



www.ranapk.com

Rana Abubakar Khan

If you want to learn computer programming then contact with me

truefriendlion@gmail.com

Join FB group for VU help

www.facebook.com/groups/vu1234/

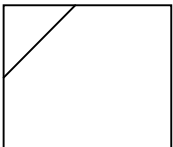
CS507_subjective_2011 (solved)

1. Define entity in flow diagram (2 marks)

Entity Represents sources of data received by the system or destinations of the data produced by the system. E.g. Customers, suppliers, purchase department



If the entity is repeated in the DFD, the same symbol with the addition of a bar in the left hand corner is used and looks like.

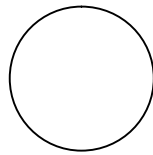


2. What are functions of connectors in DFD (3 marks)



www.ranapk.com

1. If the flowchart becomes complex, it is better to use connector symbols to reduce the number of flow lines.
2. Avoid the intersection of flow lines if you want to make it more effective and better way of communication.



A connector

3. How risks can be measured (3 marks)

There are two keys to good risk assessment. The first is better quality and more timely information about the risks as they evolve, so that the element of surprise is reduced.

The second is tools such as risk-adjusted discount rates, simulations, scenario analysis, and VaR to convert the raw data into risk measures.

4. Differentiate CRM and KIA (5 marks)

MKIS is a type of Information System that helps the firm to achieve following objectives:

1. Identification of customers for firm's products and services.
2. Development of those products and services to meet customers' needs
3. Promotion of the products and services, and
4. Provision of after sale customer support



www.ranapk.com

CRM

1. Maintains and enhances customer base
2. Encourages customer loyalty
3. Gaining more customers' wallet-share
4. The more effective a company's customer retention and defection management strategy, the less they need to plug the gap with new customers, who are expensive to recruit.
5. CRM help in establishing communication to encourage customers to share information about their

5. Risk based audit approach (5 marks)



Risk Based Audit Approach



This approach to audit proceeds with following steps

1. Understanding the business process
2. Understanding the control structure built in the system
3. Understanding of inherent risks (risks which are covered through instituting) controls, which can occur in the absence of controls e.g.
 - Political legal factors affecting the business,
 - Nature of industry the organization exists
4. Risk assessment
5. Categorization of risks identified
6. Define objective. (Marks 2)



www.ranapk.com

Objectives

We just mentioned that a control mechanism should compare actual output with expected/Ideal output. But before this is being done, there needs to be a list of specific objectives which define expected output.

7. Define scanners. (Marks 2)

The scanner checks or scans the operating system and other application soft wares installed on the hard drives. While scanning, it checks the bit patterns in all software against the bit patterns contained in the virus definitions of the scanner. If they found similar, they are labeled as virus.

8. Identify purposes of systems and procedures. (Marks 3)

Purpose of Systems & Procedures

The basic purpose behind setting up systems and procedures is to make available information when required. But when procedures are organized in a logical manner to form systems, the value of information as an output of a system enhances. When technology is added to the system, scope of a system changes to include hardware, software and designs linked together in accordance with the procedures contained in that system to give a purposeful architecture



9. What are the types of Supply Chain Management? (Marks 3)

Types of Supply Chains

Supply chain may exist in various forms depending on the need of the business:

1. **Made to Store** – Focuses on tracking customer demand in real time, so that the production process can restock the finished goods inventory.
2. **Continuous Replenishment** – focuses on constant replacement of inventory by working closely with suppliers. Applicable to environments with stable demand patterns



www.ranapk.com

www.ranapk.com

3. **Built to order** – Focuses on careful management of component inventories and delivery of needed supplies along the supply chain. A solution to this potential inventory problem is to utilize many common components across several production lines and in several locations

10. Briefly describe the process of risk mitigation? (Marks 5)

- **Risk assumption:** To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level.
- **Risk Avoidance:** To avoid the risk by eliminating the risk cause and e.g. forgo certain functions of the system or shut down the system when risks are identified.
- **Risk Limitation:** To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising vulnerability e.g. use of supporting preventive and detective controls.
- **Risk Planning:** To manage risk by developing risk mitigation plan that predicts implements and maintains controls.
- **Research and acknowledgement:** To lower the risk of loss by acknowledging vulnerability or flaw and researching controls to correct the vulnerability.
- **Risk Transference:** To transfer the risk by using other options to compensate loss such as purchasing insurance.

11. What is critical success factor?

Critical success factor

Critical Success Factor (CSF) is a business term for an element which is necessary for an organization or project to achieve its mission. For example, for an international package delivery system, CSF's can be identified such as safe transport of customer consignments, timely delivery of consignment, online status confirmation system to inform customers and proper packaging and handling.



www.ranapk.com

12. Define Message passing?

Message-Passing

Several objects may collaborate to fulfill each system action. For example, “Record CD sale” is a process, which could involve a CD stock item, a sales transaction, a sales assistant, etc. These objects involved in the process of CD sale communicate by sending each other message

13. What is an entity?

An entity is an object that exists and is distinguishable from other objects. An entity is described using a set of attributes. For example specific person, company, event, plant, crop, department, section, cost center.

14. Why we need to secure information systems? (Marks: 2)

Sound security is fundamental to achieving this assurance. Furthermore, there is a need for organizations to protect themselves against the risks inherent with the use of information systems while simultaneously recognizing the benefits that can accrue from having secure information systems. Thus, as dependence on information systems increases, security is universally recognized as a pervasive, critically needed, quality.

15. Identify the types of change management? (Marks: 2)

Types of Change

Organizational Development: This is the more gradual and evolutionary approach to change. It bases on the assumption that it is possible to align corporate objectives with the individual employees’ objectives. In practice, however, this will rarely be possible.



www.ranapk.com

Reengineering: This is known as corporate transformation or business transformation. It is the more radical form of change management, since it challenges all elements of processes or structures that have evolved over time.

16. Briefly discuss Risk Determination? (Marks: 2)

Risk determination phase assesses the risk and level of risk to IT system.

The inputs of this phase are

1. Likelihood of threat exploitation
2. Magnitude of impact
3. Adequacy of planned and current controls

The output is the determination of risk and associated risk levels.

17. What are hackers? (Marks: 3)

Hackers

A hacker is a person who attempts to invade the privacy of the system. In fact he attempts to gain unauthorized entry to a computer system by circumventing the system's access controls. Hackers are normally skilled programmers, and have been known to crack system passwords, with quite an ease. Initially hackers used to aim at simply copying the desired information from the system. But now the trend has been to corrupt the desired information.

18. Discuss Technical Limitations of Ecommerce in business? (Marks: 3)



www.ranapk.com

Technological Limitations

1. Lack of universal standards for quality, security, and reliability
2. The telecommunications bandwidth is insufficient, especially for m-commerce (electronic commerce via mobile phones).
3. Difficulty in integrating e-commerce infrastructure with current organizational IT systems - Many companies use IT systems, which are old (i.e. legacy systems). These were developed to support different needs and different kinds of software and applications. These systems contain valuable business information but have to be integrated with new ones. In many occasions this is extremely difficult. When it comes to full integration with back-office operations, for example, the cost of integrating legacy systems with modern ones may be greater than that of actually scrapping them completely

19. Identify roles and responsibilities (Marks: 3)

Roles & Responsibility

For security to be effective, it is imperative that individual roles, responsibilities are clearly communicated and understood by all. Organizations must assign security related functions in the appropriate manner to nominated employees. Responsibilities to consider include:

1. **Executive Management** — assigned overall responsibility for the security of information;
2. **Information Systems Security Professionals** — responsible for the design, implementation, management, and review of the organization's security policy, standards, measures, practices, and procedures;
3. **Data Owners** — responsible for determining sensitivity or classification levels of the data as well as maintaining accuracy and integrity of the data resident on the information system;
4. **Process Owners** — responsible for ensuring that appropriate security, consistent with the organization's security policy, is embedded in their information systems;
5. **Technology providers** — responsible for assisting with the implementation of information security;
6. **Users** — responsible for following the procedures set out in the organization's security policy; and



7. Information Systems Auditors — responsible for providing independent assurance to management on the appropriateness of the security objectives.

20. Differentiate CRM from ERP (Marks: 3)

ERP & CRM

Customer has become of critical importance in the modern day business. Early on, organizations used to focus more on how much has been sold what has been produced. But now the focus is quite different. Focus has been placed on the requirements of the customer, providing quality service and quickness of response to customer queries. Analysis of the customer data from their personal habits to spending one's have become a crucial element of doing a successful business. ERP has this unique potential to improve the quality of customer handling.

21. Briefly describes Incremental Model? (Marks: 3)

In incremental models, software is built not written. Software is constructed step by step in the same way a building is constructed. The product is designed, implemented, integrated and tested as a series of incremental builds, where a build consists of code pieces from various modules interacting together to provide a specific functional capability and testable as a whole.

22. What do u know about Key stroke Monitoring? (Marks: 3)

A record of every keystroke---- often called keystroke monitoring. Keystroke monitoring is the process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails.

23. Parameter of audit trail and risk based audit approach

Audit Trails

Establishing clear audit trails is an absolute must as much as managing physical environmental risks. They help in identifying the start and execution of transaction from the cradle to the grave. Audit logs to be kept should also record the errors



www.ranapk.com

occurring and possible actions should be taken to mitigate risks. Maintaining audit logs also helps in drilling down for investigation purposes. Exception report can also be prepared from these audit logs.

24. Scope of Security

Scope of Security

The concept of security applies to all information. Security relates to the protection of valuable assets against loss, disclosure, or damage. Valuable assets are the data or information recorded, processed, stored, shared, transmitted, or retrieved from an electronic medium. The data or information must be protected against harm from threats that will lead to its loss, inaccessibility, alteration or wrongful disclosure.

25. What is Business Process Reengineering?

“Reengineering is the fundamental rethinking and redesign of business processes to achieve dramatic improvements in critical, contemporary measures of performance, such as cost, quality, service and speed.”

26. To understand the ESS

Executive Support System (ESS) is a reporting tool (software) that allows you to turn your organization's data into useful summarized reports. These reports are generally used by executive level managers for quick access to reports coming from all company levels and departments such as billing, cost accounting, staffing, scheduling, and more.

27. Risk management

Risk management in a newly computerized environment and that in an ongoing operation will have to be viewed differently. In an ongoing operation, risk management itself cannot be done without evidence collection and evidence of risks



www.ranapk.com

Phases of Risk Management

Following are various phases of SDLC

- System Characterization
- Threat Identification
- Vulnerability Identification
- Control Analysis
- Likelihood Determination
- Impact Analysis
- Risk Identification
- Control Recommendation
- Results Documentation
- Implementation
- Monitoring

28. To understand the iterative system



Iterative Models

In these models customer feed back is taken at each phase and project is modified accordingly – if need be. Prototypes are used in these models.



29. Logical threat

Logical Threat

This refers to damage caused to the software and data without any physical damage to the computers. Consequently there can be a situation where the damage of data or software may render the hardware itself unusable. For example the virus or bug being installed to corrupt data or software might create BAD SECTORS on the hard drive, leading to its preferable removal from the computer.

30. What is Digital certification?



www.ranapk.com

Digital Certificates

1. The digital equivalent of an ID card is also called "digital IDs," digital certificates are issued by a trusted third party known as a "certification authority" (CA) such as VeriSign and Thawte.
2. For example, CBR requires a NIFT class 2 digital certificate in order to facilitate filing return electronically
3. NIFT itself is an affiliate of Verisign Inc. working as certification authority in Pakistan.
4. The certificate is valid for one year.
5. The certificate is attached to email every time a message is attached and sent to recipient.
6. The CA verifies that a public key belongs to a specific company or individual (the "subject"), and the validation process it goes through to determine if the subject is who it claims to be depends on the level of certification and the CA itself

31. What are information assets? (2 marks)

"Information assets are secure when the expected losses that will occur from threats eventuating over sometime are at an acceptable level."

32. What are the challenges faced by security association of USA?

Information system security association of USA has listed down following ethical challenges

1. Misrepresentation of certifications, skills
2. Abuse of privileges
3. Inappropriate monitoring
4. Withholding information
5. Divulging information inappropriately
6. Overstating issues
7. Conflicts of interest
8. Management / employee / client issues

33. Why organization attracts towards implementation of ERP?



www.ranapk.com

There are some reasons attracting companies to take up ERP.

1. Planning the operations
2. Integrated customer related information – order tracking with customer database, inventory and shipment at different locations.
3. Standardized HR information – A company with multiple business units will require a comprehensive and all-encompassing method of locating employees and communicating with them.
4. Integrated financial information and analysis
5. Monitoring the operations including those of sub-vendors and manufacturers
6. Standardization analysis of financial and non financial information for decision making control/regulation.
7. We will now listen to the views of the State Bank Of Pakistan's CIO on the subject.

34. Define MRP?

1. Materials Requirement Planning (MRP) utilizes software applications for scheduling timely material procurement.
2. MRP generates schedules for the operations and raw material purchases based on the production requirements of finished goods, the structure of the production system, the current inventories levels and the lot sizing procedure for each operation

35. What is the purpose of audit log?

The audit log is maintained only for the list of activities specified for which the log is to be maintained.

36. What are the methods to avoid internet attack?

1. Define the problem
2. Consolidate standards and purchasing power
3. Think risks
4. Fix configurations
5. Better people mean more secure networks
6. Identify problems early and react fast



www.ranapk.com

37. What is web security threat?

Web Security Threats

There are two major classes of security threats

- Passive Attacks
- Active Attacks

38. What are the components of BCP?

Components of BCP

The business continuity plan includes:

1. The disaster recovery plan that is used to recover a facility rendered inoperable, including relocating operation into a new location.
2. The operations plan that is to be followed by the business units while recovery is taking place.
3. The restoration plan that is used to return operations to normality whether in a restored or new facility.

39. What are antivirus software?

Use of antivirus software is another very important technical control against the spread of virus.

- 1) Scanners
- 2) Active monitors
- 3) Behavior blockers
- 4) Logical intrusion





www.ranapk.com

40. What is the data driven support system? (3 marks)

Data driven DSS is use large pool of data in major organizational systems. They help to extract information from large quantities of data stored. These systems rely on Data Warehouses created from Transaction Processing systems. They use following techniques for data analysis

- Online analytical processing, and
- Data mining

41. Identify the information that is required before conducting the impact analysis?

(3 marks)

Before beginning the impact analysis, it is necessary to obtain the following necessary information.

- System mission
- System and data criticality
- System and data sensitivity

42. What does u understand by supply chain management?
(3 marks)

Supply chain management (SCM) is the process of planning, implementing, and controlling the operations of the supply chain with the purpose to satisfy customer requirements as efficiently as possible. Supply chain management spans all movement and storage of raw materials, work-in- process inventory, and finished goods from pointof-origin to point-of-consumption. In literal terms, supply chain refers to the flow of materials from their sources (suppliers) to the company and then inside the company for processing. Today the concept is much broader, including flow of materials, information, payments, and services from suppliers to factories and warehouses to end customers. This reduces uncertainty and risks in the supply chain thereby positively affecting inventory levels, cycle time, business processes

43. Discuss why firewall is the primary method keeping a computer can be secure from intruders. (5 marks)



www.ranapk.com

Firewall

Firewall is the primary method for keeping a computer secure from intruders. A firewall allows or blocks traffic into and out of a private network or the user's computer. Firewalls are widely used to give users secure access to the Internet as well as to separate a company's public Web server from its internal network. Firewalls are also used to keep internal network segments secure; for example, the accounting network might be vulnerable to snooping from within the enterprise. In the home, a personal firewall typically comes with or is installed in the user's computer. Personal firewalls may also detect outbound traffic to guard against spy ware, which could be sending your surfing habits to a Web site. They alert you when software makes an outbound request for the first time. In the organization, a firewall can be a stand-alone machine or software in a server. It can be as simple as a single server or it may comprise a combination of servers each performing some type of firewall processing.

44. Discuss the detail of the 4 categories' of ethical issue (5 marks)

Privacy issues

Following aspects should be covered when privacy is dealt with.

- What kind of surveillance should be used by an employer on an employee?
- What things can keep to themselves and not be forced to reveal to others?
- What information about individuals should be kept in database and how secure is the information there – Issues of Data Protection
- What can be revealed to others about oneself if one is required to do so?

Accuracy Issues

Following are some of the accuracy issues.

- How can we ensure that information will be processed and presented properly?
- Who is responsible for checking the correctness of information collected?
- Is there any track of errors, omissions made in the database and who has made them at what time.
- Who is to be held accountable for the changes made in data base, whether authorized or unauthorized, intentional or unintentional?



WWW.RANAPK.COM

www.ranapk.com

Property Issues

Following are some of the property issues.

- There has to be defined owner of the information
- Issues of software piracy
- Use of corporate computers for private use
- Who should access which component of information database?

Accessibility Issues

These mostly comprise of two aspects.

- Extent of access to be given to various employees in the organization.
- The definition of privileges of each person.

45. Write a complete note on the Focal Point. (5 marks)

A corporate-level facilitator may serve as a focal point for assessments throughout the company, including those pertaining to information security because of familiarity with the tools and the reporting requirements. Each business unit in an organization may have a designated individual responsible for the business unit's risk assessment activities. The computer hardware and software company, may also create a team for the purpose of improving the overall risk assessment process and reviewing results of risk assessments in the hardware and software systems from the perspective of offering a better, reliable and risk free product.

46. Identify aspects which re necessary to be covered when property issues for privacy is deal with. (2 marks)

Property Issues

Following are some of the property issues.

- There has to be defined owner of the information
- Issues of software piracy
- Use of corporate computers for private use



www.ranapk.com

- Who should access which component of information database?

47. Define centralized processing (2 marks)

Centralized Processing is performed in one computer or in a cluster of coupled computers in a single location. Centralized processing was the architecture that evolved from the very first computers

48. Identify the role of senior management and BODs in risk management Process?

(2 marks)

The senior management and the board of Directors are responsible for identifying, assessing, prioritizing, managing and controlling risks.

49. What should be the most important information required for large organization in your opinion? (3 marks)

Information Requirements of Large Organizations

With such a large structure, it is inevitable that the detailed planning should be made for proper management control, for both short term and long term.

- ☐ Performance measurement against plans / targets



50. What are the sources of critical success factor? (Marks: 5)



www.ranapk.com

Sources of critical success factor

1. Industry CSFs resulting from specific industry characteristics;
2. CSF's resulting from the chosen competitive strategy of the business e.g. quick and timely delivery may be critical to courier service business
3. Environmental CSFs resulting from economic or technological changes; and
4. Temporal CSFs resulting from internal organizational needs and changes

51. What is Stand Alone Processing?

Self contained is a micro computer that is not connected to a network. Processing on this computer is called stand alone processing.

52. What is an event-oriented log?

An event-oriented log ---- this usually contain records describing system events, application events, or user events. An audit trail should include sufficient information to establish what events occurred and who (or what) caused them.

53. Write down the steps or order of EC fulfillment

The Steps of Order Fulfillment

1. Payment Clearance
2. In-stock availability
3. Packaging, shipment
4. Insuring
5. Production (planning, execution)
6. Plant services
7. Purchasing, warehousing
8. Customer contacts
9. Returns (Reverse logistics)
10. Demand forecast
11. Accounting, billing



www.ranapk.com

12. Reverse logistics



54. Types of threats (5 marks)



Threats can be divided in to two broad categories

1. Physical threat

This refers to the damage caused to the physical infrastructure of the information systems.

Examples are natural disasters (Fire, earth quake, flood), pollution, energy variations and physical Intrusion.

2. Logical

This refers to damage caused to the software and data without physical presence. Examples are viruses and worms, logical intrusion commonly referred to as hacking.

55. Describe control analysis (marks 5)

The goal of this step is to analyze the controls that have been implemented or are planned for implementation by the organizations to minimize or eliminate the likelihood of occurrence of threat. To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment. Security controls encompass the use of technical and non-technical methods. Technical methods are safeguards that are incorporated into computer hardware, software and firmware such as controls mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software, etc. Non technical controls are management and operational controls such as security policies and operational procedures and personnel, physical and environmental security. The control categories for both technical and non technical control methods can be further classified as either preventive or detective.



www.ranapk.com

56. How to secure the system through virus (marks 5)

Technical methods of preventing viruses can be implemented through software. The following actions can reduce the risk of infection to hardware and operating systems, 1) Use boot virus protection (i-e., built-in, firmware-based virus protection).

- 2) Use remote booting, local hard drive of the system is not used for the boot up process.
- 3) Use a hardware-based password.
- 4) Use write-protected tabs on diskettes.
- 5) Use of antivirus software is another very important technical control against the spread of virus

57. List any general 6 impacts (3 marks)

In generic terms the following types of impact could occur:

1. Loss of income
2. Increased cost of recovery (correcting information and re-establishing services)
3. Increased cost of retrospectively securing systems
4. Loss of information (critical data, proprietary information, contracts)
5. Loss of trade secrets
6. Damage to reputation
7. Degraded performance in network systems
8. Legal and regulatory non-compliance
9. Failure to meet contractual commitments

58. Define CRM (3 marks)

- 1) CRM is a business strategy that goes beyond increasing transaction volume.
- 2) Its objectives are to increase profitability, revenue, and customer satisfaction.
- 3) To achieve CRM, a company wide set of tools, technologies, and procedures promote the relationship with the customer to increase sales.
- 4) Thus, CRM is primarily a strategic business and process issue rather than a technical issue.



www.ranapk.com

59. Describe security audit (3marks)

Going online exposes an entity to more hazards than otherwise. This requires implementation of effective controls and checks to secure both the company's online data from undesired manipulation, and the customer's information and orders. The organization may hire an audit firm to offer these services and check the integrity of the website. Web audits help in gaining a web rating which enhances the credibility of the audits. There are different levels of audits, tailored to your needs and your budget.

Among the issues we can carefully review on your site, resulting in a detailed report with recommendations:

- Performance, page load time
- Graphics optimization
- Navigation usability, consistency
- Browser compatibility
- Content formatting consistency
- Accessibility compliance with ADA guidelines and Section 508 Standards
- Broken links
- Page errors, script errors
- search engine ranking
- interface layout

60. Components of IDS and its limitations (3 marks)

Components of IDS

An IDS comprises on the following:

1. Sensors that is responsible for collecting data. The data can be in the form of network packets, log files, system call traces, etc.
2. Analyzers that receive input from sensors and determines intrusive activity.
3. An administration: it contains intrusion definitions applied by the analyzers.
4. A user interface



www.ranapk.com

Limitations of IDS

IDS can not help with the following weaknesses:

1. Incorrectness or scope limitation in the manner threats are defined
2. Application-level vulnerabilities
3. Backdoors into application
4. Weakness in identification and authentication schemes

61. Define IDS (2 marks)

Intrusion Detection Systems (IDS)

Another element to securing networks is an intrusion detection system (IDS). IDS are used in complement to firewalls. An IDS works in conjunction with routers and firewalls by monitoring network usage anomalies. It protects a company's information systems resources from external as well as internal misuse.

62. Describe Trojans virus (2 marks)

Trojan horse – Users execute the program written by the penetrator. The program undertakes unauthorized activities e.g. a copy of the sensitive data.

63. Define data and information----- (2 marks)

Data vs. Information

Data represents facts of any kind. In the process of recording important particulars of any event, it is the discretion of the management, what should be recorded and how it should be presented. However when this data is processed or reformatted, it becomes information. Information is a subset of data which adds to the knowledge.



www.ranapk.com

Information should be relevant so-that it is valuable for the recipient. Although the processed form of information is more valuable than the raw form of data, still all information is not of value for every one.

Distributing common information to every one may result in waste of time and confusion. Irrelevant information has no value.

64. Attributes of ERP, explain_____ (5 marks)

Attributes of an ERP software

ERP applications address the complete business process. ERP applications are modular generally covering all aspects of the business as each aspect is dependant upon the other.

Thus you will generally find certain standard modules as part of ERP software which are manufacturing, supply chain, financials, CRM, human resources and warehouse management. It may also be stated that depending upon business size , phased approach may be opted to implement the ERP. A phased approach becomes necessary because of business process realignment and implementation issues particulars relating to change in habits of the users.

During the past, the software laid greater stress on financial transactions and their cumulative result with information for other department being provided as a secondary objective. ERP is extended to the enterprise level, encompassing not only the organization but also the entities external to organization i.e. suppliers and customer.

65. What are the change agents, explain their role in change----- (3 marks)

Change agents

A person or a team who leads a change project or business-wide initiative by defining, researching, planning, building business support and carefully selecting volunteers to be part of a change team.

Change Agent is comfortable with leading change initiatives with uncertain outcomes and systematically considers new and better ways of doing things.



www.ranapk.com

66. Property issues regarding privacy----- (3 marks)

Property Issues

Following are some of the property issues.

- There has to be defined owner of the information
- Issues of software piracy
- Use of corporate computers for private use
- Who should access which component of information database?

67. What is ethics and code of ethics----- (3 marks)

a) Ethics

Ethics are moral choice made by individual in relation to the rest of the community, rules of governing members and standards of acceptable behaviour. **b) Code of ethics**

Code of ethics is collection of rules as guide for the members of the organization.

68. What are physical threats----- (3 marks)

Physical threats

The risks of physical damage render the computer hardware becomes useless due to the damage caused to it by natural disasters (Fire, earth quake, flood), pollution-Dust, energy Variations. Reasonable measures should be taken to avoid undesirable consequences.

69. Input of risk determination----- (2 marks)

The inputs of to this phase are

1. Likelihood of threat exploitation
2. Magnitude of impact



3. Adequacy of planned and current controls

70. How the scanners are used as the technical control against the spread of viruses?

Scanners

They scan the operating system and application software for any virus based on the viruses they contain. Every virus has a different bit pattern. These unique bit patterns act as an identity for the virus and are called signatures. These signatures are available in virus definitions. Every scanner contains in it certain virus definitions which in fact are signatures (bit patterns) for various kinds of virus. The scanner checks or scans the operating system and other application soft wares installed on the hard drives. While scanning, it checks the bit patterns in all software against the bit patterns contained in the virus definitions of the scanner. If they found similar, they are labeled as virus.

71. What is logical intrusion?

The skills needed to exploit logical exposures are more technical and complex as compared to physical exposures.

Generally a similar term used in relation to logical intrusion is hacking.

In the 1990's dotcom boom encouraged many organizations to use internet for executing transactions. Initially internet used was more oriented to providing information to the general public. With the enhanced focus of the organizations to reduce operational costs, and increase sales, the use of internet started increasing.

72. Identify the rule that DFD as an analytical tool follows the rule in achieving the level of standardization?

The DFD as an analytical tool follows certain rules. These rules help in achieving the level of standardization.

- There should be no black holes, gray holes, miracles.
- Do not leave things unlabeled
- The DFD should not include data flows that are unassociated with the process.

73. Identify any two methods of IS integration?



www.ranapk.com

Connect Existing Modules/system

The basic concept is to maximize the use of existing systems and minimize the changes in them.

Good integration allows the addition of new applications to existing ones and the connection of systems to intranets and the internet. This approach extends the life of applications and saves tremendous amounts of money. However, connecting existing system may be difficult and expensive in many cases. Old systems were built and developed over a number of years encompassing technologies and platforms of various specifications.

42.3 Using SCM Software

Supply chain management (SCM) is the process of planning, implementing, and controlling the operations of the supply chain with the purpose to satisfy customer requirements as efficiently as possible. Supply chain management spans all movement and storage of raw materials, work-in- process inventory, and finished goods from point-of-origin to point-of-consumption. In literal terms, supply chain refers to the flow of materials from their sources (suppliers) to the company and then inside the company for processing. Today the concept is much broader, including flow of materials, information, payments, and services from suppliers to factories and warehouses to end customers. This reduces uncertainty and risks in the supply chain thereby positively affecting inventory levels, cycle time, business processes

74. What is E-Supply chain?



E. Supply Chain Management refers to the flow of physical goods and associated information from the source to the consumer. Key E. Supply chain activities include purchasing, materials management, distribution, customer service, and inventory forecasting. Effectively managing these processes is critical to the success of any online operation

75. What is off-page connector?

Use to connect remote flowchart portion on different pages. One flow line enters or exits.

76. Discuss various steps in threat

Steps in threat identification

Following steps are followed in this phase

1. Threat source identification – sources vary from being human to natural threats



www.ranapk.com

2. Motivation and threat actions – Reasons why someone should instigate a threat and what actions he can take in such instigation are discovered.

77. How can we make our password secure?

1: Keep secret

2: Don't write anywhere

3: Always use the password with combination of letters, numbers, upper and lower cases 4: change password regular basis

78. Identify components of Intrusion detection system?

Components of IDS

An IDS comprises on the following:

- Sensors that is responsible for collecting data. The data can be in the form of network packets, log files, system call traces, etc.
- Analyzers that receive input from sensors and determines intrusive activity.
- An administration: it contains intrusion definitions applied by the analyzers.
- A user interface

79. List any two tolls used to implement TQM?

80. Risk variance ----- (2 marks)

81. How to secure threats from internet (3marks)

82. The role of audit in MIS----- (3 marks)

83. Identify the tangible or intangible in supply Chan management? (Marks: 5)

84. What is entity relationship management? (2 marks)

85. Security measure are adopted in IS



www.ranapk.com

86. Define the term ‘intruders’ and how they can be classified according to the way they operate? (Marks 5)

87. How E-Commerce is beneficial to business and society? (Marks 5)