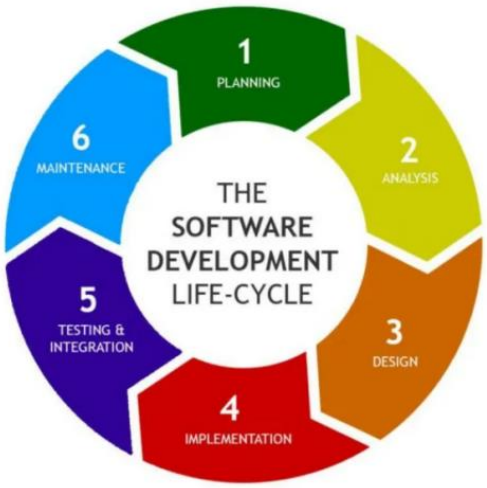
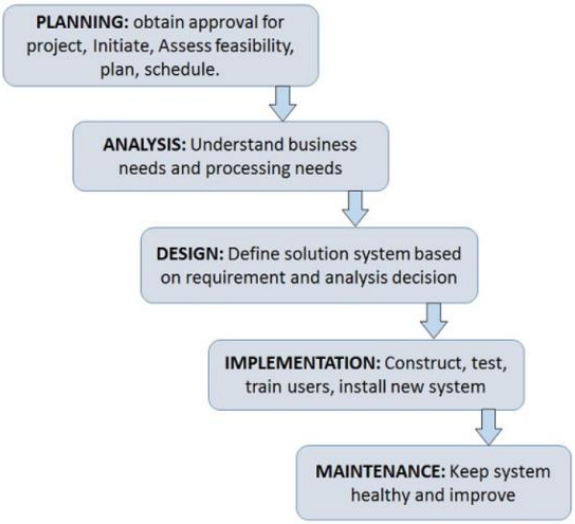
7. INFORMATION SYSTEMS

Information System: The SDLC (planning, analysis, design, implementation, maintenance phases). System security.





1. What is information system? The examples of Information systems
2. What is SDLC?
3. What are the main phases of SDLC? Briefly describe each phase.
4. What are the most common threats to information systems?
5. How to protect information systems from threats?
6. What is data center?

Information systems are combinations of hardware, software, and telecommunications networks built to collect, store, and process data. Business firms and other organizations rely on information systems to carry out and manage their operations, interact with their customers and suppliers, and compete in the marketplace. There are various types of information systems, for example: transaction processing systems (TPS), management information systems (MIS), decision-support systems (DSS), and executive support systems (ESS). An information system progresses through several phases as it is developed, used, and finally retired. These phases encompass a **System Development Life Cycle**, usually referred to as the **SDLC.**

- ✓ **Planning**. Assemble the project team, justify the project, choose the development methodology, develop a project schedule, produce a project development plan.
- ✓ **Analysis**. Activities for analysis phase are: study the current system, determine the system requirements (for a new or revised information system), and write requirements report.The project team determines requirements by interviewing users and studying successful information systems that solve similar problems. Another way to determine requirements is to construct a prototype.
- ✓ **Design**. The project team must figure out how the new system will fulfill the requirements specified in the System Requirements Report. The project team chooses a solution, selects hardware and software, and designs detailed application specifications.
- ✓ **Implementation**. During the Implementation phase of the SDLC, the project team supervises the tasks necessary to construct the new information system. The tasks that take place during the implementation phase can include: purchase and install hardware and/or software, create applications, test applications, finalize documentation, train users, convert data, convert to new system.
- ✓ **Maintenance**. The Maintenance phase is the last and the longest SDLC phase and it lasts until the system is retired. It involves day-to-day operation of the system, making modifications to improve performance, and correcting problems. Three key concepts ensure good quality of maintenance service: reliability, availability, and serviceability.

7 PHASES OF THE SYSTEM-DEVELOPMENT LIFE CYCLE

The ***System Development Life Cycle*** (SDLC for short) is a multistep, iterative process, structured in a methodical way.

This process is used to model or provide a framework for technical and non-technical activities to deliver a quality system which meets or exceeds a business's expectations or manage decision-making progression. Following are the **seven phases** of the SDLC.

1 Planning

The purpose of this first phase is to find out the scope of the problem and determine solutions. Resources, costs, time, benefits and other items should be considered here.

2 Systems Analysis & Requirements

The second phase is where teams consider the functional requirements of the project or solution. It's also where system analysis takes place—or analyzing the needs of the end users to ensure the new system can meet their expectations.

3 Systems Design

The third phase describes, in detail, the necessary specifications, features and operations that will satisfy the functional requirements of the proposed system which will be in place.

4 Development

Now the real work begins! The development phase marks the end of the initial section of the process. Additionally, this phase signifies the start of production. The development stage is also characterized by instillation & change.

5 Integration & Testing

This phase involves systems integration and system testing (of programs and procedures)—normally carried out by a Quality Assurance (QA) professional—to determine if the proposed design meets the initial set of business goals.

6 Implementation

The sixth phase is when the majority of the code for the program is written, and when the project is put into production by moving the data and components from the old system and placing them in the new system via a direct cutover.

7 Operations & Maintenance

The last phase is when end users can fine-tune the system, if they wish, to boost performance, add new capabilities or meet additional user requirements.

Information system data security.

As with personal computers, common **threats** to corporate information systems include natural disasters, power outages, equipment failures, human errors, software failures, security breaches, acts of war, and malware. When a company's brand is used without authorization, the company has become a victim of **identity theft.** Corporate identity attacks can undermine customer confidence, overwhelm customer service, generate bad publicity and result in lost revenues.

To help minimize risks the hardware and software for most corporate information systems are housed in **data centers**. A data center is a specialized facility designed to hold and protect computer systems and data. Most data centers limit physical access using password protection and fingerprint identification systems.

Several **proactive measures** can protect information systems from threats. These measures can be grouped into four: deterrents, preventive countermeasures, corrective procedures and detection activities.

Deterrents reduce the likelihood of deliberate attack. Both physical deterrents, such as limiting access to critical servers, and common deterrents, such as multi-level authentication, password protection, and biometric identification fall under this category.

Preventive countermeasures shield **vulnerabilities** to render an attack unsuccessful or reduce its impact. Firewalls that prevent unauthorized access to a system and encryption that makes stolen data indecipherable are examples of preventive countermeasures.

Corrective procedures reduce the effect of an attack. Data backups, disaster recovery plans, and the availability of redundant hardware devices all are examples of corrective procedures.

Detection activities recognize attacks and trigger preventive countermeasures or corrective procedures. For example, antivirus software detects viruses entering a system and can be configured to perform corrective procedures such as removing the virus and quarantining infected files.