

# CS507 FINAL TERM SOLVED SUBJECTIVE (VISIT VURANK FOR MORE)

---

**Question No: 1 ( Marks: 2 )**

What are the information requirements of the service sector?

**Answer:**

**Information requirements of Service Sector**

- Quality of service provided.
- Mode of delivery
- Customer Satisfaction
- Time Scheduling
- Resource Management

**Question No: 2 ( Marks: 2 )**

Define Business Continuity Planning (BCP) ?

**Answer:** Business Continuity Planning (BCP) is a methodology used to create a plan for how an organization will resume partially or completely interrupted critical functions within a predetermined time after a disaster or disruption.”

**Question No: 3 ( Marks: 2 )**

Identify different types of Information assets ?

- 1- **Security Policy**
- 2- **Security Program**

**Question No: 4 ( Marks: 2 )**

Identify components of Intrusion detection system ?

**Answer: Components of IDS**

An IDS comprises on the following:

- Sensors that are 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

**Question No: 5 vuzs ( Marks: 3 )**

What is the necessary information needed to begin impact analysis?

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

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

**Question No: 6 ( Marks: 3 )**

Define Active attacks?

**Answer:** Active attacks may include obtaining unauthorized access to modify data or programs, causing a denial of service, escalating privileges, accessing other systems. They affect the integrity, availability and authentication attributes of network security.

**Question No: 7 ( Marks: 3 )**

Why is it needed for Accounting information system (AIS) to be linked with all other information systems in an organization?

**Answer:** Accounting information system (AIS) is linked to all the information systems in an organization. This is important because the data required for proper book keeping and generation of transactional reports is extracted from all over the organization. For instance sales information can be sought only from marketing information system and stock information is available in manufacturing information system.

**Question No: 8 ( Marks: 3 )**

**Identify any six factors that should be considered in order for change to be successful?**

**Answer:**

**Following factors should be considered in order for change to be successful:**

- What are the implications and barriers to successful implementation?
- What processes will we need to change/introduce?
- Who will feel threatened by the change?
- How do we change people's behavior?
- How will success be measured and what value will success Have for the business and individual?
- Is the proposed change aligned with the strategic plan?

**Question No: 9 ( Marks: 5 )**

What do you understand by Privacy? How can privacy be protected? List threats to Privacy.

**Answer:**

Privacy means the quality or condition of being secluded from the presence or view of others, the state of being free from unsanctioned intrusion: *a person's right to privacy*, the state of being concealed; secrecy.

**Protecting Privacy**

The rights of privacy must be balanced against the needs of the society. Every society has to decide somewhere on the gray area between hiding all and knowing all extremes. Public's rights to know is superior to the individual's rights of privacy. Usually public and individual's rights stand in conflict with each other. Since government agencies have their concerns in priority e.g. criminal investigation, undesirable social activities. Various aspects can be seen as a threat to privacy.(vuzs)

**Threats to Privacy**

- Electronic surveillance
- Data Profiling
- Online Privacy
- Workplace monitoring
- Location tracking
- Background checks
- Financial privacy
- Medical record and genetic profiling
- Digital right
- Intellectual property rights
- Taxation Issues

**Question No: 10 ( Marks: 5 )**

Give any two examples to prove that Audit trails help to provide variants from normal behavior which may lead to unauthorized usage of resources.

**Answer:** Audit trails help to provide variants from normal behavior which may lead to unauthorized usage of resources. For example

- Audit trails can be used together with access controls to identify and provide information about users suspected of improper modification of data (e.g., introducing errors into a database).
- An audit trail may record "before" and "after" images, also called snapshots of records.

**Question No: 11 vuzs ( Marks: 5 )**

**Identify and define the types of active attacks ?**

**Answer:** After getting proper information about system in passive attacks intruder will obtain unauthorized access to modify data or programs, causing a

denial of service, escalating privileges, accessing other systems. They affect the integrity, availability and authentication attributes of network security.

### **Types of Active attacks**

Common form of active attacks may include the following:

- **Masquerading** – involves carrying out unauthorized activity by impersonating a legitimate user of the system.
- **Piggybacking** – involves intercepting communications between the operating system and the user and modifying them or substituting new messages.
- **Spoofing** – A penetrator fools users into thinking they are interacting with the operating system. He duplicates logon procedure and captures pass word.
- **Backdoors/trapdoors** – it allows user to employ the facilities of the operating system without being subject to the normal controls.(vuzs)
- **Trojan Horse** – Users execute the program written by the penetrator. The program undertakes unauthorized activities e.g. a copy of the sensitive data.

**Question No: 12 vuzs ( Marks: 3 )**

**Differentiate between Incremental and iterative models with the help of one example each.**

**Answer: Incremental vs. Iterative**

These sound similar, and sometimes are equated but there is a subtle difference:

- **Incremental:** add to the product at each phase
- **Iterative:** re-do the product at each phase

**Example:(vuzs)**

#### **Building a House**

- **Incremental:** Starts with a modest house, keep adding rooms and upgrades to it.
- **Iterative:** The design/construction map of the house is amended and improved and repeated until all the requirements are fulfilled.

**Question No: 13 ( Marks: 3 )**

**Define Risk Determination. Identify its inputs and outputs.**

**Answer:** 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.

**Question No: 14 ( Marks: 2 )**

**What is the basic purpose of setting up systems and procedures. Give your own opinion.**

**Answer:** The basic purpose of setting up system and procedures is to make available information when it is required

**Question No: 15 ( Marks: 2 )**

**Define threat and identify its types.**

**Answer:** Threat is an act or event which can cause loss. Threats are of two types logical threats and physical threats.

**Question No: 16 ( Marks: 2 )**

**List any two types of information that can be used as input for vulnerability?**

**Answer:**

- 1- Any audit comments
- 2- Security requirements

**Question No: 17 ( Marks: 2 )**

What are the basic components of DSS?

**There are two major components**

- **DSS data base** – is a collection of current and historical data from internal external sources. It can be a massive data warehouse.
- **Decision Support Software system** – is the set of software tools used for data analysis.

**Question No: 18 ( Marks: 2 )**

**Define the following:**

**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.

**Question No: 19 ( Marks: 2 )**

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.

**Question No: 20 ( Marks: 2 )**

Define intrusion detection?

Intrusion Detection is a process that identifies the attempts to penetrate the system and gain unauthorized access.

**Question No: 21 ( Marks: 3 )**

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

**Question No: 23 ( Marks: 3 )**

What is Data Driven Decision Support System?

Data driven DSS 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

**Question No: 24 ( Marks: 3 )**

Define Re-engineering?

Re engineering is the fundamental rethinking and redesigning of business process to achieve dramatic improvement in critical, contemporary measures of performance, such as cost, quality, service and speed.

**Question No: 25 ( Marks: 5 )**

**List any five reasons that attract organizations to ERP?**

**Answer:**

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

Question No: 26 ( Marks: 3 )

How virus and worms can be transmitted into computers? Identify any three sources?

**Answer:**

Virus or worms are transmitted easily from the internet by downloading files to computers web browsers. Other methods of infection occur from files received through online services, computer bulletin board systems, local area networks.

Viruses can be placed in various programs, for instance

1. Free Software – software downloaded from the net
2. Pirated software – cheaper than original versions
3. Games software – wide appeal and high chances
4. Email attachments – quick to spread
5. Portable hard and flash drives – employees take disks home and may work on their own personal PC, which have not been cleaned or have suitable anti-viruses installed on them.

Question No: 27 ( Marks: 3 )

How the information is kept in the purchase system?

Question No: 28 ( Marks: 2 )

What is information Quality Checklist?

**Answer:**

The information can also be ranked in accordance with the qualities it has in it. The experts have devised certain criteria to evaluate the quality of information. Those some points which are used to evaluate the quality are known as quality checks.

Question No: 29 ( Marks: 2 )

What are Active monitors? Define.

**Answer:**

This software serves the concurrent monitoring as the system is being used. They act as a guard against viruses while the operating system is performing various functions e.g connected to internet, transferring data, etc.

**Question No: 30 vuzs (Marks: 3)**

Briefly describe Incremental Model.

**Answer:** 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.

**Question No: 31 ( Marks: 3 )**

Information system security association of USA has listed many ethical challenges, identify any three of them?

**Answer:**

1. Misrepresentation of certifications, skills
2. Abuse of privileges
3. Inappropriate monitoring

**Question No: 39 ( Marks: 5 )**

**What do you think what are the key benefits of Ecommerce to organizations?**

**Answer: Advantages of E-Commerce to the Online Business**

- E-Commerce helps to Increase the sales revenue to the business
- Business people can spend less money and earn high profits with e-commerce
- Easily we can track the segment of customers who are happy with purchasing goods through online
- Instantaneous global sales presence in quick time
- We can Operate the business in 24 \*7 basis
- Easily we can increase our business customers
- We set up shop anywhere in the world, self-governing of geographical locations
- Inexpensive way to turn your Web site into a revenue center
- Reduce Customer Support costs via e-mail marketing & customary newsletters
- We can create customized mailing list
- Easily we can drive free traffic to the website
- We can easily promote our business website by using various promotional activities such as Search Engine Optimization, Pay Per Click Management, Email Marketing, Social Media Optimization, Online Banner Advertisement, Online Branding and Affiliate Management.

**Question No: 32 ( Marks: 5 )**

**What do you understand by Disaster Recovery Planning?**

A disaster recovery plan is a comprehensive statement of consistent actions to be taken before, during and after a disaster. The plan should be documented and tested to ensure the continuity of operations and availability of critical resources in the event of a disaster.

This typically details the process IT personnel will use to restore the computer systems. Disaster recovery plans may be included in the business continuity plan or as a separate document all together. Business continuity plan may not be comprehensively available in a non-critical environment but Disaster Recovery Plan should be there at least to manage and help organization to recover from disasters. A subcomponent of business continuity plan is the IT disaster recovery plan. IS processing is one operation of many that keep the organization not only alive but also successful, which makes it of strategic importance.

**Question No: 33 ( Marks: 2 )**

List information Requirements for Medium sizes organizations.

**Answer:**

Planning for required Information  
Monitoring of information of planning.

**Question No: 34 ( Marks: 2 )**

Why we need to secure information systems?

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.

**Question No: 35 ( Marks: 3 )**

**What is access control? Give example**

Answer:

**Access Controls**

These controls establish the interface between the would-be user of the computer system and the computer itself. These controls monitor the initial handshaking procedure of the user with the operating system. **For example** when a customer enter the card and the pin code in an automatic

teller machine (ATM), the access controls are exercised by the system to block unwanted or illegitimate access.

**Question No: 36 vuzs ( Marks: 3 )**

**Risk mitigation is a process that takes place after the process of risk assessment has been completed. Discuss briefly various risk mitigation options?**

**Answer:**

- **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 a vulnerability e.g. use of supporting preventive and detective controls.
- **Risk Planning:** To manage risk by developing a 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.

**Question No: 37 ( Marks: 3 )**

**Differentiate CRM from ERP ?**

**Answer:**

**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.

**Question No: 38 ( Marks: 5 )**

**Differentiate Impact analysis from Risk determination?**

This phase relates to analyzing how much the information assets are exposed to various threats identified and thus quantifying the loss caused to the asset through this threat.

This phase relates to analysis of both physical and logical threats. It measures level of risk is to determine the adverse impact resulting into a successful exercise of vulnerability. The information can be obtained from existing organizational documentation, such as the mission impact analysis report or asset criticality assessment report. A business impact analysis report or asset criticality assessment report. The adverse impact of a security event can be described in terms of loss or delay of any or all of the three security goals. Confidentiality, integrity, availability.

**Question No: 39 ( Marks: 2 )**

What are the physical threats for Information System.

**Answer: 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.

**Question No: 40 ( Marks: 2 )**

List any two types of information that can be used as input for vulnerability.

Following information is used as an input

2. Any audit comments
3. Security requirements

**Question No: 41 ( Marks: 2 )**

List down different types of SUPPLY CHAIN.

**Types of Supply Chains**

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

1. Made to Store
2. Continuous Replenishment
3. Built to order

**Question No: 42 ( Marks: 3 )**

What do u know about Key stroke Monitoring? (3)

**Answer :**

**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.

**Question No: 43 ( Marks: 3 )**

Identify roles and responsibilities of any three professionals in an organization.

**Answer:**

**1-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;

**2-Process Owners** — responsible for ensuring that appropriate security, consistent with the organization's security policy, is embedded in their information systems;

**3-Technology providers** — responsible for assisting with the implementation of information security

Draw backs of ESP system. (3)

**Question No: 44 ( Marks: 5 )**

Classify E-Commerce into different classes. (5)

The most prevalent of E-Commerce models can be classified as under:

1. Business to Consumer (B2C)
  2. Business to Business (B2B),
  3. Business to Employee (B2E),
  4. Consumer to Consumer (C2C) and
  5. E-Government
- Government to Citizens/Customers (G2C)
  - Government to Business (G2B)
  - Government to Government (G2G)

**Question No: 45 ( Marks: 5 )**

Incorporate Risk management SDLC? identify its phases?

For each phase of SDLC, the process of risk management is no different. Rather it is iterative process which can be performed at each major phase. Every step of development has its own risks which need to be handled and addressed separately. Hence managing risk in SDLC means managing risk of each phase of life cycle.

**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