ISA Pinnacle

VISA *for* DISA

Day 1

ICAI Information Systems Audit 3.0 Course

For JAN 2025 AT

Batch XXVI

6 Hours Exam Practice session for
ISA AT Exam to be held on 25th Jan 2025

ISA AT PINNACLE

Exam-Oriented Webinar with 200 Model Questions

Monday ◊ 20th JAN 2025 ◊ 07:00 PM to 09:00 PM ◊ www.3spro.blogspot.com

CA Dr GOPAL KRISHNA RAJU

Chartered Accountant, Insolvency Professional, Registered Valuer & Arbitrator

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 document is based on the ICAI ISA Background Material – Download link given below

https://www.icai.org/post/isa-background-material

Exam Pointers

- There is no negative marking in the ISA-AT exam.
- Answer all questions.
- The ISA-AT exam is an OMR-based exam with multiple choice questions.
- Each correct answer = one mark.
- There is no penalty for incorrect answers.

Module Snapshot – Weightage & Questions

Module	Contents	Pages	Weight (%)	Questions
1	Information Systems Audit Process	185	**18**	36
2	GRC & BCM	149	**16**	32
3	SDLC	133	**18**	36
4	IS Operations & Management	97	**18**	36
5	Protection of Information Assets	125	**22**	44
6	Emerging Technologies	77	**8**	16
Total		**766**	**100**	**200**

1. Senior management look for assurance from IS Auditors on the …… …… ……. of IT controls as implemented and also seek advice on best deployment of IT for achieving business objectives.

a) Confidentiality, Integrity and Availability

b) Reliability, Availability and Effectiveness

c) Fiduciary, Quality and Security

d) Availability, Adequacy and Appropriateness

1/1 - Page 1; para 1.2

2. ..... can be visualized with a flowchart as a sequence of activities, decision points or with a Process Matrix showing interrelated activities based on data flow in the process.

a) Information system

b) Business Process

c) Secure system

d) Internal control

1/1 - Page 3; para 1.3

3. IS Audit could also be carried out as a part of internal audit or as a specialized audit of IT environment such as …….; except

a) penetration testing

b) audit of data centre

c) regression testing

d) audit of Business Continuity Plan

e) review of IT strategy

1/1 - Page 3; para 1.4

4. An IS Audit means .....

a) Audit of automated information processing system only

b) Audit of non-automated processes only

c) Audit of non-automated processes and their Interfaces to the Automated processes.

d) Audit of Automated information processing systems and Audit of non-automated processes and their Interfaces to the automated processes.

1/1 - Page 5; para 1.5.2

5. The / An ……..

1. considers the overall business objectives, business processes and their dependencies throughout the enterprise.
2. considers the full value chain of the enterprise
3. considers a full life-cycle of IT related business activities, including transformation programs, investments, projects and operations.
4. includes a logical and workable segmentation of the overall risk environment.
5. needs to be reviewed and updated on a regular basis due to the constantly changing internal and external requirements.

a) Risk Universe

b) Risk Management

c) IT Risk

d) Risk Based Audit

1/1 - Page 6; para 1.6.1

6. An organization can choose to reject risk by ignoring it, which can be dangerous and should be ……..

a) Qualified in IS Audit report

b) Mitigated by implementing controls

c) Within the risk appetite

d) Considered a red flag by the IS Auditor

1/1 - Page 7; para 1.6.2

7. SA 330 requires IS Auditors to review whether management has designed and implemented appropriate risk remediation measures. Usually the IS Auditor ……. ……..

a) Would provide recommendations for risk remediation as part of the Audit Report.

b) Should not provide recommendations for risk remediation as part of the Audit Report.

c) Provide recommendations on the residual risks that have been identified as critical and are not appropriately mitigated.

d) Do not provide recommendations on the residual risks that have been identified as critical and are not appropriately mitigated.

1/1 - Page 8; para 1.7

8. The ……. includes projects and initiatives related to the organisation's strategic plan, and it may be organised by business units, product or service lines, processes, programs, systems or controls or by risk category/ prioritisation.

a) Risk Universe

b) Audit Universe

c) Meta verse

d) Gen verse

1/1 - Page 8; para 1.8

9. Audit risk can be high, moderate or low depending on the ……..

a) sample size selected by the auditor

b) overall risk of management which is on account of entity's business operations as a whole.

c) appropriate assessment of the control environment.

d) materiality

1/1 - Page 10; para 1.9.1

10. Internal Controls is said to be a mechanism that is established by organizations which is a sum of ……..

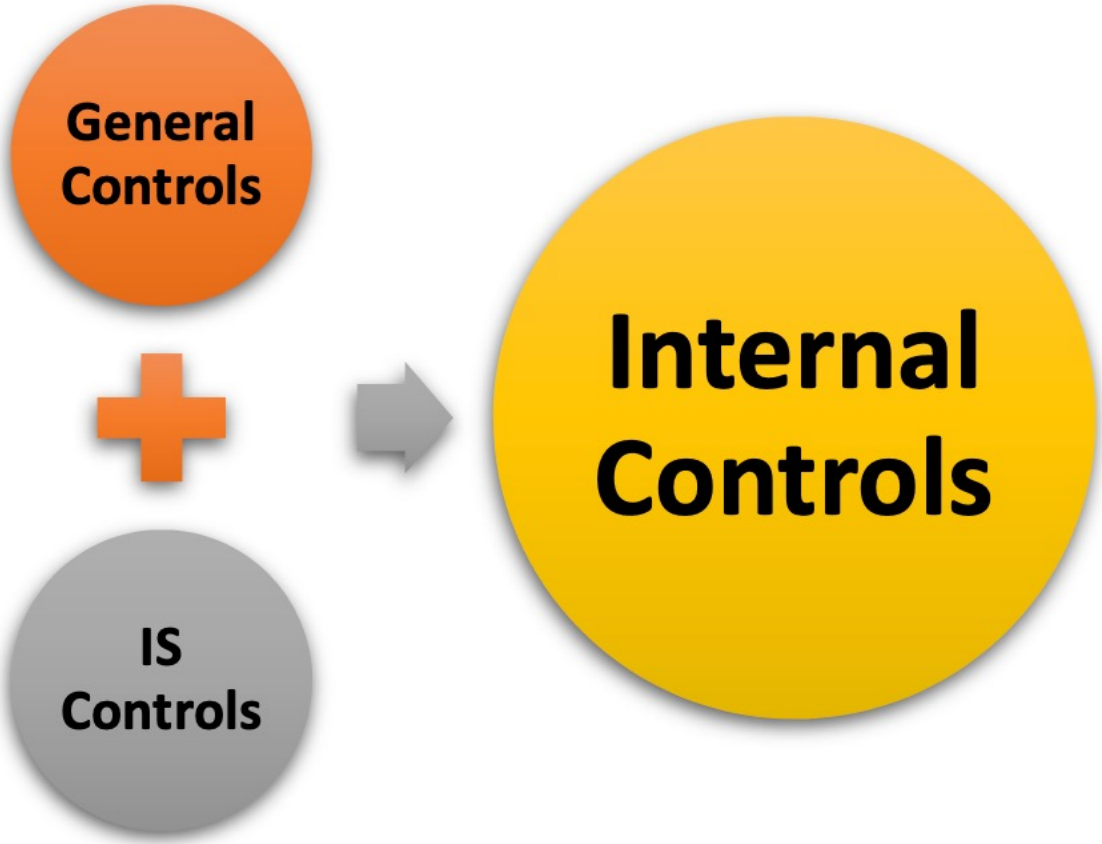
a) Application Controls + IT General Controls

b) General controls + Application controls

c) General controls + IS controls

d) IS Controls + IT General Controls

1/1 - Page 13; para 1.10.1


General Controls
IS Controls
Internal Controls

11. The composition and constitution of the IS audit function should ideally be decided by the …….. ……. which should be the prime reporting authority for the IS Audit function.

a) Board of Directors (BOD)

b) Audit Committee (AC)

c) Nomination and Remuneration Committee (NRC)

d) Chief Operating Decision Maker (CODM)

1/1 - Page 14; para 1.11

12. ……. is to express an opinion on whether the internal control system set up and operated by the organisation for the purpose of managing risks to the achievement of the objectives was suitably designed and operated effectively in the period.

a) Audit objective

b) Control objective

c) IS Audit objective

d) Application control objective

1/2 - Page 24; para 2.3.1

13. The engagement letter should clearly address the ……; except

a) Responsibility

b) Authority

c) Accountability

d) Purpose

1/2 - Page 27; para 2.4.2

14. The scope of audit would be specifically determined by the ……., in case of internal audit and is set by ……., if it is as per regulatory requirement

a) Management; Statute

b) Regulator; Statute

c) Statute; Management

d) Management; Regulator

1/2 - Page 29; para 2.5

15. As per SA 300 on "Planning" issued by ICAI; the extent of planning will vary according to ……; except

a) the size of the entity

b) the complexity of the audit

c) the IS Auditor's experience with the entity

d) the IS Auditor's knowledge of Audit

1/2 - Page 30; para 2.6

16. Integrity of Information means it is accurate and reliable and has not been subtly changed or tampered with by an unauthorized party or program. Integrity includes; except

a) Authenticity

b) Reliability

c) Non-repudiation

d) Accountability

1/2 - Page 34; para 2.7.3

17. As per SA 315; The IS Auditor should obtain a …….. knowledge of the entity and of the nature of ownership, management, regulatory environment and operations of the entity.

a) Preliminary

b) Conceptual

c) Procedural

d) Posteriori

1/2 - Page 35; para 2.8.1

18. Section 43A of the (Indian) Information Technology Act, 2000, provides that a body corporate possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates and is negligent in implementing and maintaining reasonable security practices and procedures resulting in wrongful loss or wrongful gain to any person, then such body corporate may be held liable to pay damages by way of compensation to the person so affected. The upper limit specified for the compensation that can be claimed by the affected party in such circumstances are:

a) Rs 50 Lakhs

b) Rs 100 Lakhs

c) Rs 500 Lakhs

d) No Upper Limit Specified

1/2 - Page 37; para 2.8.4

19. ……. formally specifies an Information Security Management System (ISMS), a suite of activities concerning the management of information security risks.

a) ISO/IEC 27001: 2022

b) ISO/IEC 27002: 2022

c) ISO/IEC 27001: 2013

d) ISO/IEC 27002: 2013

1/2 - Page 38; para 2.8.4

20. During the exit interview the IS Auditor should do the following; except

a) Ensure that the facts represented in the report are correct

b) Ensure that the recommendations are realistic and cost effective, and if not, seek alternatives through negotiation with Auditee management

c) Recommend implementation dates for agreed on recommendations

d) Follow up is conducted to determine whether management has taken appropriate corrective actions.

1/2 - Page 81; para 2.22

21. Qualitative terms need to be used for risk ranking when ……..; except

a) When risks do not lend themselves to quantification

b) When credible data is not available

c) When obtaining and analysing data is not cost-effective

d) When it brings greater degree of precision and measurability to the risk assessment process

1/2 - Page 80; para 2.21

22. Which type of evidence is usually not conclusive because it is not from an independent source?

a) Analytical procedures

b) Inquiries of the Client

c) Recalculation

d) External confirmations

1/2 - Page 70; para 2.17.2

23. What is one of the responsibilities of the IS Auditor when utilizing external service providers according to ISACA standards?

a) Delegating all professional liability to the external provider

b) Communicating audit objectives, scope and methodology through a formal engagement letter

c) Relying solely on external service providers' reports without review

d) Avoiding the use of external experts altogether

1/2 - Page 78; para 2.19

24. What is the primary focus of an IS Auditor when reviewing an IS environment?

a) To review the financial statements of the organization

b) To ensure that the organization's IT infrastructure is up to date

c) To review the risk assessment, mitigation controls, and residual risk acceptance

d) To manage the organization's IT projects

1/1 - Page 7; para 1.6.2

25. Which of the following best describes 'control risk' in the context of an IS audit?

a) The likelihood that the IS auditor's procedures will not detect material errors.

b) The assessment of the likelihood that risk exceeds tolerable levels and is not prevented or detected by internal controls.

c) The absence of internal controls, leading to a high inherent risk.

d) The risk that fraud might be committed by collusion between employees, overriding existing controls.

1/1 - Page 10; para 1.9.1

26. What is the critical recommendation for maintaining user accountability in entity's Operating System and Operations Package?

a) Implementing a two-factor authentication system.

b) Documenting and having senior management authorize in writing the users.

c) Using biometric access control exclusively.

d) Outsourcing user management to an external provider.

1 - Page 157; Appendix 3

27. What is the primary purpose of substantive testing in an audit?

a) To verify the design of controls

b) To ensure compliance with regulations

c) To validate the amounts of financial transactions

d) To test the operational effectiveness of processes

gkr@kgrca.in | www.3spro.blogspot.com

28. Which of the following is an example of compliance testing in an audit where sampling could be considered?

a) Re-performance of a complex calculation on a sample of accounts

b) User access rights evaluation

c) Haphazard sampling procedure

d) Assessment of judgmental sampling techniques

1/2 - Page 66; 2.14

29. In the context of enterprise risk management, why is it recommended not to depict IT risk as having a hierarchical dependency on other risk categories?

a) Because IT risk is only a component of operational risk.

b) Because IT risk can influence multiple types of risk, including strategic and credit risk.

c) Because IT risk is irrelevant to strategic decision making.

d) Because IT risk is already covered under environmental risk.

gkr@kgrca.in | www.3spro.blogspot.com

30. What is included in the Final Report deliverable for the audit assignment?

a) Draft Report with findings and risk analysis

b) Checklist used for the audit

c) Executive summary with recommendations

d) Management Comments and agreed priority plan of action based on exposure analysis

Page 155; Appendix 2

31. Which of the following documents establishes standards for audit and assurance professionals in the field of information technology?

a) Cyber Security Guidelines and Framework

b) IT and Cyber Risk Management

c) Information Technology Assurance Framework (ITAF)

d) Report on working group of FinTech and Digital Banking

Page 39; Para 2.9.1

32. What is a significant risk associated with the presence of unnecessary files on a server?

a) Improved server performance

b) Enhanced data security

c) Non-compliance with security policies

d) Increased processing speed

Page 168; Para 7.3

33. Under which section of the Information Technology Act, 2000 is a body corporate held liable for negligence in maintaining security practices for sensitive personal data?

a) Section 7A

b) Section 43A

c) Section 17C

d) Section 66F

Page 37; Para 2.8.4

34. What is the primary purpose of risk assessment procedures in IS Audit according to SA 315?

a) To directly provide sufficient audit evidence for audit opinion.

b) To assist in identifying and assessing risks and assertion levels.

c) To independently verify the accuracy of financial statements.

d) To ensure IT systems are free from errors.

Page 8; Para 1.7

35. Why is it necessary to perform an application control review for specialized systems?

a) To ensure compliance with international standards

b) To enhance the functional capabilities of the system

c) To identify and mitigate potential risks specific to the system

d) To improve user interface and user experience

Page 120; Para 5.2

36. What is a critical requirement for digital evidence to be admissible in court proceedings?

a) The evidence must be collected by a recognized law enforcement agency.

b) The evidence should be preserved and documented with a chain of custody.

c) The evidence must be stored in a secure, encrypted format.

d) The evidence should be analyzed using state-of-the-art forensic software.

Page 71; Para 2.17.3

37. What is the primary objective of Business Continuity Management (BCM)?

a) To eliminate all risks for the organization

b) To ensure zero downtime during a crisis

c) To recover from a crisis as fast as possible and at the lowest cost

d) To anticipate every possible crisis scenario

#2 - Page 92; Para 5.4.2

38. What is the primary difference between a 'mirror site/active recovery site' and a 'hot site' in terms of disaster recovery for information systems?

a) A mirror site requires full redundancy while a hot site is a shared facility.

b) A mirror site is a temporary fix while a hot site is permanent.

c) A mirror site is cheaper than a hot site.

d) A hot site offers better uptime guarantees than a mirror site.

#2 - Page 116; Para 5.15.1

39. Which of the following best describes Operational Risks?

a) Risks associated with the nature of business.

b) Risks associated with fluctuations in the market affecting the customer base.

c) Risks associated with failure of operations within the organization.

d) Risks associated with financial decisions and the environment.

#2 - Page 26; Para 2.3.1

40. Which step in the risk management process involves assessing the probability and frequency of risk occurrences?

a) Risk Identification

b) Risk Evaluation

c) Determine Likelihood of Risk

d) Risk Monitoring

#2 - Page 32/35; Para 2.4.1.1 / 2.4.3

41. What is a key characteristic of a disaster recovery plan (DRP) that aims to make it effective in various disaster scenarios?

a) It is threat-independent, meaning it functions regardless of the type of disaster.

b) It is specifically tailored to a single type of disaster like fires or floods.

c) It requires static processes that do not change over time.

d) It focuses on hardware recovery only.

#2 - Page 98; Para 5.10

42. What is a key consideration when managing risks associated with changes in infrastructure and IT processes?

a) Implementing new software without evaluation.

b) Ignoring incident response outcomes.

c) Reviewing the capacity of existing systems like uninterruptible power supplies.

d) Relying solely on regulatory compliance.

#2 - Page 38; Para 2.4.6

43. What is the primary responsibility of the personnel or human resource function in managing a business continuity plan?

a) Ensuring employee satisfaction and engagement

b) Notifying plan administrators of all personnel changes

c) Maintaining the company's financial health

d) Developing new marketing strategies

#2 - Page 110; Para 5.13.2.1

44. What is the main purpose of ISO/IEC 27031:2011?

a) To describe the general principles of business continuity planning.

b) To provide a framework for ICT readiness for business continuity.

c) To establish organizational rules for preventing disruptive incidents.

d) To specify performance criteria for hardware and software procurement.

#2 - Page 110; Para 5.13.2.1

45. Which of the following best describes a 'vulnerability' in the context of risk management?

a) A strategy to minimize the impact of a risk.

b) The likelihood of a threat exploiting a weakness.

c) A weakness that gets exploited due to a threat.

d) The impact of a threat on normal functioning.

#2 - Page 110; Para 5.13.2.1

46. What is the core focus of the 'Culture, Ethics and Behavior' component in COBIT 2019?

a) The integration of advanced technology.

b) The adherence to organizational and individual values.

c) The management of financial resources.

d) The establishment of a centralized IT department.

#2 - Page 74; Para 4.4.1

47. Which of the following best describes the approach recommended by ISO 27001:2005 for implementing controls in an organization?

a) Implement controls for all assets equally without prioritization.

b) Prioritize controls based on risk evaluation results and apply them to critical assets.

c) Focus only on network security regardless of asset importance.

d) Use a fixed list of controls irrespective of organizational changes.

#2 - Page 34; Para 2.4.1.4

48. What are some of the responsibilities corporates have under the Information Technology Act 2000, amended in 2008, regarding the collection of personally identifiable information (PII)?

a) Ensure the security of PII to prevent identity theft.

b) Regularly update and review their data security policies.

c) Impose penalties for non-compliance on individual employees.

d) Maintain privacy of information with prescribed compliance standards.

#2 - Page 40; Para 2.7

49. The level to which an enterprise can accept financial loss from a new initiative is:

a) Risk tolerance

b) Risk management

c) Risk appetite

d) Risk acceptance

#2 - Page 31; Para 2.4

50. What is the key difference between a hot site and a cold site in terms of backup and recovery processes?

a) A hot site has minimal startup costs, while a cold site includes real-time process capabilities.

b) A hot site includes backed-up data and hardware, whereas a cold site does not include backed-up data or pre-installed hardware.

c) A cold site functions in real time like a financial institution's hot site.

d) Both sites require the same recovery time after a disaster.

#2 - Page 116; Para 5.15.1

51. Which international standard specifically provides guidelines for governance of IT and organizational risk management, and is noted for its utility in compliance and risk assessment?

a) COBIT 2019

b) ISO 27001

c) ISO 31000

d) ISO 38500: 2015

#2 - Page 23; Para 2.2.2

51. Which international standard specifically provides guidelines for governance of IT and organizational risk management, and is noted for its utility in compliance and risk assessment?

a) COBIT 2019

b) ISO 27001

c) ISO 31000

d) ISO 38500: 2015

#2 - Page 23; Para 2.2.2

51. Which international standard specifically provides guidelines for governance of IT and organizational risk management, and is noted for its utility in compliance and risk assessment?

a) COBIT 2019

b) ISO 27001

c) ISO 31000

d) ISO 38500: 2015

#2 - Page 23; Para 2.2.2

52. Key business requirements for information also called as information criteria need to be present in information generated. These are; except

a) Reliability

b) Availability

c) Validity

d) Confidentiality

1/109;

53. Applications of Artificial Intelligence in the cognitive science area are; except

a) Expert Systems

b) Learning Systems

c) Neural Networks

d) Intelligent Agents

e) Natural Languages

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

54. IS auditors are expected to comply standards on Audit Performance by following ITAF 3rd Edition issued by …….

a) ISACA, Illinois

b) IEEE, New Jersey

c) AICPA, North Carolina

d) IIA, Florida

gkr@kgrca.in | www.3spro.blogspot.com

55. IS Controls can be classified into 3 broad categories; except

a) Fiduciary

b) Integrity

c) Quality

d) Security

gkr@kgrca.in | www.3spro.blogspot.com

56. A/An …… is a standard solicitation document used by various organisations to compete for contract opportunities.

a) Audit Charter

b) Audit Engagement Letter (EL)

c) Request for Proposal (RFP)

d) Scope of Work

1/25;

57. …….. is defined as "The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the organization's resources are used responsibly"

a) Corporate Governance

b) Enterprise Governance

c) Business Governance

d) Performance Governance

2/2;

58. …… is defined as the system by which a company or enterprise is directed and controlled to achieve the objective of increasing shareholder value by enhancing economic performance.

a) Corporate Governance

b) Enterprise Governance

c) Business Governance

d) Performance Governance

2/4;

59. Enterprise Governance of Information and Technology (EGIT) is a sub-set of ……. and facilitates implementation of a framework of IS controls within an enterprise as relevant and encompassing all key areas.

a) Corporate Governance

b) Enterprise Governance

c) Business Governance

d) Performance Governance

2/7;

60. Implementing EGIT from ..... perspective would require viewing the enterprise at macro level and consider not only the business but also the external linkages.

a) Conformance

b) Corporate

c) Performance

d) Business

2/8;

61. Implementing EGIT from …….. perspective the enterprise has to be viewed at internal level and the focus on the processes and activities within the enterprise.

a) Conformance

b) Corporate

c) Performance

d) Business

gkr@kgrca.in | www.3spro.blogspot.com

62. Achieving better governance starts with the business, and more specifically with understanding its strategy and goals. IT management should be involved early in the business strategy definition process, especially in those companies that are highly dependent on IT. The IT goals should …… to the business goals.

a) Be aligned

b) Not to aligned

c) Involved

d) Devolved

gkr@kgrca.in | www.3spro.blogspot.com

63. IT strategy committee has to operate at the ……. and the IT steering committee has to operate at ……. with each committee having specific responsibility, authority and membership.

a) Executive Level; Board Level

b) Board Level; Operational Level

c) Operational Level; Board Level

d) Board Level; Executive Level

gkr@kgrca.in | www.3spro.blogspot.com

64. Institute of Internal Auditors define …….. as a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

a) Corporate Governance

b) Enterprise Governance

c) Enterprise Risk Management (ERM)

d) Enterprise Governance of Information and Technology (EGIT)

2/12;

65. From a risk management point of view, the BEST approach when implementing a large and complex IT infrastructure is:

a) A big bang deployment after proof of concept

b) Prototyping and a one-phase deployment

c) A deployment plan based on sequenced phases

d) To simulate the new infrastructure before deployment

66. The GREATEST risk posed by an improperly implemented Intrusion Prevention System (IPS) is:

a) That there will be too many alerts for system administrators to verify

b) Decreased network performance due to IPS traffic

c) The blocking of critical systems or services due to false triggers

d) Reliance on specialized expertise within the IT organization

67. To determine if unauthorized changes have been made to production code the BEST audit procedure is to:

a) Examine the change control system records and trace them forward to object code files

b) Review access control permissions operating within the production program libraries

c) Examine object code to find instances of changes and trace them back to change control records.

d) Review change approved designations established within the change control system.

68. To address an organization disaster recovery requirements, backup intervals should not exceed ……..?

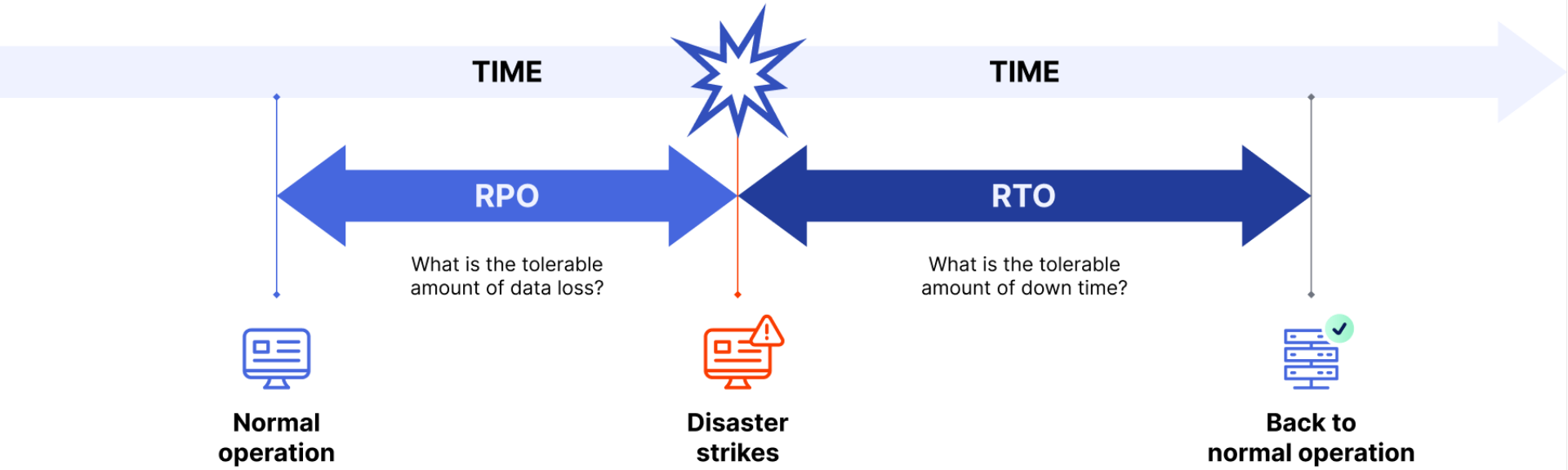
a) Service level objective (SLO)

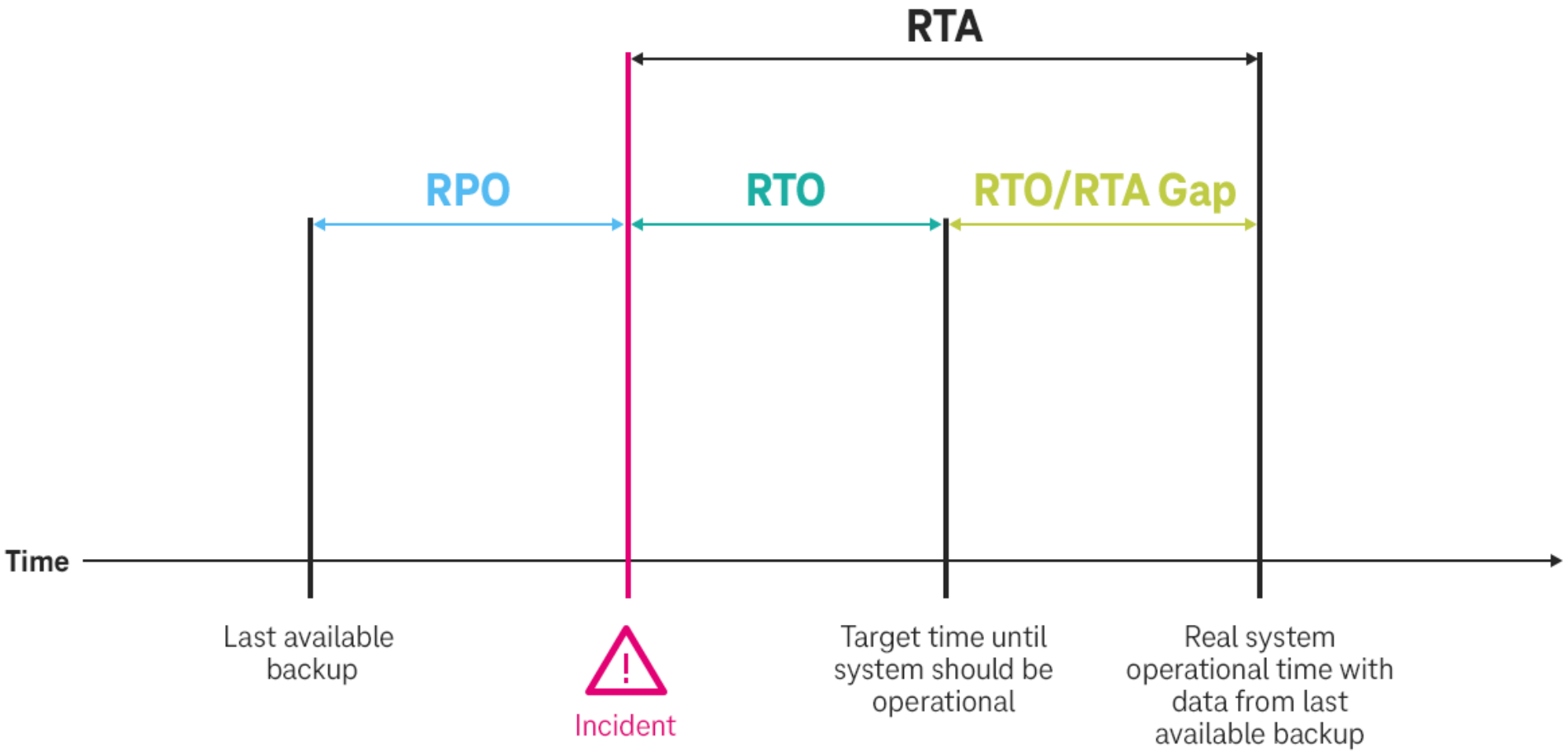
b) Recovery time objective (RTO)

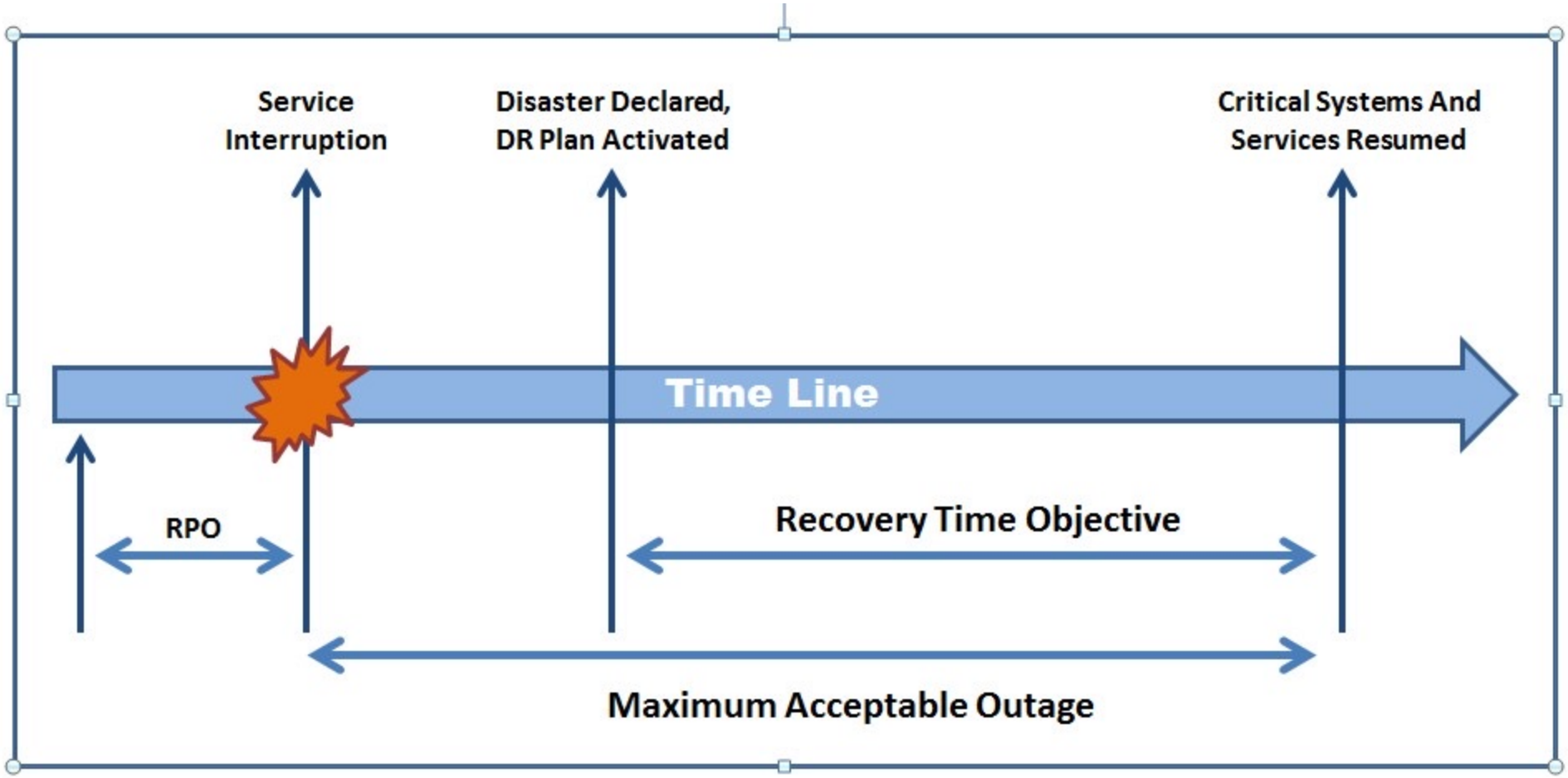
c) Recovery point objective (RPO)

d) Maximum acceptable outage (MAO)

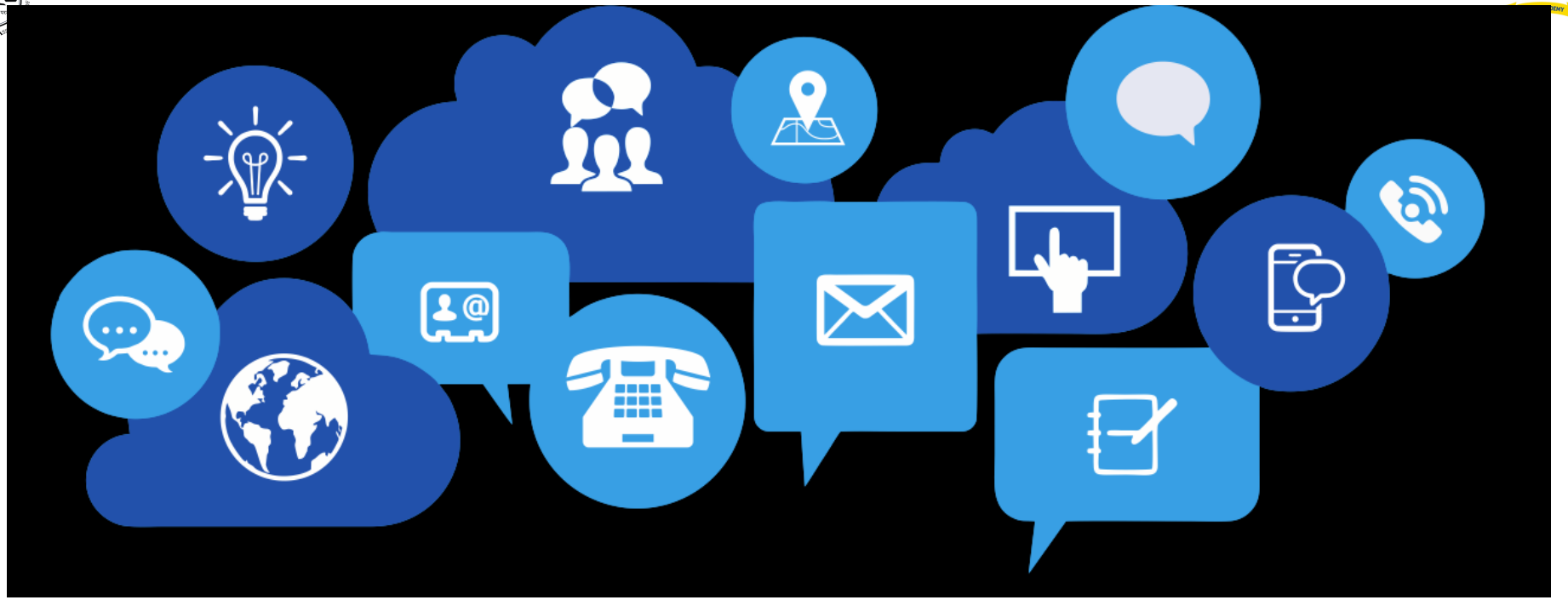
#2 - Page 23; Para 2.2.2


TIME
TIME
RPO
RTO
What is the tolerable amount of data loss?
What is the tolerable amount of down time?
Normal operation
Disaster strikes
Back to normal operation


RTA
RPO
RTO
RTO/RTA Gap
Time
Last available backup
Incident
Target time until system should be operational
Real system operational time with data from last available backup


Service Interruption
Disaster Declared, DR Plan Activated
Critical Systems And Services Resumed
Time Line
RPO
Recovery Time Objective
Maximum Acceptable Outage

1	d	11	b	21	d	31	c	41	a	51	b	61	c/d
2	b	12	a	22	b	32	c	42	c	52	c	62	a
3	c	13	d	23	b	33	b	43	b	53	e	63	d
4	d	14	a	24	c	34	b	44	b	54	a	64	c
5	a	15	d	25	b	35	c	45	c	55	b	65	c
6	d	16	b	26	b	36	b	46	b	56	c	66	c
7	a/c	17	a	27	c	37	c	47	b	57	b	67	c
8	b	18	d	28	b	38	a	48	a	58	a	68	c
9	a	19	a/c	29	b	39	c	49	c	59	a		
10	c	20	d	30	d	40	c	50	b	60	a/b		



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