subsequent differential backup.***
 - ***Restores are slower than with full backups.***
 - ***Restores are a little more complicated than full backups but simpler than incremental backups. Only the full backup set and the last differential backup are needed to perform a restore.***
- (iv) ***Mirror back-up: Mirror backups are, as the name suggests, a mirror of the source being backed up. With mirror backups, when a file in the source is deleted, that file is eventually also deleted in the mirror backup. Because of this, mirror backups should be used with caution as a file that is deleted by accident, sabotage or through a virus may also cause that same file in mirror to be deleted as well. Some do not consider a mirror to be a backup.***

Further, a mirror backup is identical to a full backup, with the exception that the files are not compressed in zip files and they cannot be protected with a password. A mirror backup is most frequently used to create an exact copy of the backup data.

For example - Many online backup services offer a mirror backup with a 30 day delete. This means that when you delete a file on your source, that file is kept on the storage server for at least 30 days before it is eventually deleted. This helps strike a balance offering a level of safety while not allowing the backups to keep



growing since online storage can be relatively expensive. Many backup software utilities do provide support for mirror backups.

Advantages

- *The backup is clean and does not contain old and obsolete files.*

Disadvantages

- *There is a chance that files in the source deleted accidentally, by sabotage or through a virus may also be deleted from the backup mirror.*

	<p>generators</p> <ul style="list-style-type: none"> • Humidity, temperature, and voltage control are maintained and acceptable levels • Emergency lighting, power outages and routes are ly located. 	
	<p>l and rsonnel are l understand</p> <p>· procedures ented and</p>	<ul style="list-style-type: none"> • Interview security personnel to ensure their awareness and responsibilities. • Review training records and documentation. Determine the scope and
 		
<h2>CH 6: AUDITING OF IS</h2>		
		inspection plan.

Audit Trails

is provided below in Table 6.7.1 and has already been discussed in detail in Chapter - 3 of the Study Material.

Table 6.7.1: Types of Managerial Controls

Controls	Scope
Top Management and Information Systems Management Controls	Discusses the top management's role in planning, organizing, leading and controlling the information systems function. Also provides advice to top management in relation to long-run policy decision making and translates long-run policies into short-run goals and objectives.
System Development Management Controls	Provides a contingency perspective on models of the information systems development process that auditors can use as a basis for evidence collection and evaluation.

Programming Management Controls	<i>Discusses the major phases in the program life cycle and the important controls that should be exercised in each phase.</i>
Data Resource Management Controls	<i>Discusses the role of database administrator and the controls that should be exercised in each phase.</i>
Quality Assurance Management Controls	<i>Discusses the major functions that quality assurance management should perform to ensure that the development, implementation, operation, and maintenance of information systems conform to quality standards.</i>
Security Management Controls	<i>Discusses the major functions performed by operations by security administrators to identify major threats to the IS functions and to design, implement, operate, and maintain controls that reduce expected losses from these threats to an acceptable level.</i>
Operations Management Controls	<i>Discusses the major functions performed by operations management to ensure the day-to-day operations of the IS function are well controlled.</i>

The auditors play a vital role in evaluating the performance of various controls under managerial controls. Some of the key areas that auditors should pay attention to while evaluating Managerial controls and its types are provided below:

6.7.1 Top Management and Information Systems Management Controls

The major activities that senior management must perform are – Planning, Organizing, Controlling and Leading (already explained in Chapter – 3 of the Study Material). The Role of auditor at each activity is discussed below:

- **Planning:** *Auditors need to evaluate whether top management has formulated a high-quality information system's plan that is appropriate to the needs of an organization or not. A poor-quality information system is ineffective and inefficient leading to losing of its competitive position within the marketplace.*
- **Organizing:** *Auditors should be concerned about how well top management acquires and manages staff resources for three reasons:*
 - *The effectiveness of the IS function depends primarily on the quality of its staff. The IS staff need to remain up to date and motivated in their jobs.*
 - *Intense competition and high turnover have made acquiring and retaining good information system staff a complex activity.*
 - *Empirical research indicates that the employees of an organization are the most likely persons to perpetrate irregularities.*
- **Leading:** *Generally, the auditors examine variables that often indicate when motivation problems exist or suggest poor leadership. For example - staff turnover statistics, frequent failure of projects to meet their budget and absenteeism level to evaluate the leading function. Auditors may use both formal and informal sources*

of evidence to evaluate how well top managers' communicate with their staff. The formal sources include IS plans, documents standards and policies whereas the informal sources of evidence include interviews with IS staff about their level of satisfaction with the top management. Auditors must try to assess both the short-run and long-run consequences of poor communications within the information systems function and to assess the implications for asset safeguarding, data integrity, system effectiveness, and system efficiency.

- ***Controlling:*** Auditors should focus on subset of the control activities that should be performed by top management – namely, those aimed at ensuring that the information systems function accomplishes its objectives at a global level. Auditors must evaluate whether top management's choice to the means of control over the users of IS services is likely to be effective or not.

6.7.2 System Development Management Controls

Three different types of audits may be conducted during system development process as discussed in the Table 6.7.2:

Table 6.7.2: Different types of Audit during System Development Process

Concurrent Audit	Auditors are members of the system development team. They assist the team in improving the quality of systems development for the specific system they are building and implementing.
Post - implementation Audit	Auditors seek to help an organization learn from its experiences in the development of a specific application system. In addition, they might be evaluating whether the system needs to be scrapped, continued, or modified in some way.
General Audit	Auditors evaluate systems development controls overall. They seek to determine whether they can reduce the extent of substantive testing needed to form an audit opinion about management's assertions relating to the financial statements for systems effectiveness and efficiency.

An external auditor is more likely to undertake general audits rather than concurrent or post-implementation audits of the systems development process. For internal auditors, management might require that they participate in the development of material application systems or undertake post-implementation reviews of material application systems as a matter of course.

6.7.3 Programming Management Controls

Some of the major concerns that an auditor should address under different activities involved in Programming Management Control Phase are provided in Table 6.7.3 as under:

Table 6.7.3: Audit Trails under Programming Management Controls

Phase	Audit Trails
Planning	<ul style="list-style-type: none"> • They should evaluate whether the nature of and extent of planning are appropriate to the different types of software that are developed or acquired. • They must evaluate how well the planning work is being undertaken.
Control	<ul style="list-style-type: none"> • They must evaluate whether the nature of and extent of control activities undertaken are appropriate for the different types of software that are developed or acquired. • They must gather evidence on whether the control procedures are operating reliably. For example - they might first choose a sample of past and current software development and acquisition projects carried out at different locations in the organization they are auditing.
Design	<ul style="list-style-type: none"> • Auditors should find out whether programmers use some type of systematic approach to design. • Auditors can obtain evidence of the design practices used by undertaking interviews, observations, and reviews of documentation.
Coding	<ul style="list-style-type: none"> • Auditors should seek evidence – <ul style="list-style-type: none"> ○ On the level of care exercised by programming management in choosing a module implementation and integration strategy. ○ To determine whether programming management ensures that programmers follow structured programming conventions. ○ To check whether programmers employ automated facilities to assist them with their coding work.
Testing	<ul style="list-style-type: none"> • Auditors can use interviews, observations, and examination of documentation to evaluate how well unit testing is conducted. • Auditors are most likely concerned primarily with the quality of integration testing work carried out by information systems professionals rather than end users. • Auditor's primary concern is to see that whole-of-program tests have been undertaken for all material programs and that these tests have been well-designed and executed.
Operation and Maintenance	<ul style="list-style-type: none"> • Auditors need to ensure effectively and timely reporting of maintenance needs occurs and maintenance is carried out in a well-controlled manner.

	<ul style="list-style-type: none"> • <i>Auditors should ensure that management has implemented a review system and assigned responsibility for monitoring the status of operational programs.</i>
--	--

6.7.4 Data Resource Management Controls

- *Auditors should determine what controls are exercised to maintain data integrity. They might also interview database users to determine their level of awareness of these controls.*
- *Auditors might employ test data to evaluate whether access controls and update controls are working.*

6.7.5 Quality Assurance Management Controls

- *Auditors might use interviews, observations and reviews of documentation to evaluate how well Quality Assurance (QA) personnel perform their monitoring role.*
- *Auditors might evaluate how well QA personnel make recommendations for improved standards or processes through interviews, observations, and reviews of documentation.*
- *Auditors can evaluate how well QA personnel undertake the reporting function and training through interviews, observations, and reviews of documentation.*

6.7.6 Security Management Controls

- *Auditors must evaluate whether security administrators are conducting ongoing, high-quality security reviews or not;*
- *Auditors check whether the organizations audited have appropriate, high-quality disaster recovery plan in place; and*
- *Auditors check whether the organizations have opted for an appropriate insurance plan or not.*

6.7.7 Operations Management Controls

- *Auditors should pay concern to see whether the documentation is maintained securely and that it is issued only to authorized personnel.*
- *Auditors can use interviews, observations, and review of documentation to evaluate -*
 - *the activities of documentation librarians;*
 - *how well operations management undertakes the capacity planning and performance monitoring function;*
 - *the reliability of outsourcing vendor controls;*
 - *whether operations management is monitoring compliance with the outsourcing contract; and*
 - *whether operations management regularly assesses the financial viability of any outsourcing vendors that an organization uses.*

CH 8: EMERGING TECHNOLOGIES

8.2 Grid Computing

The computing resources in most of the organizations are underutilized but are necessary for certain operations. The idea of Grid computing is to make use of such non-utilized computing power by the needy organizations, and thereby the Return On Investment (ROI) on computing investments can be increased.

Thus, Grid computing is a network of computing or processor machines managed with a kind of software such as middleware, in order to access and use the resources remotely. The managing activity of grid resources through the middleware is called Grid Services. Grid Services provide access control, security, access to data including digital libraries and databases, and access to large-scale interactive and long-term storage facilities.

Grid Computing is more popular due to the following reasons:

- It has the ability to make use of unused computing power, and thus, it is a cost-effective solution (reducing investments, only recurring costs).
- This enables heterogeneous resources of computers to work cooperatively and collaboratively to solve a scientific problem.

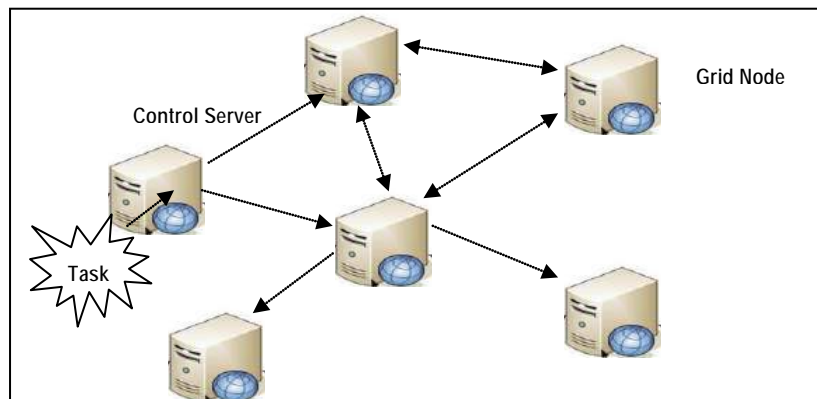


Fig. 8.2.1: Grid Computing Scenario

Grid computing requires the use of software that can divide and carve out pieces of a program as one large system image to several thousand computers. One concern about grid is that if one piece of the software on a node fails, other pieces of the software on other nodes may fail (as shown in Fig. 8.2.1). This is alleviated if that component has a failover component on another node, but problems can still arise if components rely on other pieces of software to accomplish one or more grid computing tasks. Large system images and associated hardware to operate and maintain them, can contribute to large capital and operating expenses.

8.3 Cloud Computing

Cloud computing, simply means the use of computing resources as a service through networks, typically the Internet. The Internet is commonly visualized as clouds; hence the term

The details are given as follow:

- **Front End Architecture:** The front end of the cloud computing system comprises of the client's devices (or computer network) and some applications needed for accessing the cloud computing system. All the cloud computing systems do not give the same interface to users. Web services like electronic mail programs use some existing web browsers such as Firefox, Microsoft's internet explorer or Apple's Safari. Other types of systems have some unique applications which provide network access to its clients.
- **Back End Architecture:** Back end refers to some service facilitating peripherals. In cloud computing, the back end is cloud itself, which may encompass various computer machines, data storage systems and servers. Groups of these clouds make up a whole cloud computing system. Theoretically, a cloud computing system can include any type of web application program such as video games to applications for data processing, software development and entertainment. Usually, every application would have its individual dedicated server for services.

A central server is established to be used for administering the whole system. It is also used for monitoring client's demand as well as traffic to ensure that everything of system runs without any problem. There are some set of rules, technically referred as protocols, are followed by this server and it uses a special type of software known as middleware. Middleware allows computers that are connected on networks to communicate with each other. If any cloud computing service provider has many customers, then there's likely to be very high demand for huge storage space. Many companies that are service providers need hundreds of storage devices. The cloud computing system must have a redundant back-up copy of all the data of its client's.

8.3.4 Cloud Computing Environment

The Cloud Computing environment can consist of multiple types of clouds based on their deployment and usage. Such typical Cloud computing environments, catering to special requirements, are briefly described as follows (given in Fig. 8.3.3).

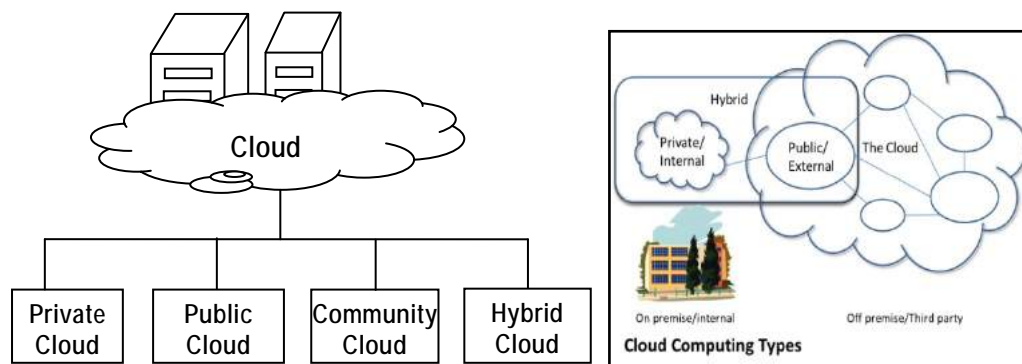


Fig. 8.3.3: Cloud Deployment Models*

*Source: www.synergy.gs

- (a) **Private Cloud:** This cloud computing environment resides within the boundaries of an organization and is used exclusively for the organization's benefits. These are also called Internal Clouds or Corporate Clouds. *Private Clouds can either be private to the organization and managed by the single organization (On-Premise Private Cloud) or can be managed by third party (Outsourced Private Cloud).* They are built primarily by IT departments within enterprises, who seek to optimize utilization of infrastructure resources within the enterprise by provisioning the infrastructure with applications using the concepts of grid and virtualization.

Certain characteristics of Private Cloud are as follows:

- **Secure:** *The private cloud is secure as it is deployed and managed by the organization itself, and hence there is least chance of data being leaked out of the cloud.*
- **Central Control:** *As usual, the private cloud is managed by the organization itself, there is no need for the organization to rely on anybody and its controlled by the organization itself.*
- **Weak Service Level Agreements (SLAs):** *SLAs play a very important role in any cloud service deployment model as they are defined as agreements between the user and the service provider in private cloud. In private cloud, either Formal SLAs do not exist or are weak as it is between the organization and user of the same organization. Thus, high availability and good service may or may not be available.*

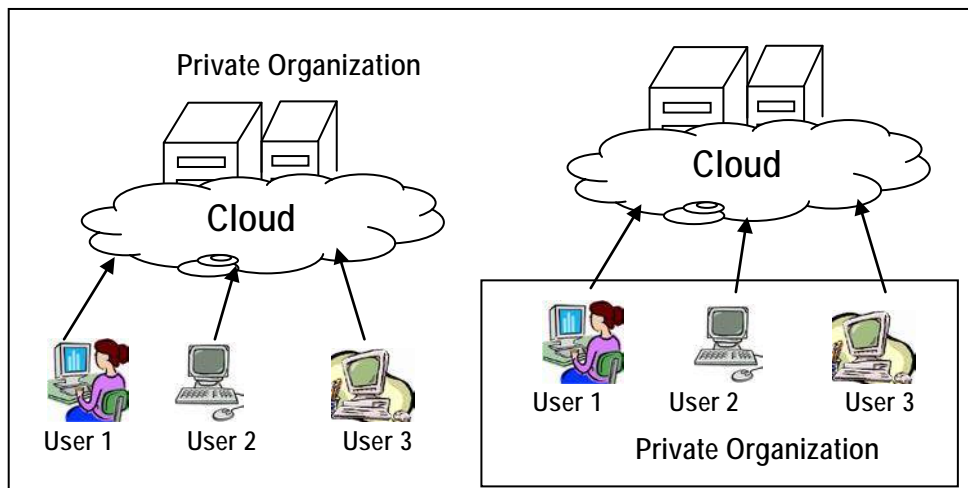


Fig. 8.3.4: On-premise and Outsourced Private Cloud respectively

Fig. 8.3.4 depicts the pictorial representation of On-Premise and Outsourced Private clouds respectively.

The advantages of Private Cloud include the following:

- It improves average server utilization; allow usage of low-cost servers and hardware while providing higher efficiencies; thus reducing the costs that a greater number of servers would otherwise entail.
- *It provides a high level of security and privacy to the user.*
- *It is small in size and controlled and maintained by the organization.*

Moreover, one major limitation is that IT teams in the organization may have to invest in buying, building and managing the clouds independently. **Budget is a constraint in private clouds and they also have loose SLAs.**

However, the major differences between On-Premise Private Cloud and Outsourced Private Cloud are given in Table 8.3.1 below:

Table 8.3.1: Differences between On-Premise and Outsourced Private Cloud

	<i>On-Premise Private Cloud</i>	<i>Outsourced Private Cloud</i>
<i>Management</i>	<i>Managed by the organization itself.</i>	<i>Managed by the third party. Everything is same as usual private cloud except that here the cloud is outsourced.</i>
<i>Service Level Agreements (SLAs)</i>	<i>SLAs are defined between the organization and its users. Users have broader access rights than general public cloud users and service providers are able to efficiently provide the service because of small user base and mostly efficient network.</i>	<i>These are usually followed strictly as it is a third party organization.</i>
<i>Network</i>	<i>Network management and network issue resolving are easier. The networks usually have high bandwidth and low latency.</i>	<i>The cloud is fully deployed at the third party site and organizations connect to the third party by means of either a dedicated connection or through Internet.</i>
<i>Security and Data Privacy</i>	<i>Comparatively, it is more resistant to attacks than any other cloud and the security attacks are possible from an internal user only.</i>	<i>Cloud is relatively less secure and the security threat is from the third party and the internal employee.</i>

<i>Location</i>	<i>The data is usually stored in the same geographical location where the cloud users are present. In case of several physical locations, the cloud is distributed over several places and is accessed using the Internet.</i>	<i>The cloud is located off site and when there is a change of location the data need to be transmitted through long distances.</i>
<i>Performance</i>	<i>The performance depends on the network and resources and can be controlled by the network management team.</i>	<i>The performance of the cloud depends on the third party that is outsourcing the cloud.</i>

- (b) **Public Cloud:** The public cloud is the cloud infrastructure that is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organizations, or some combination of them. Typically, public clouds are administrated by third parties or vendors over the Internet, and the services are offered on pay-per-use basis. These are also called Provider Clouds. *Public cloud consists of users from all over the world wherein a user can simply purchase resources on an hourly basis and work with the resources which are available in the cloud provider's premises.*

Characteristics of Public Cloud are as follows:

- **Highly Scalable:** *The resources in the public cloud are large in number and the service providers make sure that all requests are granted. Hence public clouds are considered to be scalable.*
- **Affordable:** *The cloud is offered to the public on a pay-as-you-go basis; hence the user has to pay only for what he or she is using (using on a per-hour basis). And this does not involve any cost related to the deployment.*
- **Less Secure:** *Since it is offered by a third party and they have full control over the cloud, the public cloud is less secure out of all the other deployment models.*
- **Highly Available:** *It is highly available because anybody from any part of the world can access the public cloud with proper permission, and this is not possible in other models as geographical or other access restrictions might be there.*
- **Stringent SLAs:** *As the service provider's business reputation and customer strength are totally dependent on the cloud services, they follow the SLAs strictly and violations are avoided.*

The Advantages of Public Cloud include the following:

- It is widely used in the development, deployment and management of enterprise applications, at affordable costs.
- It allows the organizations to deliver highly scalable and reliable applications rapidly and at more affordable costs.
- *There is no need for establishing infrastructure for setting up and maintaining the cloud.*
- *Strict SLAs are followed.*
- *There is no limit for the number of users.*

Moreover, one of the limitations is security assurance and thereby building trust among the clients is far from desired but slowly liable to happen. *Further, privacy and organizational autonomy are not possible.*

- (c) **Hybrid Cloud:** This is a combination of both at least one private (internal) and at least one public (external) cloud computing environments - usually, consisting of infrastructure, platforms and applications. *The usual method of using the hybrid cloud is to have a private cloud initially, and then for additional resources, the public cloud is used. The hybrid cloud can be regarded as a private cloud extended to the public cloud and aims at utilizing the power of the public cloud by retaining the properties of the private cloud.* It is typically offered in either of two ways. A vendor has a private cloud and forms a partnership with a public cloud provider or a public cloud provider forms a partnership/franchise with a vendor that provides private cloud platforms. Fig. 8.3.5 depicts Hybrid Cloud.

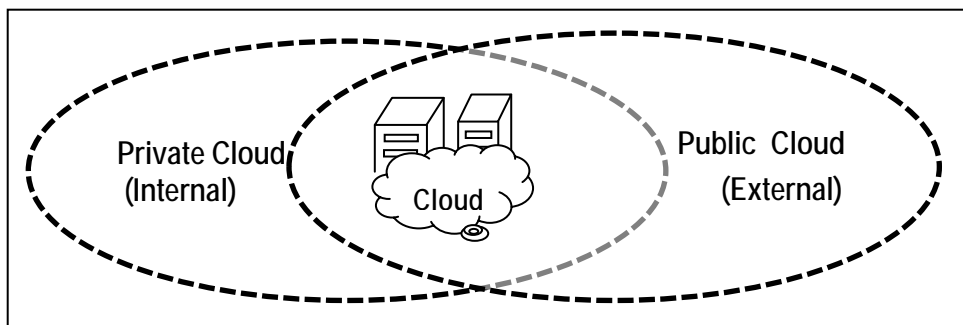


Fig. 8.3.5: Hybrid Cloud

Characteristics of Hybrid Cloud are as follows:

- **Scalable:** *The hybrid cloud has the property of public cloud with a private cloud environment and as the public cloud is scalable; the hybrid cloud with the help of its public counterpart is also scalable.*

- Partially Secure: The private cloud is considered as secured and public cloud has high risk of security breach. The hybrid cloud thus cannot be fully termed as secure but as partially secure.
- Stringent SLAs: Overall the SLAs are more stringent than the private cloud and might be as per the public cloud service providers.
- Complex Cloud Management: Cloud management is complex as it involves more than one type of deployment models and also the number of users is high.

The Advantages of Hybrid Cloud include the following:

- It is highly scalable and gives the power of both private and public clouds.
- It provides better security than the public cloud.

The limitation of Hybrid Cloud is that the security features are not as good as the public cloud and complex to manage.

- (d) Community Cloud: The community cloud is the cloud infrastructure that is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (eg. mission security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party or some combination of them, and it may exist on or off premises. In this, a private cloud is shared between several organizations. Fig. 8.3.6 depicts Community Cloud. This model is suitable for organizations that cannot afford a private cloud and cannot rely on the public cloud either.

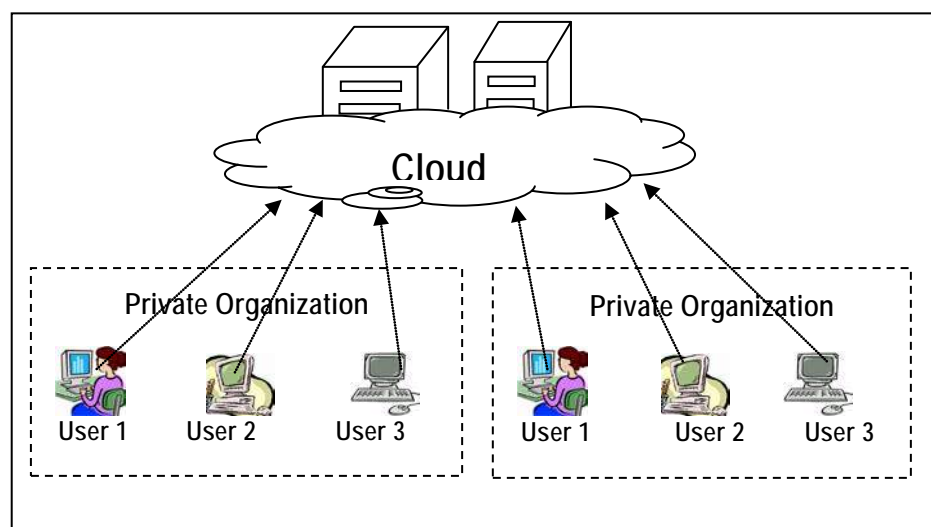


Fig. 8.3.6: Community Cloud

Characteristics of Community Clouds are as follows:

- *Collaborative and Distributive Maintenance:* *In this, no single company has full control over the whole cloud. This is usually distributive and hence better cooperation provides better results.*
- *Partially Secure:* *This refers to the property of the community cloud where few organizations share the cloud, so there is a possibility that the data can be leaked from one organization to another, though it is safe from the external world.*
- *Cost Effective:* *As the complete cloud is being shared by several organizations or community, not only the responsibility gets shared; the community cloud becomes cost effective too.*

Advantages of Community Clouds are as follows:

- *It allows establishing a low-cost private cloud.*
- *It allows collaborative work on the cloud.*
- *It allows sharing of responsibilities among the organizations.*
- *It has better security than the public cloud.*

The limitation of the community cloud is that the autonomy of the organization is lost and some of the security features are not as good as the private cloud. It is not suitable in the cases where there is no collaboration.

8.3.5 Cloud Computing Service Models

Cloud computing is a model that enables the end users to access the shared pool of resources such as compute, network, storage, database and application as an on-demand service without the need to buy or own it. The services are provided and managed by the service provider, reducing the management effort from the end user side. The essential characteristics of the cloud include on-demand, self service, broad network access, resource pooling, rapid elasticity, and measured service. The National Institute of Standards and Technology (NIST) defines three basic service models - Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). These are pictorially presented in Fig. 8.3.7.

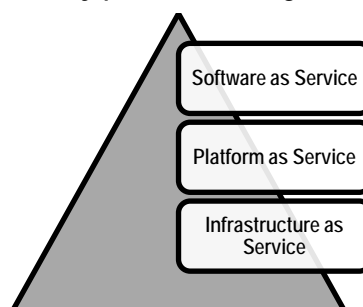


Fig. 8.3.7: Cloud Computing Basic Service Models

- (a) **Infrastructure as a Service (IaaS)**: IaaS, a hardware-level service, provides computing resources such as processing power, memory, storage, and networks for cloud users to run their application on-demand. This allows users to maximize the utilization of computing capacities without having to own and manage their own resources.

IaaS changes the computing from a physical infrastructure to a virtual infrastructure through virtual computing; storage; and network resources by abstracting the physical resources. IaaS providers offer computers, more often virtual machines and other resources as service; the infrastructure / storage required to host the services ourselves i.e. makes us the system administrator and manage hardware/storage, network and computing resources. In order to deploy their applications, cloud clients install operating-system images and their application software on the cloud infrastructure. *The end-users or IT architects will use the infrastructure resources in the form of Virtual machines (VMs) and design virtual infrastructure, network load balancers etc., based on their needs. The IT architects need not maintain the physical servers as it is maintained by the service providers.*

Examples of IaaS providers include Amazon Web Services (AWS), Google Compute Engine, OpenStack and Eucalyptus.

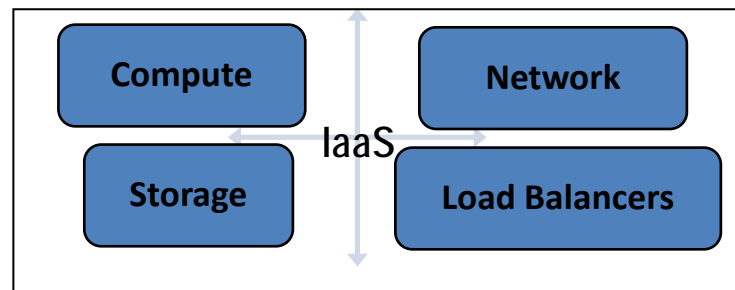


Fig. 8.3.8: Services offered by IaaS providers

A typical IaaS provider may provide the following services as shown in the Fig. 8.3.8:

- (a) **Compute**: Computing as a Service includes virtual Central Processing Units (CPUs) and virtual main memory for the Virtual Machines (VMs) that are provisioned to the end users.
- (b) **Storage**: STaaS provides back-end storage for the VM images. Some of the IaaS providers also provide the back end for storing files.
- (c) **Network**: Network as a Service (NaaS) provides virtual networking components such as virtual router, switch, and bridge for the VMs.
- (d) **Load Balancers**: Load balancing as a Service may provide load balancing capability at the infrastructure layer.

Characteristics of IaaS are as follows:

- Web access to the resources: The IaaS model enables the IT users to access infrastructure resources over the Internet. When accessing a huge computing power, the IT user need not get physical access to the servers.
- Centralized management: The resources distributed across different parts are controlled from any management console that ensures effective resource management and effective resource utilization.
- Elasticity and Dynamic Scaling: Depending on the load, IaaS services can provide the resources and elastic services where the usage of resources can be increased or decreased according to the requirements.
- Shared infrastructure: IaaS follows a one-to-many delivery model and allows multiple IT users to share the same physical infrastructure and thus ensure high resource utilization.
- Metered Services: IaaS allows the IT users to rent the computing resources instead of buying it. The services consumed by the IT user will be measured, and the users will be charged by the IaaS providers based on the amount of usage.

The different instances of IaaS are as follows:

- Network as a Service (NaaS): NaaS, an instance of IaaS, provides users with needed data communication capacity to accommodate bursts in data traffic during data-intensive activities such as video conferencing or large file downloads. It is an ability given to the end-users to access virtual network services that are provided by the service provider over the Internet on pay-per-use basis. NaaS allows network architects to create virtual networks; virtual network interface cards (NICs), virtual routers, virtual switches, and other networking components. It further allows the network architect to deploy custom routing protocols and enables the design of efficient in-network services, such as data aggregation, stream processing, and caching. NaaS providers operate using three common service models: Virtual Private Network (VPN), Bandwidth on Demand (BoD) and Mobile Virtual Network (MVN).
- Storage as a Service (STaaS): STaaS, an instance of IaaS, provides storage infrastructure on a subscription basis to users who want a low-cost and convenient way to store data, synchronize data across multiple devices, manage off-site backups, mitigate risks of disaster recovery, and preserve records for the long-term. It is an ability given to the end users to store the data on the storage services provided by the service provider. STaaS allows the end users to access the files at any time from any place. STaaS provider provides the virtual storage that is abstracted from the physical storage of any cloud data center. STaaS is also a cloud business model that is delivered as a utility.
- Database as a Service (DBaaS): This is also related to IaaS and provides users with seamless mechanisms to create, store, and access databases at a host site on

demand. It is an ability given to the end users to access the database service without the need to install and maintain it on the pay-per-use basis. The end users can access the database services through any Application Programming Interfaces (APIs) or Web User Interfaces provided by the service provider.

- Backend as a Service (BaaS): It is a type of IaaS, that provides web and mobile app developers a way to connect their applications to backend cloud storage with added services such as user management, push notifications, social network services integration using custom software development kits and application programming interfaces.
- Desktop as a Service (DTaaS): It is an instance of IaaS that provides ability to the end users to use desktop virtualization without buying and managing their own infrastructure. DTaaS is a pay-per-use cloud service delivery model in which the service provider manages the back-end responsibilities of data storage, backup, security and upgrades. The end-users are responsible for securing and managing their own desktop images, applications, and security. These services are simple to deploy, are highly secure, and produce better experience on almost all devices.
- (b) Platform as a Service (PaaS): PaaS provides the users the ability to develop and deploy an application on the development platform provided by the service provider. In traditional application development, the application will be developed locally and will be hosted in the central location. In stand-alone application development, the application will be developed by traditional development platforms result in licensing - based software, whereas PaaS changes the application development from local machine to online. For example- Google AppEngine, Windows Azure Compute etc.

Typical PaaS providers may provide programming languages, application frameworks, databases, and testing tools apart from some build tools, deployment tools and software load balancers as a service in some cases (Refer Fig. 8.3.9).

- Programming Languages: PaaS providers provide a wide variety of programming languages like Java, PHP, Python, Ruby etc. for the developers to develop applications.
- Application Frameworks: PaaS vendors provide application development framework like Joomla, WordPress, Sinatra etc. for application development.
- Database: Along with PaaS platforms, PaaS providers provide some of the popular databases like ClearDB, Cloudant, Redis etc. so that application can communicate with the databases.
- Other Tools: PaaS providers provide all the tools that are required to develop, test, and deploy an application.

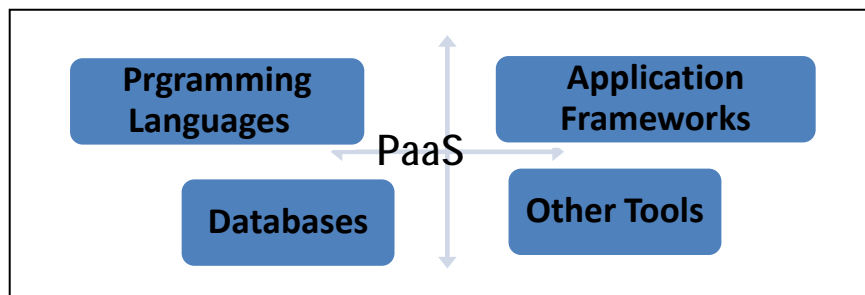


Fig. 8.3.9: Services offered by PaaS providers

Characteristics of PaaS are as follows:

- **All in One:** Most of the PaaS providers offer services like programming languages to develop, test, deploy, host and maintain applications in the same Integrated Development Environment (IDE).
 - **Web access to the development platform:** PaaS provides web access to the development platform that helps the developers to create, modify, test, and deploy different applications on the same platform.
 - **Offline Access:** To enable offline development, some of the PaaS providers allow the developer to synchronize their local IDE with the PaaS services. The developers can develop an application locally and deploy it online whenever they are connected to the Internet.
 - **Built-in Scalability:** PaaS services provide built-in scalability to an application that is developed using any particular PaaS. This ensures that the application is capable of handling varying loads efficiently.
 - **Collaborative Platform:** To enable collaboration among developers, most of the PaaS providers provide tools for project planning and communication.
 - **Diverse Client Tools:** PaaS providers offer a wide variety of client tools like Web User Interface (UI), Application Programming Interface (API) etc. to help the developers to choose the tool of their choice.
- (c) **Software as a Service (SaaS):** SaaS provides ability to the end users to access an application over the Internet that is hosted and managed by the service provider. Thus, the end users are exempted from managing or controlling an application the development platform, and the underlying infrastructure. SaaS changes the way the software is delivered to the customers.

In the traditional software model, the software is delivered as a license-based product that needs to be installed in the end user device. Since SaaS is delivered as an on-demand service over the Internet, there is no need to install the software to the end-user's devices. SaaS services can be accessed or disconnected at any time based on the end user's needs.

SaaS provides users to access large variety of applications over internets that are hosted on service provider's infrastructure. For example, one can make his/her own word

document in Google docs online, s/he can edit a photo online on pixlr.com so s/he need not install the photo editing software on his/her system- thus Google is provisioning software as a service.

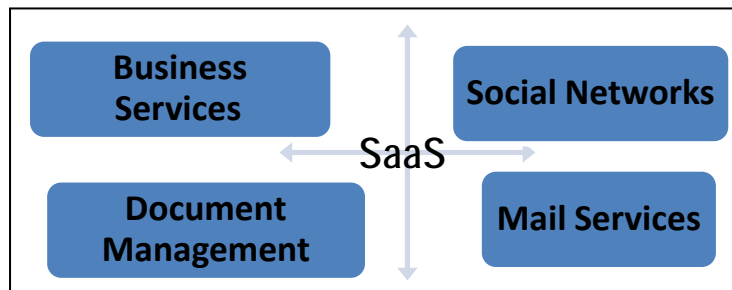


Fig. 8.3.10: Services offered by SaaS providers

The services provided by SaaS as depicted in Fig. 8.3.10 are as follows:

- (a) **Business Services:** SaaS providers provide a variety of business services to startup companies that includes ERP, CRM, billing, sales, and human resources.
- (b) **Social Networks:** Since the number of users of the social networking sites is increasing exponentially, cloud computing is the perfect match for handling the variable load.
- (c) **Document Management:** Most of the SaaS providers provide services to create, manage, and track electronic documents as most of the enterprises extensively use electronic documents.
- (d) **Mail Services:** To handle the unpredictable number of users and the load on e-mail services, most of the email providers offer their services as SaaS services.

Characteristics of SaaS are as follows:

- **One to Many:** SaaS services are delivered as one-to-many models where a single instance of the application can be shared by multiple customers.
- **Web Access:** SaaS services allow the end users to access the application from any location of the device is connected to the Internet.
- **Centralized Management:** Since SaaS services are hosted and managed from the central location, the SaaS providers perform the automatic updates to ensure that each customer is accessing the most recent version of the application without any user-side updates.
- **Multi-device Support:** SaaS services can be accessed from any end user devices such as desktops, laptops, tablets, smartphones, and thin clients.
- **Better Scalability:** Most of the SaaS services leverage PaaS and IaaS for its development and deployment and ensure a better scalability than traditional software.

- High Availability: SaaS services ensure 99.99% availability of user data as proper backup and recovery mechanisms are implemented.
- API Integration: SaaS services have the capability of integrating with other software or service through standard APIs.

The different instances of SaaS are as follows:

- Testing as a Service (TaaS): This provides users with software testing capabilities such as generation of test data, generation of test cases, execution of test cases and test result evaluation on a pay-per-use basis.
- API as a Service (APIaaS): This allows users to explore functionality of Web services such as Google Maps, Payroll processing, and credit card processing services etc.
- Email as a Service (EaaS): This provides users with an integrated system of emailing, office automation, records management, migration, and integration services with archiving, spam blocking, malware protection, and compliance features.

(d) Other Cloud Service Models

- Communication as a Service (CaaS): CaaS has evolved in the same lines as SaaS. CaaS is an outsourced enterprise communication solution that can be leased from a single vendor. The CaaS vendor is responsible for all hardware and software management and offers guaranteed Quality of Service (QoS). It allows businesses to selectively deploy communication devices and modes on a pay-as-you-go, as-needed basis. This approach eliminates the large capital investments. Examples are: Voice over IP (VoIP), Instant Messaging (IM), Collaboration and Videoconferencing application using fixed and mobile devices.
- Data as a Service (DaaS): DaaS provides data on demand to a diverse set of users, systems or application. The data may include text, images, sounds, and videos. Data encryption and operating system authentication are commonly provided for security. DaaS users have access to high-quality data in a centralized place and pay by volume or data type, as needed. However, as the data is owned by the providers, users can only perform read operations on the data. DaaS is highly used in geography data services and financial data services.
- Security as a Service (SECaaS): It is an ability given to the end user to access the security service provided by the service provider on a pay-per-use basis. It is a new approach to security in which cloud security is moved into the cloud itself whereby cloud service users will be protected from within the cloud using a unified approach to threats. Four mechanisms of Cloud security that are currently provided are Email filtering, Web content filtering, Vulnerability management and Identity management.

- *Identity as a Service (IDaaS)*: It is an ability given to the end users; typically an organization or enterprise; to access the authentication infrastructure that is built, hosted, managed and provided by the third party service provider. Generally, IDaaS includes directory services, authentication services, risk and event monitoring, single sign-on services, and identity and profile management.

8.4.1 Components of Mobile Computing

The key components of Mobile Computing are as follows:

- **Mobile Communication:** This refers to the infrastructure put in place to ensure that seamless and reliable communication goes on. This would include communication properties, protocols, data formats and concrete technologies.
- **Mobile Hardware:** This includes mobile devices or device components that receive or access the service of mobility. They would range from Portable laptops, Smart Phones, Tablet PCs, and Personal Digital Assistants (PDA) that use an existing and established network to operate on. At the back end, there are various servers like Application Servers, Database Servers and Servers with wireless support, WAP gateway, a Communications Server and/or MCSS (Mobile Communications Server Switch) or a wireless gateway embedded in wireless carrier's network (this server provide communications functionality to allow the handheld device to communicate with the internet or Intranet Infrastructure). The characteristics of mobile computing hardware are defined by the size and form factor, weight, microprocessor, primary storage, secondary storage, screen size and type, means of input, means of output, battery life, communications capabilities, expandability and durability of the device.
- **Mobile Software:** Mobile Software is the actual programme that runs on the mobile hardware and deals with the characteristics and requirements of mobile applications. It is the operating system of that appliance and is the essential component that makes the mobile device operates. Mobile applications popularly called Apps are being developed by organizations for use by customers but these apps could represent risks, in terms of flow of data as well as personal identification risks, introduction of malware and access to personal information of mobile owner.

8.4.2 How Mobile Computing Works?

Here is how Mobile Computing works:

- The user enters or access data using the application on handheld computing device.
- Using one of several connecting technologies, the new data are transmitted from handheld to site's information system where files are updated and the new data are accessible to other system user.
- Now both systems (handheld and site's computer) have the same information and are in sync.
- The process work the same way starting from the other direction.

The process is similar to the way a worker's desktop PC access the organization's applications, except that user's device is not physically connected to the organization's system. The communication between the user device and site's information systems

uses different methods for transferring and synchronizing data, some involving the use of Radio Frequency (RF) technology.

8.4.3 Mobile Computing Services

The ability to share information across a wireless platform is becoming more vital to the today's business communication needs. Various companies design and develop several wireless applications and solutions for Blackberry, iPhone, Google Android G1, iPad, Windows Mobile, Symbian, Brew devices, PDA, Palm & Pocket PC. Mobile Computing Services allow mobile workforces to access a full range of corporate services and information from anywhere, at any time and it improves the productivity of a mobile workforce by connecting them to corporate information systems and by automating paper-based processes.

8.4.4 Benefits of Mobile Computing

In general, Mobile Computing is a versatile and strategic technology that increases information quality and accessibility, enhances operational efficiency, and improves management effectiveness. But, more specifically, it leads to a range of tangible benefits, including the following:

- It provides mobile workforce with remote access to work order details, such as work order location, contact information, required completion date, asset history relevant warranties/service contracts.
- It enables mobile sales personnel to update work order status in real-time, facilitating excellent communication.
- It facilitates access to corporate services and information at any time, from anywhere.
- It provides remote access to the corporate Knowledgebase at the job location.
- It enables to improve management effectiveness by enhancing information quality, information flow, and ability to control a mobile workforce.

8.4.5 Limitations of Mobile Computing

- **Insufficient Bandwidth:** *Mobile Internet access is generally slower than direct cable connections using technologies such as General Packet Radio Service (GPRS) and Enhanced Data for GSM (Global System for Mobile Communication) Evolution (EDGE), and more recently 3G networks. These networks are usually available within range of commercial cell phone towers. Higher speed wireless LANs are inexpensive but have very limited range.*
- **Security Standards:** *When working mobile, one is dependent on public networks, requiring careful use of Virtual Private Network (VPN). Security is a major concern while concerning the mobile computing standards. One can easily attack the VPN through a huge number of networks interconnected through the line.*
- **Power consumption:** *When a power outlet or portable generator is not available, mobile computers must rely entirely on battery power. Combined with the compact size of many mobile devices, this often means unusually expensive batteries must*

be used to obtain the necessary battery life. Mobile computing should also look into Greener IT in such a way that it saves the power or increases the battery life.

- Transmission interferences: Weather, terrain, and the range from the nearest signal point can all interfere with signal reception. Reception in tunnels, some buildings, and rural areas is often poor.
- Potential health hazards: People who use mobile devices while driving are often distracted from driving and are thus assumed to be more likely involved in traffic accidents. Cell phones may interfere with sensitive medical devices. There are allegations that cell phone signals may cause health problems.
- Human interface with device: Screens and keyboards tend to be small, which may make them hard to use. Alternate input methods such as speech or handwriting recognition require training.

8.4.6 Issues in Mobile Computing

- Security Issues: Wireless networks have relatively more security requirements than wired network. A number of approaches have been suggested and also the use of encryption has been proposed.
 - Confidentiality: Preventing unauthorized users from gaining access to critical information of any particular user.
 - Integrity: Ensures unauthorized modification, destruction or creation of information cannot take place.
 - Availability: Ensuring authorized users getting the access they require.
 - Legitimate: Ensuring that only authorized users have access to services.
 - Accountability: Ensuring that the users are held responsible for their security related activities by arranging the user and his/her activities are linked if and when necessary.
- Bandwidth: Bandwidth utilization can be improved by logging (bulk operations against short requests) and compression of data before transmission. The technique of caching frequently accessed data items can play an important role in reducing contention in narrow bandwidth wireless networks. The cached data can help improve query response time. Since mobile clients often disconnect to conserve battery power the cached data can support disconnected operations.
- Location Intelligence: As the mobile computers move, they encounter networks with different features. A mobile computer must be able to switch from infrared mode to radio mode as it moves from indoors to outdoors. Additionally it should be capable of switching from cellular mode of operation to satellite mode as the computer moves from urban and rural areas. In mobile computing; as computers are working in cells and are being serviced by different network providers, the physical distance may not reflect the true network distance. A small movement may result in a much longer path if cell or network boundaries are crossed. It will

also lead to updating of the location dependent information as described above. This can increase the network latency as well as risk of disconnection. Service connections must be dynamically transferred to the nearest server. However, when load balancing is a priority this may not be possible.

- **Power Consumption:** Mobile Computers will rely on their batteries as the primary power source. Batteries should be ideally as light as possible but at the same time they should be capable of longer operation times. Power consumption should be minimized to increase battery life. Chips can be redesigned to operate at lower voltages. Power management can also help. Individual Components, be powered down when they are idle.
- **Revising the technical architecture:** Mobile users are demanding and are important to the business world. To provide complete connectivity among users; the current communication technology must be revised to incorporate mobile connectivity. Additionally, application and data architectures must also be revised to support the demands put upon them by the mobile connectivity.
- **Reliability, coverage, capacity, and cost:** At present; wireless network is less reliable, have less geographic coverage and reduced bandwidth, are slower, and cost more than the wired-line network services. It is important to find ways to use this new resource more efficiently by designing innovative applications.
- **Integration with legacy mainframe and emerging client/server applications:** Application development paradigms are changing. As a result of the IT industry's original focus on mainframes, a huge inventory of applications using communications interfaces that are basically incompatible with mobile connectivity have been accumulated. Still the application development trend is geared towards wired network.
- **End-to-end design and performance:** Since mobile computing involves multiple networks (including wired) and multiple application server platforms; end-to-end technical compatibility, server capacity design, and network response time estimates are difficult to achieve.
- **Business challenges:** In addition to these technical challenges, mobile computing also faces business challenges. This is due to the lack of trained professionals to bring the mobile technology to the general people and development of pilot projects for testing its capabilities.

8.5 Green Computing

Green computing or Green IT refers to the study and practice of environmentally sustainable computing or IT. In other words, it is the study and practice of establishing / using computers and IT resources in a more efficient and environmentally friendly and responsible way. Computers consume a lot of natural resources, from the raw materials needed to manufacture them, the power used to run them, and the problems of disposing them at the end of their life cycle. This can include "designing, manufacturing, using, and disposing of computers, servers,

and associated subsystems - such as monitors, printers, storage devices, and networking and communications systems - efficiently and effectively with minimal or no impact on the environment”.

The objective of Green computing is to reduce the use of hazardous materials, maximize energy efficiency during the product’s lifetime, and promote the recyclability or biodegradability of defunct products and factory waste. Such practices include the implementation of energy-efficient Central Processing Units (CPUs), servers and peripherals as well as reduced resource consumption and proper disposal of electronic waste (e-waste).

8.5.1 Relevant Facts

All businesses are increasingly dependent on technology, and small business is no exception. We work on our PCs, notebooks and smart phones all day, connected to servers running 24x7. Since the technology refresh cycle is fast, these devices quickly become obsolete, and at some point - more often sooner than later - we dispose of old devices and replace them with new ones. We use massive quantities of paper and ink to print documents, many of which we promptly send to the circular file.

In the process, most businesses waste resources, in the form of energy, paper, money and time - resources we could invest to develop new products or services, or to hire and train employees. Even if we aren’t a tree hugger, it makes good business sense to green our IT environment and culture. Fortunately, there are many simple steps one can take to do this, no matter what the size of the business, or how far someone is in the process. Many IT vendors have major initiatives underway to green their products, services and practices. These include building computers with more environmentally friendly materials, designing them to be consume less energy, providing recycling programs to dispose of old systems, developing virtualization and cloud computing alternatives, and providing tips to businesses that want to go green.

8.5.2 Green Computing Best Practices

Government regulation, however well-intentioned, is only part of an overall green computing philosophy. The work habits of computer users and businesses can be modified to minimize adverse impact on the global environment. Some of such steps for Green IT include the following:

Develop a sustainable Green Computing plan

- ***Involve stakeholders to include checklists, recycling policies, recommendations for disposal of used equipment, government guidelines and recommendations for purchasing green computer equipment in organizational policies and plans;***
- Encourage the IT community for using the best practices and encourage them to consider green computing practices and guidelines.
- On-going communication about and campus commitment to green IT best practices to produce notable results.

- *Include power usage, reduction of paper consumption, as well as recommendations for new equipment and recycling old machines in organizational policies and plans; and*
- *Use cloud computing so that multiple organizations share the same computing resources, thus increasing the utilization by making more efficient use of hardware resources.*

Recycle

- *Dispose e-waste according to central, state and local regulations;*
- *Discard used or unwanted electronic equipment in a convenient and environmentally responsible manner as computers emit harmful emissions;*
- *Manufacturers must offer safe end-of-life management and recycling options when products become unusable; and*
- *Recycle computers through manufacturer's recycling services.*

Make environmentally sound purchase decisions

- *Purchase of desktop computers, notebooks and monitors based on environmental attributes;*
- *Provide a clear, consistent set of performance criteria for the design of products;*
- *Recognize manufacturer efforts to reduce the environmental impact of products by reducing or eliminating environmentally sensitive materials, designing for longevity and reducing packaging materials; and*
- *Use Server and storage virtualization that can help to improve resource utilization, reduce energy costs and simplify maintenance.*

Reduce Paper Consumption

- *Reduce paper consumption by use of e-mail and electronic archiving;*
- *Use of "track changes" feature in electronic documents, rather than redline corrections on paper;*
- *Use online marketing rather than paper based marketing; e-mail marketing solutions that are greener, more affordable, flexible and interactive than direct mail; free and low-cost online invoicing solutions that help cut down on paper waste; and*
- *While printing documents; make sure to use both sides of the paper, recycle regularly, use smaller fonts and margins, and selectively print required pages.*

Conserve Energy

- *Use Liquid Crystal Display (LCD) monitors rather than Cathode Ray Tube (CRT) monitors;*

- *Develop a thin-client strategy wherein thin clients are smaller, cheaper, simpler for manufacturers to build than traditional PCs or notebooks and most importantly use about half the power of a traditional desktop PC;*
- Use notebook computers rather than desktop computers whenever possible;
- Use the power-management features to turn off hard drives and displays after several minutes of inactivity;
- Power-down the CPU and all peripherals during extended periods of inactivity;
- Try to do computer-related tasks during contiguous, intensive blocks of time, leaving hardware off at other times;
- Power-up and power-down energy-intensive peripherals such as laser printers according to need;
- Employ alternative energy sources for computing workstations, servers, networks and data centers; and
- *Adapt more of Web conferencing offers instead of travelling to meetings in order to go green and save energy.*

8.5.3 Green IT Security Services and Challenges

IT solution providers are offering green security services in many ways. What to look in green security products, the challenges in the security services market and how security services fare in a recession. If administered properly with other green computing technologies, green security can be a cost-efficient and lucrative green IT service for solution providers. The basic aim is to increase the customer's energy savings through green security services and assess that 'how sustainable computing technology can immediately help the environment'. Green IT services present many benefits for clients as well as providers, but knowing 'how to evaluate a client's infrastructure to accommodate green technology is really a vital issue'.

Moreover, apart from the common security issues, the green security emphasizes the role of security tools, methods and practices that reduce a company's environmental impact. But to estimate the scope, to cope with the lack of green security services in the market and get advice on conserving power and purchasing switches is very important and needs a high level of sensitivity. Learning about the challenges of implementing green security and the best practices is a major hope, as the artifacts are still evolving.

8.6 Bring Your Own Device (BYOD)

BYOD (Bring Your Own Device) refers to business policy that allows employees to use their preferred computing devices, like smart phones and laptops for business purposes. It means employees are welcome to use personal devices (laptops, smart phones, tablets etc.) to connect to the corporate network to access information and application. The BYOD policy has rendered the workspaces flexible, empowering employees to be mobile and giving them the right to work beyond their required hours. The continuous influx of readily improving technological devices has led to the mass adoption of smart phones, tablets and laptops,

challenging the long-standing policy of working on company-owned devices. Though it has led to an increase in employees' satisfaction but also reduced IT desktop costs for organizations as employees are willing to buy, maintain and update devices in return for a one-time investment cost to be paid by the organization.

In the early 1990s, executing different tasks necessitated the use of different devices. For instance, an mp3 player was needed to listen to music; whereas chores, tasks and schedules were tracked by a PDA. An addition to this, list was a bulky laptop and a camera and it seemed waiting till eternity that we would ever have a single device to suit our different needs. However, remarkable advances in technology in the last decade have made it possible to perform all the above mentioned tasks using a single hi-tech device. Different technologies can work in synergy with each other, which improves user productivity and convenience.

8.6.1 Advantages of BYOD

- **Happy Employees:** *Employees love to use their own devices when at work. This also reduces the number of devices an employee has to carry; otherwise he would be carrying his personal as well as organization provided devices.*
- **Lower IT budgets:** *The employees could involve financial savings to the organization since employees would be using the devices they already possess, thus reducing the outlay of the organization in providing devices to them.*
- **IT reduces support requirement:** *IT department does not have to provide end user support and maintenance for all these devices resulting in cost savings.*
- **Early adoption of new Technologies:** *Employees are generally proactive in adoption of new technologies that result in enhanced productivity of employees leading to overall growth of business.*
- **Increased employee efficiency:** *The efficiency of employees is more when the employee works on his/her own device. In an organization provided devices, employees have to learn and there is a learning curve involved in it.*

8.6.2 Emerging BYOD Threats

Every business decision is accompanied with a set of threats and so is BYOD program too; it is not immune from them. As outlined in the Gartner survey, a BYOD program that allows access to corporate network, emails, client data etc. is one of the top security concerns for enterprises. Overall, these risks can be classified into four areas as outlined below:

- **Network Risks:** It is normally exemplified and hidden in 'Lack of Device Visibility'. When company-owned devices are used by all employees within an organization, the organization's IT practice has complete visibility of the devices connected to the network. This helps to analyze traffic and data exchanged over the Internet. As BYOD permits employees to carry their own devices (smart phones, laptops for business use), the IT practice team is unaware about the number of devices being connected to the network. As network visibility is of high importance, this lack of visibility can be hazardous. For example, if a virus hits the network and all the devices connected to the network need be

scanned, it is probable that some of the devices would miss out on this routine scan operation. In addition to this, the network security lines become blurred when BYOD is implemented.

- **Device Risks:** It is normally exemplified and hidden in 'Loss of Devices'. A lost or stolen device can result in an enormous financial and reputational embarrassment to an organization as the device may hold sensitive corporate information. Data lost from stolen or lost devices ranks as the top security threats as per the rankings released by Cloud Security Alliance. With easy access to company emails as well as corporate intranet, company trade secrets can be easily retrieved from a misplaced device.
- **Application Risks:** It is normally exemplified and hidden in 'Application Viruses and Malware'. A related report revealed that a majority of employees' phones and smart devices that were connected to the corporate network weren't protected by security software. With an increase in mobile usage, mobile vulnerabilities have increased concurrently. Organizations are not clear in deciding that 'who is responsible for device security – the organization or the user'.
- **Implementation Risks:** It is normally exemplified and hidden in 'Weak BYOD Policy'. The effective implementation of the BYOD program should not only cover the technical issues mentioned above but also mandate the development of a robust implementation policy. Because corporate knowledge and data are key assets of an organization, the absence of a strong BYOD policy would fail to communicate employee expectations, thereby increasing the chances of device misuse. In addition to this, a weak policy fails to educate the user, thereby increasing vulnerability to the above mentioned threats.

8.6.3 Mobile Computing and BYOD

Mobile computing, including BYOD is the single most radical shift in business since the PC revolution of the 1980s. Over the next decade, it will have a huge impact on how people work and live, how companies operate, and on the IT infrastructure. These services will focus on the issues and opportunities surrounding the new way to communicate and consume computing services. Mobile computing is not just PCs on the move. Mobile devices such as smart phones, tablets, and the iPod Touch, the last PDA standing are a radically different kind of devices, designed from the ground up as end points of data networks both internal corporate networks and the Internet rather than primarily as stand-alone devices. They are optimized for mobility, which means that they have to be light, easy to handle, and maximize battery life. Where laptops has a three hour battery life, the tablet and smartphone regularly run 12 hours or more between charging and serve as windows into the Cloud.

8.7 Social Media, Web 2.0 and Web 3.0

Related aspects of Social Media, Web 2.0 and Web 3.0 are as given:

8.7.1 Social Media

While considering a network, we imagine a set of entities connected with each other on a logical or a physical basis. Physical networks like computer networks are those that can be planned, implemented and managed very optimally and efficiently. However, when we move from physical to logical networks, the visualization becomes much more difficult. Social

created such as Blogging, Social Networking, Communities, Mash-ups, and Tagging. The power of Web 2.0 is the creation of new relationships between collaborators and information.

The components of Web 2.0 help to create and sustain social. Blogging is the art of social conversation and have replaced personal home pages and this helps for a more consolidated flow of thoughts and ideas. Wikis have enabled collaborative contribution and authoring among distributed teams. Tagging or folksonomy is a collaborative means of identifying information widgets to increase the power of any web site and searching required information in a faster way. Combined with other such concepts, Web 2.0 provides an ideal platform for implementing and helping Social Networks to grow.

8.7.3 Components of Web 2.0 for Social Networks

In today's environment, computer literacy is at its peak and tools that are aided through the computerization age are most effective in keeping alive a concept as complicated as Social Networks. The beauty of Web 2.0 fitment to Social Networks is that all the components of Web 2.0 are built for the growth and sustenance of Social Networks. Major components that have been considered in Web 2.0 include the following:

- **Communities:** These are an online space formed by a group of individuals to share their thoughts, ideas and have a variety of tools to promote Social Networking. There are a number of tools available online, now-a-days to create communities, which are very cost efficient as well as easy to use.
- ***RSS-generated Syndication: RSS is a format for syndicating web content that allows feed the freshly published web content to the users through the RSS reader.***
- ***Blogging: A blog is a journal, diary, or a personal website that is maintained on the internet, and it is updated frequently by the user. Blogging allows a user to make a post to a web log or a blog. Blogs give the users of a Social Network the freedom to express their thoughts in a free form basis and help in generation and discussion of topics.***
- ***Wiki: A Wiki is a set of co-related pages on a particular subject and allow users to share content. Wikis replace the complex document management systems and are very easy to create and maintain.***
- ***Usage of Ajax and other new technologies: Ajax is a way of developing web applications that combines XHTML and CSS (Cascading Style Sheets) standards-based presentation that allows the interaction with the web page and data interchange with XML (eXtensible Markup Language) and XSLT (eXtensible Stylesheet Language Transformations).***
- ***Folksonomy: This allows the free classification of information available on the web, which helps the users to classify and find information, using approaches such as tagging. Also known as Social Bookmarking, the bookmarks in a folder are not stored on the user's computer rather tagged pages are stored on the web increasing the accessibility from any computer connected to the Internet.***
- ***File Sharing/Podcasting: This is the facility, which helps users to send their media files and related content online for other people of the network to see and contribute.***

- **Mash-ups:** This is the facility, by using which people on the internet can congregate services from multiple vendors to create a completely new service. An example may be combining the location information from a mobile service provider and the map facility of Google maps in order to find the exact information of a cell phone device from the internet, just by entering the cell number.

As we see from the above components of Web 2.0, each of them contribute to help the implementation and continued existence of social Networks on a meaningful basis. While wikis and communities help to create an online space for the networks, Blogging, Folksonomy and file sharing help to information flow across the virtual world of the social networking community (as shown in Fig. 8.7.1).

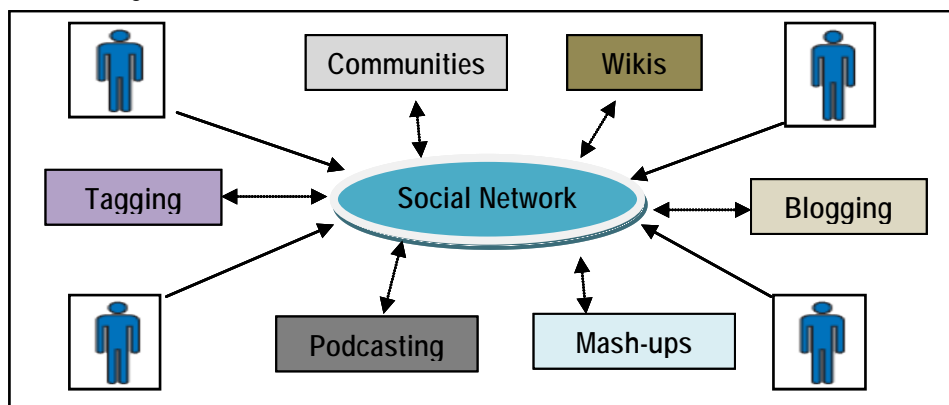


Fig. 8.7.1: Information flow in Social Networks

There is a lot of contribution that Web 2.0 has already made for social networks as well as other areas. Areas like space exploration, scientific experimentation, social sciences along with the area of collaborative research through social networks are something that Web 2.0 practitioners can actively contribute. The social impact that the technology is making via social networks is also making aware of the power and flexibility and is making Web 2.0 an integral part of social networks throughout the world.

As time progresses, the technology is becoming more secure, robust, transparent and much more user-oriented. New features like online video conferencing instead of scrap messages/blogs and Object Oriented Programming will also help in introducing new features within the social network.

8.7.4 Types and Behavior of Social Networks

The nature of social networks makes its variety. We have various types of social networks based on needs and goals. Compartmentalizing social networks is quite a challenging activity. Social networks exist in various domains-within and outside organizations, within and outside geographical boundaries, within and outside social boundaries and many other areas. Such huge variations make the reach of social networks grow to all sectors of the society. Keeping these in mind, the main categories identified are given below:

- **Social Contact Networks:** These types of networks are formed to keep contact with friends and family. These have become the most popular sites on the network today.

There are numerous reports detailing how doctors are connecting using Web 2.0 for increasing their knowledgebase.

Social networks built on Web 2.0 concepts has become so cost affordable and easy to use that more and more people are migrating to this wave. This has also helped NGO's and other social service organizations to create meaningful social networks to reach out to people in a much more structured manner and in turn benefit the needy and deprived sector of the society. Web 2.0 finds applications in different fields, some of which are as follows:

- ***Social Media: Social Media/Social Network is an important application of web 2.0 as it provides a fundamental shift in the way people communicate and share information. The social web offers a number of online tools and platforms that could be used by the users to share their data, perspectives, and opinions among other user communities.***
- ***Marketing: Web 2.0 offers excellent opportunities for marketing by engaging customers in various stages of the product development cycle. It allows the marketers to collaborate with consumers on various aspects such as product development, service enhancement, and promotion. Collaboration with the business partners and consumers can be improved by the companies by utilizing the tools provided by Web 2.0 paradigm. Consumer-oriented companies use networks such as Twitter and Facebook as common elements of multichannel promotion of their products.***
- ***Education: Web 2.0 technologies can help the education scenario by providing students and faculty with more opportunities to interact and collaborate with their peers. By utilizing the tools of Web 2.0, the students get the opportunity to share what they learn with other peers by collaborating with them.***

8.7.7 Benefits and Challenges for Social Networks using Web 2.0

Web 2.0 has provided a number of benefits to social networks. It provides a platform where users of the network need not to worry about the implementation or underlying technology at a very affordable cost and a very easy pickup time. Concepts of Web 2.0 like blogging are some things that people do on a day-to-day basis and no new knowledge skills are required. Web 2.0 techniques are very people centric activities and thus, adaptation is very fast. People are coming much closer to another and all social and geographical boundaries are being reduced at lightning speed, which is one of the biggest sustenance factors for any social network. Using Web 2.0 also increases the social collaboration to a very high degree and this in turn helps in achieving the goals for a social network.

There are a number of challenges that are faced within the implementation of social networks using Web 2.0 concepts. One of the major aspects is data security and privacy and in such public domains, there is a huge chance of data leak and confidentiality loss because there are usually no centrally mandated administrative services to take care of such aspects. Privacy of individual users also arises and can create a huge problem if malicious users somehow manage to perpetuate the social networks. This is more important for public utility networks like doctors and police. A majority of the social networks are offline, and for bringing these

under the purview of online social networks, a lot of education and advertising needs to be done, which itself becomes a cost burden, when the people involved are not computer literate. This becomes more viable in the areas of the world that are developing and do not have the basic amenities. The fact is that these areas are the ones that can benefit the most using social networks in an online mode and a huge amount of effort would be needed to help them using the technologies.

Web 2.0 has introduced a number of powerful features that social networks are utilizing. These have provided significant advances, which can be seen by the worldwide acceptance of networking sites with these technologies. In spite of all challenges, the worldwide acceptance of social networks and its implementation using Web 2.0 is here to stay and flourish. It is up to us to participate in this movement and continue to contribute towards the betterment of the technology and concept for more contribution to the society as a whole.

8.7.8 Web 3.0

The term Web 3.0, also known as the Semantic Web, describes sites wherein the computers will be generated raw data on their own without direct user interaction. Web 3.0 is considered as the next logical step in the evolution of the Internet and Web technologies. For Web 1.0 and Web 2.0; the Internet is confined within the physical walls of the computer, but as more and more devices such as smartphones, cars and other household appliances become connected to the web, the Internet will be omnipresent and could be utilized in the most efficient manner.

Web 2.0 technologies allows the use of read/write web, blogs, interactive web applications, rich media, tagging or folksonomy while sharing content, and also social networking sites focusing on communities. At the same time, Web 3.0 standard uses semantic web technology, drag and drop mash-ups, widgets, user behavior, user engagement, and consolidation of dynamic web contents depending on the interest of the individual users. Web 3.0 technology uses the "Data Web" Technology, which features the data records that are publishable and reusable on the web through query-able formats. The Web 3.0 standard also incorporates the latest researches in the field of artificial intelligence.

An example of typical Web 3.0 application is the one that uses content management systems along with artificial intelligence. These systems are capable of answering the questions posed by the users, because the application is able to think on its own and find the most probable answer, depending on the context, to the query submitted by the user. In this way, Web 3.0 can also be described as a "machine to user" standard in the internet.

The two major components of Web 3.0 are as follows:

- *Semantic Web: This provides the web user a common framework that could be used to share and reuse the data across various applications, enterprises, and community boundaries. This allows the data and information to be readily intercepted by machines, so that the machines are able to take contextual*

decisions on their own by finding, combining and acting upon relevant information on the web.

- Web Services: *It is a software system that supports computer-to-computer interaction over the Internet. For example - the popular photo-sharing website Flickr provides a web service that could be utilized and the developers to programmatically interface with Flickr in order to search for images.*

To conclude, Web 3.0 helps to achieve a more connected open and intelligent web applications using the concepts of natural language processing machine learning, machine reasoning and autonomous agents.

