Fast Track Webinar Series

VISA *for* DISA

Day 2

ICAI Information Systems Audit 3.0 Course

for JAN 2025 AT

INFORMATION SYSTEMS AUDIT 3.0 COURSE

Module - 2

Governance and Management of Enterprise Information Technology, Risk Management, Compliance & BCM Section

Wednesday ◊ 15th JAN 2025 ◊ 08:30 AM to 09:30 AM ◊ www.3spro.blogspot.com

CA Dr GOPAL KRISHNA RAJU

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 – AT by ET (Elimination Technique)
- All references made in this material is based on the BGM of ICAI – Module 2 – Link below

https://resource.cdn.icai.org/60972daab49637bgmisa-mod2.pdf

ISA Assessment Test (AT)

- After completing ISA ET with minimum marks, you have to register online for the ISA Assessment that is conducted by the Examination Department of the Institute. It is important to note that members have to fill the ISA AT Form issued/hosted on www.icai.org, by the Examination Department.
- Total Marks: 200, passing criteria is 60% marks flat.
- After passing the ISA AT, DISA Certificates are dispatched by the exam department. In Case of any difficulty, Additional Secretary (Exams.), ICAI - C-1, Sector-1, Noida should be contacted by e-mail at isa_examhelpline@icai.in Helpline Desk telephone Nos.0120- 3054851/52/53/54/35/36.
- Please do let us know if you require further assistance/ support/ clarifications by e-mail to isa@icai.in / isa2@icai.in

Snapshot

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

Module 2

Governance and Management of Enterprise Information Technology, Risk Management, Compliance and Business Continuity Management

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

Reference Material for ICAI ISA PQC

Basic

- ISA Background Material 3.0
- DISA AT Mock Test Papers

Additional

- COBIT 2019 Design Guide

  2019-Design-Guide.aspx

Chapter 1

Concepts of Governance and Management of Information Systems

1. Who is responsible for establishing right structure of decision-making accountabilities?

a) Senior management / BOD

b) Operational management

c) Chief information officer

d) IT steering committee

Page 1 ; Para 1.2

2. The MOST important benefit of implementing Governance of Enterprise IT (EGIT) is?

a) Monitor and measure enterprise performance

b) Provide guidance to IT to achieve business objectives

c) Run the companies to meet shareholders' interest

d) Ensure strategic alignment of IT with business

Page 63 ; Para 3.7.1

3. The primary / ultimate objective of Corporate Governance is: ?

a) Reduce IT cost in line with enterprise objectives and performance.

b) Optimise implementation of IT Controls in line with business needs

c) Implement security policies and procedures using best practices.

d) Increase shareholder value by enhancing economic performance.

Page 5 ; Para 1.2.6

4. The ultimate objective of Governance of Enterprise IT is to ensure that IT activities in an enterprise are directed and controlled to achieve business objectives for meeting the needs of:

a) **Shareholders**

b) **Stakeholders**

c) **Investors**

d) **Regulators**

Page 60 ; Para 3.5

5. Which of the following is a key component of Corporate Governance?

a) Employee rights

b) Security policy

c) Transparency

d) Risk assessment

Page 6 ; Para 1.3

6. Effective Governance of Enterprise IT requires processes to ensure that:

a) risk is maintained at a level acceptable for IT management

b) the business strategy is derived from an IT strategy

c) IT governance is separate and distinct from the overall governance

d) the IT strategy extends the organization's strategies and objectives.

Page 65 ; Para 3.7.2

Governance of Enterprise IT (GEIT) refers to ensuring and enabling information technology and related support and enabling enterprise strategy, as well as realization of enterprise objectives.

- GEIT also enables compliance with the enterprise's regulatory obligations. GEIT is an important part of a comprehensive enterprise governance program.
- Information technology (IT) governance is a subset discipline of corporate governance, focused on information technology (IT) and its performance and risk management.
- The interest in IT governance is due to the ongoing need within organizations to focus value creation efforts on an organization's strategic objectives and to better manage the performance of those responsible for creating this value in the best interest of all stakeholders.
- It has evolved from The Principles of Scientific Management, Total Quality Management and ISO 9001 Quality management system.

7. Business Governance helps the Board by enabling them to understand:

a) enterprise functions

b) risk assessment

c) key performance drivers

d) Key controls

Page 3 ; Para 1.2.3

Key performance drivers (KPDs) are the day-to-day activities that are required in order to produce the desired KPI results. If the KPDs are correctly identified, then, for the most part, positive results in KPDs should lead to positive KPIs.

8. The effectiveness of the IT governance structure and processes are directly dependent upon level of involvement of

a) Heads of Business units

b) Internal auditor department

c) Technology management

d) Board/senior management

Page 8 ; Para 1.4.1

9. Which of the following is one of the key benefits of EGIT?

a) Identification of relevant laws, regulations and policies requiring compliance.

b) Improved transparency and understanding of IT's contribution to business

c) Better utilization of human resources by using automation

d) Increased revenues and higher Return on investments.

Page 63 ; Para 3.7

Key Benefits of EGIT

- It ensures that IT-related decisions are made in line with enterprise objectives.
- It ensures that IT-related processes are overseen transparent and effectively.
- It confirms compliance with legal and regulatory requirements.
- It ensures that the governance requirement of the board is met.

10. Which of the following is the primary objective for implementing ERM?

a) Implement right level of controls.

b) Better availability of information.

c) Tighter security at lower cost.

d) Implement IT best practices.

Page 12 ; Para 1.5

ERM

- **Enterprise risk management** (**ERM**) in business includes the methods and processes used by organizations to **manage risks and seize opportunities** related to the achievement of their objectives.
- ERM provides a framework for risk management, which typically involves identifying particular events or circumstances relevant to the organization's objectives (threats and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring process.
- By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall.

Risk comes from not knowing what you're doing. Risk is just an expensive substitute for information.

Chapter 2

GRC Frameworks and Risk Management Practices

11. The most important requirement for IT governance function to be effective is:

a) Monitoring

b) Evaluation

c) Directing

d) Managing

Page 4 ; Para 1.2.5

IT governance ensures that IT decisions focus on: Evaluating and directing the use of IT to support the organization. Monitoring the use of IT to achieve plans. Using the IT strategy and policies to accomplish its purpose.

12. The MOST important **benefit of implementing IT risk management process is that it helps in:**

a) optimizing internal control framework.

b) ensuring residual risk is at acceptable level.

c) prioritizing business functions for audit planning.

d) complying with regulatory requirements.

Page 26 ; Para 2.3.1

Residual Risk

- The **residual risk** is the amount of risk or danger associated with an action or event remaining after natural or inherent risks have been reduced by risk controls. The general formula to calculate residual risk is
- **Residual Risk = Inherent Risk – Impact of Risk Controls**
- where the general concept of risk is (threats × vulnerability) or, alternatively, (severity × probability).
- An example of residual risk is given by the use of automotive seat-belts. Installation and use of seat-belts reduces the overall severity and probability of injury in an automotive accident; however, probability of injury remains when in use, *that is*, a remainder of residual risk.
- In the economic context, residual means “the quantity left over at the end of a process; a remainder”
- In the property rights model it is the shareholder that holds the residual risk and therefore the residual profit.

13. Which of the following is a major risk factor?

a) Existence of inflationary trends.

b) Vendor launches new software.

c) Board of directors elects new chairman.

d) Change in government post elections.

14. 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

Risk appetite is the level of risk that an organization is prepared to accept in pursuit of its objectives, before action is deemed necessary to reduce the risk. It represents a balance between the potential benefits of innovation and the threats, that change inevitably brings.

15. Designing and implementing a control to reduce the likelihood and/or impact of risk materializing is a:

a) Risk acceptance

b) Risk transfer

c) Risk treatment

d) Risk appetite

Risk tolerance is an investor's ability to psychologically endure the potential of losing money on an investment. A person's **risk tolerance** can change throughout his life and determines what type of investments he or she is likely to make.

16. Which of the following is a valid risk statement?

a) Network service provider is unable to meet bandwidth.

b) Hacker attempts to launch attack on web site.

c) Application server crash due to power failure.

d) Delay in servicing customers due to network congestion.

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

17. Which of the following is primary reason for periodic review of risk? The changes in:

a) risk factors

b) risk appetite

c) budget

d) risk strategy

Page 29; Para 2.3.3; Page 37

18. Which of the following is a strategic IT risk?

a) IS audit may not identify critical non-compliance.

b) Non-availability of networks impacting services to customers.

c) New application may not achieve expected benefits.

d) Defer replacement of obsolete hardware.

19. Which of the following is the most essential action after evaluation of inherent risks?

a) **Evaluate implemented controls.**

b) **Update risk register.**

c) **Prepare heat map.**

d) **Prioritized evaluated risk.**

Chapter 3

Key Components of A Governance System

20. Which of the following is most important resource of the organization?

a) Policies and procedures

b) IT infrastructure and applications

c) Information and data

d) Culture, ethics and behaviour

Page 57 ; Para 3.3.5

21. Which of the following is most important characteristic of policies?

a) Must be limited in number.

b) Requires framework to implement.

c) Reviewed periodically.

d) Non-intrusive and logical.

Page 51 ; Para 3.3.1

22. Primary function of a process is to:

a) Act on input and generate output.

b) Define activities to be performed.

c) Focus on achieving business goals.

d) Comply with adopted standards.

Page 52 ; Para 3.3.2

23. Effective organizational structure focuses on:

a) Defining designations.

b) Delegating responsibility.

c) Defining escalation path.

d) Deciding span of control.

Page 53 ; Para 3.3.3

24. Prioritization of IT initiatives within organization is primarily based on:

a) Results of risk assessments

b) Expected benefit realization

c) Recommendations of CIO

d) Rate of obsolescence of IT

25. Primary objective of IT steering committee is to:

a) Align IT initiatives with business

b) Approve and manage IT projects

c) Supervise IT and business operations

d) Decide IT strategy for organization

Page 55 ; Para 3.3.3.2

An **IT steering committee** is a **committee** of senior executives to direct, review, and approve IT strategic plans, oversee major initiatives, and allocate resources. It is not involved in day-to-day management of the IT organization. Rather, the **steering committee** establishes IT priorities for the business as a whole.

26. Which of the following is best control for building requisite skills and competencies within organization?

a) Hiring only highly qualified people

b) Outsourcing the critical operations

c) Conducting skill enhancement training

d) Defining skill requirements in job description

Chapter 4

Performance Management Systems

27. Which of the following is best approach for monitoring the performance of IT resources?

a) Compare lag indicators against expected thresholds

b) Monitor lead indicators with industry best practices

c) Define thresholds for lag indicators based on long term plan

d) Lead indicators have corresponding lag indicator.

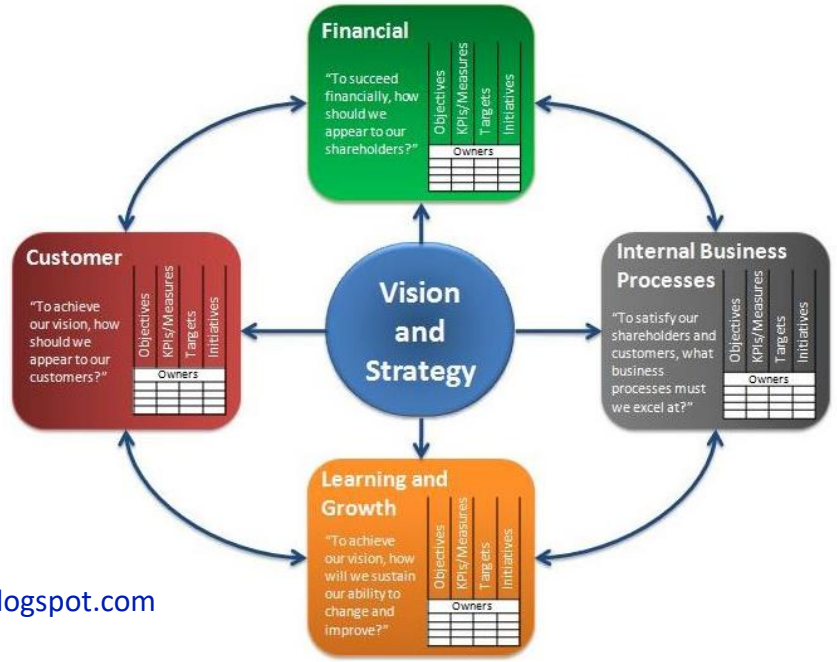
28. Performance monitoring using Balanced Score Card is most useful since it primarily focuses on:

a) **Management perspective**

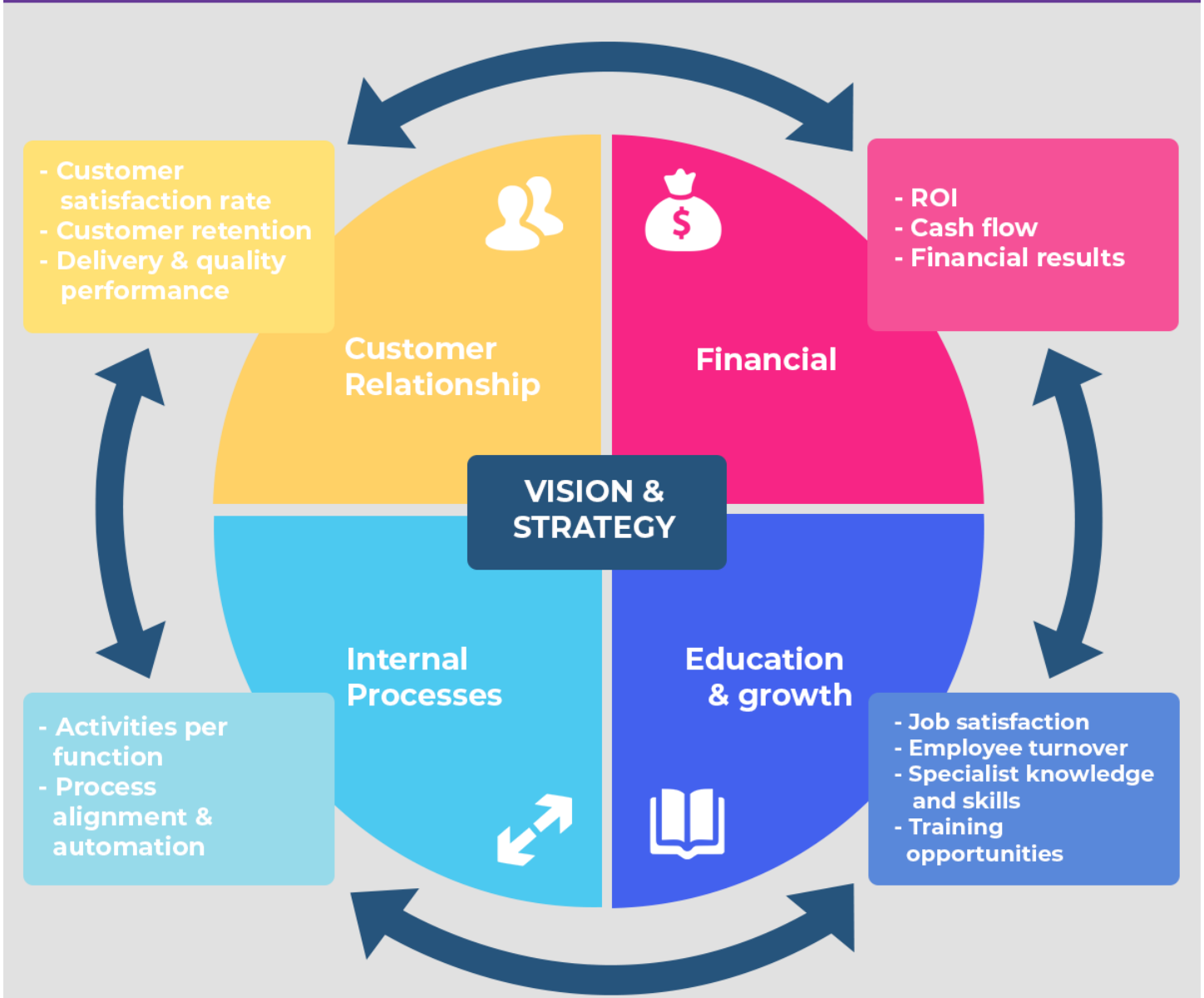
b) **Product and services**

c) **Customer perspectives**

d) **Service delivery processes**



BALANCED SCORECARD



29. Which of the following is NOT considered as an example of a lead indicator?

a) Number of gaps with respect to industry standard.

b) Comparative market position of organization.

c) Percentage of growth achieved over three years.

d) Improvement in customer satisfaction survey.

Leading Indicator:

- An indicator of performance that might predict future success.

Examples:

- User guide usage
- Calories per day
- Using safety equipment

Lagging Indicator:

- An indicator of *past* performance that measures how we performed.

Examples:

- Customer satisfaction
- Weight
- Number of deaths

Leading and *Lagging* indicators are time-based

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

30. The PRIMARY objective of base lining IT resource performance with business process owners is to:

a) define and implement lead and lag indicators.

b) ensure resource planning is aligned with industry.

c) assess cost effectiveness of outsourcing contracts.

d) benchmark expected performance measurement.

31. Which of the following is BEST measure to optimize performance of skilled IT human resources?

a) Include personal development plan in job description.

b) Document personal expectations during exit interviews.

c) Implement ‘Bring Your Own Device (BYOD)’ policy.

d) Monitor performance measure against baseline.

32. IT resource optimization plan should primarily focus on:

a) Reducing cost of resources

b) Ensuring availability

c) Conducting training programs

d) Information security issues

33. The PRIMARY objective of implementing performance measurement metrics for information assets is to:

a) decide appropriate controls to be implemented to protect IT assets.

b) compare performance of IT assets with industry best practices.

c) determine contribution of assets to achievement of process goals.

d) determine span of control during life cycle of IT assets.

34. Which of the following is the PRIMARY purpose of optimizing the use of IT resources within an enterprise?

a) To increase likelihood of benefit realization.

b) To ensure readiness for future change.

c) To reduce cost of IT investments.

d) To address dependency on IT capabilities.

35. While monitoring the performance of IT resources the PRIMARY focus of senior management is to ensure that:

a) IT sourcing strategies focus on using third party services.

b) IT resource replacements are approved as per IT strategic plan.

c) key goals and metrics for all IT resources are identified.

d) resources are allocated in accordance with expected performance.

36. Organization considering deploying application using cloud computing services provided by third party service provider. The MAIN advantage of this arrangement is that it will:

a) minimize risks associated with IT

b) help in optimizing resource utilization.

c) ensure availability of skilled resources.

d) reduce investment in IT infrastructure.

Chapter 5

Business Continuity Management

37. Which of the following is MOST important to have in a disaster recovery plan?

a) Backup of compiled object programs

b) Reciprocal processing agreement / arrangement

c) Phone contact list

d) Supply of special forms / Claim Forms

Page 100 ; Para 5.12.1

Business Continuity
&
Disaster Recovery Plan

Comparison Chart

Business Continuity Plan	Disaster Recovery Plan
BCP is a plan of action to ensure continuity of business operations before, during and after disasters and disruptive events.	DRP is a subset of business continuity planning to mitigate the impact of a disaster and recovery of critical IT systems.
BCP focuses on the operational elements within an organization to allow the business to function normally without any downtime.	DRP focuses on certain aspects of an organization that ensure normal functioning of the IT operations.
BCP provides a long-term, strategic approach to get back to regular operations.	DRP takes a more tactical approach to deal with unplanned incidents.
BCP focuses on keeping an organization functional during the disaster and immediately after.	DRP focuses on mitigating the impact of a disaster and addressing the immediate aftermath.

38. Which of the following BEST describes difference between a DRP and a BCP? The DRP:

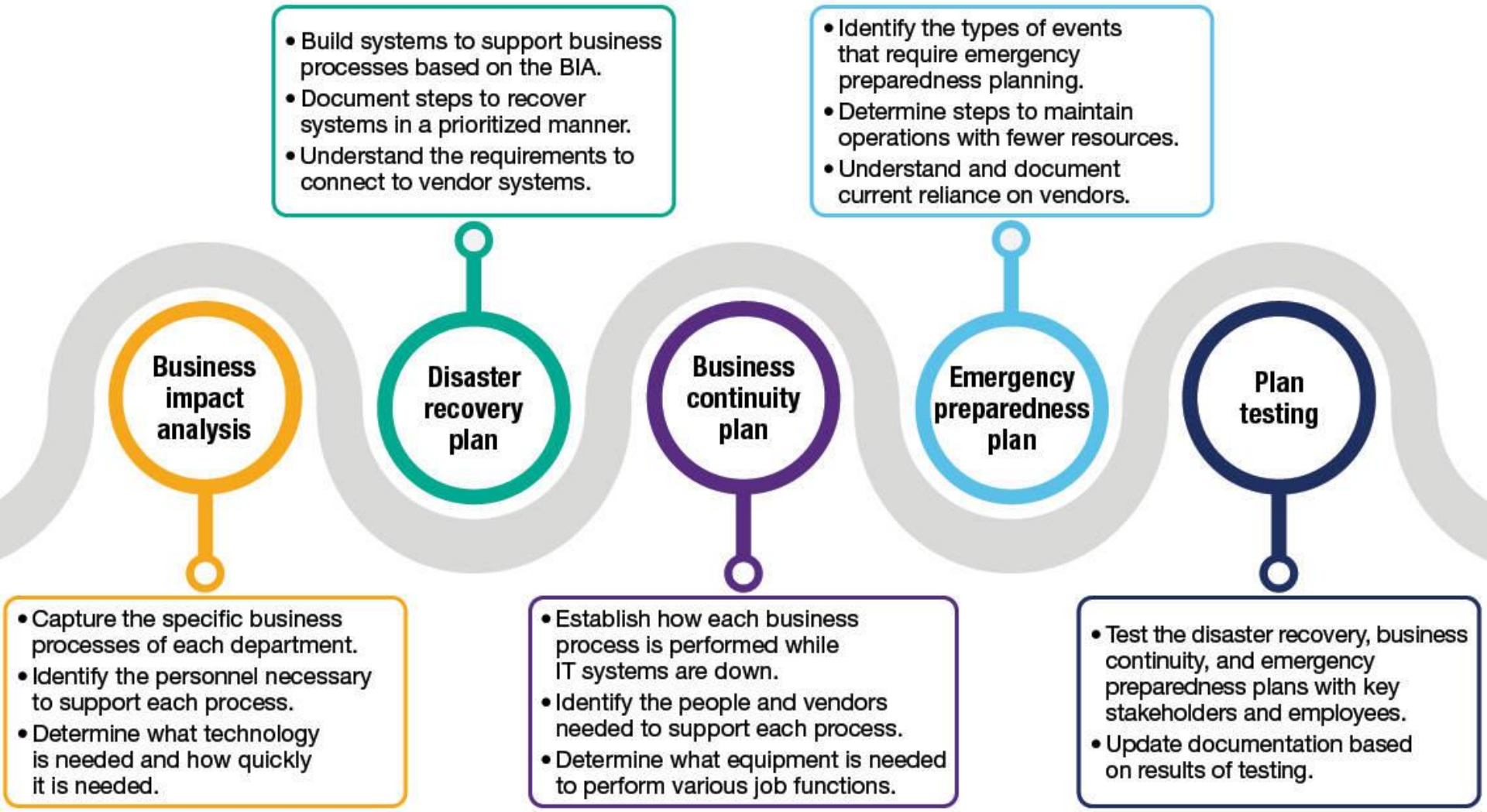
a) works for natural disasters whereas BCP works for unplanned operating incidents such as technical failures.

b) works for business process recovery and information systems whereas BCP works only for information systems.

c) defines all needed actions to restore to normal operation after an un-planned incident whereas BCP deals with sustaining critical operations needed to continue working after an un-planned incident.

d) is the awareness process for employees whereas BCP contains procedures to recover the operation

Page 90 ; Para 5.3.3


Business impact analysis
• Capture the specific business processes of each department.
• Identify the personnel necessary to support each process.
• Determine what technology is needed and how quickly it is needed.
Disaster recovery plan
• Build systems to support business processes based on the BIA.
• Document steps to recover systems in a prioritized manner.
• Understand the requirements to connect to vendor systems.
Business continuity plan
• Establish how each business process is performed while IT systems are down.
• Identify the people and vendors needed to support each process.
• Determine what equipment is needed to perform various job functions.
Emergency preparedness plan
• Identify the types of events that require emergency preparedness planning.
• Determine steps to maintain operations with fewer resources.
• Understand and document current reliance on vendors.
Plan testing
• Test the disaster recovery, business continuity, and emergency preparedness plans with key stakeholders and employees.
• Update documentation based on results of testing.

39. The MOST significant level of BCP program development effort is generally required during the:

a) Early stages of planning.

b) Evaluation stage.

c) Maintenance stage.

d) Testing Stage.

40. An advantage of the use of hot sites as a backup alternative is:

a) The costs related with hot sites are low.

b) That hot sites can be used for a long amount of time.

c) That hot sites do not require that equipment and systems software be compatible with the primary installation being backed up.

d) That hot sites can be made ready for operation within a short span of time.

Page 116 ; Para 5.15.1.2

System Deadlock

- In concurrent computing, a deadlock is a state in which each member of a group waits for another member, including itself, to take action, such as sending a message or more commonly releasing a lock.
- Deadlocks are a common problem in **multiprocessing systems, parallel computing, and distributed systems**, where software and hardware locks are used to arbitrate shared resources and implement process synchronization.
- In an **operating system**, a deadlock occurs when a process or thread enters a waiting state because a requested system resource is held by another waiting process, which in turn is waiting for another resource held by another waiting process. If a process is unable to change its state indefinitely because the resources requested by it are being used by another waiting process, then the system is said to be in a deadlock.
- In a **communications system**, deadlocks occur mainly due to lost or corrupt signals rather than resource contention.

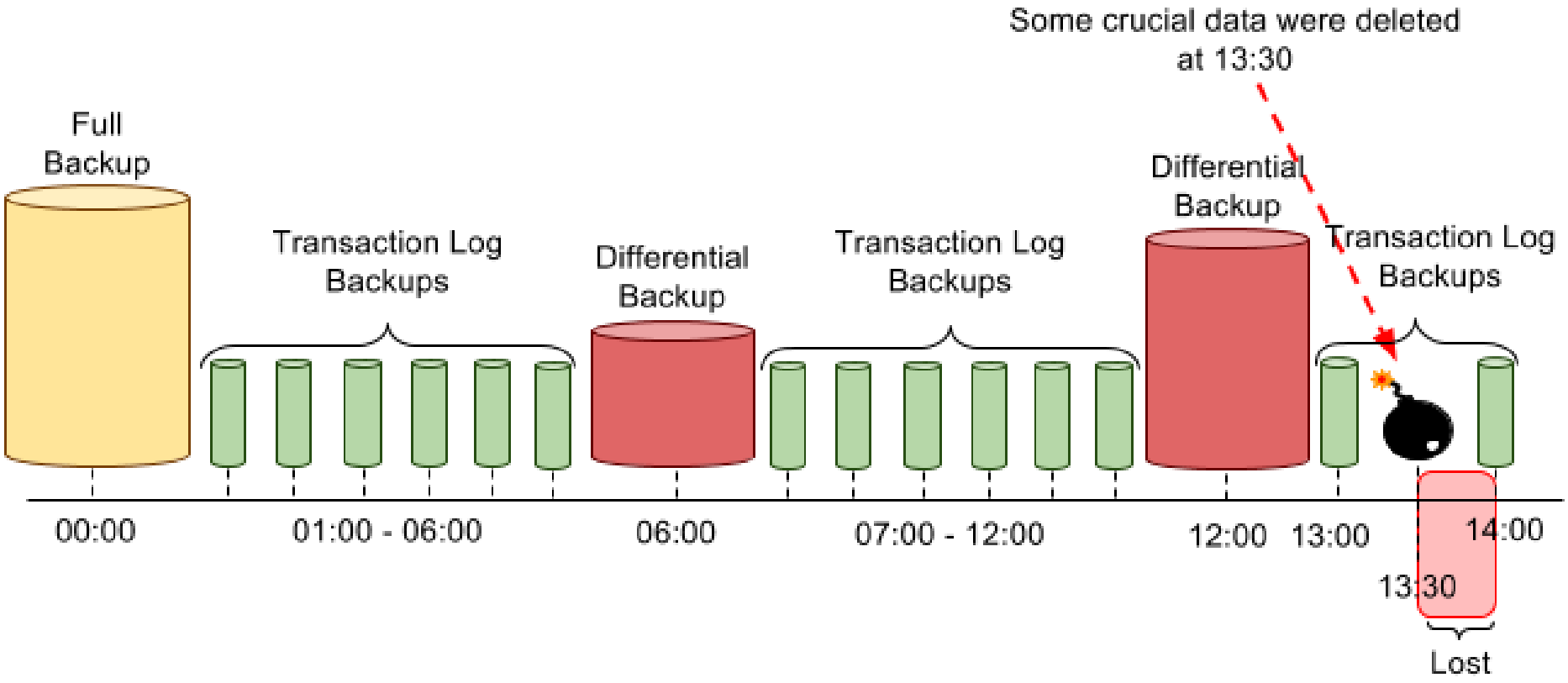
41. All of the following are security and control concerns associated with disaster recovery procedures EXCEPT:

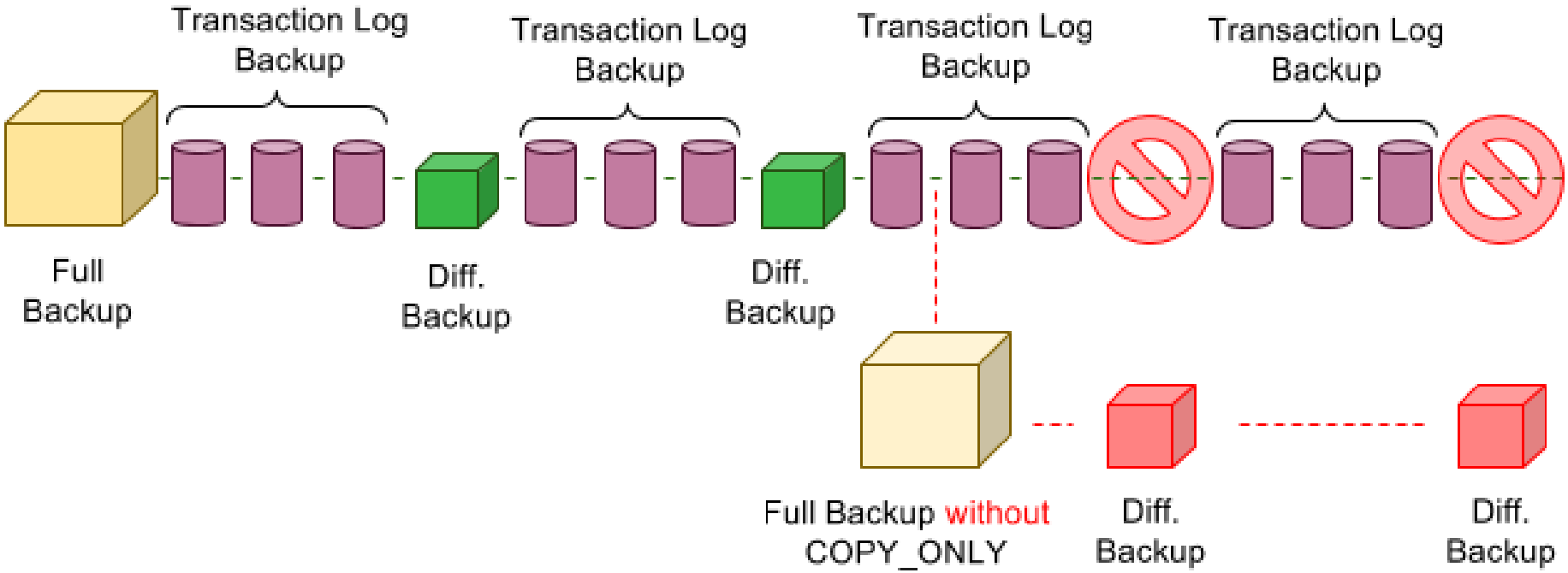
a) Loss of audit trail.

b) Insufficient documentation of procedures.

c) Inability to restart under control.

d) Inability to resolve system deadlock.


Some crucial data were deleted
at 13:30
Full
Backup
Transaction Log
Backups
Differential
Backup
Transaction Log
Backups
Differential
Backup
Transaction Log
Backups
00:00
01:00 - 06:00
06:00
07:00 - 12:00
12:00
13:00
13:30
14:00
Lost


Transaction Log Backup
Transaction Log Backup
Transaction Log Backup
Transaction Log Backup
Full Backup
Diff. Backup
Diff. Backup
Full Backup without COPY_ONLY
Diff. Backup
Diff. Backup

42. As updates to an online order entry system are processed, the updates are recorded on a transaction tape and a hard copy transaction log. At the end of the day, the order entry files are backed up onto tape. During the backup procedure, the disk drive malfunctions and the order entry files are lost. Which of the following are necessary to restore these files?

a) The previous day's backup file and the current transaction tape

b) The previous day's transaction file and the current transaction tape

c) The current transaction tape and the current hardcopy transaction log

d) The current hardcopy transaction log and the previous day's transaction file

43. An IS auditor reviewing an organisation's information systems disaster recovery plan should verify that it is:

a) Tested every 1 month.

b) Regularly reviewed and updated.

c) Approved by the chief executive officer

d) Approved by the top management

Page 121 ; Para 5.18

Alternate site selection criteria

Site	Cost	Hardware	Telecom	Set-up Time	Location
Cold Site	Low	None	None	Long	Fixed
Warm Site	Medium	Partial	Partial / Full	Medium	Fixed
Hot Site	Medium / High	Full	Full	Short	Fixed
Mobile Site	High	Dependent	Dependent	Dependent	Not Fixed
Mirrored Site	Very High	Full	Full	None	Fixed

44. Which of the following offsite information processing facility conditions would cause an IS auditor the GREATEST concern?

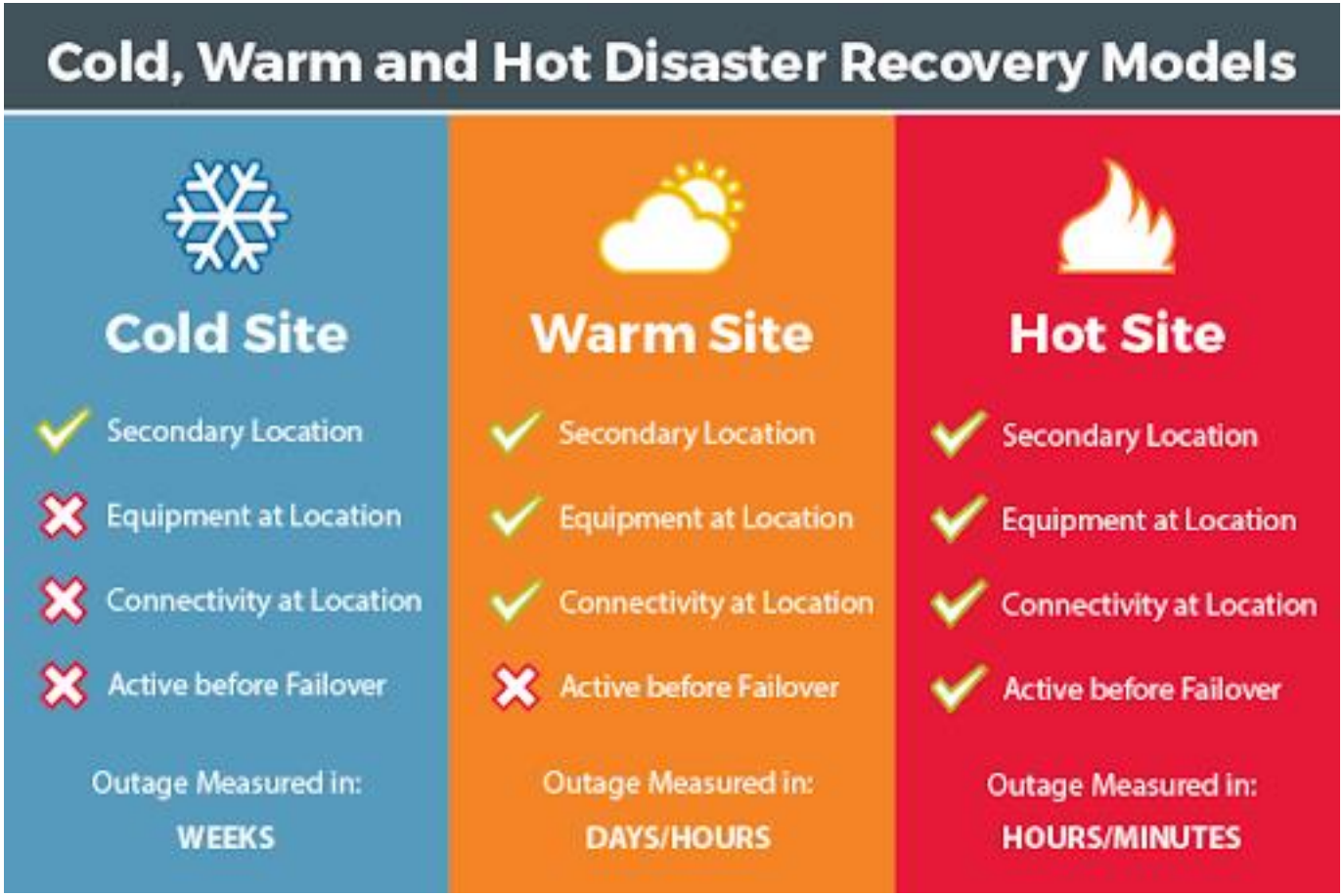
a) Company name is clearly visible on the facility.

b) The facility is located outside city limits from the originating city.

c) The facility does not have any windows.

d) The facility entrance is located in the back of the building rather than the front.

Page 117 ; Para 5.15.2


Cold, Warm and Hot Disaster Recovery Models
Cold Site
Secondary Location
Equipment at Location
Connectivity at Location
Active before Failover
Outage Measured in:
WEEKS
Warm Site
Secondary Location
Equipment at Location
Connectivity at Location
Active before Failover
Outage Measured in:
DAYS/HOURS
Hot Site
Secondary Location
Equipment at Location
Connectivity at Location
Active before Failover
Outage Measured in:
HOURS/MINUTES

45. Which of the following methods of results analysis, during the testing of the business continuity plan (BCP), provides the BEST assurance that the plan is workable?

a) Quantitatively measuring the results of the test

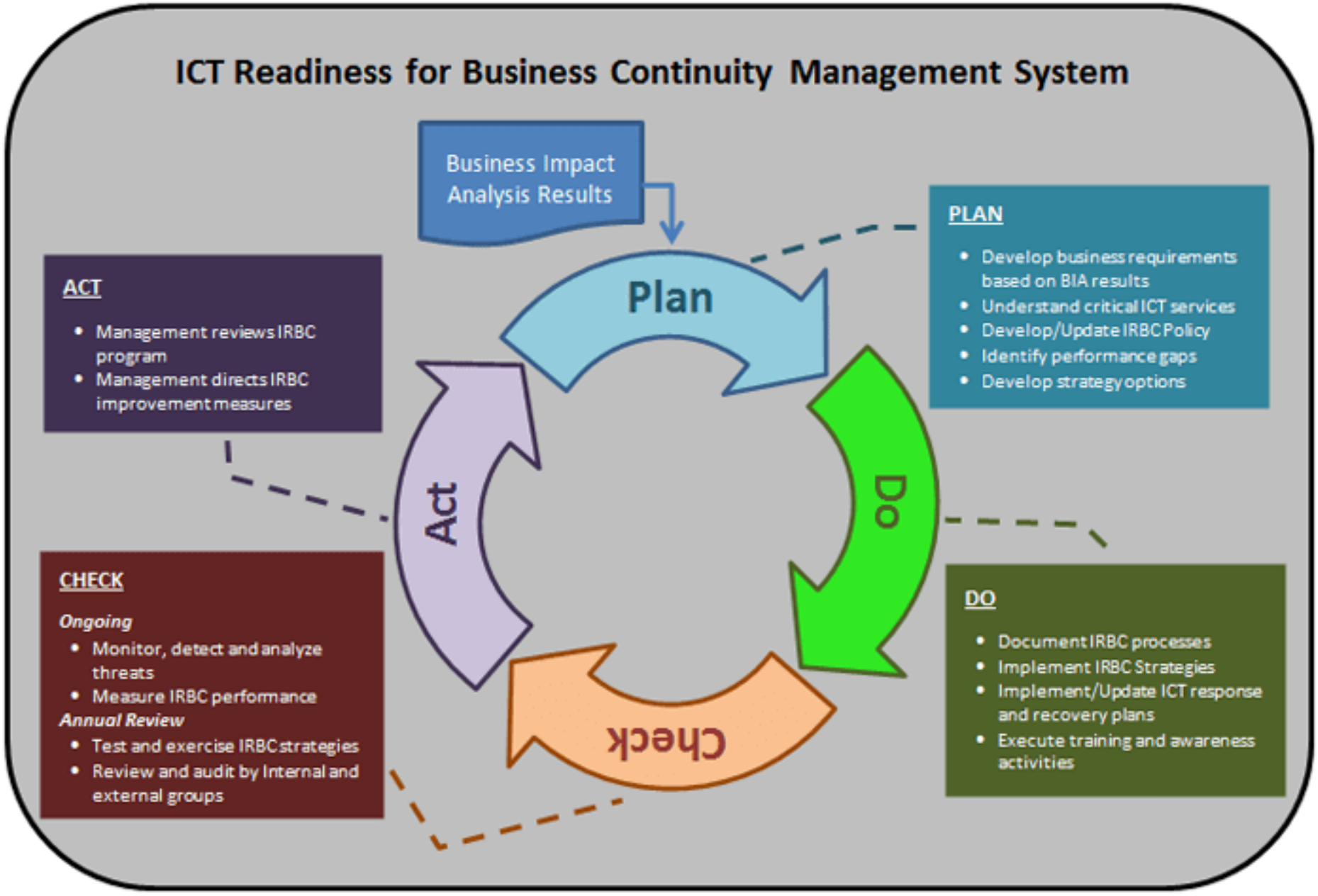
b) Measurement of accuracy

c) Elapsed time for completion of prescribed tasks

d) Evaluation of the observed test results

Page 132 ; Point 6

ICT Readiness for Business Continuity Management System




ISO
ISO 27031
Cybersecurity
Incident Response

46. The scope of ISO/IEC 27031:2011 encompasses the following …… except

a) all events and incidents (including security related) that could have an impact on ICT infrastructure and systems

b) an organization to measure performance parameters that correlate to its IRBC in a consistent and recognized manner

c) applies only to private and non-governmental organization irrespective of size

d) ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents, and related disruptions, that could affect continuity of critical business functions.

Page 123 ; Para 5.20

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

47. The focus of ISO 22301 is to ensure continuity of business delivery of products and services after occurrence of disruptive events. This is done by ……. except

a) finding out business continuity priorities (through business impact analysis)

b) what potential disruptive events can affect business operations (through risk assessment)

c) defining what needs to be done to prevent such events from happening

d) defining how to recover minimal and normal operations in the longest time possible (i.e., risk mitigation or risk treatment).

Page 122 ; Para 5.19

Business continuity planning

- Identify
  - Key assets
  - Vital services
  - Threats
  - Risks
- Risk planning
  - ID risk
    - Likelihood
    - Severity
  - Mitigation options
    - Avoid
    - Reduce
    - Transfer
  - Response and recovery plans
  - Staff
    - Communication
    - Training
  - Update periodically
- Threats
  - Natural disasters
    - Earthquake
    - Hurricane
    - Flood
  - Accidents
    - Fire
    - Utility outage
  - Malicious
    - Sabotage
    - Terrorism
    - Cyber attack
  - Market
    - Suppliers
    - Competitors
    - Consumer trends
  - Political
    - Legislation

48. During a ……., a disaster is replicated event to the point of ceasing normal production operations.

a) Checklist test

b) Structured walk through test

c) Simulation test

d) Parallel test

e) Full interruption test

Page 119 ; Para 5.17

FIT

- A Full Interruption Test is an exercise which all recovery procedures and strategy are tested.
- It actually replicates a disaster by halting production.

Off-Site Data Recovery Revisited

- **Electronic vaulting**: batch transfer of data to an off-site facility
- **Remote journaling**: transfer of live transactions to an off-site facility
- **Database shadowing**: storage of duplicate online transaction data, along with databases, at a remote site with a redundant server
- Relocation strategy with an off-site data storage recovery strategy allows reestablishment of critical business functions at a remote location

OFF-SITE DATA BACKUPS TECHNOLOGIES
(Electronic Vaulting, Remote Journaling, Remote Mirroring)

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

49. ……. ……. is a backup type where the data is backed up to an offsite location. The data is backed up, generally, through batch process and transferred through communication lines to a server at an alternate location.

a) Electronic Vaulting

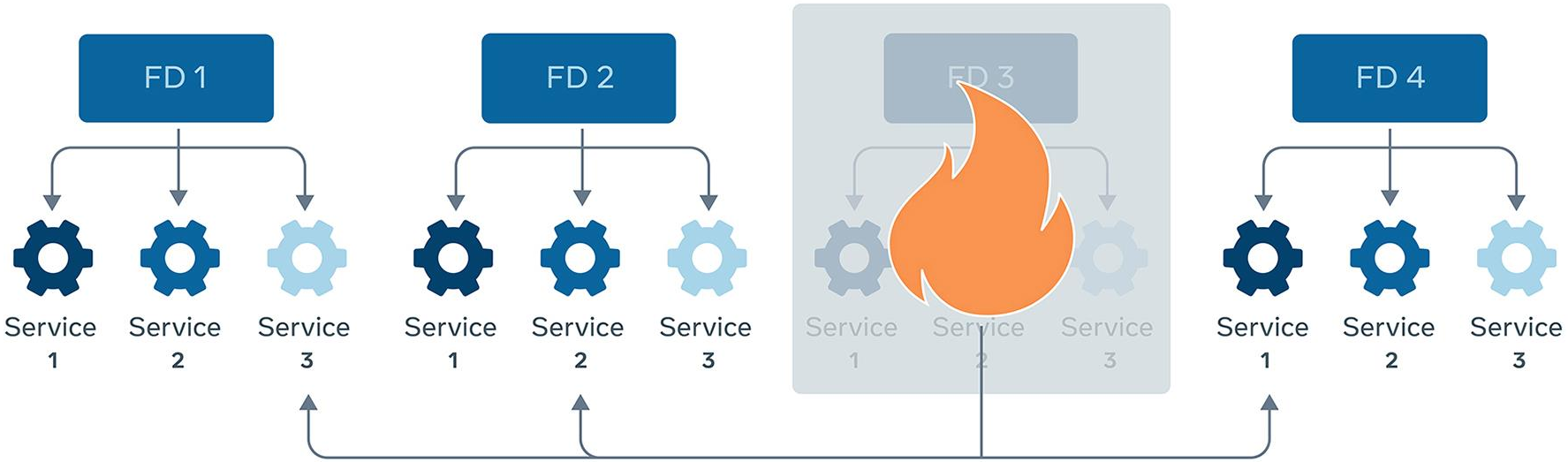
b) Remote Journaling

c) Database Shadowing

d) Disk Imaging

e) Remote Mirroring

Page 119 ; Para 5.16.2



Fault-tolerance is the property that enables a system (often computer-based) to continue operating properly in the event of the failure of (or one or more faults within) some of its components.

50. The basic characteristics of fault tolerance requires the following; except

a) No single point of failure.

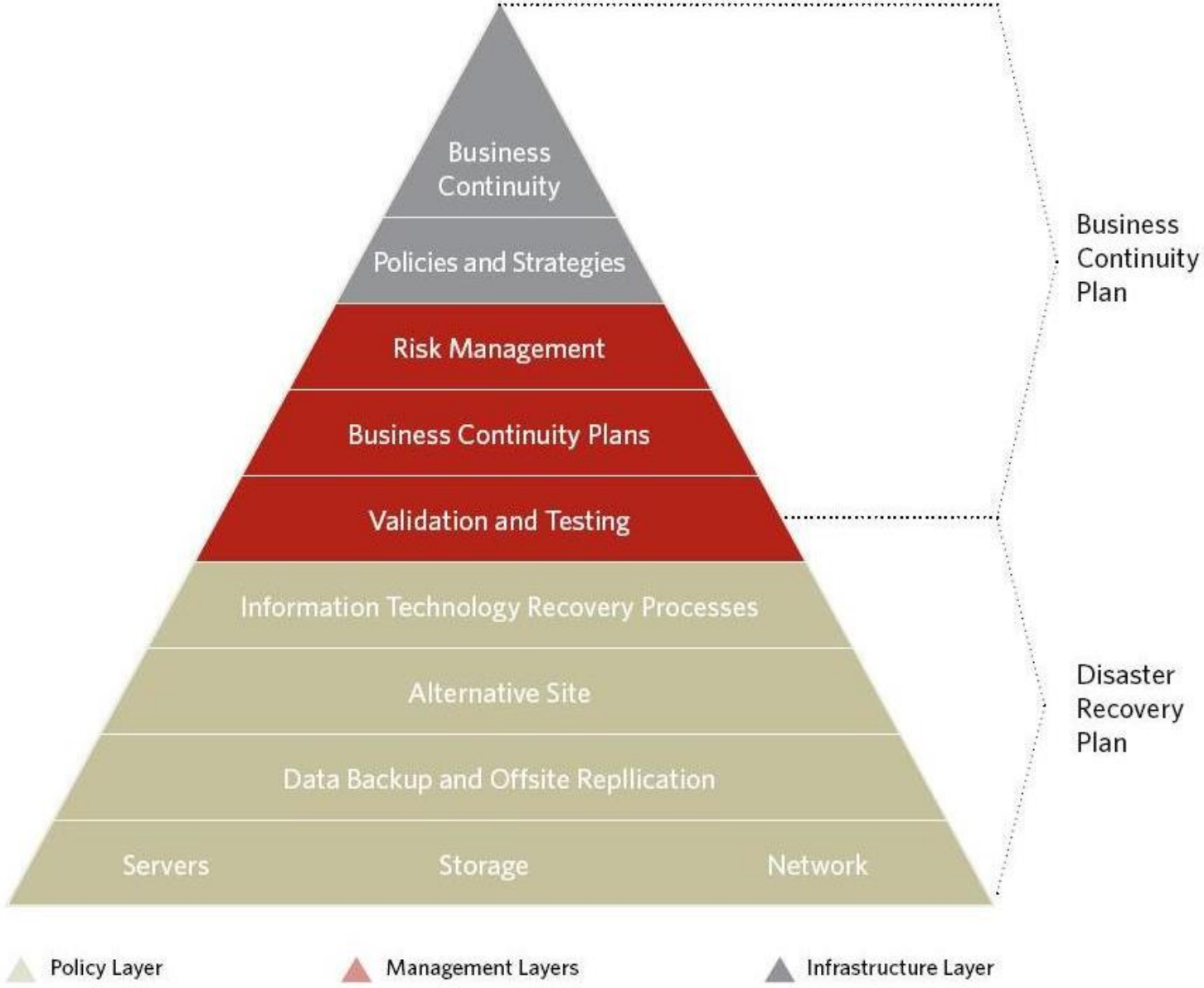
b) No single point of repair.

c) Fault isolation to the failing component.

d) No Fault containment to prevent propagation of the failure.

e) Availability of reversion modes.

Page 118 ; Para 5.16


Business Continuity
Policies and Strategies
Risk Management
Business Continuity Plans
Validation and Testing
Information Technology Recovery Processes
Alternative Site
Data Backup and Offsite Repllication
Servers
Storage
Network
Business Continuity Plan
Disaster Recovery Plan
Policy Layer
Management Layers
Infrastructure Layer

LET'S CHECK IT OUT

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

ISA AT Exam Focus areas - अंतिम मिनट की तैयारी

a) Vulnerability Assessment – Page 33

b) GPDR – EU – Page 42

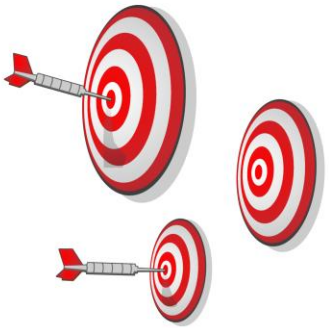
c) Digital Personal Data Protection Act, 2023 – 43

d) RBI – Master Direction on IT GRC and Assurance Practices -

e) Bank – BCP

f) ISO – 27031

g) Alternative Sites – Cold/Warm/Hot/Mirror



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

51. Event or disruptions that cause significant impact and may have an effect on outside clients is …….

a) Problem/Incident

b) Minor disaster

c) Major disaster

d) Catastrophic disaster

Page 109 ; Para 5.13.2.1

52. Live tests especially could create disaster if not planned properly because they use real people and real resources in real conditions, probably during normal working hours. Live tests should only be considered …….

a) after the BCP has been tested in full

b) after all Recovery Team members fully trained

c) before the BCP has been tested in full

d) after the BCP has been tested in full and all Recovery Team members fully trained

Module 2: Page 120 ; Para 5.17

53. ……. is a parallel processing of transactions to an alternate site. The alternate site is fully operational at all times and introduces a very high level of fault tolerance.

a) Electronic Vaulting

b) Remote Journaling

c) Database Shadowing

d) Mirror-Site

Module 2: Page 119 ; Para 5.16.2

54. ……. is the property that enables a system to continue operating properly in the event of the failure of some of its components.

a) Fault Tolerance

b) Replication

c) Redundancy

d) Diversity

Module 2: Page 118 ; Para 5.16.1

55. The single most reliable system backup strategy is to have fully redundant systems called ……

a) Hot Site

b) Warm Site

c) Near Site

d) Active Recovery Site

Module 2: Page 116 ; Para 5.15.1

56. The difference between incremental backup and differential backup is that ……

a) While a *differential backup* only includes the data that has changed since the previous backup, an *incremental backup* contains all of the data that has changed since the last full backup

b) while an *incremental backup* only includes the data that has changed since the previous backup, a *differential backup* contains all of the data that has changed since the last full backup

c) While a *differential backup* captures all files on the disk or within the folder selected for backup, an *incremental backup* contains all of the data that has changed since the last full backup

d) While an *incremental backup* captures all files on the disk or within the folder selected for backup, a *differential backup* contains all of the data that has changed since the last full backup

Module 2: Page 112 ; Para 5.15.1

57. Out of the following definition of disaster classification which event or disruption is a minor one?

a) Event or disruptions that cause no significant damage

b) Event or disruption that has significant impact and adversely affect the organisation's "going concern" status

c) Event or disruption that causes limited financial impact

d) Event or disruptions that cause significant impact and may have an effect on outside clients

Page 109; Para 5.13.2.1

58. The DRP should contain information about the …….; except

a) the vital records details

b) location where vital records are stored

c) who is in charge of that vital record

d) contains information about what is stored online

Page 100; Para 5.12.1

59. The primary role of this ..... team is to conduct research on data that could lead to a crisis and develop actions that would effectively handle these threats.

a) Business Continuity Team

b) Contingency Planning Team

c) Disaster Recovery Team

d) Incident Response Team

Page 97; Para 5.9.1

60. The objective of ……. is to counteract interruptions to business activities and to protect critical business processes from the impact of major failures or disasters

a) Business Continuity Plan (BCP)

b) Business Continuity Management (BCM)

c) Disaster Recovery Plan (DRP)

d) Minimum Business Continuity Objective (MBCO)

Page 97; Para 5.9.1

61. ISO/IEC 27031:2011 applies to …….. developing its ICT readiness for business continuity program (IRBC), and requiring its ICT services/infrastructures to be ready to support business operations in the event of emerging events and incidents, and related disruptions, that could affect continuity (including security) of critical business functions.

a) Private Organisation only

b) Governmental Organisation only

c) Non-Governmental Organisation only

d) Private, Governmental, and Non-governmental, irrespective of size

Page 123; Para 5.20

62. The Basel Committee on E Banking underlines that banks should also ensure that periodic …. are conducted about business continuity and contingency planning; except

a) Independent Internal Audit

b) Independent IS Audit

c) Independent Internal and External Audit

d) Independent External Audit

Page 122; Para 5.18.3.1

63. In a BCP Audit, the IS auditor is expected ……

a) to identify operational risks and to provide recommendations to mitigate them

b) to evaluate the processes of developing and maintaining documented, communicated, and tested plans for continuity of business operations and IS processing in the event of a disruption

c) to assess the ability of the organisation to continue all critical operations during a contingency and recover from a disaster within the defined critical recovery time period

d) to assess the plan of action for each type of expected contingency and its adequacy in meeting contingency requirements

Page 121; Para 5.18.1

64. During every phase of the BCP test, a detailed documentation of observations, problems and resolutions should be maintained. This documentation can be of great assistance during ……..

a) A parallel test

b) A simulation test

c) An actual disaster

d) Full interruption test

Page 120; Para 5.17

65. …… is providing multiple identical instances of the same system or subsystem, directing tasks or requests to all of them in parallel, and choosing the correct result on the basis of a quorum

a) Replication

b) Redundancy

c) Diversity

d) Fault-tolerance

Page 118; Para 5.16.1

66. Data can be sent electronically via a remote backup service, which is known as ……..

a) Electronic Vaulting

b) Remote Journaling

c) Database Shadowing

d) Mirror-Site

Page 117; Para 5.15.2

67. The Strategic Scorecard has 4 basic elements aimed at helping the board to ensure that all strategic aspects are covered by making the board aware of what work is being done; except

a) Strategic Position

b) Strategic Future

c) Strategic Implementation

d) Strategic Risks

e) Strategic Option

Page 82; Para 4.7

68. A Balanced Scorecard, as defined by Robert S. Kaplan and David P. Norton, groups objectives, measures, targets, and initiatives into 4 perspectives; except

a) Financial

b) Customer

c) Learning and Growth

d) Internal Process

e) Sustainability

Page 79; Para 4.6.1

69. …… is the first pre-requisite of performance management

a) Governance

b) Strategy

c) Risk Management

d) Goal Setting

e) Compliance

Page 74; Para 4.4

70. Use of IT through outside vendors reduces capital expenditure (capex) but increases revenue expenditure (Opex) or it can be said that ……. IS Auditors who are required to evaluate such alternatives have to consider not only the cost benefit analysis but also the associated risks and how these risks have been mitigated through implementation of appropriate controls.

a) Capex is converted to Opex

b) Opex is converted to Capex

c) Only Reduction of Capex

d) Only Increase in Opex

Page 68; Para 3.7.8

71. The Governance processes of ISO 38500 and COBIT 2019 primarily focus on ……..

a) Planning, Directing and Controlling (PDC)

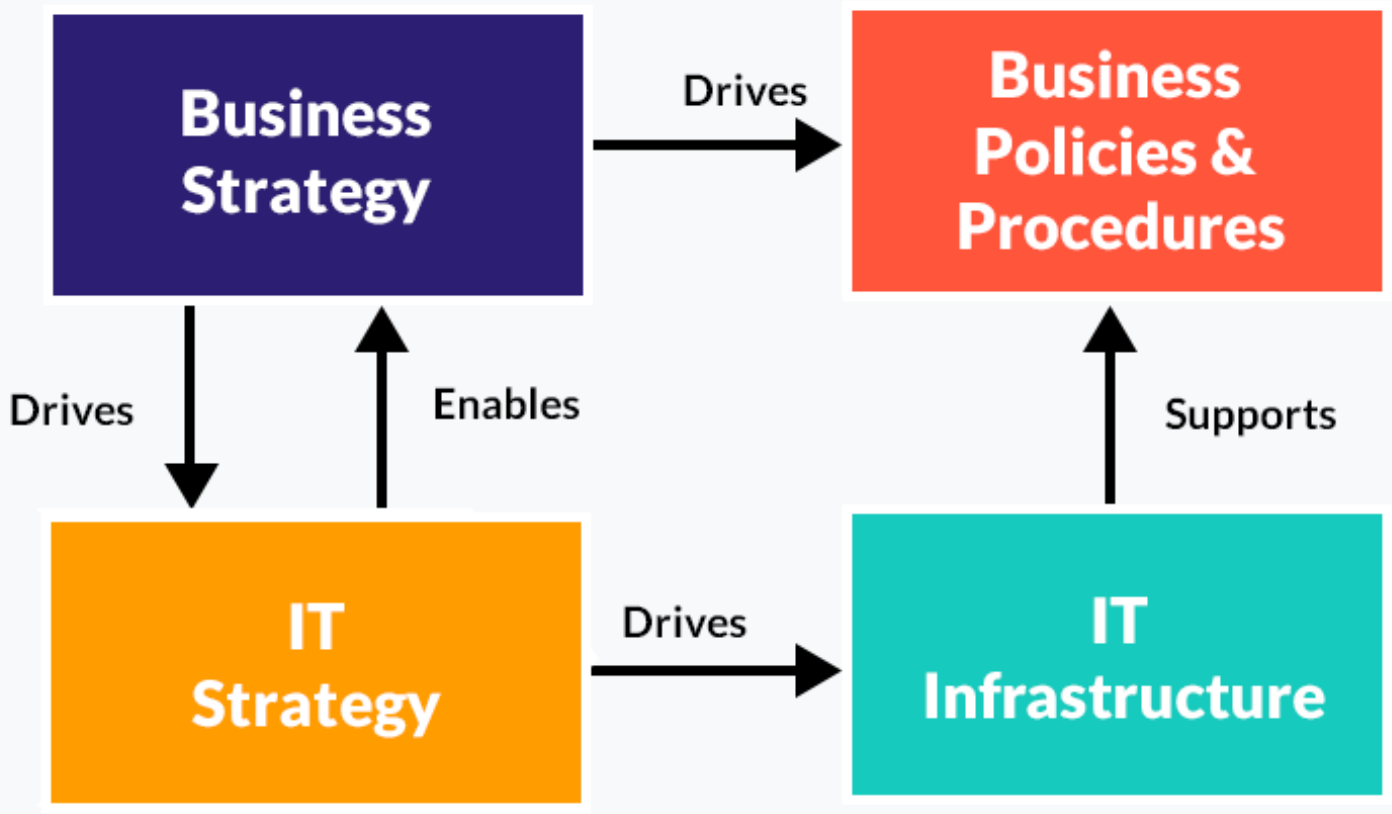
b) Evaluate, Direct and Monitor (EDM)

c) Performance Measurement (PM)

d) Taking corrective action

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

IT to Business Strategy Alignment



72. The key management practices, which are required for aligning IT strategy with enterprise strategy, are the following, except;

a) Understand enterprise direction

b) Conduct gap analysis

c) Communicate the IT Strategy and direction

d) Value optimization

Page 65; Para 3.7.2

73. …….. is a key enabler of corporate business strategy.

a) CEO

b) CFO

c) CTO

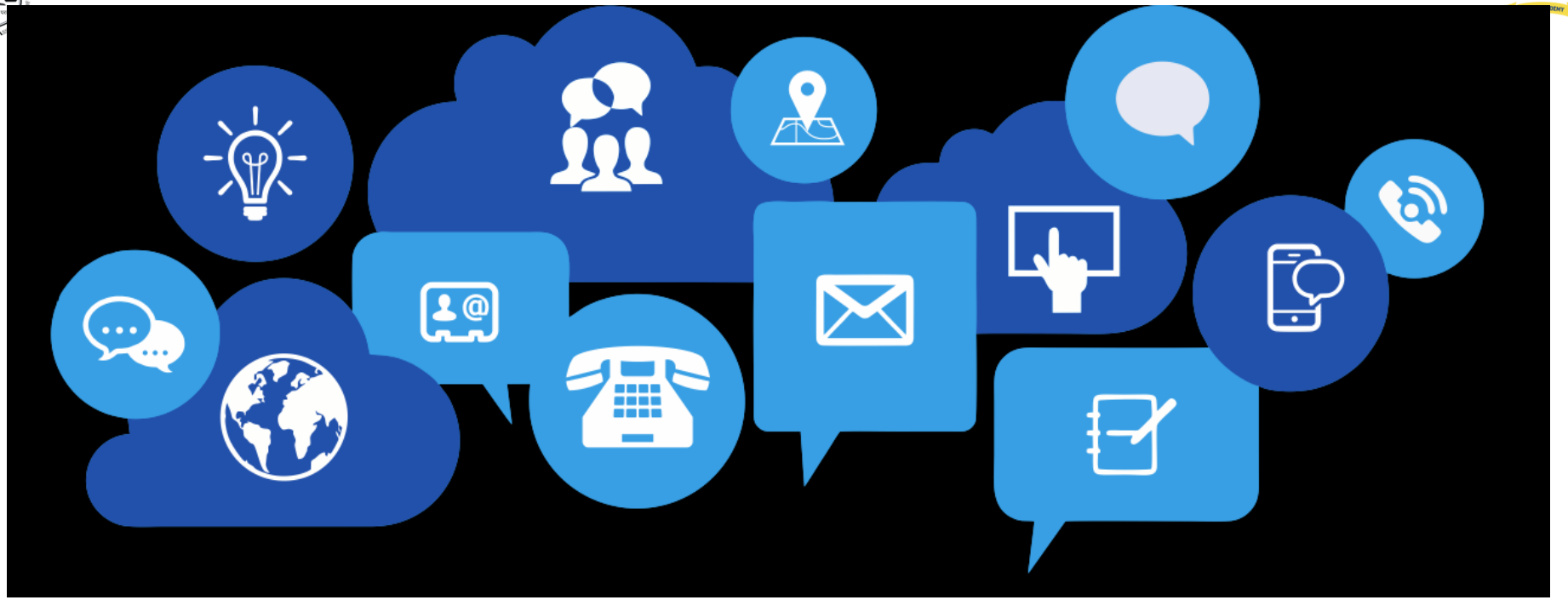
d) IT

e) COO

Page 63; Para 3.7.1

LET'S CHECK IT OUT

51	c	61	d	71	b						
52	d	62	b	72	d						
53	b	63	a	73	d						
54	a	64	c								
55	d	65	a								
56	b	66	a								
57	c	67	b								
58	d	68	e								
59	b	69	d								
60	b	70	a								



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