# *Solutions of CA-FINAL ISCA MAY 2013 Paper*

***Disclaimer Clause :*** *These solutions are prepared by expert faculty team of Resonance. Views and answers provided may differ from that would be given by ICAI due to difference in assumptions taken in support of the answers. In such case answers as provided by ICAI will be deemed as final.*

**1. (a) The following activities are performed in the phase of system requirement analysis :**

- To identify and consult the stake owners to determine their expectations and resolve their conflicts.
- To analyze requirements to detect and correct conflicts and determine priorities.
- To verify the requirements are complete, consistent, unambiguous, verifiable, modifiable, testable and traceable.
- The gather data or find facts using tools like-interviewing, research/document collection, questionnaires, observation.
- To model activities such as developing models to document Data Flow Diagrams E-R Diagrams.
- To document activities such as interview,questionnaires, report etc. and development of a system (data) dictionary to document the modeling activities.

  Document / Deliverable : A systems requirements report.

**(b) Boundary control techniques are used in user control :**

- **Cryptography :** deals with programs for transformation data into codes that are meaningless to anyone who does not possess the authentication to access the respective system resource of file. A cryptographic technique encrypts data (clear text) into cryptogram (cipher text) and its strengths depends on the time and cost to decipher the cipher text by a cryptanalyst. The three techniques of cryptography are transposition (permute the order of characters within a set of data), substitution (replace text with a key-text) and product cipher (combination of transposition and substitution)
- **Password :** User identification by an authentication mechanism with personal characteristics like name, birth date employee code, function, designation or a combination of two or more of these can be used as a password boundary access control. A few best practices followed to avoid failures in this control system are minimum password length, avoid usage of common dictionary words, periodic change of password, encryption of passwords and number of entry attempts.
- **Personal Identification Numbers (PIN) :** The personal identification number is similar to a password assigned to a user of by an institution based on the user characteristics and encrypted using a cryptographic algorithm, or the institute generates a random number stored in its database independent to user identification details, or a customer selected number. Hence a PIN or a digital signature are exposed to vulnerabilities while insurance or delivery validation transmission and storage.
- **Identification Cards :** Identification cards are used to store information required in an authentication process. These cards used to identify a users are to be controlled through the application for a card preparation of the card, issue use and card return or card termination phases.

**(c) Implementation Guidelines for ERP :** There are certain general guidelines, which are to be followed before starting the implementation of an ERP package.

- Understanding the corporate needs and culture of the organization and then adopt the implementation technique to match these factors.
- Doing a business process redesign exercise prior to starting the implementation.
- Establishing a good communication network across the organizations.
- Providing a strong and effective leadership so that people down the line are well motivated.
- Finding an efficient and capable project manager.
- Creating a balanced team of implementation consultants who can work together as a team.

- Selecting a goods implementation methodology with minimum customisation.
- Training end users.
- Adapting the new system and making the required changes in the working environment to make effective use of the system in future.

**(d)** In drafting IS security policy for Business Continuity planning, following points should be addressed.

- A Business Continuity Plan (BCP) must be maintained, tested and updated if necessary. All staff must be made aware of it.
- A Business Continuity and Impact Assessment must be conducted annually.
- Suppliers of network service must be contractually obliged to provide a predetermined minimum service level.

**2.** **(a)** **The goal of a Prototype Model Approach of Software Development :** The traditional approach sometimes may take years to analyze, design and implement a system. In order to avoid such delays, organizations are increasingly using prototyping techniques to develop smaller systems such as DSS, MIS and Export systems. The goal of prototyping approach is to develop sa small or pilot version called a prototype of part or all of a system. A prototype is a usable system or system component that is built quickly and at a lesser cost, and with the intention of being modifying or replacing it by a full-scale and fully operational system. As users work with the prototype, they make suggestions about the ways to improve it. These suggestions are then incorporate into another prototype, which is also used an evaluated as son on. Finally when a prototype, which is also used and evaluated and so on. Finally when a prototype is developed that satisfies all users requirements either it is refined and turned into the final system or it is scrapped. If it is scrapped, the knowledge gained from building the prototype is used to develop the real system.

**Strengths**

- Improves both user participation in system development and communication among project stakeholders.
- Especially useful for resolving unclear objectives; developing and validating user requirements; experimenting with or comparing various design solutions ,or investigating both performance and the human computer interface.
- Potential exists for exploiting knowledge gained in an early iteration as later iterations are developed.
- Helps to easily identify confusing or difficult functions and missing functionality.
- May generate specifications for a production application.
- (Encourages innovation and flexible designs.
- Provides quick implementation of an incomplete, but functional, application.
- Prototyping requires intensive involvement by the system users. Therefore, it typically results in a better definition of these users' needs and requirements than does the traditional systems development approach.
- A very short time period (e.g., a week) is normally required to develop and start experimenting with a prototype. This short time period allows system users to immediately evaluate proposed system changes.
- Since system users experiment with each version of the prototype through an interactive process, errors are hopefully detected and eliminated early in the developmental process. As a result, the information system ultimately implemented should be more reliable and less costly to develop than when the traditional systems development approach is employed.

**(b) Following activities are involved in system conversion**

- **Procedure conversion :** Operating procedures should be completely documented for the new system that applies to both computer-operations and functional area operations. Before any parallel or conversion activities can start, operating procedures must be clearly spelled out for personnel in the functional areas undergoing changes. Information on input, data files, methods, procedures, output, and internal control must be presented in clear, concise and understandable terms for the average reader. Written operating procedures must be supplemented by oral communication during the training sessions on the system change.
- **File conversion :** Because large files of information must be converted from one medium to another, this phase should be started long before programming and testing are completed. The cost and related problems of file conversion are significant whether they involve on-line files (common database) or off-line files.

  In order for the conversion to be as accurate as possible, file conversion programs must be thoroughly tested. Adequate control, such as record counts and control totals, should be required output of the conversion program. The existing computer files should be kept for a period of time until sufficient files are accumulated for back up. This is necessary in case the files must be reconstructed from scratch after a "bug" is discovered later in the conversion routine.
- **System conversion :** After on-line and off-line files have been converted and the reliability of the new system has been confirmed for a functional area, daily processing can be shifted from the existing information system to the new one. All transactions initiated after this time are processed on the new system. System development team members should be present to assist and to answer any questions that might develop. Consideration should be given to operating the old system for some more time to permit checking and balancing the total results of both systems.
- **Scheduling personnel and equipment :** Scheduling data processing operations of a new information system for the first time is a difficult task for the system manager. As users become more familiar with the new system, however, the job becomes more routine.

  Schedules should be set up by the system manager in conjunction with departmental managers of operational units serviced by the equipment. The master schedule for next month should provide sufficient computer time to handle all required processing.

**(c) Executive Information System Differ from Traditional Information System in Following ways :**

| Dimensions of Difference | Executive Information System | Traditional Information System |
|---|---|---|
| Level of management | For top or near top executives. | For lower staff. |
| Nature of Information Access | Specific issuesl problems and aggregate reports | Status reporting |
| Nature of information provided | Online tools and analysis. | Offline status reporting. |
| Information Sources | More external, less internal | Internal |
| Drill down facility to go through details at successive | Available. | Not available |
| Information format | Text with graphics | Tabular |
| Nature of interface | User-friendly | Computer-operator generated. |

**3. (a) The scope of output control of an application system is :** To provide functions that determines the data content available. To users, data format, timeliness of data and how data is prepared and routed to users.

**Various type of out put control which are enforced for confidentiality, integrity and consistency of output are as follows :**

- **Storage and logging of sensitive, critical forms :** Pre-printed stationery should be stored securely to prevent unauthorized destruction or removal and usage. Only authorized persons should be allowed access to stationery supplies such as security forms, negotiable instruments etc.
- **Logging of output program executions :** When programs used for output of data are executed, it should be logged and monitored. In the absence of control over such output program executions, confidentiality of data could be compromised.
- **Spooling/Queuing : "**Spool" is an acronym for "Simultaneous Peripherals Operations Online". This is a process used to ensure that the user is able to continue working, even before the print operation is completed. When a file is to be printed, the operating system stores the data stream to be sent to the printer in a temporary file on the hard disk. This file is them "spooled" to the printer as soon as the printer is ready to accept the data. This intermediate storage of output could lead to unauthorized disclosure and/or modification. A queue is the list of documents waiting to be printed on a particular printer. This queue should not be subject to unauthorized modifications.
- **Controls over printing :** it should be ensured that unauthorized disclosure of information I printed is prevented. Users must be trained to select the correct printer and access restrictions may be placed on the workstations that can be used for printing.
- **Report distribution and collection controls :** Distribution of reports should be made in a secure way to ensure unauthorized disclosure of data. It should be made immediately after printing to ensure that the time gap between generation and distribution is reduced. A log should be maintained as to what reports were generated and to whom it was distributed. Where users have to collect reports the user should be responsible for timely collection of the report especially if it is printed in a public area. A log should be maintained as to what reports where printed and which of them where collected. Uncollected reports should be stored securely.
- **Retention controls :** Retention controls consider the duration for which outputs should be retained before being destroyed. Consideration should be given to the type of medium on which the output is stored. Retention control requires that a date should be determined for each output item produced. Various factors ranging from the need of the output, use of the output, to legislative requirements would affect the retention period
- **Existence/Recovery Controls :** are needed to recover output in the event that it is lost or destroyed. If the output is written to a spool of files or report files and has been kept, then recovering and new generation is easy and straight-forward. The state of a transaction at a point of time with before and after images. Check/restart helps in recovery when a hardware problem causes a program that prints customer invoices to abort in midstream.

**(b) Expert Systems:** An Expert System is highly developed DSS that utilizes knowledge generally possessed by an expert to share a problem. Expert System are software systems that imitate the reasoning processes of human experts and provide decision makers with the type of advice they would normally receive from such expert systems. For instance, an expert system in the area of investment portfolio management might ask its user a number of specific questions relating to investments for a particular client like - how much can be invested, Does the client have any preferences regarding specific types of securities? And so on.

Still Expert Systems are not always the answer to managerial or organizational problems. Some of the properties that potential applications should posses to qualify for Expert System development are as follows:

- **Availability :** One or more experts are capable of communicating how they go about solving the problems to which the Expert System will be applied.

- **Complexity :** Solution of the problems for which the Expert Systems will be used is a complex task that requires logical inference processing, which would not be easily handled by conventional information processing.
- **Domain :** The domain, or subject area, of the problem is relatively small and limited to a relatively well-defined problem area.
- **Expertise :** Solutions to the problem require the efforts of experts. That is, only a few possess the knowledge, techniques, and intuition needed.
- **Structure :** The solution process must be able to cope with ill-structured, uncertain, missing, and conflicting data, and a dynamic problem-solving situation.

**(c) Packet Filter Firewalls :** Packet filter firewalls evaluate the headers of each incoming and outgoing packet to ensure it has a valid internal address, originates from a permitted external address, connects to an authorized protocol or service, and contains valid basic header instructions. If the packet does not match the pre-defined policy for allowed traffic, then the firewall drops the packet. Packet filters generally do not analyze the packet contents beyond the header information. Many routers contain access control lists (ACLs) that allow for packet-filtering capabilities.

Dynamic packet filtering incorporates stateful inspection primarily for performance benefits. Before re-examining every packet, the firewall checks each packet as it arrives to determine whether it is part of an existing connection. If it verifies that the packet belongs to an established connection, then it forwards the packet without subjecting it to the firewall rule set.

**'Weaknesses associated with packet filtering firewalls include the following:**

- The system is unable to prevent attacks that exploit application-specific vulnerabilities and functions because the packet filter does not examine packet contents,
- Logging functionality is limited to the same information used to make access control decisions.
- Most do not support advanced user authentication schemes.
- Firewalls are generally vulnerable to attacks and exploitation that take advantage of vulnerabilities in network protocols.
- The firewalls are easy to misconfigure, which allows traffic to pass that should be blocked.

**4. (a) System Control Audit Review File (SCARF):** The system control audit review file (SCARF) technique involves embedding audit software modules within a host application system to provide continuous monitoring of the system's transactions. The information collected is written onto a special audit file- the SCARF master files. Auditors then examine the information contained on this file to see if some aspect of the application system needs follow-up. In many ways, the SCARF technique is like the snapshot technique along with other data collection capabilities.

Auditors might use SCARF to collect the following types of information:

- **Application system errors :**SCARF audit routines provide an independent check on the quality of system processing, whether there are any design and programming errors as well as errors that could creep into the system when it is modified and maintained.
- **Policy and procedural variances :** Organizations have to adhere to the policies, procedures and standards of the organization and the industry to which they belong. SCARF audit routines can be used to check when variations from these policies, procedures and standards have occurred.
- **System exception :** SCARF can be used to monitor different types of application system exceptions. For example, salespersons might be given some leeway in the prices they charge to customers. SCARF can be used to see how frequently salespersons override the standard price.
- **Statistical sample :** Some embedded audit routines might be statistical sampling routines, SCARF provides a convenient way of collecting all the sample information together on one file and use analytical review tools thereon.
- **Snapshots and extended records -** Snapshots and extended records can be written into the SCARF file and printed when required.

- **Profiling data :** Auditors can use embedded audit routines to collect data to build profiles of system users. Deviations from these profiles indicate that there may be some errors or irregularities.
- **Performance measurement :** Auditors can use embedded routines to collect data that is useful for measuring or improving the performance of an application system.

**(b) Business Impact Analysis :** Business Impact Analysis (BIA) is essentially a means of systematically assessing the potential impacts resulting from various events or incidents. It enables the business continuity team to identify critical systems, processes and functions, assess the economic impact of incidents and disasters that result in a denial of access to the system, services and facilities, and assess the "pain threshold," that is, the length of time business units can survive without access to the system, services and facilities.

The business impact analysis is intended to help understand the degree of potential loss (and various other unwanted effects) which could occur. This will cover not just direct financial loss, but other issues, such as reputation damage, regulatory effects, etc.

A number of tasks are to be undertaken in this phase as enumerated under:

- **Identify organisational risks :** This includes single point of failure and infrastructure risks. The objective is to identify risks and opportunities and to minimise potential threats that may lead to a disaster.
- Identify critical business processes.
- Identify and quantify threats! risks to critical business processes both in terms of outage and financial impact.
- Identify dependencies and interdependencies of critical business processes and the order in which they must be restored.
- Determine the maximum allowable downtime for each business process.
- Identify the type and the quantity of resources required for recovery e.g. tables chairs, faxes, photocopies, safe, desktops, printers, etc.
- Determine the impact to the organisation in the event of a disaster, e.g. financial reputation, etc.

**(c) [Section 22] Application for license :**

**(1)** Every application for issue of a license shall be in such form as may be prescribed by the Central Government,

**(2)** Every application for issue of a license shall be accompanied by

**(a)** a certification practice statement;

**(b)** a statement including the procedures with respect to identification of the applicant;

**(c)** payment of such fees, not exceeding twenty-five thousand rupees as may be prescribed by the Central Government;

**(d)** such other documents, as may be prescribed by the Central Government.

Section 23 provides that the application for renewal of a licence shall be in such form and accompanied by such fees not exceeding Rs.5,000 which may be prescribed by the Central :government. In 1TAA 2008, Section 23 is given as follows:

**5. (a) Asset Classification and Security Classification an control :** Following are control and objective of this classifications:

- An inventory of assets must be maintained. This must include physical, software and information assets.
- A formal, documented classification scheme (as set out in the Information Classification Policy) should be in place and all staff must comply with it.
- The originator or 'owner' of an item of information (e.g. a document, file, diskette, printed report, screen display, e-mail, etc.) should provide a security classification, where appropriate.
- The handling of information, which is protectively marked CONFIDENTIAL or above must be specifically approved (i.e. above RESTRICTED).

- Exchanges of data and software between organizations must be controlled. Organizations to whom information is to be sent must be informed of the protective marking associated with that information, in order to establish that it will be handled by personnel with a suitable clearance corresponding to the protective marking.
- Appropriate procedures for information labeling and handling must be agreed and put into practice.
- Classified waste must be disposed of appropriately and securely.

**(b) The purposes of a risk evaluation is to :**

- identify the probabilities of failures and threats,
- calculate the exposure, i.e., the damage or loss to assets, and
- make control recommendations keeping the cost-benefit analysis in mind. 5.7.1 Techniques for

**Techniques for Risk Evaluation :** Following are some of the techniques that are available to assess and evaluate risks.

- Judgement and intuition
- The Delphi approach
- Scoring
- Quantitative Techniques
- Qualitative Techniques

**(a)** In many situations the auditors have to use their **judgement and intuition** for risk assessment. This mainly depends on the personal and professional experience of the auditors and their understanding of the system and its environment. Together with it is required a systematic education and ongoing professional updating.

**(b)** The **Delphi Technique** was first used by the Rand Corporation for obtaining a consensus opinion. Here a panel of experts is appointed. Each expert gives his opinion in a written and independent manner. They enlist the estimate of the cost, benefits and the reasons why a particular system should be chosen, the risks and the exposures of the system. These estimates are then compiled together. The estimates within a pre-decided acceptable range are taken. The process may be repeated four times for revising the estimates falling beyond the range. Then a curve is drawn taking all the estimates as points on the graph. The median is drawn and this is the consensus opinion.

**(c)** In the **Scoring approach** the risks in the system and their respective exposures are listed. Weights are then assigned to the risk and to the exposures depending on the severity, impact on occurrence, and costs involved. The product of the risk weight with the exposure weight of every characteristic gives us the weighted score. The sum of these weighted score gives us the risk and exposure score of the system. System risk and exposure is then ranked according to the scores obtained.

**(d)** **Quantitative techniques** involve the calculating an annual loss exposure value based on the probability of the event and the exposure in terms of estimated costs. This helps the organisation to select cost effective solutions. It is the assessment of potential damage in the event of occurrence of unfavourable events, keeping in mind how often such an event may occur.

**(e)** **Qualitative techniques** are by far the most widely used approach to risk analysis. Probability data is not required and only estimated potential loss is used. Most qualitative risk analysis methodologies make use of a number of interrelated elements:

- **Threats :** These are things that can go wrong or that can 'attack' the system. Examples, might include fire or fraud. Threats are ever present for every system.
- **Vulnerabilities :** These make a system more prone to attack by a threat or make an attack more likely to have some success or impact. For example, for fire, vulnerability would be the presence of inflammable materials (e.g. paper).

- **Controls** : These are the countermeasures for vulnerabilities. There are four types:
  - **(i)** Deterrent controls reduce the likelihood of a deliberate attack
  - **(ii)** Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact
  - **(iii)** Corrective controls reduce the effect of an attack
  - **(iv)** Detective controls discover attacks and trigger preventative or corrective controls.

**(c) Information Security Policy :** A Policy is a plan or course of action, designed to influence and determine decisions, actions and other matters. The security policy is a set of laws, rules, and practices that regulates how assets, including sensitive information are managed, protected, and distributed within the user organization.

An information Security policy addresses many issues such as disclosure, integrity and availability concerns, who may access what information and in what manner, basis on which access decision is made, maximized sharing versus least privilege, separation of duties, who controls and who owns the information, and authority issues.

**Issues to address :** This policy does not need to be extremely extensive, but clearly state senior management's commitment to information security, be under change and version control and be signed by the appropriate senior manager. The policy should at least address the following issues:

- A definition of information security,
- Reasons why information security is important to the organisation, and its goals and principles,
- A brief explanation of the security policies, principles, standards and compliance requirements,
- Definition of all relevant information security responsibilities
- Reference to supporting documentation.

**6. (a) (i) Release Management** is used for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure. Proper Software and Hardware Control ensure the availability of licensed, tested, and version certified software and hardware, which will function correctly and respectively with the available hardware. Quality control during the development and implementation of new hardware and software is also the responsibility of Release Management. This guarantees that all software can be conceptually optimized to meet the demands of the business processes. The goals of release management are:

- Plan to rollout of software
- Design and implement procedures for the distribution and installation of change to IT systems.
- Effectively communicate and manage expectations of the customer during the planning and rollout of new releases.
- Control the distribution and installation of changes to IT system.

**(ii) ICT Infrastructure Management :** ICT Infrastructure Management processes recommend best practice for requirements analysis, planning, design, deployment and ongoing operations of management and technical support of an ICT Infrastructure. The Infrastructure Management processes describe those processes within ITIL that directly relate to ICT equipment and software that is involved in providing ICT services to customers.

- **(a)** ICT Design and Planning
- **(b)** ICT Deployment
- **(c)** ICT Operations
- **(d)** ICT Technical Support

**(b) (Section 66 Al Punishment for sending offensive messages through communication service, etc.(Introduced vide 1TAA 2008) :**

Any person who sends, by means of a computer resource or a communication device,

**(a)** any information that is grossly offensive or has menacing character; or

**(b)** any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently by making use of such computer resource or a communication device,

**(c)** any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008) shall be punishable with imprisonment for a term which may extend to three years and with fine.

**(c)** Every company that intends to implement ERP has to reengineer its processes in one form or the other. This process is known as Business Process Reengineering (BPR)

**Some Typical processes with descriptions**

| Process | Description |
|---|---|
| Forecasting | Shows sales, Fund Flows etc over a long period of time say next two years. |
| Fund management | The necessity of funds and the way to raise these funds. Uncertainty and Risk factors to be considered. Simulation with 'What if" type analysis |
| Price Planning | Determines the price at which products are offered. Involves application of technology to pricing support such as commercial database services. Also feedback and sensitivity analysis |
| Budget Allocation | Using computerised algorithms to estimate desirable mix of funds allocated to various functions. |
| Material requirement Planning | Process of making new products from raw materials and include predicting scheduling, requirement planning. Also activities for monitoring and planning of actual production. |
| Quality control | Takes care of activities to ensure that the products are of desired quality. |

**7. (a) Purpose of the audit policy :** Purpose of this audit policy is to provide the guidelines to the audit team to conduct an audit on IT based infrastructure system. The Audit is done to protect entire system from the most common security threats which includes the following:

- Access to confidential data,
- Unauthorized access of the department computers,
- Password disclosure compromise,
- Virus infections,
- Denial of service attacks,
- Open ports, which may be accessed from outsiders, and
- Unrestricted modems unnecessarily open ports.

Audits may be conducted to ensure integrity, confidentiality and availability of information and resources.

The IS Audit Policy should lay out the objective and the scope of the Policy. An IS audit is conducted to :

- safeguard the Information System Assets/Resources,
- maintain the Data Integrity,
- maintain the System Effectiveness,
- ensure System Efficiency, and
- comply with Information System related policies, guidelines, circulars, and any other instructions requiring compliance in whatever name called.

**(b) Used in Disaster Recovery Plan**

The best audit tool and technique is a periodic simulation of a disaster. Other audit techniques would include observations, interviews, checklists, inquiries, meetings, questionnaires and documentation reviews. These tools and methods may be categorised as under:

- **Automated Tools :** Automated tools make it possible to review large computer systems for a variety of flaws in a short time period. They can be used to find threats and vulnerabilities such as weak access controls, weak passwords, lack of integrity of the system software, etc.
- **Internal Control Auditing :** This includes inquiry, observation and testing. The process can detect illegal acts, errors, irregularities or lack of compliance of laws and regulations.
- **Disaster and Security Checklists :** A checklist can be used against which the system can be audited. The checklist should be based upon disaster recovery policies and practices, which form the base line. Checklists can also be used to verify changes to the system from contingency point of view.
- **Penetration Testing :** Penetration testing can be used to locate vulnerabilities.

**(c) Risk assessment** is a critical step in disaster and business continuity planning. Risk assessment is necessary for developing a well tested contingency plan. Risk assessment is the analysis of threats to resources (assets) and the determination of the amount of protection necessary to adequately safeguard the resources, so that vital systems, operations, and services can be resumed to normal status in the minimum time in case of a disaster. Disasters may lead to vulnerable data and crucial information suddenly becoming unavailable. The unavailability of data may be due to the non-existence or inadequate testing of the existing plan. Risk assessment is a useful technique to assess the risks involved in the event of unavailability of information, to prioritise applications, identify exposures and develop recovery scenarios. The areas to be focussed upon are:

**(a) Prioritisation :** All applications are inventoried and critical ones identified. Each of the critical applications is reviewed to assess its impact on the organization, in case a disaster occurs. Subsequently, appropriate recovery plans are developed.

**(b) Identifying critical applications:** Amongst the applications currently being processed the critical applications are identified. Further analysis is done to determine specific jobs in the applications which may be more critical. Even through the critical value would be determined based on its present value, future changes should not be ignored.

**(c) Assessing their impact on the organisation :** Business continuity planning should not concentrate only on business disruption but should also take into account other organisatioal functions which may be affect. The areas to be considered include.:

- Legal liabilities
- Interruptions of customers services.
- Possible Losses.
- Likelihood of fraud and recovery procedures.

**(d) Identifying critical applications:** Amongst the applications currently being processed the critical applications are identified. Further analysis is done to determine specific jobs in the applications which may be more critical. Even through the critical value would be determined based on its present value, future changes should not be ignored.

**(e) Assess Insurance coverage:** The information system insurance policy should be multiperil policy designed to provide various types of coverage. Depending on the individual organizations and the extent of coverage required, suitable modifications may be made to the comprehensive list provided below:

- Hardware facilities :
- Software Reconstruction :
- Extra Expenses:
- Business interruption :
- Valuable paper and records :
- Errors and omissions:
- Fidelity coverage:
- Media transportation

**(f) Identification of exposure and implications:** It is not possible to accurately predict as to when and how a disaster would occur. So, it is necessary to estimate the probability and frequency of diester.

**(g) Development of recovery plant:** The plan should be designed to provide for recovery from total destruction of a site.

**(d) Reasons Why do ERP projects fail so often?**

At its simplest level, ERP is a set of best practices for performing the various duties in the departments of your company, including in finance, manufacturing and the warehouse. To get the most from the software, you have to get people inside your company to adopt the work methods outlined in the software. If the people in the different departments that will use ERP don't agree that the work methods embedded in the software are better than the ones they currently use, they will resist using the software or will want IT to change the software to match the ways they currently do things. This is where ERP projects break down. Political fights erupt over how or even whether the software will be installed. IT gets bogged down in long, expensive customisation efforts to modify the ERP software to fit with powerful business barons' wishes. Customisations make the software more unstable and harder to maintain when it finally does come to life. Because ERP covers so much of what a business does, a failure in the software can bring a company to a halt, literally. The mistake companies make is assuming that changing people's habits will be easier than customising the software. It's not. Getting people inside your company to use the software to improve the ways they do their jobs is by far the harder challenge. If people are resistant to change, then the ERP project is more likely to fail.

**(e) Section 19 of Information Technology (Amendment) Act, 2008** provides for the power of the Controller with the previous approval of the Central Government to grant recognition to foreign Certifying Authorities subject to such conditions and restrictions as may be imposed by regulations. As per ITAA 2008, Section 19 is given as under:

**(Section 19) Recognition of foreign Certifying Authorities :**

**(1)** Subject to such conditions and restrictions as may be specified by regulations, the Controller may with the previous approval of the Central Government, and by notification in the Official Gazette, recognize any foreign Certifying Authority as a Certifying Authority for the purposes of this Act.

**(2)** Where any Certifying Authority is recognized under sub-section (1), the Electronic Signature Certificate issued by such Certifying Authority shall be valid for the purposes of this Act.

**(3)** The Controller may if he is satisfied that any Certifying Authority has contravened any of the conditions and restrictions subject to which it was granted recognition under sub section (1) he may, for reasons to be recorded in writing, by notification in the Official Gazette, revoke such recognition.