Test Series: March, 2016

MOCK TEST PAPER – 2

FINAL COURSE: GROUP – II

PAPER – 6: INFORMATION SYSTEMS CONTROL & AUDIT

SUGGESTED ANSWERS/HINTS

1. (a) (i) The SEBI norms for selection of Auditors are as follows:

- Auditor must have minimum 3 years of experience in IT audit of Securities Industry participants e.g. stock exchanges, clearing houses, depositories etc. The audit experience should have covered all the Major Areas mentioned under SEBI's Audit Terms of Reference (TOR).
- The Auditor must have experience in/direct access to experienced resources in the areas covered under TOR. It is recommended that resources employed shall have relevant industry recognized certifications e.g. CISA (Certified Information Systems Auditor) from ISACA, CISM (Certified Information Securities Manager) from ISACA, GSNA (GIAC Systems and Network Auditor), CISSP (Certified Information Systems Security Professional) from International Information Systems Security Certification Consortium, commonly known as $(ISC)^2$.
- The Auditor should have IT audit/governance frameworks and processes conforming to industry leading practices like CoBIT.
- The Auditor must not have any conflict of interest in conducting fair, objective and independent audit of the Exchange/Depository. It should not have been engaged over the last three years in any consulting engagement with any departments/units of the entity being audited.
- The Auditor may not have any cases pending against its previous auditees, which fall under SEBI's jurisdiction, which point to its incompetence and/or unsuitability to perform the audit task.

(ii) From the perspective of the IS Audit, the following are the possible advantages of System Development Life Cycle (SDLC):

- The IS auditor can have clear understanding of various phases of the SDLC on the basis of the detailed documentation created during each phase of the SDLC.
- The IS Auditor on the basis of his/her examination, can state in his/her report about the compliance by the IS management of the procedures, if any, set by the management.

- The IS Auditor, if has a technical knowledge and ability of different areas of SDLC, can be a guide during the various phases of SDLC.
- The IS auditor can provide an evaluation of the methods and techniques used through the various development phases of the SDLC.

(b) Following are the major techniques to commit cyber frauds:

- Hacking: It refers to unauthorized access and use of computer systems, usually by means of personal computer and a telecommunication network. Normally, hackers do not intend to cause any damage.
- Cracking: Crackers are hackers with malicious intentions, which means, un-authorized entry. Now across the world hacking is a general term, with two nomenclatures namely: Ethical and Un-ethical hacking. Un-ethical hacking is classified as Cracking.
- Data Diddling: Changing data before, during, or after it is entered into the system in order to delete, alter, or add key system data is referred as data diddling.
- Data Leakage: It refers to the unauthorized copying of company data such as computer files.
- Denial of Service (DoS) Attack: It refers to an action or series of actions that prevents access to a software system by its intended/authorized users; causes the delay of its time-critical operations; or prevents any part of the system from functioning.
- Internet Terrorism: It refers to the using Internet to disrupt electronic commerce and to destroy company and individual communications.
- Logic Time Bombs: These are the program that lies idle until some specified circumstances or a particular time triggers it. Once triggered, the bomb sabotages the system by destroying programs, data or both.
- Masquerading or Impersonation: In this case, perpetrator gains access to the system by pretending to be an authorized user.
- Password Cracking: Intruder penetrates a system's defense, steals the file containing valid passwords, decrypts them and then uses them to gain access to system resources such as programs, files and data.
- Piggybacking: It refers to the tapping into a telecommunication line and latching on to a legitimate user before s/he logs into the system.
- Round Down: Computer rounds down all interest calculations to 2 decimal places. Remaining fraction is placed in account controlled by perpetrator.

- Scavenging or Dumpster Diving: It refers to the gaining access to confidential information by searching corporate records.
- Social Engineering Techniques: In this case, perpetrator tricks an employee into giving out the information needed to get into the system.
- Super Zapping: It refers to the unauthorized use of special system programs to bypass regular system controls and performs illegal acts.
- Trap Door: In this technique, perpetrator enters in the system using a back door that bypasses normal system controls and perpetrates fraud.

2. (a) Black Box Testing: Black Box Testing takes an external perspective of the test object, to derive test cases. These tests can be functional or non-functional, though usually functional. The test designer selects typical inputs including simple, extreme, valid and invalid input-cases and executes to uncover errors. There is no knowledge of the test object's internal structure.

   This method of test design is applicable to all levels of software testing i.e. unit, integration, functional testing, system and acceptance. The higher the level, hence the bigger and more complex the box, the more one is forced to use black box testing to simplify. While this method can uncover unimplemented parts of the specification, one cannot be sure that all existent paths are tested. If a module performs a function, which is not supposed to, the black box test does not identify it.

   White Box Testing: It uses an internal perspective of the system to design test cases based on internal structure. It requires programming skills to identify all paths through the software. The tester chooses test case inputs to exercise paths through the code and determines the appropriate outputs. Since the tests are based on the actual implementation, if the implementation changes, the tests probably will need to change, too. It is applicable at the unit, integration and system levels of the testing process; it is typically applied to the unit. While it normally tests paths within a unit, it can also test paths between units during integration, and between subsystems during a system level test. After obtaining a clear picture of the internal workings of a product, tests can be conducted to ensure that the internal operation of the product conforms to specifications and all the internal components are adequately exercised.

   (b) Emergency Plan: The Emergency Plan specifies the actions to be undertaken immediately when a disaster occurs. Management must identify those situations that require the plan to be invoked e.g., major fire, major structural damage, and terrorist attack. The actions to be initiated can vary depending on the nature of the disaster that occurs. If an enterprise undertakes a comprehensive security review program, the threat identification and exposure analysis phases involve identifying those situations that require the emergency plan to be invoked.

When the situations that evoke the plan have been identified, four aspects of the emergency plan must be articulated. First, the plan must show 'who is to be notified immediately when the disaster occurs - management, police, fire department, medicos, and so on'. Second, the plan must show actions to be undertaken, such as shutdown of equipment, removal of files, and termination of power. Third, any evacuation procedures required must be specified. Fourth, return procedures (e.g., conditions that must be met before the site is considered safe) must be designated. In all cases, the personnel responsible for the actions must be identified, and the protocols to be followed must be specified clearly.

Test Plan: The purpose of the Test Plan is to identify deficiencies in the emergency, backup, or recovery plans or in the preparedness of an organization and its personnel for facing a disaster. It must enable a range of disasters to be simulated and specify the criteria by which the emergency, backup, and recovery plans can be deemed satisfactory. Periodically, test plans must be invoked. Unfortunately, top managers are often unwilling to carry out a test because daily operations are disrupted. They also fear a real disaster could arise as a result of the test procedures.

To facilitate testing, a phased approach can be adopted. First, the disaster recovery plan can be tested by desk checking and inspection and walkthroughs, much like the validation procedures adopted for programs. Next, a disaster can be simulated at a convenient time-for example, during a slow period in the day. Anyone, who will be affected by the test (e.g. personnel and customers) also might be given prior notice of the test so they are prepared. Finally, disasters could be simulated without warning at any time. These are the acid tests of the organization's ability to recover from a catastrophe.

(c) The maintenance tasks undertaken in development of Business Continuity Planning (BCP) are to:

- Determine the ownership and responsibility for maintaining the various BCP strategies within the enterprise;
- Identify the BCP maintenance triggers to ensure that any organizational, operational, and structural changes are communicated to the personnel who are accountable for ensuring that the plan remains up-to-date;
- Determine the maintenance regime to ensure the plan remains up-to-date;
- Determine the maintenance processes to update the plan; and
- Implement version control procedures to ensure that the plan is maintained up-to-date.

3. (a) The performance of evidence collection and understanding the reliability of controls involves issues like-

- Data retention and storage: A client's storage capabilities may restrict the amount of historical data that can be retained "on-line" and readily accessible to the auditor. If the client has insufficient data retention capacities, the auditor may not be able to review a whole reporting period transactions on the computer system. For example, the client's computer system may save data on detachable storage device by summarising transactions into monthly, weekly or period end balances.
- Absence of input documents: Transaction data may be entered into the computer directly without the presence of supporting documentation e.g. input of telephone orders into a telesales system. The increasing use of EDI will result in less paperwork being available for audit examination.
- Non-availability of audit trail: The audit trails in some computer systems may exist for only a short period of time. The absence of an audit trail will make the auditor's job very difficult and may call for an audit approach which involves auditing around the computer system by seeking other sources of evidence to provide assurance that the computer input has been correctly processed and output.
- Lack of availability of printed output: The results of transaction processing may not produce a hard copy form of output, i.e. a printed record. In the absence of physical output, it may be necessary for an auditor to directly access the electronic data retained on the client's computer. This is normally achieved by having the client provide a computer terminal and being granted "read" access to the required data files.
- Audit evidence: Certain transactions may be generated automatically by the computer system. For example, a fixed asset system may automatically calculate depreciation on assets at the end of each calendar month. The depreciation charge may be automatically transferred (journalised) from the fixed assets register to the depreciation account and hence to the client's income and expenditure account.
- Legal issues: The use of computers to carry out trading activities is also increasing. More organisations in both the public and private sector intend to make use of EDI and electronic trading over the Internet. This can create problems with contracts, e.g. when is the contract made, where is it made (legal jurisdiction), what are the terms of the contract and are the parties to the contract.

  The admissibility of the evidence provided by a client's computer system may need special consideration. The laws regarding the admissibility of computer

evidence varies from one country to another. Within a country laws may even vary between one state and another. If the auditor intends to gather evidence for use in a court, s(he) should firstly find out what the local or national laws stipulate on the subject.

In addition, the admissibility of evidence may vary from one court to another. What is applicable is a civil court may not be applicable in a criminal court.

(b) Operational Layer: The operational layer audit issues include the following:

- User Accounts and Access Rights: This includes defining unique user accounts and providing them access rights appropriate to their roles and responsibilities. Auditor needs to always ensure the use of unique user IDs, and these need to be traceable to individual for whom created. In case, guest IDs are used then test of same should also be there. Likewise, vendor accounts and third-party accounts should be reviewed. In essence, users and applications should be uniquely identifiable.
- Password Controls: In general, password strength, password minimum length, password age, password non-repetition and automated lockout after three attempts should be set as a minimum. Auditor needs to check whether there are applications where password controls are weak. In case such instances are found, then auditor may look for compensating controls against such issues.
- Segregation of Duties: As frauds due to collusions / lack of segregations increase across the world, importance of the Segregation of Duties also increases. As defined earlier, Segregation of duties is a basic internal control that prevents or detects errors and irregularities by assigning to separate individuals' responsibility for initiating and recording transactions and custody of assets to separate individuals. Example to illustrate:
  - Record keeper of asset must not be asset keeper.
  - Cashier who creates a cash voucher in system, must not have right to authorize payments.
  - Maker must not be checker.

Auditor needs to check that there is no violation of above principle. Any violation may have serious repercussions, the same need to be immediately communicated to those charged with governance.

4. (a) Some of the pertinent objectives in order to achieve the goals of Cloud Computing are as follows:

- To create a highly efficient IT ecosystem, where resources are pooled together and costs are aligned with what resources are actually used;

- To access services and data from anywhere at any time;
- To scale the IT ecosystem quickly, easily and cost-effectively based on the evolving business needs;
- To consolidate IT infrastructure into a more integrated and manageable environment;
- To reduce costs related to IT energy/power consumption;
- To enable or improve "Anywhere Access" (AA) for ever increasing users; and
- To enable rapid provision of resources as needed.

(b) Steering Committee is a special high power committee of experts to accord approvals for go-ahead and implementations. Some of the functions of Steering Committee involved in SDLC are as follows:

- To provide overall directions and ensures appropriate representation of affected parties;
- To be responsible for all cost and timetables;
- To conduct a regular review of progress of the project in the meetings of steering committee, which may involve co-ordination and advisory functions; and
- To undertake corrective actions like rescheduling, re-staffing, change in the project objectives and need for redesigning.

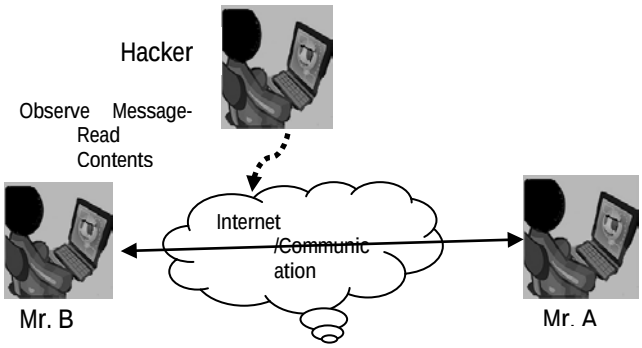
Role of Project Manager in SDLC: A project manager is normally responsible for more than one project and liaisoning with the client or the affected functions. S/he is responsible for delivery of the project deliverables within the time/budget and periodically reviews the progress of the project with the project leader and his/her team.

(c) Compensatory Controls: Controls are basically designed to reduce the probability of threats, which can exploit the vulnerabilities of an asset and cause a loss to that asset. While designing the appropriate control one thing should be kept in mind - "The cost of the lock should not be more than the cost of the assets it protects." Sometimes, while designing and implementing controls, organizations because of different constraints like financial, administrative or operational, may not be able to implement appropriate controls. In such a scenario, there should be adequate compensatory measures, which may although not be as efficient as the appropriate control, but reduce the probability of loss to the assets. Such measures are called Compensatory Controls.

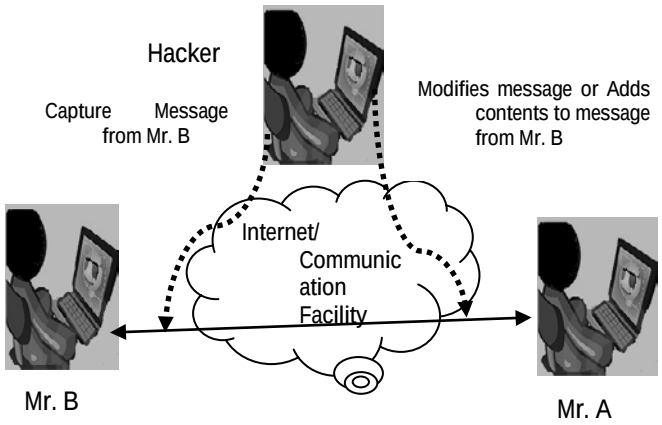
5. (a) Asynchronous Attacks: They occur in many environments where data can be moved asynchronously across telecommunication lines. Numerous transmissions must wait for the clearance of the line before data being transmitted. Data that is

waiting to be transmitted are liable to unauthorized access called asynchronous attack. These attacks are hard to detect because they are usually very small pin like insertions. There are many forms of asynchronous attacks; some of them are as follows:

- Data Leakage: Data is a critical resource for an organization to function effectively. Data leakage involves leaking information out of the computer by means of dumping files to paper or stealing computer reports and tape.
- Wire-tapping: This involves spying on information being transmitted over telecommunication network as shown in the Fig below.

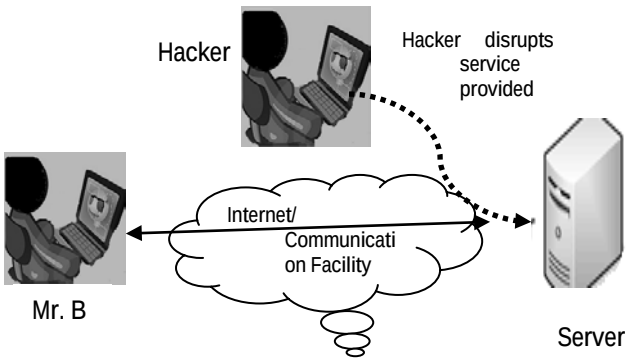


- Piggybacking: This is the act of following an authorized person through a secured door or electronically attaching to an authorized telecommunication link that intercepts and alters transmissions. This involves intercepting communication between the operating system and the user and modifying them or substituting new messages. A special terminal is tapped into the communication for this purpose as shown in the Fig. below.



- Shutting Down of the Computer/Denial of Service: This is initiated through terminals or microcomputers that are directly or indirectly connected to the

computer. Individuals, who know the high-level systems log on-ID initiate shutting down process. The security measure will function effectively if there are appropriate access controls on the logging on through a telecommunication network. When overloading happens some systems have been proved to be vulnerable to shutting themselves. Hackers use this technique to shut down computer systems over the Internet, as shown in the Fig. below.



(b) Internal controls comprise of the following five interrelated components:

- Control Environment: Elements that establish the control context in which specific accounting systems and control procedures must operate. The control environment is manifested in management's operating style, the ways authority and responsibility are assigned, the functional method of the audit committee, the methods used to plan and monitor performance and so on.
- Risk Assessment: Elements that identify and analyze the risks faced by an organisation and the way the risk can be managed. Both external and internal auditors are concerned with errors or irregularities that cause material losses to an organisation.
- Control Activities: Elements that operate to ensure transactions are authorized, duties are segregated, adequate documents and records are maintained, assets and records are safeguarded, and independent checks on performance and valuation of records. These are called accounting controls. Internal auditors are also concerned with administrative controls to achieve effectiveness and efficiency objectives.
- Information and Communication: Elements, in which information is identified, captured and exchanged in a timely and appropriate form to allow personnel to discharge their responsibilities.
- Monitoring: Elements that ensure internal controls operate reliably over time. The best internal controls are worthless if the company does not monitor them and make changes when they are not working.

(c) The benefits of Governance of Enterprise IT (GEIT) are as follows:

- It provides a consistent approach integrated and aligned with the enterprise governance approach.
- It ensures that IT-related decisions are made in line with the enterprise's strategies and objectives.
- It ensures that IT-related processes are overseen effectively and transparently.
- It confirms compliance with legal and regulatory requirements.
- It ensures that the governance requirements for board members are met.

6. (a) Programming Management Controls: Program development and implementation is a major phase within the systems development life cycle. The primary objectives of this phase are to produce or acquire and to implement high-quality programs. The program development life cycle comprises six major phases – Planning; Design; Control; Coding; Testing; and Operation and Maintenance with Control phase running in parallel for all other phases as shown in the Table below. The purpose of the control phase during software development or acquisition is to monitor progress against plan and to ensure software released for production use is authentic, accurate, and complete.

Phases of Program Development Life Cycle

Phase	Controls
Planning	Techniques like Work Breakdown Structures (WBS), Gantt Charts and PERT (Program Evaluation and Review Technique) Charts can be used to monitor progress against plan.
Design	A systematic approach to program design, such as any of the structured design approaches or object-oriented design is adopted.
Coding	Programmers must choose a module implementation and integration strategy (like Top-down, Bottom-up and Threads approach), a coding strategy (that follows the percepts of structured programming), and a documentation strategy (to ensure program code is easily readable and understandable).
Testing	Unit Testing, Integration Testing and Whole-of-Program Testing are undertaken in this. These tests are to ensure that a developed or acquired program achieves its specified requirements.
Operation and Maintenance	Management establishes formal mechanisms to monitor the status of operational programs so maintenance needs can be identified on a timely basis.

(b) Major characteristic of an effective Management Information System (MIS) are as follows:

- Management Oriented – It means that efforts for the development of the information system should start from an appraisal of management needs and overall business objectives. Such a system is not necessarily for top management only but may also meet the information requirements of middle level or operating levels of management as well.
- Management Directed – Because of management orientation of MIS, it is necessary that management should actively direct the system's development efforts. For system's effectiveness, it is necessary for management to devote their sufficient time not only at the stage of designing the system but for its review as well to ensure that the implemented system meets the specifications of the designed system.
- Integrated – The best approach for developing information systems is the integrated approach as all the functional and operational information sub-systems are tied together into one entity. An integrated Information system has the capability of generating more meaningful information to management as it takes a comprehensive view or a complete look at the interlocking sub-systems that operate within a company.
- Common Data Flows – It means the use of common input, processing and output procedures and media whenever required. Data is captured by the system analysts only once and as close to its original source as possible. Afterwards, they try to utilize a minimum of data processing procedures and sub-systems to process the data and strive to minimize the number of output documents and reports produced by the system. This eliminates duplication in data collections, simplifies operations and produces an efficient information system.
- Heavy Planning Element – An MIS usually takes one to three years and sometimes even longer period to get established firmly within a company. Therefore, a MIS designer must be present in MIS development and should consider future enterprise objectives and requirements of information as per the organization structure of the enterprise as per requirements.
- Sub System Concept – Even though the information system is viewed as a single entity, it must be broken down into digestible sub-systems, which can be implemented one at a time by developing a phased plan. The breaking down of MIS into meaningful sub-systems sets the stage for this phasing plan.
- Common Database – Database is the mortar that holds the functional systems together. It is defined as a "super-file", which consolidates and integrates data records formerly stored in many separate data files. The organization of a

database allows it to be accessed by several information sub-systems and thus, eliminates the necessity of duplication in data storage, updating, deletion and protection.

- Computerized - Though MIS can be implemented without using a computer; the use of computers increases the effectiveness of the system. In fact, its use equips the system to handle a wide variety of applications by providing their information requirements quickly. Other necessary attributes of the computer to MIS are accuracy and consistency in processing data and reduction in clerical staff. These attributes make computer a prime requirement in management information system.

(c) The following are some of the disadvantages/limitations of the use of the continuous audit system:

- Auditors should be able to obtain resources required from the organization to support development, implementation, operation, and maintenance of continuous audit techniques.
- Continuous audit techniques are more likely to be used if auditors are involved in the development work associated with a new application system.
- Auditors need the knowledge and experience of working with computer systems to be able to use continuous audit techniques effectively and efficiently.
- Continuous auditing techniques are more likely to be used where the audit trail is less visible and the costs of errors and irregularities are high.
- Continuous audit techniques are unlikely to be effective unless they are implemented in an application system that is relatively stable.

7. (a) Benefits of Enterprise Resource Planning (ERP) are as follows:

- Streamlining processes and workflows with a single integrated system.
- Reduce redundant data entry and processes and in other hand it shares information across the department.
- Establish uniform processes that are based on recognized best business practices.
- Improved workflow and efficiency.
- Improved customer satisfaction based on improved on-time delivery, increased quality, shortened delivery times.
- Reduced inventory costs resulting from better planning, tracking and forecasting of requirements.

- Turn collections faster based on better visibility into accounts and fewer billing and/or delivery errors.
- Decrease in vendor pricing by taking better advantage of quantity breaks and tracking vendor performance.
- Track actual costs of activities and perform activity based costing.
- Provide a consolidated picture of sales, inventory and receivables.

(b) The impact of cyber frauds on enterprises can be viewed under the following dimensions:

- Financial Loss: Cyber frauds lead to actual cash loss to target company/organization. For example, wrongfully withdrawal of money from bank accounts.
- Legal Repercussions: Entities hit by cyber frauds are caught in legal liabilities to their customers. Section 43A of the Information Technology Act, 2000, fixes liability for companies/organizations having secured data of customers. These entities need to ensure that such data is well protected. In case a fraudster breaks into such database, it adds to the liability of entities.
- Loss of credibility or Competitive Edge: News that an organizations database has been hit by fraudsters, leads to loss of competitive advantage. This also leads to lose credibility. There have been instances where share prices of such companies went down, as the news of such attach percolated to the market.
- Disclosure of Confidential, Sensitive or Embarrassing Information: Cyber-attack may expose critical information in public domain. For example, the instances of individuals leaking information about governments secret programs.
- Sabotage: The above situation may lead to misuse of such information by enemy country.

(c) [Section 72] Penalty for breach of confidentiality and privacy Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

(d) Integrity in Cloud Computing: Integrity refers to the prevention of unauthorized modification of data and it ensures that data is of high quality, correct, consistent and accessible. After moving the data to the cloud, owner hopes that their data and applications are secure. It should be insured that the data is not changed after being moved to the cloud. It is important to verify if one's data has been tampered with or deleted. Strong data integrity is the basis of all the service models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Methods like digital signature, Redundant Array of Independent Disks (RAID) strategies etc. are some ways to preserve integrity in Cloud computing. The most direct way to enforce the integrity control is to employ cryptographic hash function. For example, a solution is developed as underlying data structure using hash tree for authenticated network storage.

(e) Weaknesses of Waterfall Model are as follows:

- It is criticized to be inflexible, slow, costly, and cumbersome due to significant structure and tight controls.
- Project progresses forward, with only slight movement backward.
- There is a little to iterate, which may be essential in situations.
- It depends upon early identification and specification of requirements, even if the users may not be able to clearly define 'what they need early in the project'.
- Requirement inconsistencies, missing system components and unexpected development needs are often discovered during design and coding.
- Problems are often not discovered until system testing.
- System performance cannot be tested until the system is almost fully coded, and under capacity may be difficult to correct.
- It is difficult to respond to changes, which may occur later in the life cycle, and if undertaken it proves costly and are thus discouraged.
- It leads to excessive documentation, whose updation to assure integrity is an uphill task and often time-consuming.
- Written specifications are often difficult for users to read and thoroughly appreciate.
- It promotes the gap between users and developers with clear vision of responsibility.