Information systems

Information is the life-blood of an organization. Computers and information system permit information to be acquired, processed, and distributed efficiently. There are three basic types of information system.

Transaction processing system. It edits all input to ensure that it is accurate and complete. For example, a customer-order transaction is rejected if it contains an invalid account number or if the product code of the item is missing. All invalid transactions are identified so that they can be corrected.

Management information system. It accepts valid transactions from the transaction processing system to update contents of the database. The management information system can draw the data from the database and process it to provide management with information. It can be used to identify opportunities for improvement or to help determine alternative courses of action.

Decision support system. People use it to access the application database to get the key facts needed to help make decisions. A DSS can prevent several solutions for one problem. It permits the user to enter, retrieve, and analyze data.

Also, there is an expert system. It also called a knowledge-based system. It is a type of application program used to make decisions or solve problems in a particular field. Expert system is a key part of many DSS and executive information system.

And the last one is executive information system. It is an information system that caters specifically to the special information needs of executives, such as managerial planning, monitoring and analysis.

SDLC or a system development life circle contains of some phases: Planning, Analysis, Design, Implementation, Testing, Deployment and Maintenance.

So, the phase one is Planning. It includes next activities: assemble the project team, justify the project, choose the development methodology. The goal of the first phase is to create a Project Development Plan.

The goal of the Analysis phase is to produce a list of requirements for system. The second phase include next activities: study the current system, determine the system requirements and write a report.

The Design phase takes all the requirements and starts to plan the product. It may include the business rules, the user interface, layouts, color schemes, what programming languages to use, frameworks, system server design, database relationships, mobile aspects and much more.

During the Implementation phase of the SDLC, the project team supervises the tasks necessary to construct the new information system.

The phase five is Testing. It’s important phase that make sure all the functionality is working as expected, find many bugs to fix them.

The Deployment phase include setting up links, setting up the databases for real users and release managers. Once they are completed all of these tasks, the application will go live to real users. This brings us to the final phase of SDLC.

Maintenance phase is the longest and expensive phase. It monitors application, the load, the stress, everything coming on the servers by so many users logging in and using it, it doesn’t bring down the system. So, it helps to understand what does the system need to improve.

Threats against information system include natural disasters, power outages, equipment failures, human errors, software failures, security breaches, acts of war and malware.

Several proactive measures can protect information systems from threats. These measures can be grouped into four groups: deterrents, preventive countermeasures, corrective procedures and detection activities. Deterrents reduce the likelihood of deliberate attack. Preventive countermeasures shield vulnerabilities to render an attack unsuccessful or reduce its impact. Corrective procedures reduce the effect of an attack. Detection activities recognize attacks and trigger preventive countermeasures or corrective procedures.

To help minimize risks the hardware and software for most corporate information systems are housed in data centers. Physical security is critical to data centers. Most data centers limit physical access using password protection and fingerprint identification systems. Motion detectors, automated alarm systems and many other Metrics prevent unauthorized movement through the building.