Information System Controls

Information Systems controls are a set of procedures and technological measures to ensure secure and efficient operation of information within an organization. Both general and application controls are used for safeguarding information systems.

General Controls

These controls apply to information systems activities throughout an organization. The most important general controls are the measures that control access to computer systems and the information stored or transmitted over telecommunication networks. General controls include administrative measures that restrict employee access to only those processes directly relevant to their duties, thereby limiting the damage an employee can do. Some general controls are as follows.

1. **Software Controls –** Monitor the use of system software and prevent unauthorized access of software programs, system failure and computer programs.
2. **Hardware Controls –** Ensure the computer hardware is physically secure and check for equipment malfunctions. Computer equipment should be specially protected against extreme temperatures and humidity. Organizations should make provisions for backup or continued operation to maintain constant service.
3. **Computer Operations Controls –** This include controls over setup of computer processing jobs and computer operations and backup and recovery procedures for processing that ends abnormally.
4. **Data Security Controls –** Ensures critical business data on disk and tapes are not subject to unauthorized access, change or destruction while they are in use or in storage.
5. **Implementation Controls –** Audit the system development process at various points to ensure that the process is properly controlled and managed.
6. **Administrative Controls –** Formalize standards, rules, procedures and control discipline to ensure that the organization's general and application controls are properly executed and enforced.

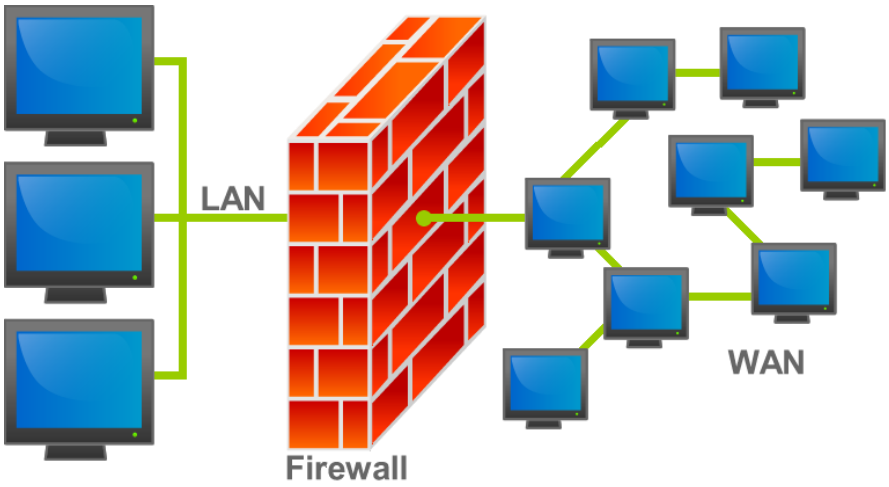
Application Controls

Application controls are specific to a given application and include measures as validating input data, regular archiving copies of various databases, and ensuring that information is disseminated only to authorized users. This can be classified as input, processing and output controls.

1. **Input Controls** – Input controls check data for accuracy and completeness when they enter the system. There are specific input controls for input authorization, data conversion, data editing and error handling.
2. **Processing Controls** – Processing controls establish that data are complete and accurate during updating. Run control totals, computer matching, and programmed edit checks are used as processing controls.
3. **Output Controls** –Output controls ensure that the results of computer processing are accurate, complete and properly distributed.

Controls in Network Information Systems

1. **Firewall –**The firewall acts like a gatekeeper that examines each user's credentials before access is granted to a network. The firewall identifies names, internet protocol (IP) addresses, applications and other characteristics of incoming traffic. It checks this information against the access rules that have been programmed in to the system by the network administrator. The firewall prevents unauthorized communication into and out of the network, allowing the organization to enforce a security policy on traffic flowing between its network and other untrusted networks, including the internet. Firewalls can deter but not completely prevent, network penetration by outsiders and should be viewed as one element in an overall security plan. To deal with internet security effectively, broader corporate policies and procedures, user responsibilities and security awareness training may be required.



2. **Intrusion Detection System –** In addition to firewalls, commercial security vendors now provide intrusion detection tools and services to protect against suspicious network traffic attempts to access files and databases. Intrusion detection systems feature full-time monitoring tools placed at the most vulnerable places. The system generates an alarm if it finds a suspicious event. Scanning software looks for patterns indicative of known methods of computer attacks such as bad password, checks to see if important files have been removed or modified and sends warnings to the system administrator. Monitoring software examines events as they are happening to discover security attacks in progress. The intrusion detection tool can be customized to shut down a particular sensitive part of a network if it receives unauthorized traffic.

3. **Antivirus software –** Antivirus software is designed to check computer systems for the presence of computer viruses. Often the software can eliminate the virus from the infected area. However, most antivirus software is effective only against viruses already known when the software was written. To remain effective, the antivirus software must be continually updated.

Information Security

Computers and the Internet are all about information seeking, storage and exchange. Hence, the topic of security in the digital realm relates to the security of information. We need to operate in a climate where our information is not stolen, damaged, compromised or restricted. The Internet, in theory, provides everyone with an equal opportunity to access and disseminate information. Yet, as many incidents have shown, this is not always the case. Governments and corporations realize the importance and value of controlling information flows, and of being able to decide when to restrict them. The security of information is further complicated by malicious individuals creating computer viruses and hacking into computer systems, often with no other motive than causing damage. The five features of a good information security are confidentiality, integrity, authentication and non repudiation.

Some of the information security mechanisms are as follows.

Windows Security

- Regularly update your operating system
- Know the locations of different files and documents on your computer
- Use a BIOS password to protect the computer at start up
- Use a lock screen function or password-protected screen saver to prevent immediate access to your computer
- Do not use an empty password or reveal your password to others
- Be careful when installing new software or buying a computer with pre-installed software.

Password Protection

- Create passwords which are 8 characters or longer
- Remember your passwords and keep them safe. Do not use easy to guess password.
- Use numbers, small letters, capitals and symbols in your password.
- Never use the same password twice
- Do not use passwords which can be directly related or linked to your personal life or interests.
- Do not share or tell anyone your important passwords.
- Change your passwords every 2-3 months.
- Remember that there are many programs available free on the Internet, which will identify your Windows password, wireless network encryption and just about any other type of computer password you may have.

Information Backup, Destruction and Recovery

- A backup strategy should include: the files to be archived, the frequency of updating the archive, location and storage of the archive.
- Sensitive information needs to be wiped from your computer.
- It is good practice to wipe temporary files, Internet cache and free space on your computer.
- Take good care of your computer's physical environment.
- If you lose a document, do a thorough search of your computer using the Windows search function and analyse your hard disk with data recovery software.

Encryption

- Encryption is the process of making your information inaccessible to all but the intended party. You can encrypt a message, an email or your entire computer.
- For secure communications utilise public key encryption. Our encryption method consists of a public and a private key. We share the public key with those who wish to communicate with us. They then encrypt a message to us using our public key.

Encryption of the internet

- Information that you send or receive on the Internet travels in an open manner.
- Some websites can help secure this information by creating an encrypted tunnel between themselves and your computer.
- The encrypted tunnel is created automatically, authenticated by you and has distinguishing features to make you aware of its existence.
- There remains a possibility of intercepting and breaking the security of this system by what is known as a Man-in-the-Middle attack.

Circumvention of internet censorship and filtering

- Website censorship can be circumvented by using a variety of software tools and methods. They differ in their complexity, reliability and success in circumventing a particular country's censorship practices.
- Keyword filtering can be overcome by using encrypted circumvention systems.

Malicious software and spam

- There are many types of malware, transmitted from computer to computer in a multitude of different ways, causing untold damage to information.
- Install and regularly update your anti-virus, anti-spyware software. Run a firewall and be extremely cautious when opening email or inserting media into your computer.
- Spam is unsolicited junk email which today constitutes an enormous part of all Internet traffic and has become a huge problem for people and networks.
- Be careful with distributing your email address and never reply to or even open spam messages.

Disaster Recovery Plan

Disaster Recovery is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. DRP is a continuous process. Once the criticality of business processes and supporting IT services, systems and data are defined, they are periodically reviewed and revisited.

Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking) and other IT infrastructure. A business continuity plan (BCP) includes planning for no-IT related aspects such as key personnel, facilities, crisis communication and reputation protection, and should refer to the disaster recovery plan (DRP) for IT related infrastructure recovery / continuity.

Recovery Point objective (RPO) and Recovery Time Objective (RTO)

In a DRP, RPO and RTO are very critical that needs to be defined and monitored. RPO is determined based on the acceptable data loss in case of disruption of operations. RTO is determined based on the acceptable downtime in case of a disruption of operations.

Steps involved in Disaster Recovery Planning

1. Identify the scope and boundaries of Disaster Recovery Plan.
2. Carry out a Business Impact Analysis (BIA)
3. Prepare the actions to recover for each disaster
4. Get the approval to DRP from the senior management
5. Each business unit need to understand its role in plan and support to maintain it.
6. The DRP project team must implement the plan and periodically check the status.

Few strategies to recover the Business Data in a Disaster situation

1. Backup made to tape and send off-site at regular intervals (Preferably daily)
2. Backups made to disk on-site and automatically copied to off-site disk, or made directly to off-site disk.
3. Replication of data to an off-site location, which overcomes the need to restore the data.
4. High availability systems which keep both the data and system replicated off-site, enabling continuous access to systems and data.
5. Wide area network optimization technology – helps improve the disaster recovery and increases network response time.

Benefits from Disaster Recovery Plan

- Information is a critical resource to any organization that helps to achieve the business objectives.
- Continuity of the Business – Ability to continue the business and serve the customer is another important result due to DRP.
- Credibility from existing stakeholders – The organization is able to keep the loyalty from the existing stakeholders and this will help the company to strengthen the position.

Information Systems Strategy

IS Strategy is a logical process that provides a 3-5 year roadmap indicating the direction of systems development, rationale, current systems, new development to consider, management strategy, implementation plan and the budget, for the IT department. This plan consist of a statement of cooperate goals and specifies how IT will support the achievement of those goals.

A typical information systems strategy will consist of the following.

1. Purpose of the plan (overview of plan, current and future business organization, key business processes, management strategy)
2. Strategic business plan (current situation, current and changing environment, major business goals, firms strategic plan)

3. Current systems (major systems supporting business functions, current infrastructure capability, difficulties in meeting business requirements, anticipated future demands)
4. New system development projects
5. Management strategy (Acquisition plan, milestones and organizational realignment internal organization, management controls, major training initiatives, personal strategy)
6. Implementation plan (progress reports, difficulties in implementation)
7. Budget requirements (requirements, potential savings, financing, acquisition cycle)

To develop an effective IS Strategy, organization must have a clear understanding of both long and short term information requirements.

Project Management Basics

Project Initiation – A project will be initiated by a project manager or sponsor gathering the information required to gain approval for the project to be created. This will be compiled in to a terms of reference or project charter that states the objective of the project, the stakeholders in the system to be produced, and the project manager and sponsor. Approval of a project initiation document (PID) or a Project Request Document (PRD) is authorization for a project to begin.

Project planning parameters–The three planning parameters areBudget (Cost), Schedule (Duration) and Effort (Resources). There is a correlation between these 3 parameters.

Software Estimation techniques

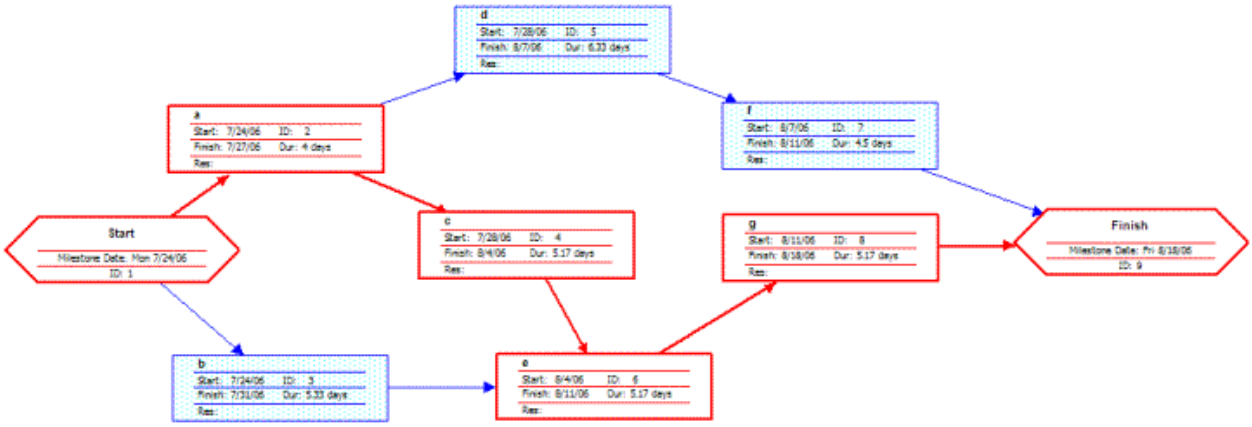
The following are some widely used software estimation techniques used.

- **Source lines of code –** although it is an outdated method, this is estimating the lines of code to be written and dividing them by the average lines of code that could be written in a unit of time.

- **Function point analysis (FPA) –** FPA is a multiple point technique widely used for estimating complexity in developing large business applications.The results of FPA are a measure of the size of an information system based on the number and complexity of the inputs, outputs, files, interfaces and queries with which a user sees and interacts.

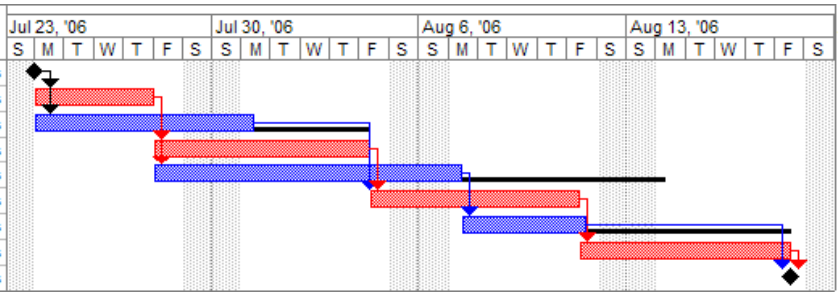
- **Three point analysis** - This applies weighting so that the most-likely estimate is weighted 4 times more than the other two estimates (optimistic and pessimistic). This formula is most valuable in estimating time or cost of activities for projects that are especially unique, such as in research and development where there are many unknowns. For projects that are similar to previous projects and there is good historical data and expert experience, the formula is less useful because you could use other techniques like analogous estimating.

PERT/Network diagram



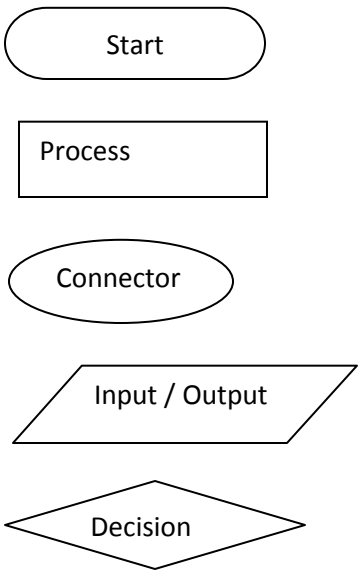
GAANT

ID	Task Name	Predecessors	Duration
1	Start		0 days
2	a	1	4 days
3	b	1	5.33 days
4	c	2	5.17 days
5	d	2	6.33 days
6	e	3,4	5.17 days
7	f	5	4.5 days
8	g	6	5.17 days
9	Finish	7,8	0 days



Project closure – Once a project is closed, all outstanding issues should be assigned, and project sponsor should be satisfied with the output. Custody of contracts and documents should be done.Lessons learnt should be documented for the benefit of future use. A post project review and post implementation review should be done.

<u>Flow Charts</u>



Example – A computer program reads students' average marks record by record. If the average is greater than 50, then the grade is "Pass" and otherwise "Fail". The grade should be displayed in the monitor, for one student and then it should read the next record. This should repeat until all student records are finished.