**Topic 7 Information System**

The SDLC (planning, analysis, design, implementation, maintenance phases).

System security.

THE SDLC

Most organizations use information systems to operate more effectively, gather information, and accomplish tasks. In this section, the term information system refers to a system that uses computers and usually includes communications networks. An information system collects, stores, and processes data to provide useful, accurate, and timely information. Today most information systems rely on computers and communications networks to store, process, and transmit information with far more efficiency than would be possible using manual systems. Every organization has its mission and all activities that take place in an organization, including those that involve computers, should contribute to this mission. One of the major functions of any information system is to help people make decisions in response to problems.

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 known as System Development Life Cycle, which provides a general outline of how an information system evolves and delineates the phases of system development. Systems analysis and design is a discipline that focuses on developing information systems according to the phases of an SDLC.

The Planning phase for an information system project includes the following activities: assemble the project team, justify the project, choose the development methodology, develop a project schedule, produce a project development plan

The goal of these activities is to create a Project Development Plan. The Project Development Plan is usually reviewed and approved by management. This planning document includes:

* A short description of the project, including its scope;
* A justification for the project, which includes an estimate of the project costs and potential financial benefits;
* A list of project team participants;
* A schedule for the project, including an outline of its phases.

Depending on the scope of the problem and the expertise of the professional staff, an information systems project can be managed by an in-house information technology department or outsourced to a development firm. A system development project team is assigned to analyse and develop an information system. Other members of an organization might also be asked to participate in various phases of the project.

Justifying a project often involves identifying problems and opportunities within an organization’s current information system. Project team members can identify problems and opportunities using a variety of techniques, such as interviews and data analysis. As part of the planning phase, the project team selects one or more methodologies that provide structure for the development effort. A system development methodology guides developer through the phases of system development and specifies what takes place in each phase; it encompasses the activities, procedures, methods, best practices, deliverables, and automated tools that system developers follow to complete the SDLC. The next activity is project scheduling. It begins in the planning phase, but stretches throughout the entire project. Project managers organize the work into tasks and milestones, which can be scheduled and assigned. As tasks are completed, the schedule is updated and adjusted. Project management software is assigned to help in planning and scheduling. It helps managers track and visualize the complex interactions between tasks. Popular project management offerings include open source software such as Open Workbench, and commercial software such as Microsoft Project. Industry standard tools for scheduling and project management include: PERT (Program Evaluation and Review Technique) is a method for analysing the time needed to complete each project task and identifying the minimum time needed to complete the total project. A WBS (work breakdown structure) breaks a complex task into a series of subtasks. A Gantt chart uses bars to show the timing of development tasks as they occur over time. Each bar on the chart represents a task; the length of a bar indicates the task’s expected duration.

ANALYSIS PHASE

The Analysis phase begins after the project team selects a development methodology, draws up the Project Plan, and receives permission to proceed from management. The goal of the analysis phase is to produce a list of requirements for a new or revised information system. Activities for analysis phase are: study the current system, determine the system requirements, 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. A systems analyst shows the prototype to users, who evaluate which features of the prototype are important for the new information system. Most new information systems are designed to replace a system or process that is already in place. It is important to study the current system to understand its strengths and weaknesses before designing a new system. After the project team studies the current system and then determines what the new system should do, system requirements are incorporated into a document called a System Requirements Report that describes the objectives for an information system. System requirements are the criteria for successfully solving problems identified in an information system. A new or updated information system should meet requirements defined by the project team. A CASE tool (computer-aided software engineering tool) is a software application designed for documenting system requirements, diagramming current and proposed information systems, scheduling development tasks, and developing computer programs.

SYSTEM DESIGN PHASE

If in the Analysis phase, the project team determines what the new information system must do, in the Design phase the project team must figure out how the new system will fulfil the requirements specified in the System Requirements Report. The project team chooses a solution, selects hardware and software, and designs detailed application specifications. There might be more than one way to solve the problems and meet the requirements identified in the analysis phase of the SDLC. Some potential solutions might be better than others, more effective, less costly, or less complex. The basis for choosing hardware and software includes general criteria, such as cost and delivery time. The project team should also consider the vendor’s reliability, expertise, and financial stability. A request for proposal (RFP) is a document that describes the information system problem and the requirements for the solution. An RFP essentially asks a vendor to recommend hardware and software for the solution, and to describe the vendor’s qualifications for implementing the solution. A request for quotation (RFQ) is a request for a formal price quotation on a list of hardware and software. A project team issues an RFQ to vendors when it knows the make and model of the equipment and the titles of the software packages needed but wants to compare prices from different vendors. Technical criteria for hardware might include processing speed, reliability, upgradability, maintenance costs, and warranty. Technical criteria for software might include reliability, compatibility, and the availability of patches to fix program errors. The project team has to consider the overall architecture based on level of automation, processing methodology, and network technology. Software alternatives might also be considered. Exactly what happens next in the system design phase depends on the type of solution selected. If a turnkey solution is selected, the next step might be to get approval to move into the implementation phase of the SDLC. In contrast, if the project team selects a solution that requires custom programming, the team’s systems analysts will create a set of application specifications that describe the way the information system’s software should interact with users, store data, process data, and format reports. But the last step in this stage is to write application specifications. There is a key element in developing an effective information system and play a critical role in ensuring that the development process proceeds efficiently.

IMPLEMENTATION PHASE

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.

As the implementation phase begins, programming languages, development tools, and application software needed for the new information system are purchased, installed, and tested to ensure that they work correctly. Software testing can reveal problems that result from incompatibilities with existing hardware and software. These problems must be corrected before continuing with system development. Testing might also reveal bugs (errors) in the software, which must be corrected by the software developer. In addition to new software, the specifications for most new information systems require new hardware, which can either replace old equipment or supplement existing equipment. When the software for an information system is created by using a programming language or an application development tool, programmers must create and test all the new software modules. When an information system is constructed using application software, the software sometimes must be customized. Software customization is the process of modifying a commercial application to reflect an organization’s needs. Customization might include modifying the user interface, enabling various security settings, selecting the menus that appear on the screen, and designing forms or reports. A rigorous testing process is the only way to make sure a new information system works. Different types of testing during the implementation phase help identify and fix problems before the information system is incorporated into day-to-day business activities. One of the most important tasks during the implementation phase is to make sure the information system is completely documented so that it can be used effectively and modified easily. The documentation for an information system can be broadly categorized as system documentation or user documentation. System documentation describes a system’s features, hardware architecture, and programming. User documentation describes how to interact with the system to accomplish specific tasks. It might also include tutorials that demonstrate how to get started and how to accomplish specific tasks. In preparation for using a new information system, users generally need training on software use and data entry. During training sessions, users learn how to interact with the interface, use the new system to perform day-to- day tasks, and find additional information in user manuals, procedure handbooks, or video tutorials. Training sessions for a new information system can be conducted by members of the project team or outsourced to professional trainers. The old data must also be loaded into the new system – a process called data conversion. System conversion refers to the process of deactivating an old information system and activating a new one. It is also referred to as a «cutover» or «to go live». When converting data from an existing computer system to a new system, a programmer can write conversion software to read the old data and convert it into a format that is usable by the new system. Without such software, users would be forced to manually re-enter data from the old system into the new system.

MAINTENANCE PHASE

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. The term quality of service (QOS) refers to the level of performance a computer system provides. Typical maintenance phase activities ensure that the system functions as well as possible. During the maintenance phase, an information system is likely to undergo many changes to meet an organization’s needs. Changes can include: operating system, application software and security upgrades, user interface revisions to make the system easier to use, application software revisions to fix bugs and add features, hardware replacements necessary to retire defective equipment or enhance performance, hardware, software, or network adjustments to maintain and enhance quality of service. Although the analysis, design, and implementation phases of the SDLC are costly, for many organizations, the maintenance phase is the most expensive because it is the longest. When an information system first goes alive, maintenance costs are high while programmers work out bugs and users clamour for suggest. After most of the bugs are fixed and users become familiar with the information system, maintenance costs decrease. As an information system near the end of its useful life span, repair costs rise, and changing business practices begin to require modifications that time-consuming and expensive to implement.

INFORMATION SYSTEM DATA SECURITY

Threats against information systems are increasing. 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. Threats to a corporate information system can affect thousands of people. Natural disasters can completely shut down a computer system, cut off service to customers, and potentially destroy the system completely. Power outages can be caused by natural disasters, overloaded power grids, planned brownouts, and rolling blackouts. Equipment failures can occur in any hardware component of a computer system. The risk of failures increases as a hardware component ages, but they can occur in brand-new hardware. Human errors are mistakes made by computer operators, for example, entering inaccurate data and failing to follow required procedures. Software failures can be caused by bugs or flawed software design. Flaws in critical software that controls air traffic or nuclear power plants can be deadly. Other bugs may cause security leaks that allow unauthorized access to corporate servers. Security breaches include stolen data, physical intrusions, and deliberate sabotage. Cyberterrorism can cause damage to critical national infrastructures such as power grids and telecommunications systems. Malware can damage just about any computer system. You might have experienced the nuisance of rooting out a virus from your personal computer.

With the escalation of online crime, corporate identity theft has become a major security threat. 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. The Internet makes it easy to steal corporate identities and use them for phishing scams and fake Web sites. It is not difficult for hackers to copy logos and other graphic elements from Web pages of legitimate sites and compile them into an official-looking e-mail message. Creating a fake Web site is also easy. Hackers can obtain a URL that's similar to one used by a legitimate company by using a different country code or using .biz instead of .com. By copying and pasting a few graphics, the site looks legitimate, too. Preventing corporate identity theft is not really feasible. With current HTTP and HTML technologies, corporations have no way to lock down their branding elements, so hackers can easily misappropriate them. Consumers will remain at risk until there is universal implementation of technology that verifies a Web site's legitimacy. Companies can take steps to protect their customers and deal quickly with identity theft incidents, but no computer system can be completely risk-free. 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.

To help minimize risks the hardware and software for most corporate information systems are housed in data centres. A data centre is a specialized facility designed to hold and protect computer systems and data. It includes special security features and is designed to proactively reduce the risk of data loss that might occur as a result of a disaster. Physical security is critical to data centres. Most data centres 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. For maximum protection, some data centres are housed in former military bunkers, abandoned mines, or limestone caves to provide protection against many natural disasters and a supply of uninterrupted power from high-capacity, battery-operated uninterruptible power supplies and backup power generators to keep computers functioning during power outages. But disaster recovery plans are also critical to data security. It is a step-by-step plan that describes the methods used to secure data against disaster and sets guidelines for how an organization will recover lost data if and when a disaster occurs. It must deal not only with calamities but also must take into account day-to-day events that could potentially cause data loss.