Chapter 1

INFORMATION SYSTEM

INSIDE THIS CHAPTER

- Information system
- Types of Informations
- Development of Information Systems
- Systems Development Life Cycle (SDLC)
- Security Systems Development Life Cycle (Sec SDLC)
- Information Security
- Need for Information Security
- Threats to Information Systems
- Information Assurance
- Cyber Security

1.1. INFORMATION SYSTEM

Information System (IS) is an integrated set of components for collecting, storing and processing data for delivery knowledge and information. Organization depends on information systems to carry out and manage their operations, interact with their customers and suppliers, and complete in the marketplace. Information systems are deployed by government to provide cost-effective services to citizens. Digital goods like software and electronic books and online services like social networkings are delivered with information systems. Individuals depend on information system for study, socializing, shopping, and banking, etc.

Figure 1.1 illustrates the three fundamental roles of the business applications of information systems. Information systems provide an organization with support for business processes and operations, decision making, and competitive advantage. It has complete management information, decision support and transaction processing. These are strategic management, tactical management and operational management which can be structured, semistructured or unstructured.

Businesses today depend on the internet, intranets, and extranets to implement and manage innovative e-business applications, see figure 1.2. Internet-based and Web-enabled enterprises and global e-business and e-commerce systems are becoming common place in the operations and management of today's business enterprises.

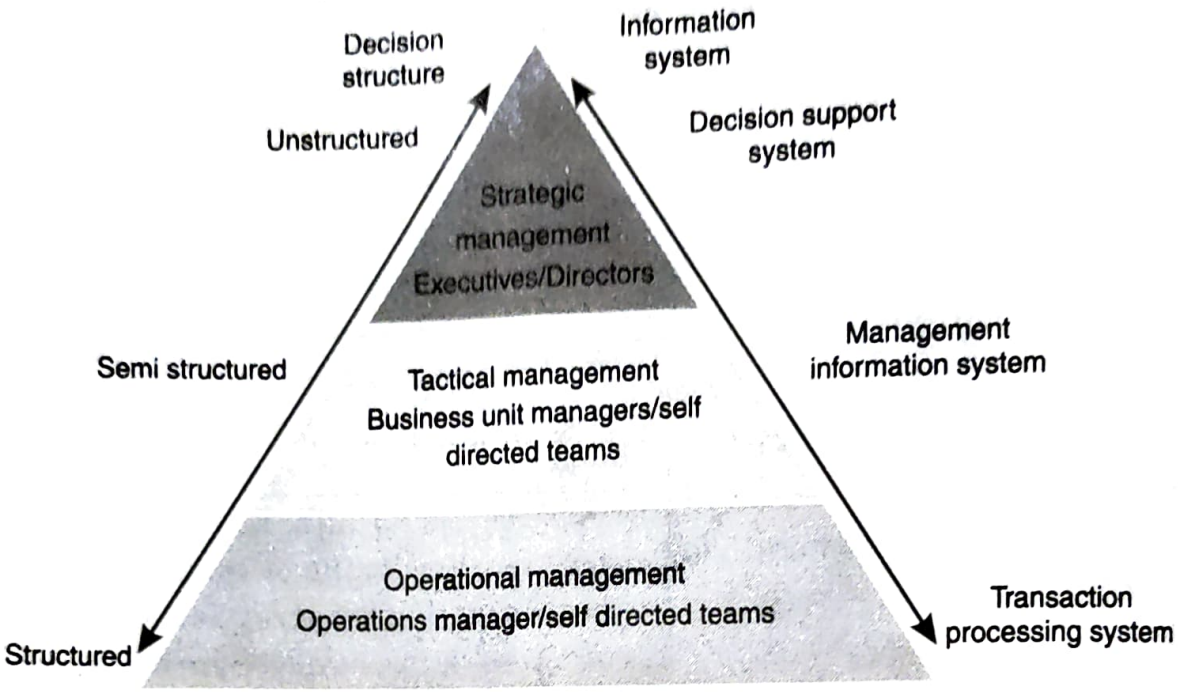
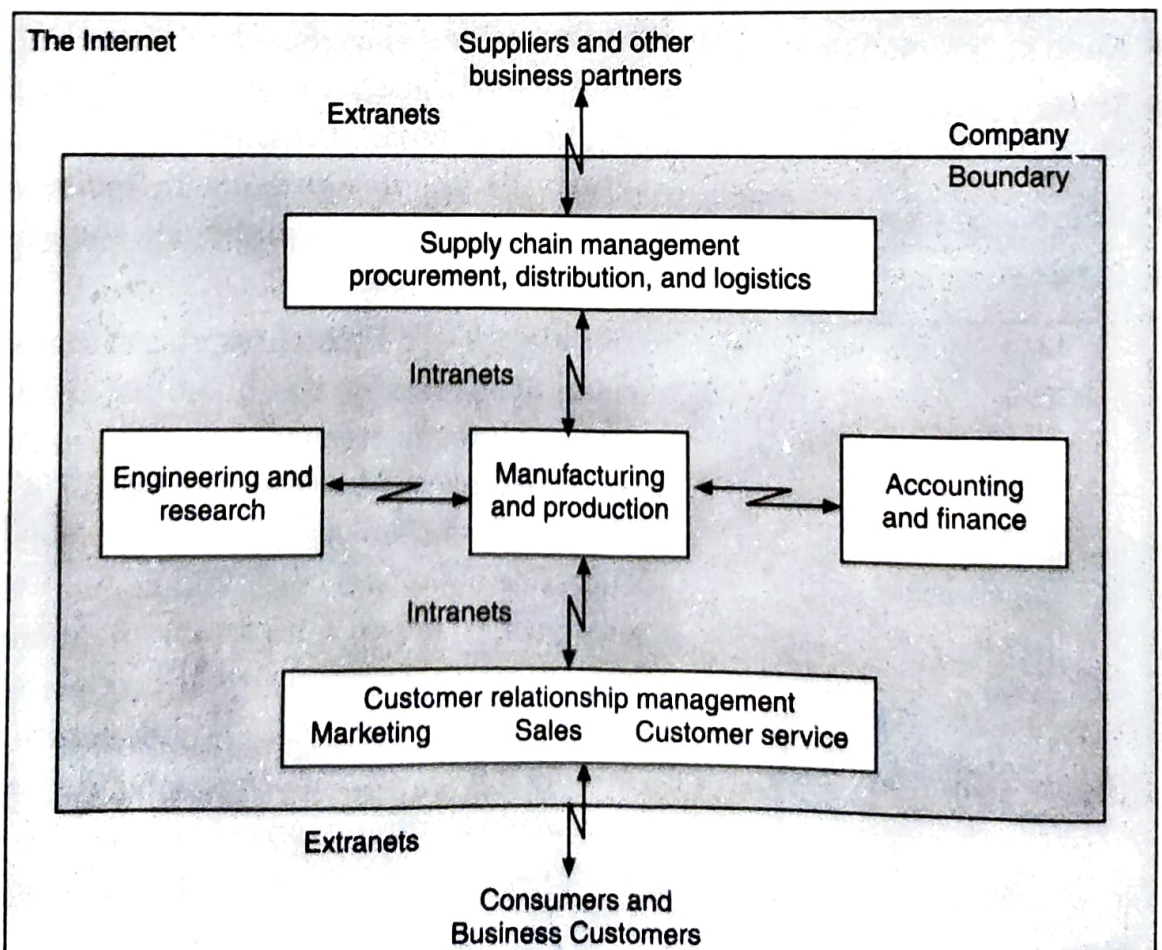


Fig. 1.1. Roles of Information System



The global usage of the Internet and the Web has enabled access to information and other resources and facilitated the forming of relationships among people and organizations on an unprecedented scale. The progress of electronic commerce our the Internet has resulted in a dramatic growth in digital interpersonal communications through e-mail and social networks, distribution of products like software, music, movies, e-books and business transactions like buying, selling, and advertising on the Web.

Information and knowledge are vital economic resources. Information systems have provided lot of opportunities but the dependence on information systems has brought new threats. There are continually new opportunities while aiming to contain the threats. The main components of information system are computer hardware and software, human resources, telecommunication, data bases and data warehouses.

Information technology is used in all kinds of businesses improve the efficiency and effectiveness of the business processes, managerial decision making, and workgroup collaboration. This strengthens the competitive positions in rapidly changing marketplaces. The information technology is used to support product development teams, customer support processes, e-commerce transactions, or any other business activity. Information technologies and systems are essential ingredient for business success.

1.2. TYPES OF INFORMATION

There are saveral methods to classify information system. Figure 1.3. illustrates the conceptual classification of information systems applications. Information systems are categorized this way to spotlight the major roles each plays in the operations and management of a business. These are expert system, knowledge management and functional management systems which support both operations and management.

(*a*) Operations Support Systems

Information systems to process data. Which produce a variety of information products for internal and external use. The role of a business firm's operations support systems is to process business transactions, control industrial processes, support enterprise communications and collaborations. It has specialized processing, transection processing, process control and interprise collaboration systems, etc.

(*i*) **Management information systems** provide information in the form of reports and displays such as sales analysis, production performance, etc.

(*ii*) **Decision support systems** provide interactive support for managers and other business professionals such as product pricing, profitability forecasting etc.

(iii) Executive information systems provide critical information tailored to the information needs of executives.

(b) Management Support Systems

The information systems support a variety of decision-making responsibilities: management information systems, decision support systems, executive information systems and also specialized processing systems.

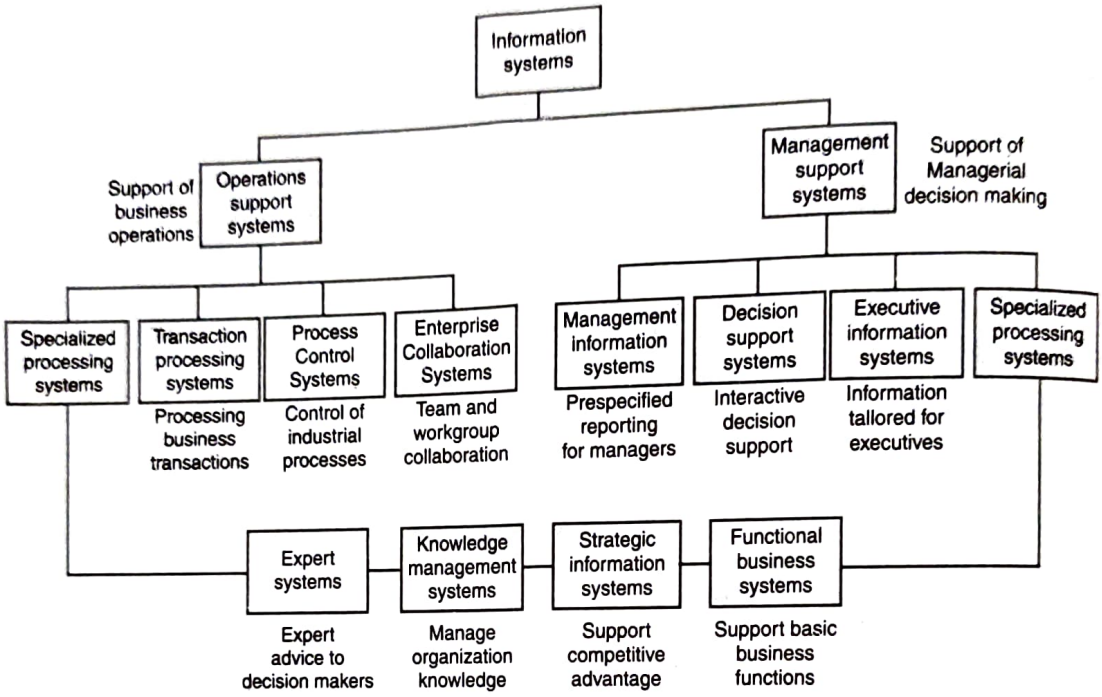


Fig. 1.3. Classification of Information Systems

(c) Specialized Information Systems (SIS)

(i) Expert systems provide expert advice and act as expert consultants to users.

(ii) Knowledge management systems support the creation, organization, and dissemination of business knowledge within the enterprise.

(iii) Strategic information systems provide a firm with strategic products, services, and capabilities for competitive advantage.

(iv) Functional business systems are support a variety of operational and managerial applications of the basic business functions of a company.

(d) Office Information System (OIS)

OIS is also known as office automation. Tasks are performed electronically using computers and other electronic devices. OIS uses word

processing, spreadsheets, databases, presentation graphics, e-mail, web browsers, web page authority, personal information management and groupware. It was communication technology such as voice mail, facsimile, video conferencing and electronic data interchange for the electronic exchange of text, graphics, audio, and video. Variety of hardware, including computers equipped with modems, video cameras, speakers, and microphones, scanners and fax machines are also used by an office information system. OIS supports both operations and management systems.

(*i*) Transaction Processing System (TPS)

It is a business activity such as a deposit, payment, order or reservation. Transaction processing systems uses batch processing. In this case, transaction data is collected over a period of time and all transaction are processed later, as a group. These days, most transactions processing systems uses online transaction processing.

(*ii*) Management Information System (MIS)

A MIS is an information system that generates accurate, timely and organized information to make decisions and supervise activities The related management information system can produce reports that recap daily sales activities, list customers with past due account balances; graph slew or fast selling products; and highlight inventory items that need reordering.

A format that an individual can review quickly and easily are summary information. A summary report contains totals, tables or graphs. For outside of a normal condition, exception information filters data to report information. The exception criteria defines the range of what is considered normal activity or status. As an example of exception report is inventory exception report. It helps to save time because they don't have to search through a detailed report, for exception. An exception report brings exceptions to the attention in an easily identifiable form.

(*iii*) Decision Support System (DSS)

Decision support systems help provide information to support decisions like need to determine how high to set yearly sales quotas based on increased sales. There are variety of DSSs for range of decisions. Data from internal and for external covers are used by a decision support system.

1.3. DEVELOPMENT OF INFORMATION SYSTEMS

In development of information systems, these are conceived, designed, and implemented using some form of systematic development process. Figure 1.4. shows that several major activities must be accomplished and managed

in a complete IS development cycle. In this development process, end users and information specialists design information system applications on the basis of an analysis of the business requirements of an organization. Business problems can be implemented and managed as a multistep process or cycle developing information systems solutions. The successful management of information systems and technologies presents major challenges to business managers and professionals.

Fig. 1.4. Development of Information Systems

Important aspects of the information systems are the security, ethical, and societal dimensions and the use of information technology in business. Information technologies can support both beneficial and detrimental effects on society in each of the are as shown in figure 1.5. Information systems deal with individuality, employment, working conditions, health, privacy, etc. and definitely crime.

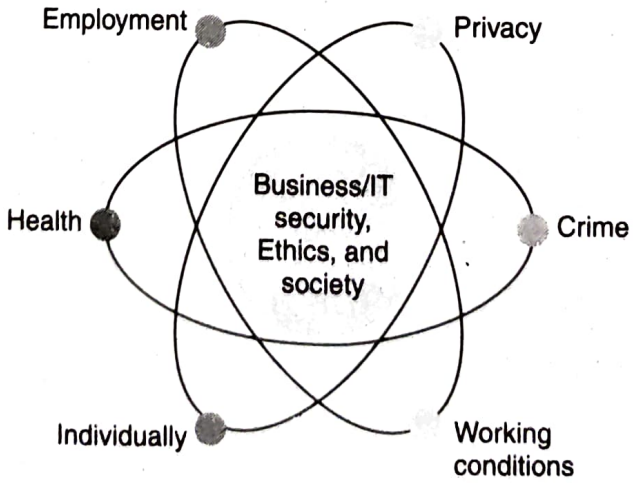


Fig. 1.5. Important aspects of information systems

There is a responsibility to promote ethical uses of information technology in the workplace. An ethical dimension needs to be considered as a business professional, responsible to make decisions about business activities and the use of information technologies that may have. In short,

complete software and communication system has to consider security aspects and build in appropriate protection.

1.4. SYSTEMS DEVELOPMENT LIFE CYCLE (SDLC)

SDLC is a methodology for the design and implementation of an information system in an organization. It is a formal approach to solving a problem based on a structured sequence of procedures. SDLC consists of 6 phases as shown in figure 1.6, which are explained.

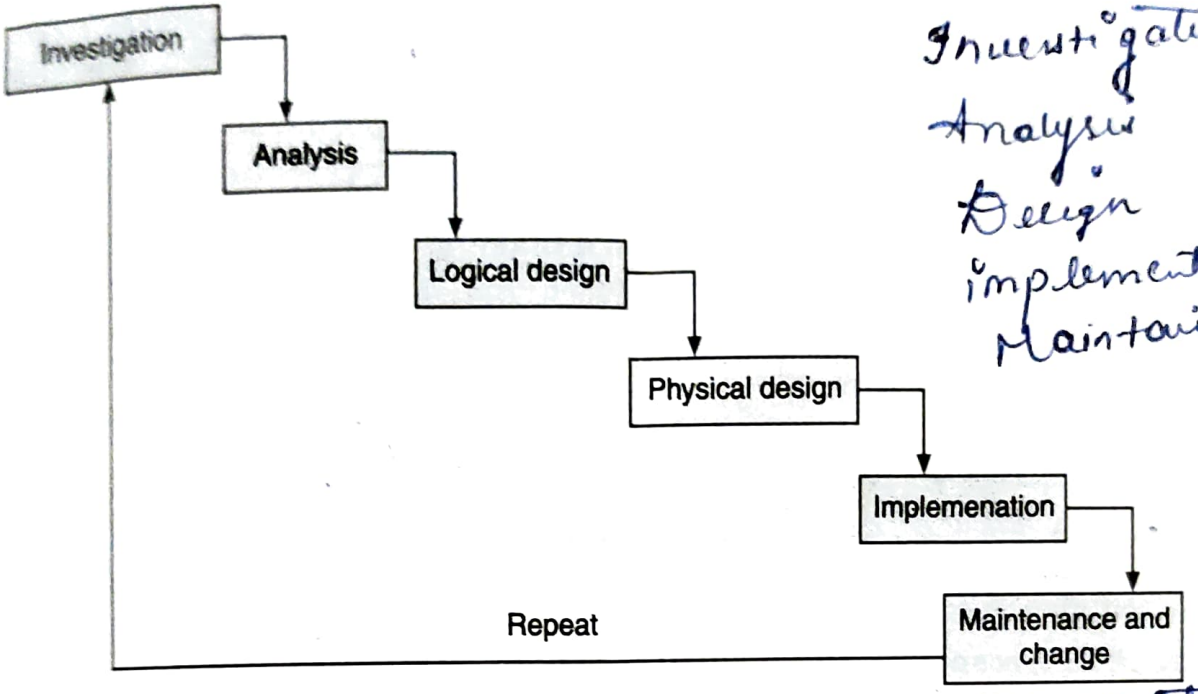


Fig. 1.6. Phases of SDLC

(*a*) Investigation

The first phase is an examination of the event or plan that initiates the process. Next, the objectives, constraints, and scope of the project are specified. At the conclusion of this phase, a feasibility analysis is performed, which assesses the economic, technical and behavioral feasibilities of the process and ensures that implementation is worth the organization's time and effort.

(*b*) Analysis

The information gained during the investigation phase are considered. This phase consists of assessments of the organization, the status of current systems, and the capability to support the proposed systems. Analysts start by determining what the new system is expected to do, and how it will interact with existing systems. Consequently, the documentation of the findings and an update of the feasibility analysis, are prepared.

(c) Logical Design

The information gained from the analysis phase is used to start creating a systems solution for a business problem. Depending on the business need, applications are selected that are capable of providing needed services. Data support and structures capable of providing the needed inputs are then chosen.

Analysts generate a number of alternative solutions, each with corresponding strengths and weaknesses, and costs and benefits. At the end of this phase, another feasibility analysis is performed.

(d) Physical Design

In the physical design phase, the specific technologies are selected to support the solutions developed in the logical design. The selected components are evaluated based on a make-or-buy decision. Final designs integrate various components and technologies.

(e) Implementation

In the phase, the needed software is created. Components are ordered, received and tested. Users are trained and supporting documentation created. The components are tested individually, they are installed and tested as a system. Another feasibility analysis is done, and the sponsors are then presented with the system for a performance review and acceptance test.

(f) Maintenance and Change

This phase consists of the tasks necessary to support and modify the system for the remainder of its useful life cycle. Periodically, the system is tested for compliance, with business needs. Upgrades, updates, and patches are managed. If the needs of the organization change, the systems that support the organization must also change. When a current system can no longer support the organization, the project is terminated and a new project is implemented.

1.5. SECURITY SYSTEMS DEVELOPMENT LIFE CYCLE (SEC SDLC)

The traditional SDLC is adapted to support the implementation of an information security project, therefore, it also has six phases.

(a) Investigation

Starting point is directive from upper management, dictating the process, outcomes, and goals of the project, as well as its budget and other

constraints. Enterprise information security policy, outlines the implementation of a security program within the organization. Teams of responsible managers, employees, and contractors are organized. Problems are analyzed. Scope specific goals and objectives, and constraints not covered in the program policy, are defined. Lastly, an organizational feasibility analysis is performed. Which determines whether the organization has the resources and commitment necessary to conduct a successful security analysis and design.

(b) Analysis

The documents from the investigation phase are studied. The development team conducts a preliminary analysis of existing security policies or programs, along with that of documented current threats and associated controls. This phase is the process of identifying, assessing, and evaluating the levels of risk facing the organization, specifically the threats to the organization's information security.

(c) Logical Design

The blueprints are developed for information security. It examines and implements key policies. The team plans the incident response actions and response to disaster. This determines feasibility of continuing and outsourcing the project.

(d) Physical Design

The information security technology needed to support the blueprint outlined in the logical design is evaluated. Alternative solutions are generated. Designs for physical security measures to support the proposed technological solutions are created. A feasibility study is done to determine the readiness of the organization for the proposed project. All parties involved have a chance to approve the project before implementation begins.

(e) Implementation

Needed software is created, components are ordered, received and tested, The security solutions are acquired, tested, implemented, and tested again Personnel issues are evaluated and specific training and education programs are conducted. At this stage, the entire tested package is presented to upper management for final approval.

(f) Maintenance and Change

In involves the constant monitoring, testing, modification, updating, and repairing to meet changing threats.

1.6. INFORMATION SECURITY

Information security relates to computing systems. Information is subjected to increasing threat of attacks, availability of number of tools and resources on internet that may be used to attack system. Enterprise system connected in network share confidential information products. There is a need of security in computing and lack of specialized resources.

There are the security concerns of software practitioners as well as those professionals, managers and users whose products, services, and well-being depend on the proper functioning of computer systems. Information security means consider available counter measures or controls, stimulate through about uncovered vulnerabilities and identify areas where more work is needed.

The vulnerabilities computing systems which are prone to exploited and the different kinds of attacks that are possible. Computing system is hardware, software, storage media, data, and people that an organization uses to perform computing tasks. An unscrupulous individual could move money from one account to another without owner's permission. Computer security specialists must consider all possible means of penetration. Moreover, the penetration analysis must be done repeatedly, and especially whenever the system and its security change. Computer security is a game with rules only for the defending team. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access.

One can view any threat as being one of four kinds: interception, interruption, modification, and fabrication. Some unauthorized party may intercept an asset, a program, or a computing system.

1.7. NEED FOR INFORMATION SECURITY

An asset of the system may be lost or become unavailable as an intruder may insert spurious transactions to a network communication system or add records to an existing database, therefore, there is a need of information security.

The purpose of information security is to devise techniques to prevent the weaknesses from being exploited. There are important aspects of any computer related system namely confidentiality, integrity and availability.

(*a*) Availability

The information must be accessible and available to users when requested so that they can carry out tasks and fulfill their responsibilities. Fault tolerance and recovery mechanisms are put into place to ensure the continuity of the availability of resources.

(b) Integrity

When a security mechanism provides integrity, it protects data, or a resource, from being altered in an unauthorized fashion. If any type of illegitimate modification does occur, the security mechanism must alert the user or administrator in some manner.

(c) Confidentiality

Confidentiality is the assurance that information is not disclosed to unauthorized individuals, programs, or processes. Control mechanisms need to be in place to dictate who can access data and what the subject can do with it once they accessed it.

Infact these three characteristics can be independent or can overlap as shown in figure 1.7. and can even be mutually exclusive. A strong protection of confidentiality can severely restrict availability.

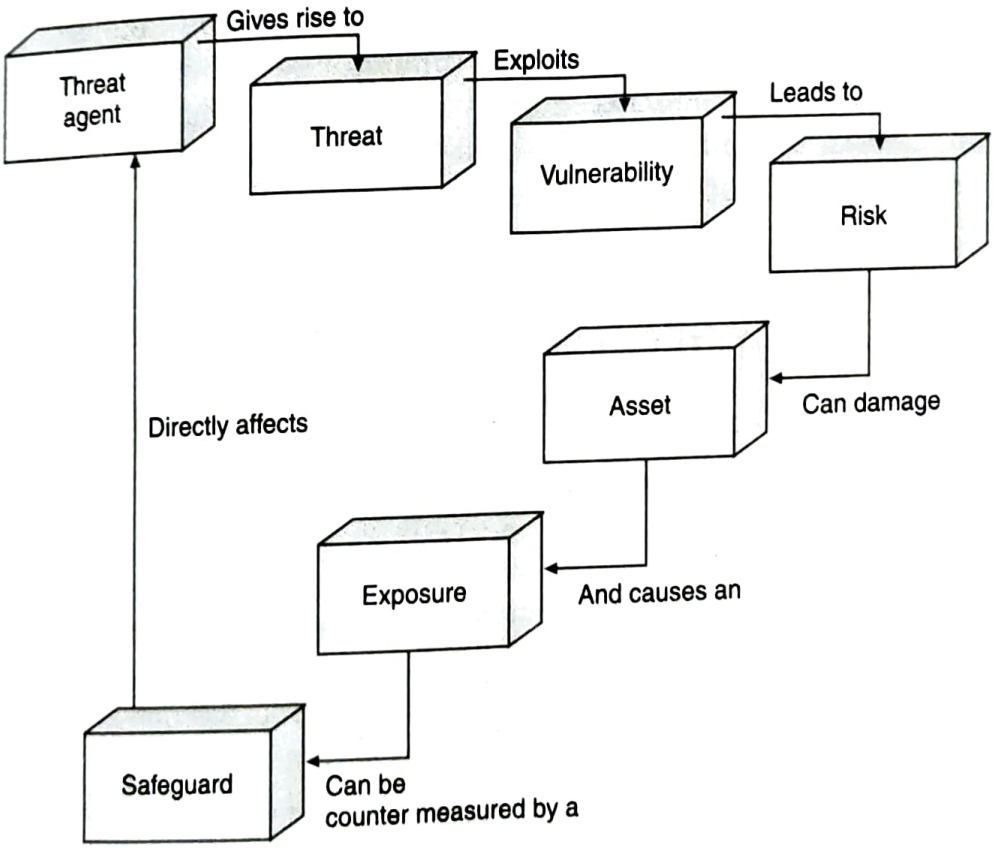


Fig. 1.7. Relationship among the different security component

It is easier to consider vulnerabilities as they apply to all three broad categories of system resources like hardware, software and data. These three assets and connections among them are all potential security weak points. Hardware is rather simple to attack by adding devices, changing them, removing them, intercepting the traffic to them, or flooding them with traffic until they can no longer function. Software can be replaced,

changed , or destroyed maliciously or it can be modified, deleted or misplaced accidentally.

Data can be gathered by many means, such as tapping wires, planting bugs in output devices, monitoring electromagnetic radiation, bribing key employees, inferring one data point from other values. The confidentiality of data is a major concern in computer security. Networks are specialized collections of hardware, software and data. Each network node is itself a computing system; as such, it experiences all the normal security problems.

1.8. THREATS TO INFORMATION SYSTEMS

Information system attackers have the potential to cripple much of the business houses and government throughout the world have access to enormous amounts of hardware, software and data.The purpose of computer security is to prevent such damage.

Most attackers are not career criminals, but rather are normal people who observe a weakness in a security system that allows them to access cash or other valuables. Cracking a computer's defenses is seen as the ultimate victimless crime. Recent attacks have shown that organized crime and professional criminals have discovered computer crime is very lucrative. Attackers use computer in the following manner:

(*a*) Targets of attack: Denial of service attack and website defacements are popular.

(*b*) Propaganda Vehicles: Web sites, web logs and e-mail lists are effective, fast, and inexpensive ways to send a message to many.

(*c*) Methods of Attack: An attack requires use of computers. The threat can be neutralized by closing the vulnerability or by blocking the attack.

Hacking is an unauthorized and the hacker does it by learning the details of computer systems. A cracker uses the knowledge of hacking for malicious purpose. An attacker can be an inside having access as an authorized user of the system. The most powerful tool in providing computer security is the scrambling or encoding. Encryption is used for the scrambling process. Encryption can virtually nullify the value of an interception and the possibility of effective modification or fabrication. Programs must be secure enough to prevent out side attack.

The hardware devices created to help in computer security. These are hardware or smart card implementation of encryption, locks or cables limiting access or deterring theft, devices to verify user's identities, firewalls, Intrusion detection systems and circuit boards that control access to storage media.

Computers security controls must be efficient enough, in terms of time, memory, human activity, or other resources used. A microcomputer application can be secured by using a combination of controls on program access to the data, on physical access to the microcomputer and storage media.

It is important to consider the weakest link. The failure in power supply that powers the firewall or the operating system and administers controls, can lead to a security failure. Computer Security ensures the confidentiality, integrity and availability of computing systems components. Areas of attacks are: hardware, software, data and the communication among them, constitute the basis of a computer security vulnerabilities.

1.9. INFORMATION ASSURANCE

The confidentiality, integrity and availability of information assets are some reasons which lead to exploitation. Attackers access to information on a target systems which may open the door to malicious code attacks. Software defects raise information assurance and security issues. Defects in software are being exploited. The primary motivation for hackers, is the money. Improving software assurance practice is a priority because of the widespread problems that defects pose the protection of the critical information infrastructure. Presently there is no way to guarantee that software is free of exploitable defects. The term for the process that addresses their problems is software assurance.

Software assurance identifies and eliminates exploitable defects in the developments acquisition, and operation of software, Software assurance guarantees that all instances of a software product are trustworthy predictable and conforment. The solution is to perform software acquisition and development work using a systematic and disciplined process. The body of knowledge that is oriented towards finding and fixing all software defects is part of software engineering. For software assurance professionals, the aim is to ensure properly running code that meet the user requirements.

Vulnerabilities are introduced at three points at the process namely design an development, distribution and updates and patches. Problems with software originate from a failure to specify the product correctly, in correct design, poor programming practice, or ineffective or inadequate review and testing. The software product are created and decisions are made about how to build it. The programmer translates the design into a computer program. Frequently, the programming stage is the source of defects. Testing is an appropriate place for information assurance professionals to be involved in software assurance. Figure 1.8. shows the

major stages involved in assuring the development of vulnerability free software.

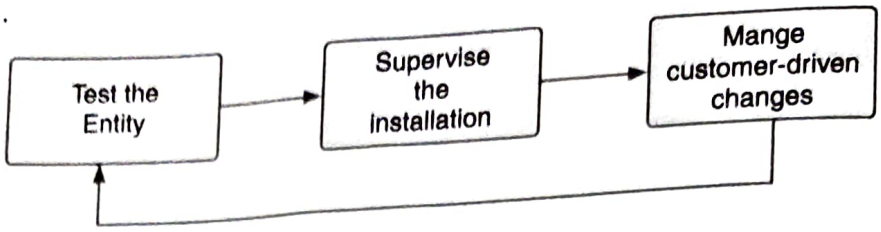


Fig. 1.8. Security in the software

The tester must have a detailed description of what the software is intended to do. Testing must provide a point of reference to confirm that the functions in the finished product align with the specified functions. The specification provides a complete, comprehensive and unambiguous statement of the behaviors that the system must exhibit. The hidden vulnerabilities may be placed in code for malicious purposes which is important to identity and eliminate them. The only way to identify hidden vulnerabilities is through code inspection.

Modern software is composed of small logical parts known as modules. The modules are defined during a design phase. That phase defines the relationship among modules and with the program structure. A rigorous code inspection is a valuable tool for information assurance and security. Serious attacks on software frequently begin with an exploitation of assumptions made by the programmer. It is important ot test each underlying assumptions using a standard method based on checklist of common programmin errors. Code reveiw checklists ensure that common code based security flaws are identified in a given piece of software. Common flaws that might be looked for during a code inspection include buffer overflow, command injection cross-site scripting, path manpulation, process control, string termination errors and unchecked return value.

After each module has passed code inspection, it is integrated into the programming system. Integration testing ensure the components have been properly integrated and their subsequent interaction do not create potential information assurance and security flaws. The process of integration testing has to be formally planned, controlled and coordinated. The integration testing plan documents actions to be taken during the testing process and specifies the test-requirements, anticipated outcome, procedures, testing responsibilities and schedules. Integration testing is important to the information assurance process.

Qualification reviewers examine each processing and security function individually to determine if it complies with all criteria for traceability, external and internal consistency and appropriateness of methods and standards. Qualification review, determine if he process elements comply

with the plan and contract. Qualification reviews are sponsored by the individual with direct responsibility for the assurance of the project.

Once the software has been accepted by the customer, it is installed in the target environment as a planned process. The installation process is a source of security vulnerabilities because the system is in transition from the control of the developer to the customer organization. Operational testing practice include intrusion detection, penetration testing, and violation assessment using boundaries called dipping levels.

Presently, companies purchase the applications as completed systems or in the form of components that are integrated into other systems. The commercial off the shelf (COTS) approach is cost effective but there should be specific consideration of the security aspects of acquisition shown in figure 1.9.

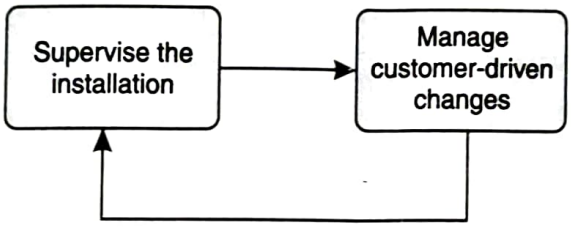


Fig. 1.9. Ensuring security in COTS software

There are standard recommendations about how to ensure security for a purchased product. Acceptance tests and associated criteria should be specified in the contract. Acceptance testing is based on the formal test plan drawn up prior to the acceptance testing process starts. Outsourcing and subcontracting magnify security problems, since there is no direct control over the developer processes except by agreement. Service level agreement (SLA) security function should be defined using a systematic process within an SLA. The range of service requirements is selected in the SLA, review the performance.

It is necessary to assign and document the information assurance related roles and responsibilities in both the contractor and customer organizations. The vender assessment process must be established by a plan that provides a road map for developing and maintaining third-party relationships. The specification of requirements is an itemized list of security behaviors to be implemented for a product The security environment has to be clearly understood to specify information assurance and security functions. The common criteria enumerates known software security attribute confirmable through direct observation and provides and encyclopedia collection of standardized adaptable security properties. The level of understanding can be employed to develop the security process. A protection profile based on standard security capabilities assessment.

Identification can be provided with the use of a username or account number. To be properly authenticated, the subject is usually required to provide a second piece to the credential set. This piece could be a password, cryptographic key or personal identification number (PIN). Accountability for the actions are taken within a system or domain. Tools used for identification, authentication, authorization, and accountability are software components that enforce access control measures.

1.10. CYBER SECURITY

Cyber Security has become an increasing strategic and economic concern. Targets of cyber attacks are major financial institutions, entertainment companies, cyber security companies and government agencies. Many of these are aimed at theft of identity or financial data. Social media and mobile devices create more opportunities for cyber attacks. Cyber warfare are intricately enmeshed with cyber crime, cyber security, cyber terrorism and cyber espionage.

Computer crime, is caused by the criminal or irresponsible actions of individuals who are taking advantage of the widespread use and vulnerability of computers and the internet and other networks. Computer crime also poses serious threats to the integrity, safety, and survival of most business systems and thus makes the development of effective security methods a top priority.

There are a dozen dangerous tools, from "scans" that ferret out weaknesses in Web site software programs to "sniffers" that rob passwords. Hacking is the unauthorized access and use of networked computer systems. Hackers can be outsiders or company employees who use the internet and other networks to steal or damage data and programs.

Unauthorized use of company-owned computer networks by employees can be private consulation or personal finances or unauthorized use of the internet on company networks. Network monitoring software, is called sniffers. It is used to monitor network traffic to evaluate network capacity, as well as to reveal evidence of improper use.

Most destructive computer crime is the creation of a computer virus or worm. A virus is a program code that cannot work without being inserted into another program. A worm is a distinct program that can run unaided. These programs copy destructive routines into the networked computer systems of anyone who accesses computers infected with the virus or who uses copies of magnetic disks taken from infected computers. Thus, a computer virus or worm can spread fast.

Use of tools like encryption selective use of sites visit or reduced used of the information help in cyber security. Privacy laws attempt to enforce

the privacy of computer-based files and communications. There is Electronic Communications Privacy Act to prevent the Computer Fraud. This prohibits intercepting data communications messages. These measures are expected to reduce stealing or destroying data.

Cyber crime attacks against the country's critical infrastructures. Cyber laws minimize damage and recovery time from cyber attacks. Actions to secure cyberspace include forensics and attack attribution, protection of networks, early watch and warnings. Damage to the economy, research, technology development, and the IT assets are secured by cyber laws.

However, it is extremely difficult for conventional law to cope with cyberspace. Some of these are given below:

(*a*) Cyberspace offers never-seen-before economic efficiency.

(*b*) Electronic information has become the main object of cyber crime.

(*c*) A software source code worth crores of rupees or a movie can be pirated across the globe within hours of their release.

(*d*) Theft of corporeal information such as CD ROMs, floppy disks is easily covered by traditional penal provisions.

(*e*) Cyberspace handles gigantic traffic volumes every second.

(*f*) Cyberspace offers enormous potential for anonymity to its members.

(*g*) Cyberspace is absolutely open to participation by all.

(*h*) Cyberspace has complete disrespect for jurisdictional boundaries.

(*i*) Cyberspace is impossible to govern and regulate using conventional law.

Chapter 2

SECURITY RISK ANALYSIS

INSIDE THIS CHAPTER

- Security Risk
- Risk Assessment
- Risk Analysis
- Documenting the Results of Risk Assessment
- Risk Audit

2.1. SECURITY RISK

A risk is the probability that a threat is capable of exploiting a known weakness or vulberability. Risk assessment is an explicit, repeatable process, which will be followed continuously by all responsible. First all the information of value to the organization has been identified, then next logical step is to itemize the risks to it. Therefore, the other necessity for effective deployment of counter measures is an understanding of the nature of the risks involved. Risk identifies and evaluates each relevant threat, determines its potential impact, and itemizes the safeguards that will be needed to control it. All risk assessments provide the probability of occurrence and the estimate of the consequences.

The basic goal of the risk assessment process is to accomplish that purpose by identifying risks with the greatest probability of occurrence and which will cause the greatest-degree of harm. Information assurance risk assessments are built around tangible evidence. That evidence that is obtained by conducting interview and documenting observations of both organizational and human behaviour.

The scope of the inquiry has to be defined precisely and be limited to a particular problem, for ensuring the effectiveness and accuracy of any particular risk assessment. The need to

point a detailed and accurate picture of all threats usually implies a series of specifically-targeted highly-integrated risk assessment that takes place over a defined period of time.

2.2. RISK ASSESSMENT

Risk assessment considers various areas of threat, electronic, human, and physical. The knowledge of specific vulnerabilities and the threats is known as a threat profile or picture threats profile, needs to be updated continuously. The risks are interdepedent in that changes to one factor which may change the situation for the other. Risk classification has two procedures namely risk identification and risk estimation. Figure 2.1 illustrates their relationship.

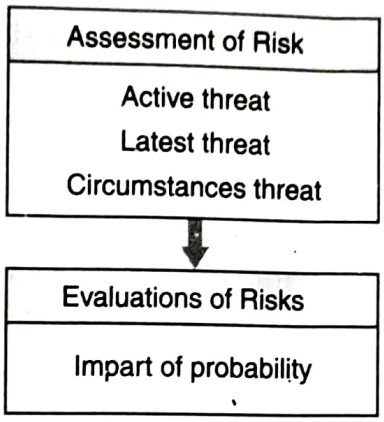


Fig. 2.1 Risk assessment relationship

Identification of risks in operations are done by compairing the current operation to the requirement of ideal practice. The analysis of these, identifies the gaps between the best practices specified by the model and the current operations. Figure 2.2. illustrates the gap analysis.

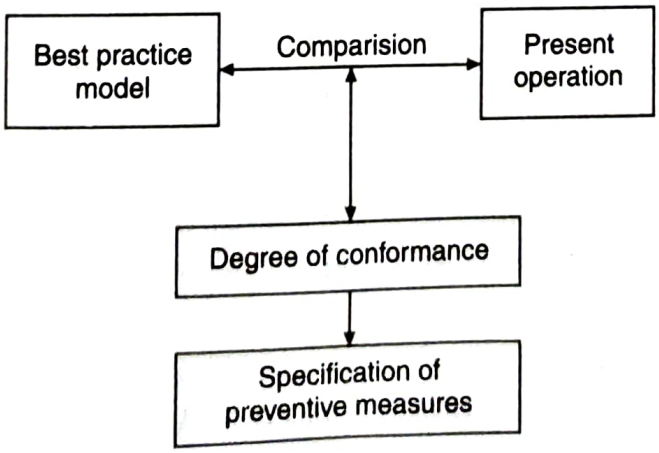


Fig. 2.2. Analysis of gap

Recommendations for best practice are compared to present practices within the organisation. The purpose of this analysis is to understand the kind of vulnerability that each gap represents. Risk classification identifies

potentially harmful risks. Variation from ideal practice that are identified through the gap analysis will have to be elevated to differentiate only those gaps that would create vulnerabilities.

Risk estimations determines the probability and impact of all threats that-have been identified through risk identification. It provides the data for the analysis and decision making about the form of the response. Severity is typically expressed in common quantitiave terms of money or time lost. Risk estimation must state the probability of occurrence and known cause and effect, relationships to each information resource. Decision making process is based on factors such as return on investment (ROI), the probability that harm will be ensured, and the probability that the event will ocurr. The adverse impacts of threats inevitably cost money, therefore, it is important to tender applicable return on investment (ROI) issues into the eventual security response. If the rate of occurrence were high, then even though the harm might be minor, a counter measure might make good business sense. A catastrophic threat is not necessarily dangerous if it only happens every several years. The estimated expense of maintaining a counter measure over one year is evaluated against the costs that will be incurred if the threat were to happen. If the expense is greater than any possible harm, then the counter measure is not included in the security response. The formula for determining annualized loss exposure (ALE) is

$$\text{ALE} = \text{Annual cost of Usage} - (\text{Annual Rate of happening} \times \text{Cost per happening})$$

2.3. RISK ANALYSIS

Expressing the likelihood of an event as a probability estimate will communicate the importance of a timely response to decision maker. The mechanism for communicating information about risk is the risk mitigation report. The risk mitigation report communicates the harm that ensures from each threat and suggests the various responses alternatives, see figure 2.3.

The functional elements that makes up that response are known as counter measures. Response application is another two stage process, which starts with a more in-depth analysis known as operational security analysis. This leads to the deployment of a concrete security solution. For operational decision making, it is important to specify a minimum degree of projection. An operational security analysis provides the information needed to assign operational priorities. Operational security analyses are performed to obtain a reliable, databased understanding of the cost/benefit situation for all identified vulnerabilities. Risk-mitigation decision are the choices made how to reduce the severity or affect of a known risk. Risk-mitigation decision also specify ways to recover from the risk.

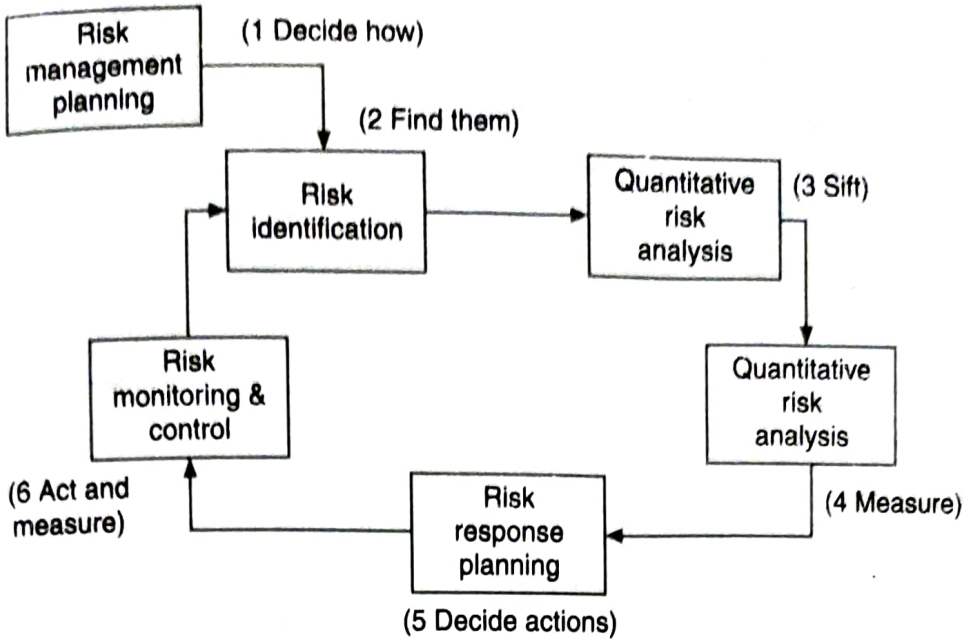


Fig. 2.3. Risk Analysis

The critical success factor for a risk valvation lie with the business case, rather than the technical one. Ways of obtaining an organizational value for an asset includes :

(*a*) Applied Information Economics.

(*b*) The Balanced Scorecard.

(c) Economic Value Added.

(*d*) Economic Value Sourced.

(*e*) Portfolio Management.

(*f*) Real Option Valuation.

The Balanced Scorecard needs that every information item should be traceable to a specific organizational goal. The data developed by the Balanced Scorecard allows an organization to value all assets appropriately. Operational risk assessments employ risk identification and estimation as the primary data-gathering mechanism and they use the risk evaluation function to decide about the nature of emerging threats.

Risk analysis identifies vulnerabilities and threats and assessing the possible impacts to determine where to implement security safeguards. Risk analysis is used to ensure that security is cost-effective relevant, timely, and responsive to threats. A risk analysis has four functions:

(*a*) Identification of assets and their value

(*b*) Identification of vulnerabilities and threats.

(c) Quantification of the probability and business impact of these potential threats.

(*d*) Providing an economic balance between the impact of the threat and the cost of the countermeasure.

Risk analysis provides a **cost/benefit comparison,** which compares the annualized cost of safeguards to the potential cost of loss. First the team must carry out project sizing to understand what assets and threats should be evaluated. Generally assessments are focused on physical security, technology security, or personnel security.

If some assets are not important, the evaluation of these assets need not be undertaken. Management should outline the scope, risk management, and compliance as well as budgetary constraints. A risk analysis helps integrate the security program objectives with the company's business objectives and requirements.

In organization must build a risk analysis team that includes individuals from many or all departments to ensure that all of the threats are identified and addressed. It should interview people in each department. The risk analysis team must also include people who understand the processes that are part of their individual departments. A lot of this information is gathered through internal surveys, interviews, or workshops.

Raising several questions helps ensure that the risk analysis team and senior management know what is important.

Although responsibility rests on senior management, but they must trust that the work they have delegated is being handled in a manner that understands, accepts the existence of, and works to minimize the risks.

The following issues should be considerations when assigning values to assets are:

(*a*) Cost of acquiring or developing the asset

(*b*) Value of the asset to owners and users

(*c*) Cost to maintain and protect the asset

(*d*) Value of the asset to hackers.

(*e*) Value of developing the information

(*f*) Price in the market of the asset

(*g*) Cost of replacement.

(*h*) Operational and production activities affected

(*i*) Liability issues if the asset is tampered.

(*j*) Usefulness and role of the asset.

The value of assets to a company may be due to reasons, including the following:

(*a*) For performing effective cost/benefit analyses

(*b*) For selecting specific countermeasures and safeguards

(*c*) For determine the level of insurance coverage to purchase

(*d*) For understand what exactly is at risk

(*e*) For conforming to due care and to comply with legal and regulatory needs requirements.

Assets may be computers, facilities, supplies or reputation, data, intellectual property. It is usually difficult to quantify the values of intangible assets, which may change over time. If a company decides the total or residual risk is too high it can purchase insurance. If a company finds the risk in low it can avoid the issue. Company can go for ***risk mitigation,*** where the risk is decreased to a level considered acceptable enough. The implementation of firewalls, training, and intrusion/detection protection systems represent types of risk mitigation.

Company can even decide to ***accept the risk.*** the company understands the level of risk it is faced with, as well as the potential cost of damage. This may be due to lack of knowledge of risk management in the security field the lack of education.

It involves establishing a standard schedule for the performance of each assessment as well as a defined process for problem reporting and corrective action. Each counter measure must have a set of observable criteria built into its specification. These criteria should be both measurable and capable of being recorded and reported meaning fully.

The actual risk assesment planning is based on organizational goals and policies and the outcome of the process must be a relevant infrastructure of procedures. Risk assessment must have to be exceptionally flexible. A risk plan should specify roles and responsibilites.

2.4. DOCUMENTING THE RESULTS OF RISK ASSESSMENT

Risk Assessment process provides a long lists of information assets with data about each of them. It helps to identify the information assets with vulnerabilities and their ranking according to those most needing protection. There are some information about the controls that exist. The final summary is the ranked vulnerability risk worksheet.

There are several basic strategies to control each of the risks from these vulnerabilities. Avoidance risk control strategy to prevents the exploitation of the vulnerability. It is done by countering threats, removing vulnerabilities in assets, limiting access to assets, aidding protective safeguards. There are three common methods of risk avoidance namely application of policy, application of training & education and application of technology.

Transference the control approach attempts to shifts the risk to other assets, other processes, or other organizations. Redisgning and architectary through rethinking how services are offered, revising deployment models, outsourcing.

Information Security mistakes made by individuals due to passwords on written on notes, leaving unattended computers on, opening e-mail attachments from strangers, poor password etiquette, laptops on the loose people who talk about passwords. Technology that enables hardware devices, installed and configured without the protection, who perform installations, unreported security violations, and not watching for dangers inside the organization.

Mitigation is the control method reduces the impact caused by the exploitation of vulnerability through planning and preparation. Mitigation needs early detection the ability of the organization to respond quickly, efficiently and effectively.

There are three types of plans for mitigation.

(a) **Incident response plan (IRP)** actions to take while incident is in progress,

(*b*) **Disaster recovery plan (DRP)** mitigation procedure.

(*c*) **Business continuity plan (BCP):** activities , if catastrophic event occurs.

It may be noticed that someone is copying information from the server without authorization, signaling violation of policy by a potential hacker or an unauthorized employee. The IRP enables the organization to take coordinated.

Disaster Recovery Plan (DRP) can include all preparations for the recovery process, strategies to limit losses during the disaster, and detailed steps to follow when attempt is stopped.

2.5. RISK AUDIT

Audit identifies nonconformances with accepted practice and identifies new risks. If new risks or non conformanes are detected, audit notifies the parties responsible for restoring conformity. Figure 2.4 outlines the audit In the case of information assurance, the primary reasons for an audit is verification of conformity with a particular strategy, plan, standard, regulation, or guideline. These audits are almost the only method for assessing operational risks in the outsourced work and controlling and ensuring the integrity of the final product, for the subcontroller and outscoured work.

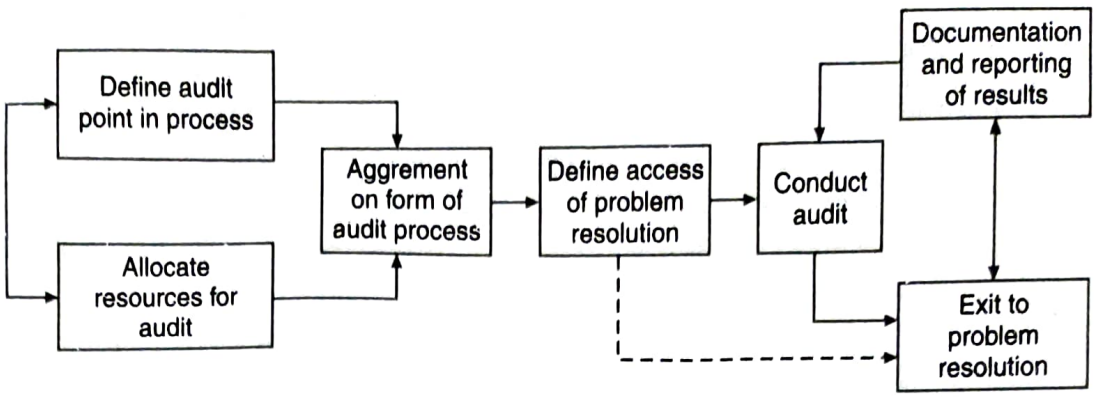


Fig. 2.4. Audit process

In the case of information assurance, the primary reasons. An audit is verification of conformity with a particular strategy, plan, standard, regulation, or guideline. In the case of subcontractor and outsecured work these audits are almost the only method for assessing operational risks in the outsourced work and controlling and ensuring the integrity of the final product. Information assurance audits assess the execution of a defined set of security processes.

The customer establishes the audit these criteria in advance of the audit. The standard is used to accredit the audited organization to some specific, level of performance the audit. The items that are addressed within that frame work include such things as software integrity and control, hardware integrity and control, database integrity and control, compliance with contracts and procedures, event and incident logs. An audit accounts for the execution of a required set of procedures over time.

The parties involved in the audit have to specifically agree on how the audit will be conducted–the scope, procedures and entry and exit criteria for the process. The audit plans and schedules audit activities, tabes responsibility for the audit.

After receiving the necessary resources, the organization schedules the process, selects the auditors, and assigns the audit roles and responsibilities. There are four types of participants in an audit process namely Auditee, Lead Auditor, Auditor and Client. The identify all relevent standard and specify those criteria. A specifically designated lead auditor always manages the team. The audtior themselves must have the technical and professional expertise required to perform a proper audit. Including working knowledge of the laws and regulations.

The auditors prepare working documents from each audit. The preparations, validation and distribution of the audit forms and checklists is one of the most important activities in the audit process because they drive the rest of the process. Electronic records have to be audited using