Fast Track Webinar Series

VISA *for* DISA

Day 4

ICAI Information Systems Audit 3.0 Course

For July 2024 AT

INFORMATION SYSTEMS AUDIT 3.0 COURSE

Module - 4
Information Systems Operations and Management

Thursday ◊ 04th JULY 2024 ◊ 08:30 AM to 09:30 AM ◊ www.3spro.blogspot.com

CA Dr GOPAL KRISHNA RAJU

Chartered Accountant, Insolvency Professional, Registered Valuer & Arbitrator

Visiting Faculty, Indian Institute of Management

Pointers

- Read the ICAI Study Material minimum 2 - 3 times for getting clarity and confidence
- **Exam Preparation Tip:** Practice eliminating the three choices by reasoning
- All references made in this material is based on the following BGM of ICAI – Module 4 – IS Operations & Management

https://resource.cdn.icai.org/60974daab49637bgmisa-mod4.pdf

Reference Material for ICAI ISA PQC

Basic

- ISA Background Material 3.0
- DISA AT Mock Test Papers

Additional

- ISC2 - The International Information System Security Certification Consortium
- ISO 22301:2012 - Business Continuity Standard
- NIST – National Institute of Standards and Technology - USA
- ISACA – Information System Audit and Control Association - USA
- DISA Manual 2.0
- CSIRT- CMU; CERT-In
- www.rbi.org.in
- IT Act 2008

Snapshot

Module	Contents	Pages	Questions
1	Information Systems Audit Process	185	60
2	GRC & BCM	149	50
3	SDLC	133	34
4	IS Operations & Management	97	40
5	Protection of Information Assets	125	
6	Emerging Technologies	77	
Total		**766**	

Module 4
Information Systems Operations & Management

Information Systems Management	**4.1**
Information Systems Operations	**4.2**
Software Operations & Management	**4.3**
Incident Response & Management	**4.4**

ISA 3.0

Weightage	Modules
18%	Information Systems Process Audit
14%	Governance and Management of Enterprise Information Technology, Risk Management, Compliance and Business Continuity Management
14%	System Development, Acquisition, Implementation and Maintenance Application System Audit
18%	Information Systems Operations and Management
18%	Protection of Information Assets
18%	Emerging Technologies

Chapter 1

Information Systems Management

1. Which of the following is a common feature for all the policies?

a) Encryption

b) Standards

c) Acceptable Use

d) Process

Acceptable Use Policy

- An acceptable use policy, acceptable usage policy or fair use policy, is a **set of rules** applied by the **owner, creator or administrator** of a network, website, or service, that restrict the ways in which the network, website or system may be used and sets guidelines as to how it should be used.

2. Which of the following is not an HRM function?

a) Recruitment

b) Cyber security training

c) Security Policy approval

d) Appraisal

3. Which of the following training an employee can acquire while working on his/her desk in the office?

a) E-learning

b) Simulator based training

c) Instructor led training

d) Hands on training

4. For an unexpected and sudden changes in technology, organisations need to be

a) Innovative

b) Agile

c) Expert

d) Doer

Agile: able to move quickly and easily

5. Who owns the data in a department?

a) System owner

b) Process owner

c) Data custodian

d) Data owner

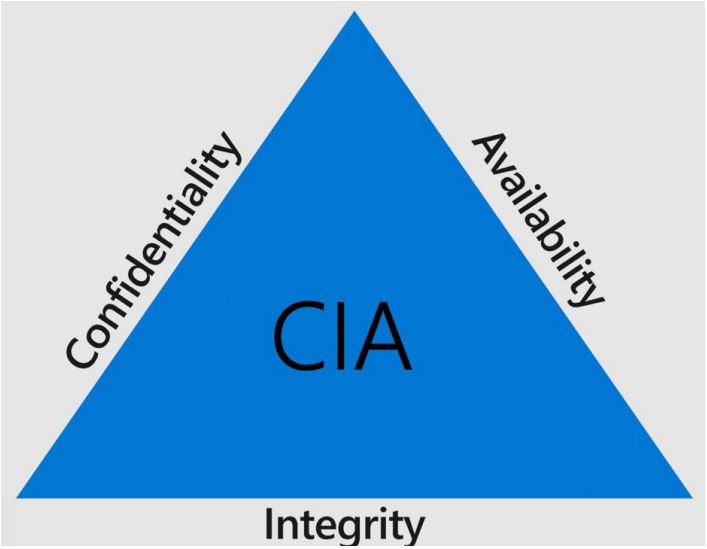
6. The GREATEST challenge in outsourcing data processing is

a) Data confidentiality

b) Distance

c) Data integrity

d) Cost



7. Which one of the following combinations of roles should be of GREATEST concern for the IS auditor?

a) Network administrators are responsible for quality assurance

b) Security administrators are system programmers

c) End users are security administrators for critical applications

d) Systems analysts are database administrators

8. Accountability for the maintenance of appropriate security measures over information assets resides with:

a) Security administrator

b) Systems administrator

c) Data and systems owners

d) Systems operations group

9. The decision-making environment of an operational level manager can be characterized as:

a) Structured

b) Semi-structured

c) Unstructured

d) None of these

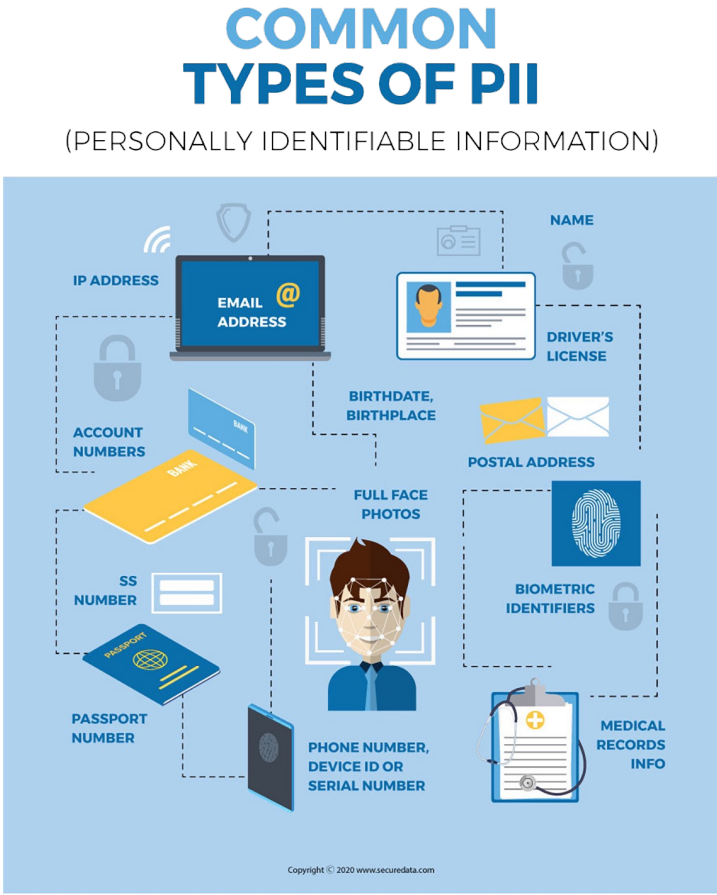
10. Which department is MOST LIKELY to store Personally identifiable information (PII) data?

a) Management

b) Information System Department

c) Marketing Department

d) Human Resource Department



Chapter 2

Information Systems Operations

11. Why should organizations want to manage logs?

a) To be informed when something unusual happens involving a system or application

b) To be able to do take action in response to a security event

c) To keep a record of all the responses to security events

d) All of the above

12. When implementing a log management program, it's BEST to start with:

a) Technology from a trusted vendor

b) The same program and process that organizations with similar business are using

c) List of top-three vendors from a published report

d) A careful review of the organization's log management and reporting needs

13. The security principle of least privilege is:

a) The practice of limiting permissions to the minimal level that will allow users to perform their jobs.

b) The practice of increasing permissions to a level that will allow users to perform their jobs and those of their supervisor.

c) The practice of limiting permissions to a level that will allow users to perform their jobs and those of their immediate colleagues.

d) The practice of increasing permissions to a level that will allow users to use the cloud services of their choice in order to get their jobs done more quickly.

14. Why does privilege creep pose a security risk?

a) Users privileges don't match their job or role and responsibilities.

b) Because with more privileges there are more responsibilities.

c) Users have more privileges than they need and may use them to perform actions outside of their job description.

d) Auditors may question about a mismatch between an individual's responsibilities and their privileges and access rights.

Threats mitigated by a user access review:

- Privilege creep
- Excessive privileges
- Access misuse and employee mistakes
- Insider threats

15. Software Configuration management is the discipline for systematically controlling

a) Changes due to the evolution of work products as the project progresses

b) The changes required due to defects being found which are to be fixed

c) Changes necessary due to change in requirements

d) All of the above

Configuration Management

- Configuration management is a systems engineering process for establishing consistency of a product's attributes throughout its life. In the technology world, configuration management is an IT management process that tracks individual configuration items of an IT system.

Configuration: an arrangement of parts or elements in a particular form, figure, or combination.

16. Which of the following is the top priority that, companies planning to implement an asset management system should examine?

a) The visual appeal of websites, internal search pages and marketing collateral

b) Number of videos, audio files and other multimedia assets available

c) Specific data needs and the business problems to be solved

d) All of the above


All assets in one place
Manage assets from any location
Understand and monitor an asset's life-cycle
ASSET MANAGEMENT SYSTEM
Identify and manage risks
Track all assets and remove ghost assets
Produce accurate and detailed audits

17. **Self-service assistance** to users provided by help-desk such as resetting passwords etc. is considered which level of assistance?

a) Level 4

b) Level 0

c) Level 2

d) Level 1

Multi-Tier IT Support

Tier 4

Support powered by software/hardware vendors

Tier 3

Handling advanced problems that need investigation on the code level

Tier 2

In-depth technical support

Tier 1

Solving basic issues, answering general questions about software functionality

Tier 0

Self-support

18. During development of a software system, which of the following will be used to maintain software integrity?

a) Configuration Management

b) Version Control

c) Change Management

d) None of the above

19. Who of the following would approve or reject major changes in configuration?

a) Management

b) Change control board (CCB)

c) User

d) System Administrator

A change control board is a group of individuals responsible for reviewing and analysing change requests and recommending or making decisions on requested changes to the baselined work. Poor change control can significantly impact the project in terms of scope, cost, time, risk, and benefits.

20. A transaction in a database management system (OLTPS) should be atomic in nature. An Atomic Transaction is:

a) Transaction should be submitted by a user

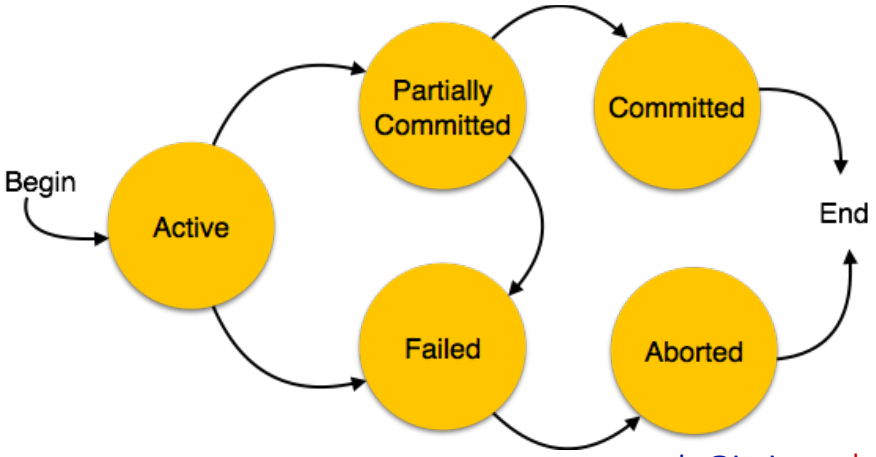
b) Transaction should be either completed or not completed at all

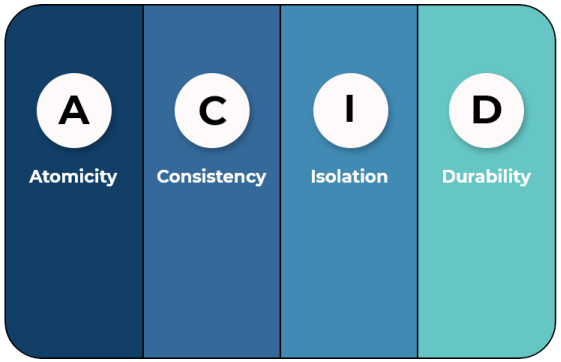
c) Transaction should fail

d) Transaction can be in-between fail and complete

Atomicity

- An atomic transaction is an indivisible and irreducible series of database operations such that **either all occurs, or nothing occurs**.
- A guarantee of atomicity prevents updates to the database occurring only partially, which can cause greater problems than rejecting the whole series outright.





Chapter 3

Software Operations & Management

21. The main focus of acceptance testing is

a) Ensuring that the system is acceptable to management

b) Accepting errors & bugs in the system

c) Ensuring that the system is acceptable to users

d) Ensuring that the system is acceptable to auditors

22. Which of the following test would be carried out when, individual software modules are combined together as a group?

a) Integration testing

b) Unit testing

c) System testing

d) White box testing

23. Which of the following should be reviewed to provide assurance of the database referential integrity

a) Field definition

b) Master table definition

c) Composite keys

d) Foreign key structure

Referential integrity refers to the accuracy and consistency of data within a relationship. In relationships, data is linked between two or more tables. This is achieved by having the foreign key (in the associated table) reference a primary key value (in the primary – or parent – table).

FOREIGN KEY

Key

Foreign Key

Student_details

ID	Name	Course
1401	Arya	Java
2109	Bran	Python
1909	Arya	C++
1405	Cersie	Python

Student_Marks

ID	Marks
1401	79
2109	85
1909	83
1405	84

24. When evaluating the effectiveness and adequacy of a preventive computer maintenance program, which of the following would be considered to be MOST helpful to an IS Auditor?

a) A system downtime log

b) Vendors' reliability figures

c) Regularly scheduled maintenance log

d) A written preventive maintenance schedule

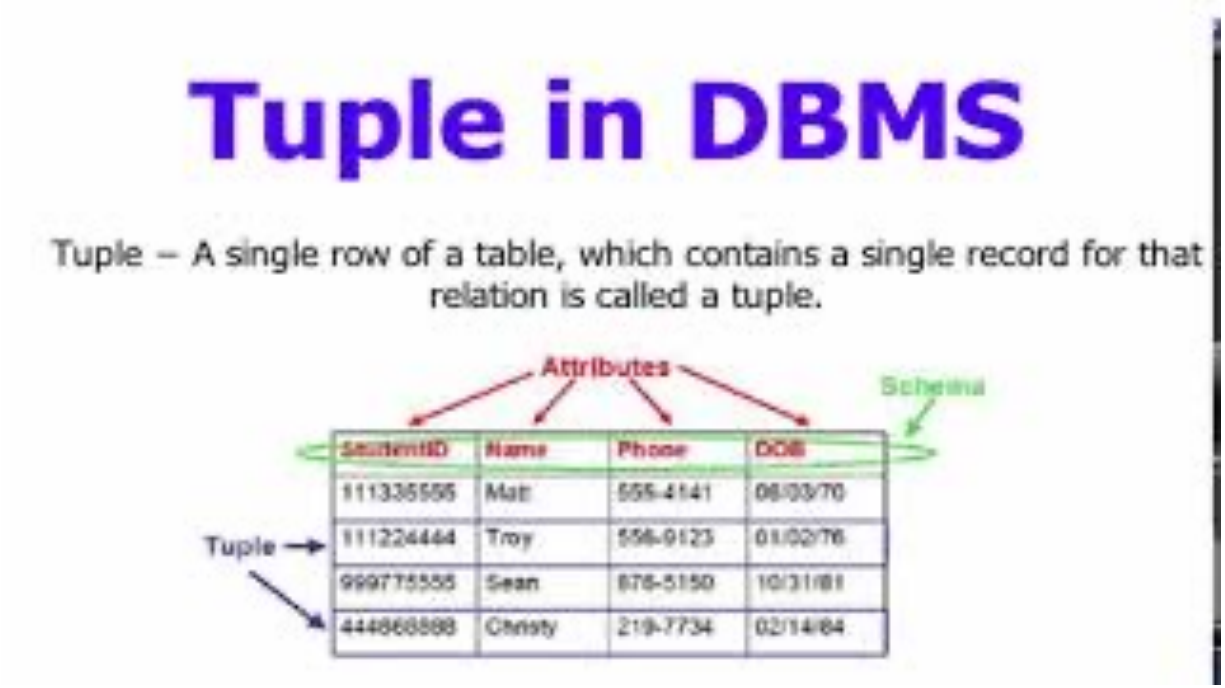
25. In a relational DBMS a record refers to which of the following

a) Tuple

b) Rows

c) Column

d) Transaction



26. Which of the following will ensure that a column in one table will have a valid value or shall be "null" in another table's column?

a) Primary key

b) Secondary key

c) SQL

d) Foreign key

Customers

Customer_ID	Name	Age	Ph_no
101	Prashant	34	12345
102	Anmol	32	54321
103	Rahul	37	21345
104	Harry	34	32145
105	James	32	41235

Products

Product_ID	Name	Price
051	Burger	5$
052	Pizza	8$
053	Ice cream	3$
054	Cold drink	3$
055	Milk	3$

Foreign Keys

Orders

Customer_ID	Product_ID	Order_Quantity
101	053	2
105	053	3
108	051	5
101	052	1
105	051	2

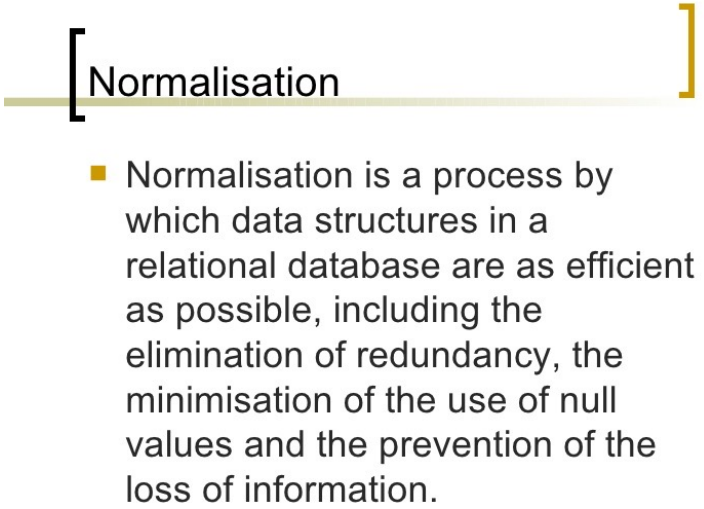
27. Database normalization is

a) Data redundancy optimization

b) Data logging and accountability

c) Streamlining data process

d) Deleting temporary files



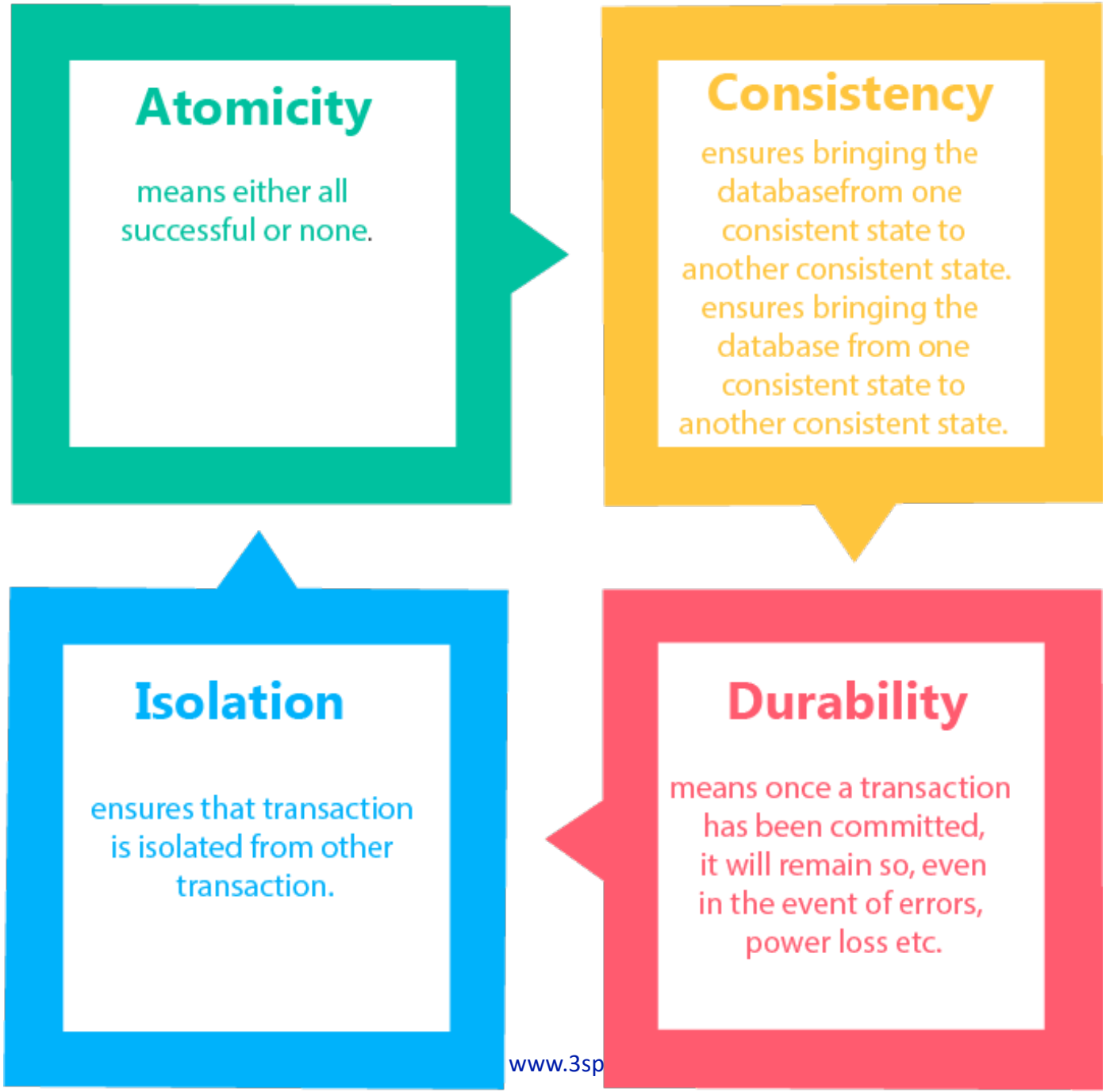
28. Which of the following is NOT a property of database transactions (OLTPS)?

a) Consistency

b) Atomicity

c) Insulation

d) Durability


Atomicity
means either all successful or none.
Consistency
ensures bringing the databasefrom one consistent state to another consistent state. ensures bringing the database from one consistent state to another consistent state.
Isolation
ensures that transaction is isolated from other transaction.
Durability
means once a transaction has been committed, it will remain so, even in the event of errors, power loss etc.

29. After discovering a security vulnerability in a third-party application that interfaces with several external systems, a patch is applied to a significant number of modules. Which of the following tests should an IS auditor recommend?

a) Stress

b) Black box

c) Interface

d) System

30. An organization has recently installed a security patch, which crashed the production server. To minimize the probability of this occurring again, an IS auditor should:

a) Apply the patch according to the patch's release notes.

b) Ensure that a good change management process is in place.

c) Thoroughly test the patch before sending it to production.

d) Approve the patch after doing a risk assessment.

Chapter 4

Incident Response and Management

According to the **National Institute of Standards and Technology (NIST)**, part of the U.S. Department of Commerce, there are four stages in the incident response lifecycle: **preparation, detection and analysis, containment, eradication, recovery, and post-incident activity**. Incident response programs typically address these stages, encompassing steps for detecting incidents, responding to these events and limiting the damage where possible.

31. Basic operation of the SIEM tools, on the logs collected from the devices is

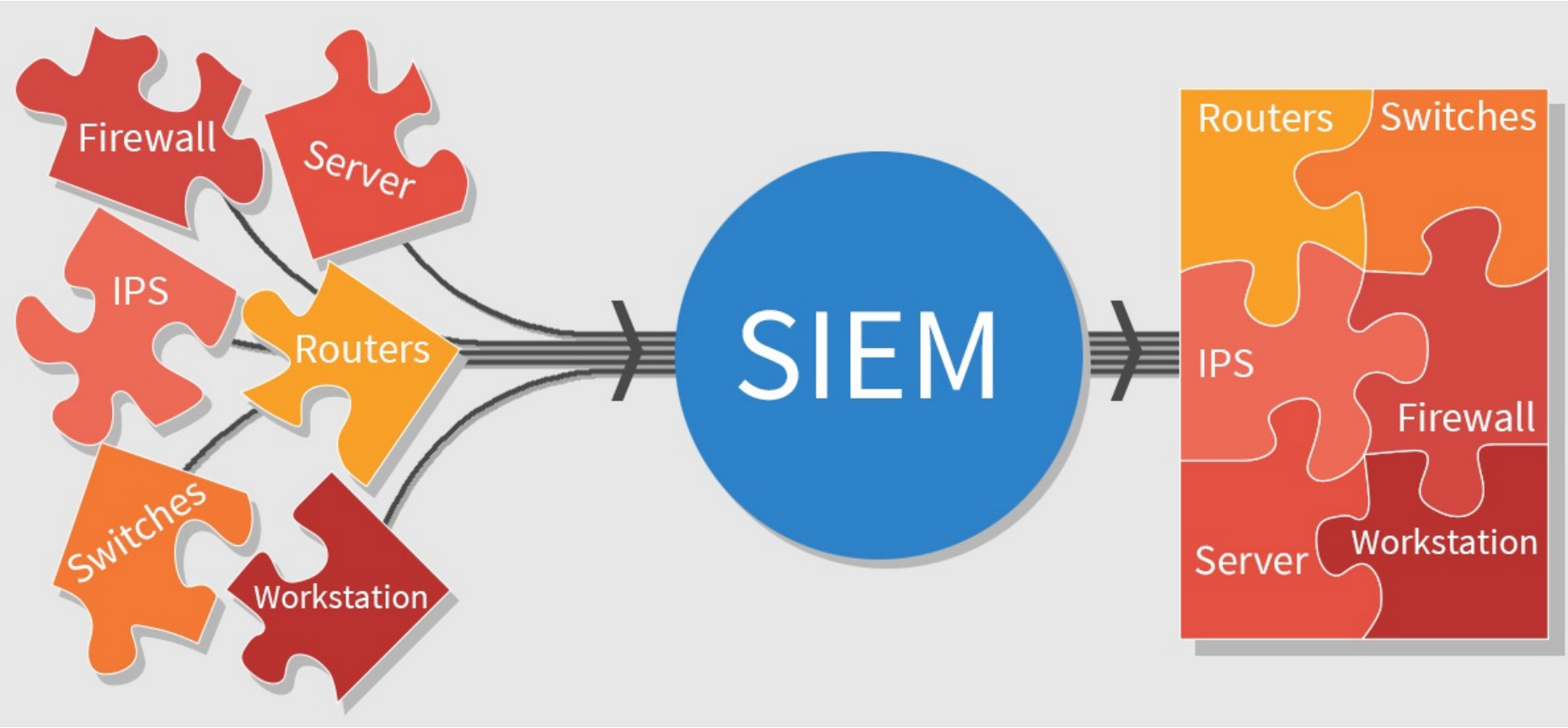
a) Correlating the log

b) Collecting the log

c) Analysing the log

d) Live Correlating the log

SIEM tools provide: Real-time visibility across an organization's information security systems. Event log management that consolidates data from numerous sources.



- Security Information and Event Management (**SIEM**) is a set of tools and services offering a holistic view of an organization's information security.
- **SIEM** tools provide: Real-time visibility across an organization's information security systems. Event log management that consolidates data from numerous sources.

32. Which of the following is not a part of SIEM tools?

a) Sensor

b) Collector

c) Agent

d) Log

33. Which one is not the part of SIEM application?

a) Risk assessment

b) Vulnerability Scanning

c) Real time monitoring

d) Normalization

34. How does a SIEM tool handle the issue of Completeness of log?

a) Encryption

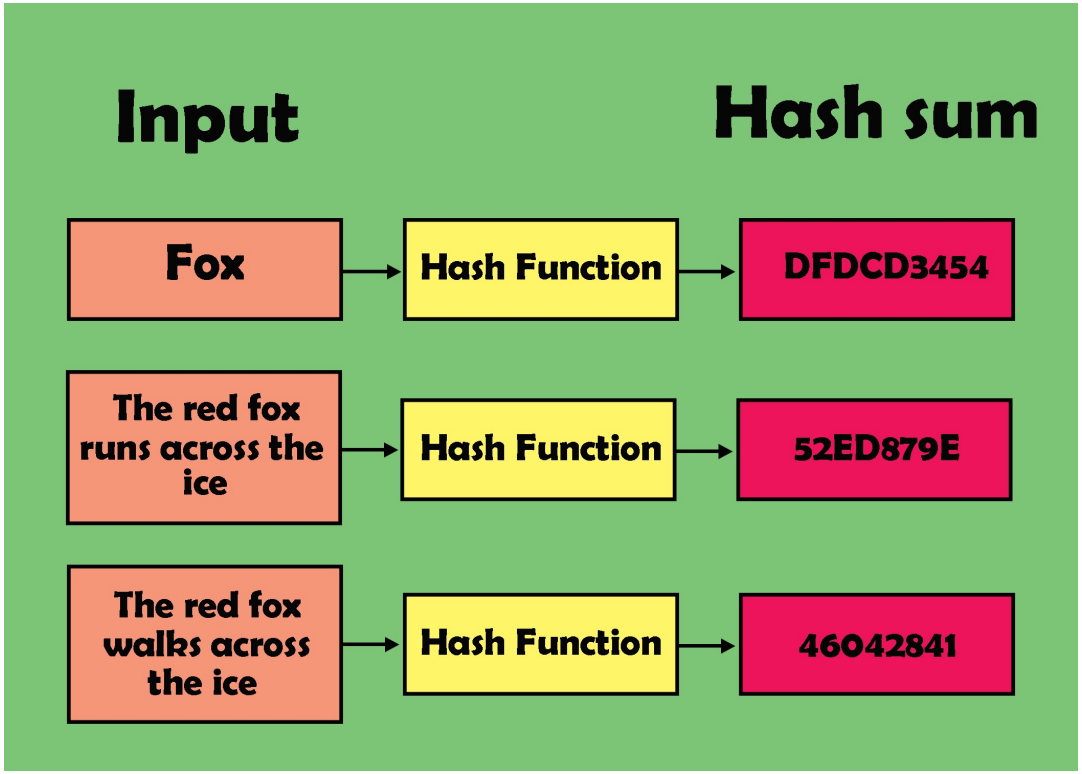
b) Hashing

c) Digital Signing

d) Time stamping

Security Incident and Event Management (SIEM) identifies, monitors, records, and analyzes security events within a real-time IT environment. It provides a centralized and comprehensive view of the security of your IT infrastructure. **SIEM utilizes the core technology of a Security Operations Center (SOC)**. This is a dedicated team of security experts who use advanced tools to thoroughly monitor your IT network infrastructure for threats, including those from malicious insiders.

- **Hashing** is the process of converting a given key into another value. A hash function is used to generate the new value according to a mathematical algorithm.
- The result of a hash function is known as a hash value or simply, a hash.



35. The computer security incident response team (CSIRT) of an organization publishes detailed descriptions of recent threats. An IS auditor's GREATEST concern should be that the users may:

a) Use this information to launch attacks

b) Forward the security alert

c) Implement individual solutions

d) Fail to understand the threat

36. The main goal of Security Operation Centre (SOC) is

a) Detect, analyse and report

b) Detect, analyse and respond

c) Collect, analyse and report

d) Collect, analyse and respond

The SOC team's goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes. Security operations centres are typically staffed with security analysts and engineers as well as managers who oversee security operations.


Log Collection
Reporting
Aggregation/
Correlation
SIEM
SOC
Research
& Development
01
0110
0001
01101
Ticketing
Threat Intelligence
Knowledge Base

37. What is the primary purpose of an incident management program?

a) Identify and assess incidents

b) Conduct lessons learned sessions

c) Alert key individuals

d) Assign responsibility

38. SOC shall be ineffective without the support of:

a) Risk

b) Budget

c) Top management

d) Quality

Incident Management Program

Prepare to handle incidents by having an incident management policy in place and establish a team to handle the incidents. A typical incident management program requires such steps:

- **Identify and report InfoSec incidents.** This step can be performed by an employee, vendor, customer, partner, device, SIEM system or even a sensor. The problem should be reported to Incident Response Team or Security Operations Centers (SOC)
- **Evaluate, analyse and assess incidents** including the criticality of the event in order to address them. Bear in mind that lots of issues might be false positives so evaluation plays a big role here
- **Respond** to incidents by either fixing the problem as quick as possible or collecting forensic evidences, even if it delays regular business operations. You definitely need a checklist or reference in case of handling an InfoSec incident.
- **Investigate (follow-up)** the problem in-depth after resolving and then document security weaknesses, report to senior management, and learn the lessons in order to change and improve the processes. Sometimes the problem should be reported to authorities or media as well in accordance with regulatory compliance laws and regulations.

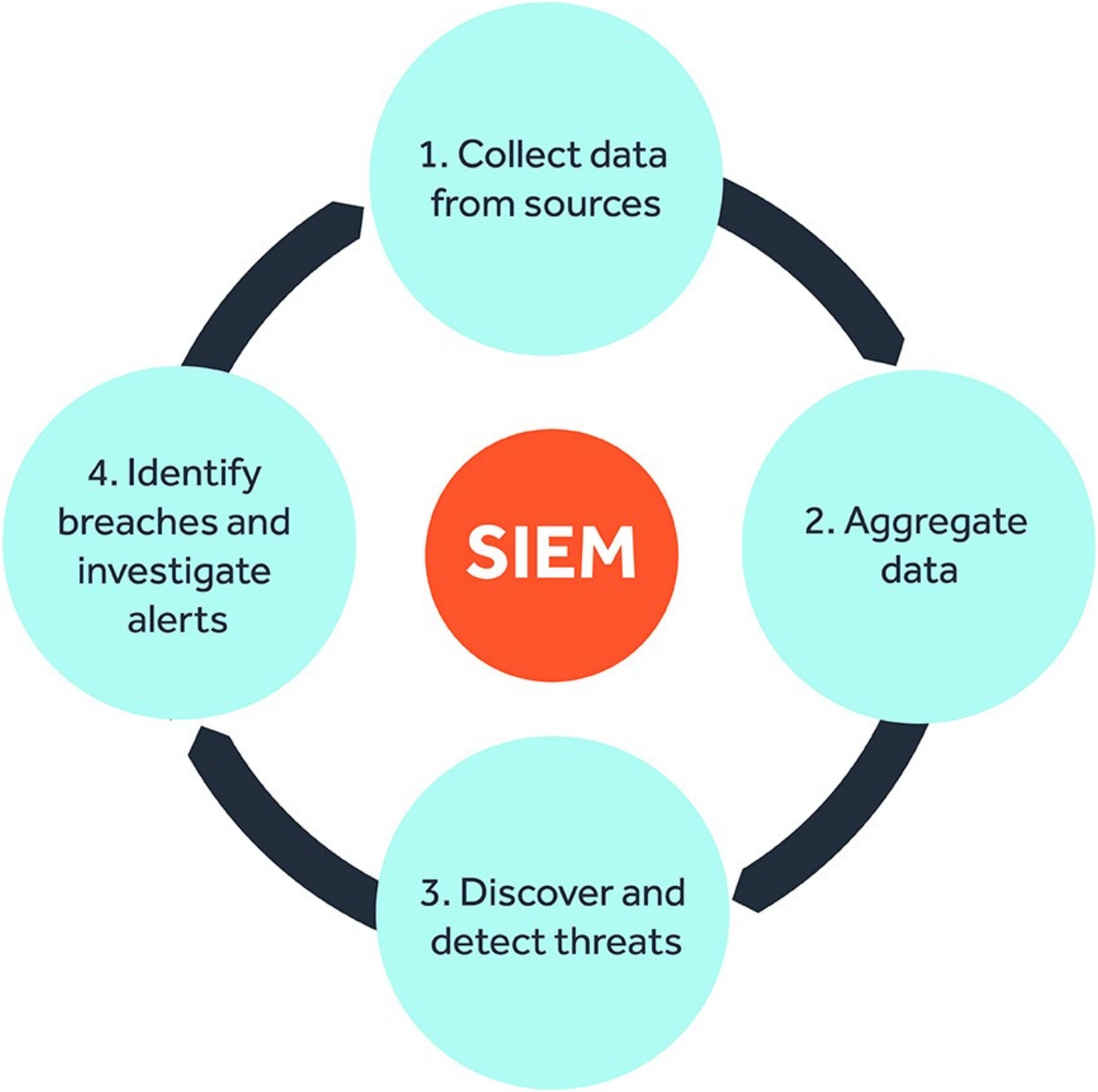
39. Phases of an incident management program

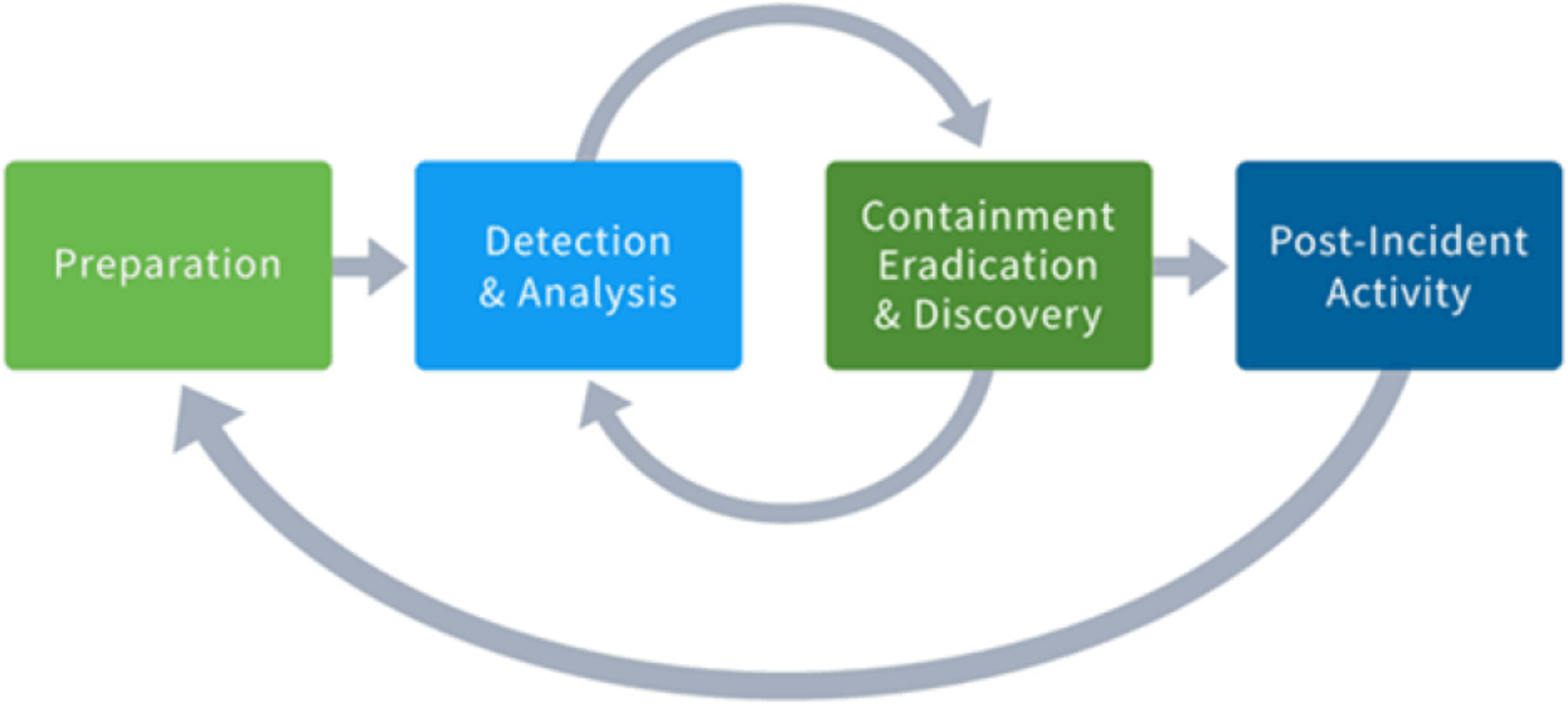
a) Prepare, Respond, and follow up

b) Plan, prepare, and respond

c) Plan, prepare and follow up

d) Prepare, plan and respond


1. Collect data from sources
2. Aggregate data
3. Discover and detect threats
4. Identify breaches and investigate alerts
SIEM


Preparation
Detection & Analysis
Containment Eradication & Discovery
Post-Incident Activity

40. Within an Incident Response Management program, the Containment phase aims to

a) Block the event

b) Reduce the impact

c) Remove the event

d) Rise the event

Containment : the action of keeping something harmful under control or within limits.

41. There are many frameworks that can be used to implement ISSM. One of them is ……., the present being ……

a) ITIL, Version 4

b) COBIT, Version 4

c) ITIL, Version 5

d) COBIT, Version 5

Page 3; Para 1.3

42. A ……. is a senior-level officer of the organization, responsible for Information and Cyber Security and data privacy of the organisation.

a) CTO

b) CIO

c) CFO

d) CISO

Page 7; Para 1.4

43. ..... is a measurable agreement between a service providing vendor and a service availing customer. There are various challenges that need to be looked into by both the parties such as clear scope of service, metrics measurement, responsibilities etc.

a) Service Level Agreement

b) Annual Maintenance Contract

c) Service Measurement Agreement

d) Preventive Maintenance Contract

Page 11; Para 1.9

44. IT Infrastructure includes the following; except

a) Electrical and network cabling

b) Local Area Network (LAN)

c) Wide Area Network (WAN)

d) HVAC

e) Data Backup

Page 18; Para 2.2 - ICT

45. Server operations management includes the following; except

a) Log management

b) User access management

c) Fire protection systems

d) Application management

e) Database management

Page 18; Para 2.2

46. Any change should be initiated through a …... . Such …… shall be done stepwise, with review and monitoring. Proper request with proper documentation with proper explanation related to what, why, how and by whom will have an effective Change Management Process.

a) CAB

b) Test Change

c) RFC

d) Change Schedule

Page 21; Para 2.4

47. A User profile is deleted by the IT department on the request sent by the .....

a) Finance Department

b) HR Department

c) User Department

d) Any of the above

Page 29; Para 2.8

48. ……. support is generally given by the device manufacturer or system developer. If an issue has come to this level, it may be required to be resolved by launching a new release or version of the device or product.

a) Level 1 Helpdesk

b) Level 2 Helpdesk

c) Level 3 Helpdesk

d) Level 4 Helpdesk

e) Level 5 Helpdesk

Page 29; Para 2.9

49. …… over a period of time is the metrics of IS system availability. It measures the system performance and serviceability to the users of an organisation.

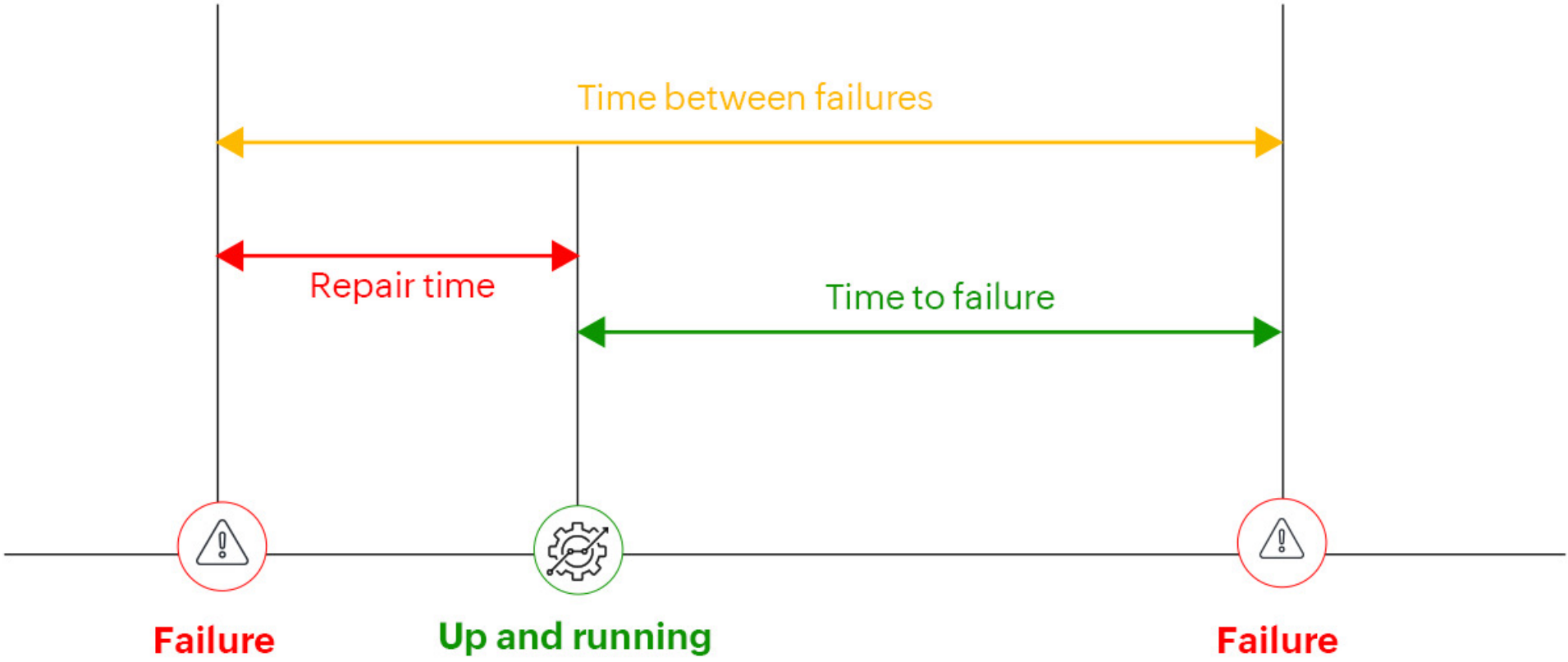
a) MTBF - Mean Time Between Failure

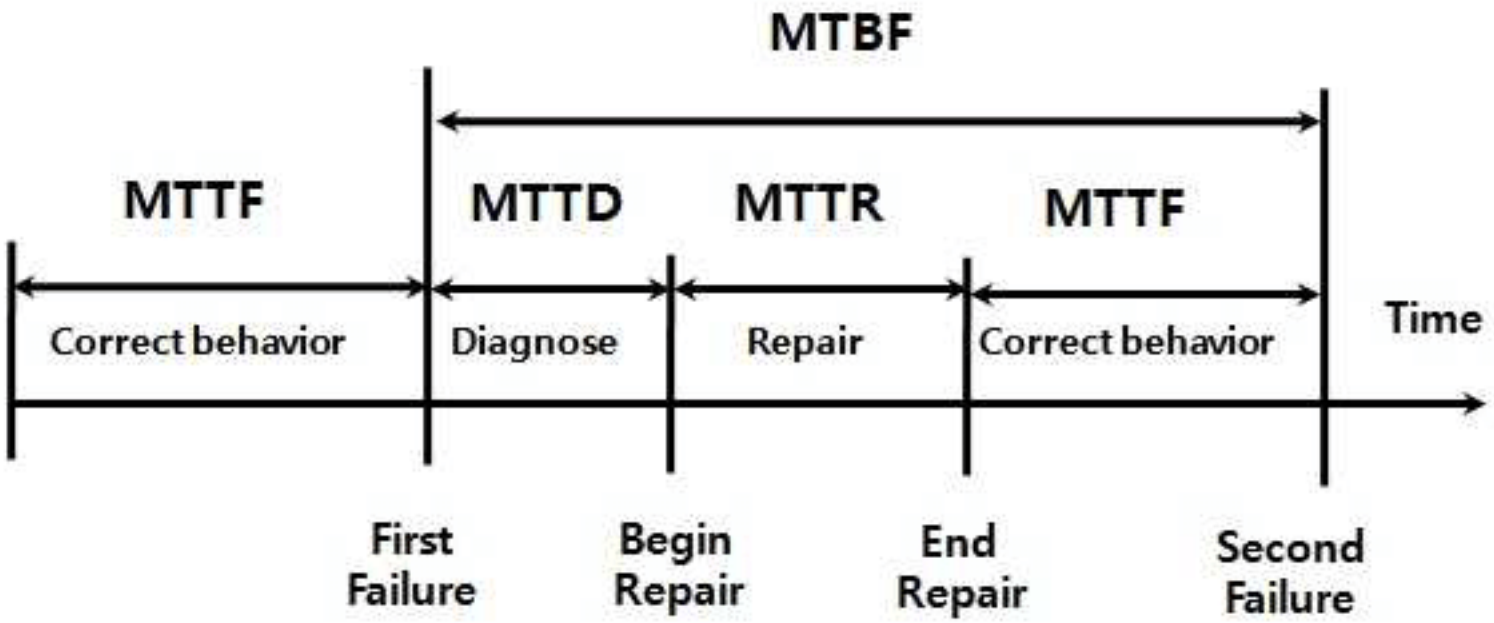
b) MTTR – Mean Time to Recover

c) VCS – Version Control System

d) CSA – Control Self-Assessment

Page 31; Para 2.10


Time between failures
Repair time
Time to failure
Failure
Up and running
Failure


MTBF
MTTF
MTTD
MTTR
MTTF
Correct behavior
Diagnose
Repair
Correct behavior
Time
First Failure
Begin Repair
End Repair
Second Failure

50. Audit evidence can take many forms. When determining the types required for an audit, the auditor must consider

a) CAATs, flowcharts, and narratives

b) Interviews, observations, and re-performance testing

c) The best evidence available that is consistent with the importance of the audit objectives

d) Inspection, confirmation, and substantive testing

51. The primary thing to consider when planning for the use of CAATs in an audit program is

A. Whether the sampling error will be at an unacceptable level

B. Whether you can trust the programmer who developed the tools of the CAATs

C. Whether the source and object codes of the programs of the CAATs match

D. The extent of the invasive access necessary to the production environment

52. The most important aspect of drawing conclusions in an audit report is to

A. Prove your initial assumptions were correct.

B. Identify control weakness based on test work performed.

C. Obtain the goals of the audit objectives and to form an opinion on the sufficiency of the control environment.

D. Determine why the client is at risk at the end of each step.

53. Things to consider (during audit) when determining what reportable findings should be are:

a) How many findings there are and how long the report would be if all findings were included?

b) Whether materiality of the findings is relevant to the audit objectives and management's tolerance for risk?

c) How the recommendations will affect the process and future audit work?

d) Whether the test samples were sufficient to support the conclusions?

54. The primary objective of performing a root cause analysis is to

a) Ask why three times.

b) Perform an analysis that justifies the recommendations.

c) Determine the costs and benefits of the proposed recommendations.

d) Ensure that you are not trying to address symptoms rather than the real problem that needs to be solved.

Above the surface you see the

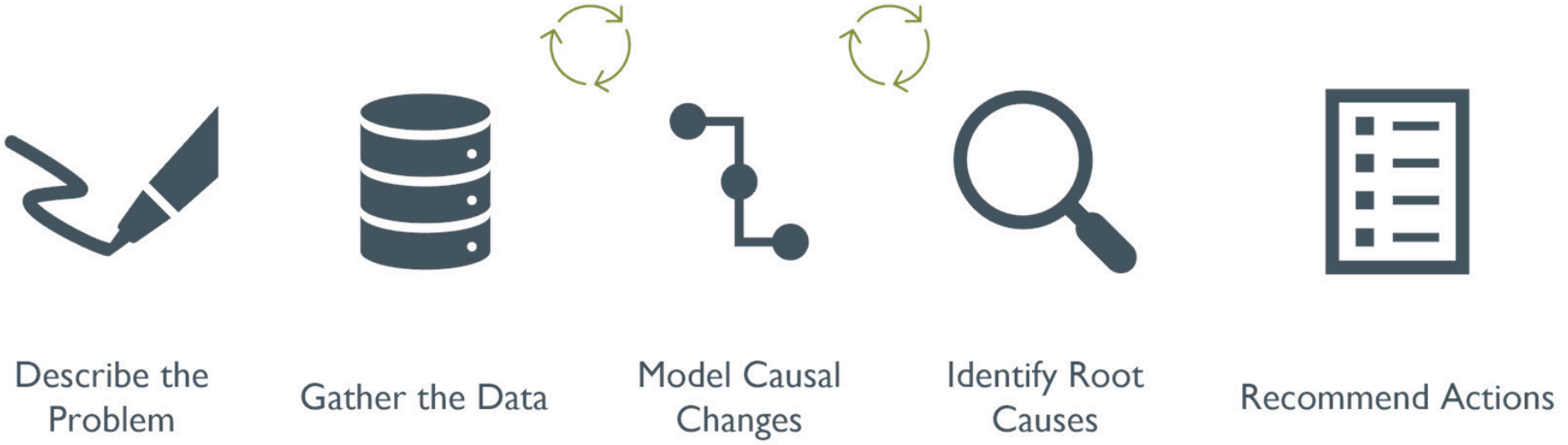
Symptoms

of the problem

Dig deeper to find the

Root Cause

of the problem


Describe the Problem
Gather the Data
Model Causal Changes
Identify Root Causes
Recommend Actions

55. The primary reason for reviewing audit work is to

a) Ensure that the conclusions, testing, and results were performed with due professional care

b) Ensure that the findings are sufficient to warrant the final reporting

c) Ensure that all of the work is completed and checked by a supervisor

d) Ensure that all of the audits are consistent in style and technique

56. Which criteria would an IS auditor consider to be the most important aspect of an organization's IS strategy?

a) It includes a mission statement

b) It identifies a mechanism for charging for its services.

c) It includes a Web-based e-commerce strategy.

d) It supports the business objectives.

57. The development of an IS security policy is ultimately the responsibility of the:

A. IS department

B. Security committee

C. Security administrator

D. Board of directors

58. Involvement of senior management is MOST important in the development of:

a) Strategic plans

b) IS policies

c) IS procedures

d) Standards and guidelines

59. The output of the risk management process is an input for making:

a) Business plans

b) Audit charters

c) Security policy decisions

d) Software design decisions

Output of Risk Management Process

- The risk management process is about making specific security related decisions, such as the **level of acceptable risk**.

60. The risks associated with electronic evidence gathering would MOST likely be reduced by an e-mail:

a) Destruction policy

b) Security policy

c) Archive policy

d) Audit policy

Archive Policy

- Retention policies control how long your messages will be saved.
- Archive policies control how long messages are left in an email folder before they're moved to an archive.
- You might be able to add or remove optional retention policies and archive policies that were set up by the person who manages your mailbox.

Retention & Destruction Policy

- A document retention and destruction policy identifies the record retention responsibilities of staff, volunteers, board members, and outsiders for maintaining and documenting the storage and destruction of the organization's documents and records.

Now lets check your answers...

1	c	11	d	21	c	31	d	41	a	51	d
2	c	12	d	22	a	32	c	42	d	52	c
3	a	13	a	23	d	33	d	43	a	53	b
4	b	14	c	24	a	34	b	44	e	54	d
5	d	15	d	25	a	35	a	45	c	55	a
6	a	16	c	26	d	36	b	46	c	56	d
7	b	17	b	27	a	37	a	47	b	57	d
8	c	18	b	28	c	38	c	48	d	58	a
9	a	19	b	29	d	39	a	49	a	59	c
10	d	20	b	30	b	40	b	50	c	60	c

Case Study

Healthcare System Implementation

- Star Hospital located in Kolkata, is one of the largest hospitals and has seven Clinics with Out Patient Department and Pathological facilities. The Hospital has invested to upgrade the facilities and has been recently rated as one of the best Super Specialty Hospitals in the country. The Hospital has seen steady growth over the past 3 years. The existing IT infrastructure including application software was inadequate to support such volume and the management recently implemented a client-server based Healthcare Information System (HIS) called Superb-10000. Superb-10000 is an enterprise resource planning software developed on tier-2 technology. HIS is package software and has been implemented by ABC Consultants in all 7 Clinics of the Hospital as well.
- Each clinic has a high-end PC serving as server, which synchronizes data with the main server located in the Hospital. Synchronization is scheduled twice a day, once at 12 am and again at 12 pm.

Case Study
Healthcare System Implementation

- Post implementation, users observed that the functionalities related to Pathology are not working as per their requirements and the users started using old standalone Pathology system. As a result consolidated MIS report could not be generated. Senior management of the Hospital was facing problem with consolidation of reports in time.
- ABC Consultant confirmed that the problems would be addressed in their next version, which would be ready for release only next year as they are migrating to 3-tier technology. ABC consultants also informed that company would not provide further support for the current 2-tier technology. However, they agreed to develop an Interface for the Pathology system for free.

Case Study
Healthcare System Implementation

The Interface will work as under:

- HIS will automatically generate text file with necessary data as required by the users at each clinic in a designated folder in the local server twice a day.
- Data once generated in Clinics will not be selected again by the Interface program.
- Identified Users having access to the folder will upload the text file through FTP to a designated folder in the Central server of the Hospital.
- No users would have access to this folder in the Hospital, HIS will run a schedule process every 12 hours to upload the data to central HIS.
- Text file once uploaded in the central HIS will be automatically deleted from the folder and will be saved in a backup folder.

Case Study
Healthcare System Implementation

Alternately they suggest that:

- The users in the hospital will generate reports from various standalone applications and this spread sheet will be imported into the interface application located centrally to generate the consolidated MIS and CXO Reports. The HIS will generate reports at each satellite HIS system in a marked folder and users will email this to its central facility of the Hospital for consolidation of these various reports using outlook mail. The system is scheduled to generate the excel sheet automatically at midnight at each of these satellite location in a separate folder for the entire day's transactions similar to a batch processing i.e. one file per day.
- A transaction once posted in the spread sheet will not be considered again by the system since it will be marked as posted flag yes in the database to avoid duplicate postings.

61. Which of the following may be greatest concern for an IS auditor, while reviewing the proposed new interface for the Pathology system?

a) System generated text files are uploaded in the Central server by users.

b) HIS is a de-centralized system resulting in various interface problems.

c) The system is based on an outdated client-server technology.

d) Users do not have access to the folder from which data is uploaded in the central server.

62. Which of the following could have identified problems with Pathology system before implementation?

a) Documentation of Users' Requirements

b) Detail SLA should have been signed with the ABC Consultants, so that support is provided.

c) Quality Assurance (QA) of the software should have been done before implementation.

d) User Acceptance Testing should have been conducted detail testing.

ISA AT Exam Focus areas - अंतिम मिनट की तैयारी

a) CERT – 76

b) IB-CART – 78

c) RFID – CISA Manual

d) Combination of Authorities – Challenge

e) ACID – Atomicity / Consistency / Isolation / Durability – OLTPS

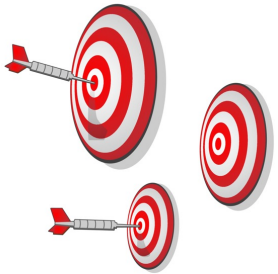
f) Referential Integrity

g) Normalisation

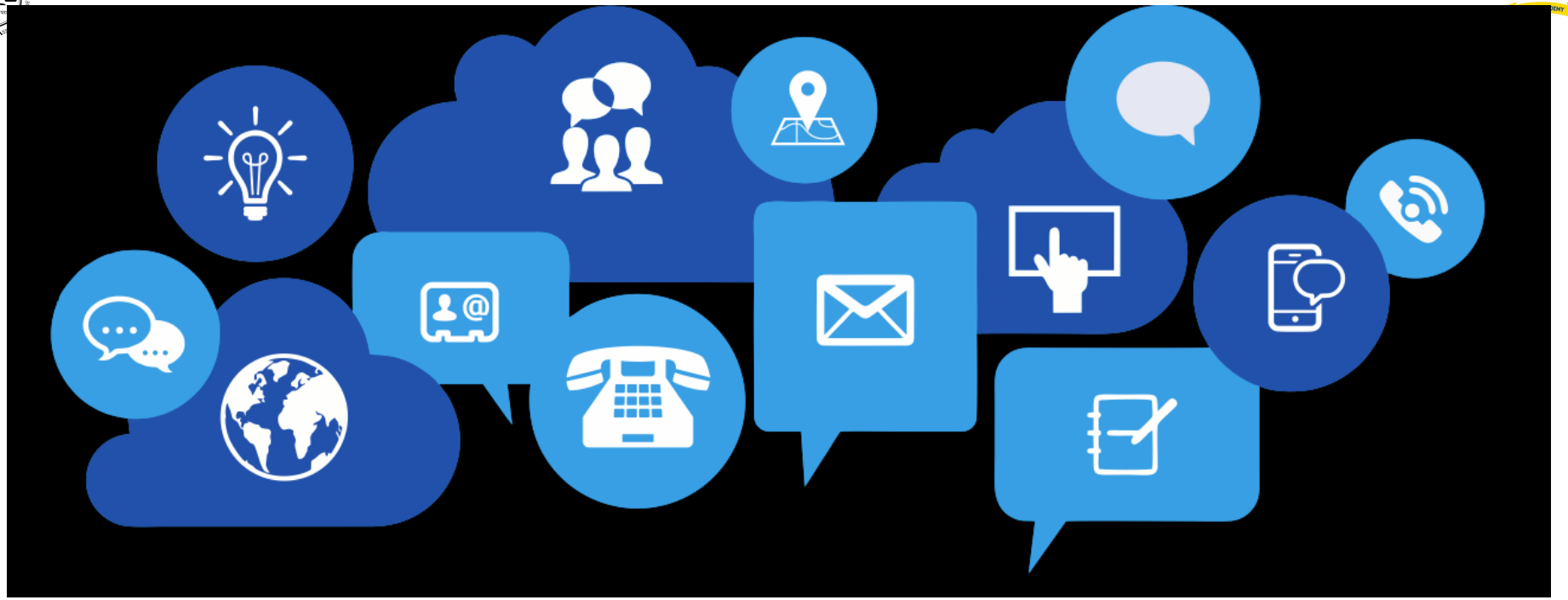
h) SIEM = SEM + SIM ; Page 79

i) SOC ; Page 72

j) National Cyber Security Policy 2013; Page 69



gkr@icai.org | www.3spro.blogspot.com



CA Dr GOPAL KRISHNA RAJU

Chartered Accountant, Insolvency Professional & Registered Valuer

Partner : K GOPAL RAO & CO | Chartered Accountants | Mumbai, Chennai, Bengaluru, Hyderabad, Trichy, Madurai & Tiruvallur

Email: gkr@icai.org Blog: www.3spro.blogspot.com

Mobile: 98400 63269 | 98401 63269