Most Important Questions for JAIIB PPB

Q1. Which of the following statements is/are correct about Bank Computerisation in India?

1. The concept of Bank Computerisation started in 1980-81.
2. In 1983, a committee was set up to study the possibilities and stages involved in bank computerisation.
3. The First Rangarajan Committee Report on bank mechanisation was submitted in 1983.
4. The Second Rangarajan Committee was constituted in the year 1985.

(a) 1,2, and 3
(b) 2, 3, and 4
(c) 1, 2, and 4
(d) Only 1, 2

Q2. Which of the following statements is/are not correct regarding Local Area Networks (LANs)?

1. LAN is a computer network that links computers, network devices, and peripherals within a localized area, such as a building.
2. LAN uses network adapters that employ special techniques to share a common medium between connected nodes.
3. The distance and the number of nodes supported in a LAN depend on the medium used to establish the network.
4. LAN usually extends beyond 100 meters for Cat5e cables.

(a) 1,2, and 3
(b) Only 4
(c) 1, 2, and 4
(d) Only 1, 2

Q3. Which of the following functions are not performed by CBS?

1. Customer accounts management
2. Office account management
3. Loans disbursal and management
4. Email Management Statement
5. Generation of Reports, multi-currency Balance sheets, and P&L Statements

(a) 1,2, and 3
(b) Only 1,2
(c) 2, 3, and 4
(d) Only 4

Q4. Read the following statements carefully.

i. The security policy should address specific capabilities of operating systems and ensure that the available security features are implemented.

ii. The password file should be encrypted.

iii. File maintenance should be a part of the normal user's access level.

iv. Access levels should not be periodically reviewed by the internal auditor.

v. The Chief information security officer should ensure that available features have been implemented.

Choose the following option is/are true regarding Logical Access Control.

(a) i, ii, and iii

(b) Only i, ii

(c) iii, iv and v

(d) i, ii and v

Q5. Which of the following services can be availed at ATMs?

1. Cash Withdrawal, Cheque Book Request, and Credit Card Payment
2. Balance Enquiry, User details updation, and Insurance Premium Payment
3. Funds Transfer, Statement Enquiry, and Aadhaar Updation
4. Utility bill payment, Cheque deposit, and Term deposit opening

(a) i, ii, and iii

(b) Only i, ii

(c) iii, iv and v

(d) All of the above

Q6. Which of the following is not true regarding payment options in credit cards?

1. The cardholder has the option to pay the entire amount as soon as the card account is debited.
2. The cardholder can pay only a certain percentage of the debited amount.
3. The cardholder cannot pay the amount in monthly installments.
4. No service fee is charged on the amount if the payment is deferred.

(a) 1 and 2 only

(b) 3 and 4 only

(c) 2, 3 and 4 only

(d) 1, 2 and 3 only

Q7. Read the following statements carefully-

i. They are made of copper wires and are prone to electromagnetic interference

ii. They are not affected by electromagnetic interference and provide high-quality transmission of signals at very high speeds

iii. They are useful for short-distance communication only

iv. They are the least popular cables currently in use due to their high cost and inconvenience

Select the correct option for optical fibre cables.

(a) i, ii, and iii

(b) Only ii

(c) iii, iv and v

(d) i, ii and v

Q8. What is the definition of EFT as per the Uniform Commercial Code (UCC) of the USA?

1. A payment system through which payment orders by a bank can be transmitted to the bank to which the order is addressed.
2. A communication system of clearing house or other association of banks.
3. A mechanism for transferring funds in real time.
4. A system for processing interbank payments.

(a) 1 only
(b) 1 and 4 only
(c) 2, 3 and 4 only
(d) 1, 2 and 3 only

Q9. Which of the following is not a facilitator of EFT in India?

i. NEFT
ii. Cheque Truncation System (CTS)
iii. Fedwire
iv. IMPS

(a) i, ii, and iii
(b) Only iii
(c) ii, iii and iv
(d) All of the above

Q10. Which of the following electronic clearing systems in India allows instant fund transfer 24x7?

i. ECS
ii. RTGS
iii. IMPS
iv. UPI

(a) i, ii, and iii
(b) Only iii
(c) Only ii
(d) All of the above

Q11. Choose the correct statement(s) regarding technology developments in the banking industry:

1. Indian banks have been investing in digital technologies to promote digital banking for the past few years.
2. Broadband internet has become more affordable to customers and has enabled banks to roll out many banking services through mobile and internet banking.
3. Implementing new technologies is always inexpensive for banks.
4. Banks no longer use demographic-based clusters to target customers.

(a) 1,2 only
(b) 1 and 4 only
(c) 2, 3 and 4 only
(d) All of the above

Q12. Which of the following statements regarding online delivery of banking services is/are correct?

i. Banks use the net to offer Internet banking services, including routine transactions such as balance enquiry, transfer between accounts, and bill payments.
ii. Banks use the internet only for selling financial products.
iii. Banks do not use the Internet for offering financial advice.
iv. Banks use the internet for offering routine transactions only.

(a) i, ii, and iii
(b) Only i
(c) Only i, ii
(d) All of the above

Q13. Read the following statements carefully-

1. Incorrect data can have serious implications in decision-making.
2. The potential impact of erroneous data can result in playing havoc with an organisation's business.
3. Inadequate control over data is the single largest factor, which promotes the scope of fraud.

Choose the correct option regarding the importance of data and software in an organization.

(a) 1,2 only
(b) 1, 3 only
(c) 2, 3 only
(d) All of the above

Q14. Which of the following statements is/are not true regarding fraudulent transactions in computerized systems?

i. Special programs such as utility programs may be used to make unauthorized changes to computerized records in a way that bypasses the validation controls built into the computer systems.
ii. Unauthorised manipulation in the important files by bypassing the security controls.
iii. Unauthorised amendments made to the payment instructions after their entry into the computer system.

(a) i, ii, and iii
(b) Only iii
(c) Only i, ii
(d) All of the above

Q15. What are the causes that facilitate computer fraud?

i. Inadequate control over data/media.
ii. Easy access mechanism of systems.
iii. Inadequate control over outputs.

(a) i, and ii
(b) ii and iii
(c) Only i,
(d) All of the above

Q16. Read the following statements carefully-

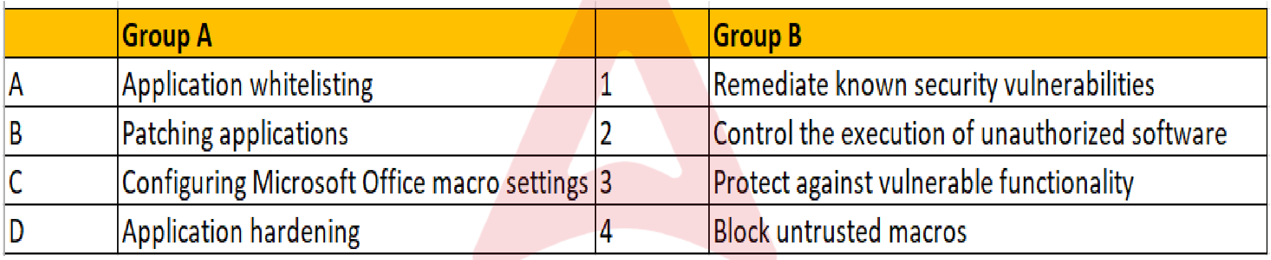
i. Administrative controls are limited to defining responsibilities and formal policies only.
ii. Transactions should be validated against limits, balances, and authorized before being processed.
iii. Stop payments, post-dated cheques, stale cheques and cheques with invalid dates should be validated.
iv. Validation of sensitive parameters like maximum/minimum days allowed, maximum/minimum rates, and drawing limits.

Select the correct option about administrative controls applicable to customer accounting.
(a) i, and ii
(b) ii, iii, and iv
(c) i, ii, and iii
(d) All of the above

Q17. Which of the following risks can arise from cyber-attacks on banks?
1. Loss of productivity due to business disruption.
2. Cost of investigation.
3. Reputational benefits.
4. Increase in investment returns.

(a) 1,2 only
(b) 2, 3 only
(c) 3, 4 only
(d) All of the above

Q18. Match the following Group A with Group B in respect of the Essential mitigation strategies for business continuity:



	Group A		Group B
A	Application whitelisting	1	Remediate known security vulnerabilities
B	Patching applications	2	Control the execution of unauthorized software
C	Configuring Microsoft Office macro settings	3	Protect against vulnerable functionality
D	Application hardening	4	Block untrusted macros

(a) A-4, B-1, C-2, D-3
(b) A-2, B-1, C-4, D-3
(c) A-3, B-2, C-4, D-1
(d) A-1, B-3, C-4, D-2

Q19. Which of the following statement is true :

I- Technologies currently being developed and tested range from a new generation of more sophisticated EMV and NFC cards to providing services through mobiles, wearables, and social media networks.

II- Advancements in technology and shifts in consumer preferences driven by SMAC (social media, mobility, analytics, cloud computing) have reduced challenges in terms of utility/efficiency, product complexity, and deployment architecture.

III- Cryptocurrencies and alternative forms of e-cash are emerging, which do not require a traditional paper-oriented payments system by using technologies that enable such smart cards to transfer value through the Internet.

IV- The new generation of tech-savvy personnel is being recruited by banks to leverage their skills in technology for maximizing productivity and excellence in customer service.

Choose the correct answer from options given:-
(a) Only I, II and III are correct.
(b) Only I, III and IV are correct.
(c) Only III and IV are correct
(d) All of above statement are correct.

Q20. Which of the following statement is true regarding chatbots are true?

I. Chatbots are driven by artificial intelligence, voice recognition, and natural language processing.

II. Chatbots are software applications that simulate conversations with real people through spoken human speech only.

III. Some real-life examples of chatbots are virtual assistants such as Google Meet, Zoom, and Google Duo.

IV. Despite these limitations, chatbots are becoming increasingly sophisticated, responsive, and more natural.

V. They can be deployed for customer service, as standalone applications, or on a website.

Choose the correct answer from options given

(a) Only I and II

(b) Only II and III

(c) Only I, IV and V

(d) All from I to V

Q21. What was the major difference between Digital Currency and Cryptocurrency?

I. Digital currencies require the user to be identified, while cryptocurrencies are partially anonymous, protecting the identity

II. Digital currencies are transparent, while cryptocurrencies are not transparent, as all the revenue streams are placed in a public chain

III. Digital currencies are decentralized, while cryptocurrencies are centralized.

IV. Many countries have legal frameworks for digital currencies, while cryptocurrencies have yet to be defined officially in many countries

Choose the correct answer from options given

(a) Only I and IV

(b) Only II and III

(c) Only I, IV and III

(d) All from I to IV

Q22. Robotic Process Automation (RPA) is a technology that uses software robots or bots to automate repetitive and rule-based tasks typically performed by humans. Which of the following is the true statement regarding RPA?

A. RPA is the practice of automating routine business practices with software robots

B. RPA are 24x7 working without fatigue, time and cost savings, zero types or copy/paste mistakes, and compliance

C. RPA is being used in banking activities like KYC, customer onboarding, loan origination, etc.

D. RPA is often applied to repetitive and mundane tasks so that employees can focus on more complex banking operations that require human interaction and decision-making

Choose the correct answer from the options given below:

(a) A, C only

(b) B, C, D only

(c) A, B, D only

(d) All of the above.

Q23. Match list I with list II

List-I	**List-II**
A.AI	i. It can be used in banking activities like secure document management, reporting, payments, treasury & securities, and trade finance.
B. RPA	ii. These are software applications that simulate conversations with real people through written or spoken human speech.
C. Chatbots	iii. It is an area of computer science that emphasizes the creation of intelligent machines and software that work and react like humans.
D. Blockchain Technology	iv. It is often applied to repetitive and mundane tasks so that employees can focus on more complex banking operation

Choose the correct answer from options given

(a) A-(iii), B-(iv), C-(ii),D-(i)

(b) A-(i), B-(iv), C-(iii), D-(ii)

(c) A-(ii), B-(iii), C-(iv), D-(i)

(d) A-(iii), B-(iv), C-(i), D-(ii)

Q24. Following are the statements related to the information system audit. State whether the statements false.

I. The objective of an information system audit changes depending on whether it is a manual or a computerized environment, and only the approach of the audit change

II. The automation of manual processes information system audit has resulted in significant improvements in efficiency, speed, and cost-effectiveness, while also reducing the likelihood of fraudulent activities

III. Security features and controls in computerized information systems could not be improved based on the suggestions made during the course of an IS audit.

IV. An information system translates itself into an effective tool to meet business goals.

Choose the incorrect statement from options given:-

(a) Only I and III are incorrect.

(b) Only I, III and IV are incorrect.

(c) Only III and IV are incorrect

(d) All of above statement are incorrect.

Q25. Match list I with list II

List-I Terms	**List-II Meaning**
A Phishing	i. They might claim to be updating their customer database, and threaten to suspend the account if the details are not provided.
B Vishing	ii. The email might contain a forged link that leads to a fake website or a message that shows a sense of urgency to get personal information
C Smishing	iii. The text might contain an URL or phone number and usually asks for immediate attention.

Choose the correct answer from options given

(a) A-(iii),B-(i), C-(ii)

(b) A-(i), B-(ii), C-(iii)

(c) A-(ii), B-(i), C-(iii)

(d) A-(iii), B-(ii), C-(i)

Q26. The modus operandi of a cyber-attack can vary depending on the goals and techniques**.** Arrange the following steps of modus operandi of a cyber-attack in ascending order.

A. Attackers can implant malware into vital systems and submit fraudulent payment instructions using a fake operator or approver.

B. Attackers must destroy proof of their operations to hide their conduct after fraudulent employed by the attacker.

C. Criminals conduct research and gather information about the target organization during the early reconnaissance period.

D. After gaining access to the network, hackers aim to gain further access privileges to penetrate the network.

Choose the correct answer from the options given below

(a) B, A, C, D

(b) C, B, A, D

(c) C, D, A, B

(d) B, D, C, A

Q27. Cybersecurity awareness refers to the knowledge and understanding of potential online threats and best practices for protecting sensitive information and systems from cyber-attacks. Identify the true statement regarding cybersecurity awareness from the following: -

i. Firms with strong cybersecurity cultures are better equipped to identify and respond to potential threats, reduce cyber incidents, and improve their ability to recover from a cyber attack.

ii. Identity theft and network hacks happen when employees unintentionally download malicious code or click dubious links.

iii. Comprehensive, hands-on training may help employees become more aware of potential hazards

iv. Data breach costs have significantly decreased.

v. Developing a cybersecurity awareness program requires delivering the right training to each team.

Choose the correct answer from options given

(a) Only ii, i and iv

(b) Only ii and iii

(c) Only i, ii, iii and v

(d) All of the above

Q28. Which of the following statement is true:

I. A type of malicious software that blocks access to a victim's data or threatens to publish it unless a payment is not made is called malware.

II. Malicious software code that intruders use to deceive individuals into believing that traditional security is protecting them during online banking transactions is called ransomware.

III. Malicious software programs that harm computers by stealing user credentials, destroying data, or performing other malicious actions is called viruses.

Choose the correct answer from options given:-

(a) Statement I, II and III are correct.

(b) Only Statement III is correct.

(c) Only Statement II is correct.

(d) All of above statement are correct.

Q29. In response to the increasing number of cyber-attacks, banks must develop a robust Cyber Incident Response (CIR) plan. Arrange the following phases of an effective incident response plan in ascending order.

I. Restoring the systems and data to their pre-incident state and resuming normal operations as quickly as possible

II. Isolating the affected systems and preventing the attacker from further infiltrating the network.

III. Eliminate the attacker's presence from the network, ensuring that all malware and other malicious code are removed

IV. Analyzing the incident and determining its scope and severity.

V. Monitoring capabilities to detect potential cyber incidents as early as possible to minimize damage.

VI. Preparation of potential cyber incidents by identifying their critical assets, creating an incident response team, and developing an incident response plan

Choose the correct answer from the options given below

(a) (VI), (II), (III), (I), (IV), (V)

(b) (VI), (V), (IV), (II), (III), (I)

(c) (VI), (V). (III), (I), (IV), (II)

(d) (VI), (II). (III), (I), (IV), (V)

Q30. Which of the following statement is not correct related to Network Behaviour Anomaly Detection (NBAD)?

i. It is a supplementary technology to systems that detect security threats based on packet signatures.

ii. NBAD-based systems are particularly helpful in detecting security threat vectors in two instances where signature-based systems cannot.

iii. NBAD program tracks critical network characteristics in real-time and generates an alarm if a strange event or trend is detected that could indicate the presence of a threat.

iv. NBAD technology/techniques are applied only to packet inspection systems.

Choose the correct answer from options given

(a) Only ii, i and iv

(b) Only i and iv

(c) Only i and iii

(d) All of the above

Q31. Match the following mitigation strategies with their meaning.

List- I Mitigation Strategies	**List- II Meaning**
a. Application whitelisting	i. to protect against risky activities and credential theft.
b. Application hardening	ii. to control the execution of unauthorized software.
c. Patching applications	iii. to remediate known security vulnerabilities
d. Multifactor authentication	iv. to protect against vulnerable functionality.

Choose the correct answer from options given

A. (a)-(ii),(b)-(iv), (c)-(iii),(d)-(i)

B. (a)-(i), (b)-(iv), (c)-(iii), (d)-(ii)

C. (a)-(ii), (b)-(iii), (c)-(iv), (d)-(i)

D. (a)-(iii), (b)-(iv), (c)-(i), (d)-(ii)

Q32. Following statements are related to security information and event management (SIEM). Identify the correct statement.

I. SIEM helps in the consolidation of multiple data points, custom dashboards, alert workflow management, and integration with other products**.**

II. SIEM provides security teams with both insight into and a record of the events taking place in an IT environment.

III. SIEM software analyses events against rules and analytics engines and indexes them for search in milliseconds.

IV. SIEM is a platform for detecting, analyzing, and responding to security threats of the next generation.

Choose the correct answer from options given:-

(a) Statement I, II and III are correct.

(b) Statement I, II and IV are correct.

(c) Statement III and IV are correct

(d) All of above statement are correct.

Q33. What was the major difference between e-RUPI and UPI?

i. e-RUPI vouchers can be redeemed at service providers' counters, whereas UPI is used for receipt or payment of money

ii. UPI is a one-time cashless and contactless payment mechanism, whereas e-RUPI is an application used for receipt or payment of money.

iii. The Reserve Bank of India operates e-RUPI, whereas the National Payments Corporation of India operates UPI.

Choose the correct answer from the options given below

(a) Only i and ii

(b) Only ii and iii

(c) Only i and iii

(d) All of the above

Q34. Fintech or Financial technology refers to the use of technology to deliver financial solutions. It includes both established financial institutions and technologically enabled financial innovations such as start-ups and big techs. Identify the correct statements related to Fintech.

I. Fintech simplifies financial transactions for consumers or businesses, making them more accessible and affordable

II. Fintech products and services are currently in use, which include peer-to-peer (P2P) lending platforms, crowdfunding, blockchain technology

III. Fintech has four elements i.e., start-ups, technology firms, customers, and traditional financial institutions like banks

IV. Fintech can alter the financial services and financial inclusion landscape fundamentally.

Choose the correct answer from options given

(a) Only I, II and IV

(b) Only I, II and III

(c) Only III and IV

(d) All of the above

Q35. Match list I with list II

List-I	**List-II**
a. e-RUPI	i. It is a technology refers to the use of technology to deliver financial solutions.
b. Fintech	ii. technology offers technological solutions that assist financial supervisory authorities in managing regulatory compliance.
c. Regtech	iii. It is a seamless one-time payment mechanism that can be redeemed by beneficiaries at merchants without using a digital payment app, card, or Internet banking
d. Suptech	iv. It refers to technological solutions that streamline and improve regulatory processes.

Choose the correct answer from options given

A. (a)-(iii),(b)-(i), (c)-(iv),(d)-(ii)

B. (a)-(iii), (b)-(iv), (c)-(i), (d)-(ii)

C. (a)-(iii), (b)-(ii), (c)-(iv), (d)-(i)

D. (a)-(iii), (b)-(iv), (c)-(ii), (d)-(i)

Q36. Management Information Systems (MIS) are computer-based information systems that transform data into meaningful information for managerial decision-making. Identify the correct regarding MIS from the following statement.

i. MIS places emphasis on the availability and timeliness of data and information.

ii. It helps in analysing customer data and assists management in making decisions scientifically in areas such as marketing and product development.

iii. It transforms data into meaningful information for decision-making.

Choose the correct answer from options given

(a) Only i and iii

(b) Only ii and iii

(c) Only i, and ii

(d) All of the above

Q37. In relation with open banking. Which of the following statement is not correct.

i. It is also known as "open customer data" and is driven by networks instead of centralization.

ii. It allows consumers to obtain a more accurate picture of their personal financial situation before taking on debt

iii. Open banking is driven by CMIs that allow third-party providers to use shared data from banks and other financial organizations

iv. It can provide consumers, financial institutions, and third-party service providers with open access to banking, transactional, and other financial data.

Choose the correct answer from options given

(a) Only I and IV

(b) Only I, II and III

(c) Only I and III

(d) All of the above

Q38. Which of the following are the stakeholders in an e-RUPI Ecosystem?

i. Bank who shall initiate the request to create e-RUPI.

ii. Corporate, State, and Union Government department, a business customer of the Bank who shall request the Bank to create e-RUPIs.

iii. Person for whom the e-RUPI is issued, who may not be a bank account holder.

iv. Specific voucher acceptance points where e-RUPI can be redeemed/used.

v. Bank provides facility/capability to the designated merchants to accept the e-RUPI (String/QR) for redemption.

Choose the correct answer from options given

(a) Only I and II

(b) Only II and III

(c) Only I, IV and V

(d) All of the above.

Solution

S1. Ans.(d)

Sol. The concept of Bank Computerisation practically started during 1980-81. In the year 1983, a committee was set up under the chairmanship of the then Deputy Governor of RBI, Dr. C. Rangarajan, to study the possibilities and stages involved in bank computerisation and prepare guidelines for the same. The Report submitted by the committee in the year 1984 was known as First Rangarajan Committee Report on bank mechanisation. Subsequent to that, computerisation in Banks gained momentum in the year 1983-84. Another Committee was constituted in the year 1988 under the chairmanship of Dr. C. Rangarajan to draw up a perspective plan on the computerisation of banks for a five-year period 1990–94.

S2. Ans.(b)

Sol. A LAN is a computer network that connects computers, network devices, and peripherals within a localized area, such as a building. LAN uses network adapters that employ special techniques to share a common medium between connected nodes. The distance and the number of nodes supported in a LAN depend on the medium used to establish the network. However, LAN will not extend beyond 100 meters for Cat5e cables.

S3. Ans.(d)

Sol. CBS performs the functions of customer accounts management, office account management, loan disbursal and management, and generation of reports, multi-currency balance sheets, and P&L statements. CBS does not perform email management. It performs customer relationship management (CRM) activities, which help in managing customer interactions and relationships.

S4. Ans.(d)

Sol. To safeguard the assets and the computer system and to maintain data integrity, the following should be ensured:

(a) The security policy addresses specific capabilities of operating systems and ensures that the available security features are implemented.

(b) The Chief information security officer should ensure that available features have been implemented.

(c) Process for granting access levels.

(d) Users should have the minimum access level needed to do their job.
(e) Users' access should be restricted to specific applications, menus within applications, files, and Servers.
(f) File maintenance should be a separate access privilege.
(g) Maintenance should be restricted to a minimum number of persons, and it should be properly approved and reviewed.
(h) The password file should be encrypted.
(i) Methods to detect security violations.
(j) Access levels should be periodically reviewed by the internal auditor.

S5. Ans.(d)
Sol. ATMs offer various services such as cash withdrawal, balance enquiry, statement enquiry, PIN change, cash deposit, cheque deposit, funds transfer, credit card payment, utility bill payment, cheque book request, insurance premium payment, recharge/top-up of mobile, DTH, etc., term deposit opening, user details updation, and Aadhaar updation.

S6. Ans.(b)
Sol. The cardholder has the option to pay the entire amount as soon as the card account is debited or pay only a certain percentage of the amount debited and pay the rest in monthly installments later. Hence Option C is incorrect as the cardholder can pay the amount in monthly installments. Option D is incorrect as a service fee is charged on the amount if the payment is deferred.

S7. Ans.(b)
Sol. They are not affected by electromagnetic interference and provide high-quality transmission of signals at very high speeds. Optical fibre has been a technological breakthrough in communication technology. It supports a data rate of 2 gigabits/sec. Fibre optics provide high-quality (low error rate) transmission of signals at very high speeds. The fibre optics transmissions are not affected by electromagnetic interference. The data transfer is through very thin glass or plastic fibres with a beam of light.

S8. Ans.(a)
Sol. A payment system through which payment orders by a bank can be transmitted to the bank to which the order is addressed. The definition of EFT as per the Uniform Commercial Code (UCC) of the USA is a payment system through which payment orders by a bank may be transmitted to the bank to which the order is addressed. This definition includes wire transfer networks, automated clearinghouses, and other communication systems of clearinghouses or other associations of banks.

S9. Ans.(b)
Sol. In India, NEFT (National Electronic Funds Transfer), RTGS (Real-time Gross Settlement), IMPS (Immediate Payment Service), UPI (Unified Payments Interface), ATMs, POS (Point of Sale), NACH (National Automated Clearing House), Cheque Truncation System (CTS) are some important facilitators of EFT. Fedwire is primarily used for processing interbank payments in the USA and is not used as a facilitator of EFT in India.

S10. Ans.(b)
Sol. IMPS or Immediate Payment Service is the electronic clearing system in India that allows instant fund transfer 24x7. The other options such as ECS, RTGS, and UPI may have certain limitations on timings or minimum transaction amounts.

S11. Ans.(a)

Sol. The passage clearly states that Indian banks have been investing in digital technologies for the past few years and broadband internet becoming more affordable has enabled banks to rollout many banking services through mobile and internet banking. However, the passage does not state that implementing new technologies is always inexpensive for banks or that banks no longer use demographic-based clusters to target customers.

S12. Ans.(b)

Sol. Banks use the net to offer Internet banking services, including routine transactions such as balance enquiry, transfer between accounts, and bill payments. This is one of the most important areas in which banks are using online delivery to serve their customers.

S13. Ans.(d)

Sol. Data is a critical resource necessary for an organization's continuing operations. Incorrect data can have serious implications for decision-making, and the potential impact of erroneous data can result in playing havoc with an organization's business. Inadequate control over data is the single largest factor that promotes the scope of fraud. Therefore, all of the above statements are correct.

S14. Ans.(b)

Sol. Fraudulent transactions can be carried out by manipulating computerized records in various ways. Unscrupulous individuals can use special programs like utility programs that bypass the validation controls built into the system to make unauthorized changes to records. They can also bypass security controls and manipulate important files. Additionally, unauthorised amendments can be made to payment instructions prior to their entry into the computer system. Therefore, options A and B are the correct statements.

S15. Ans.(d)

Sol. The causes that facilitate computer fraud are inadequate control over data/media, easy access mechanism of systems, and inadequate control over outputs. Without proper control over data/media, fraudsters can easily manipulate records and transactions to their advantage. Additionally, if systems have easy access mechanisms, it becomes easier for unscrupulous individuals to bypass security controls and make fraudulent transactions. Moreover, if there are inadequate controls over outputs, it becomes difficult to detect or prevent fraudulent transactions.

S16. Ans.(d)

Sol. Administrative controls for customer accounting can include defining responsibilities, formal policies and procedures, as well as implementing specific transactional controls. These transactional controls include validating transactions against limits and balances and ensuring authorization before processing, validating stop payments, post-dated cheques, stale cheques, and cheques with invalid dates, and verifying sensitive parameters like due dates, maximum/minimum days allowed, maximum/minimum rates, drawing limits, stop instructions, etc.

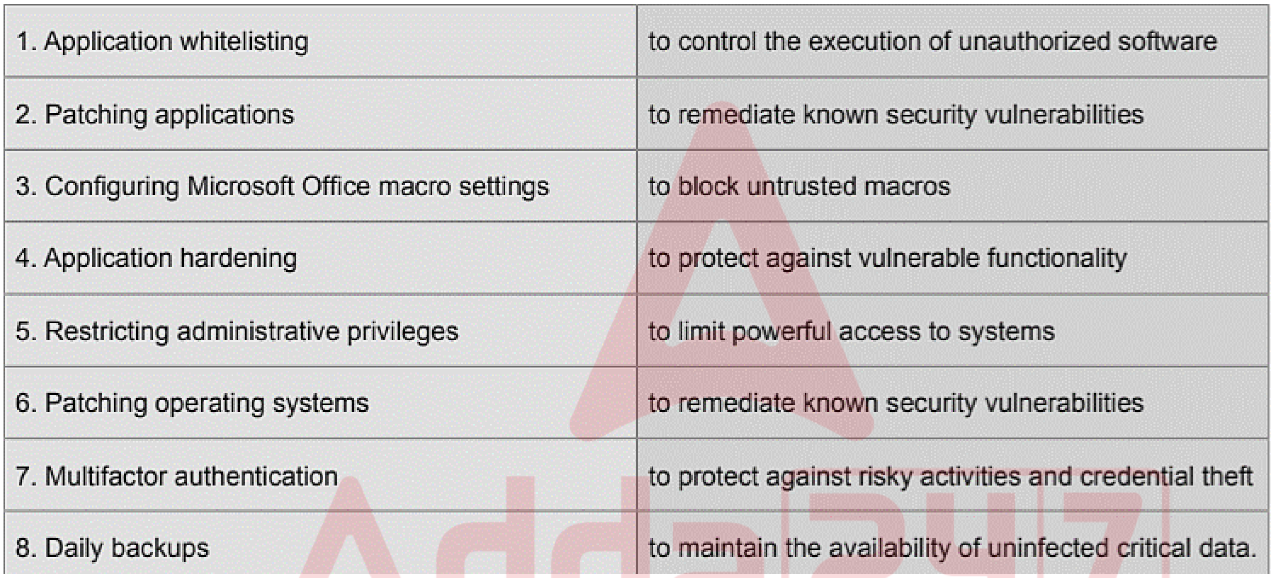
S17. Ans.(a)

Sol. The following are the risks that can arise from cyber-attacks.

- Financial loss
- Critical Data loss/breach,
- loss of productivity due to business disruption,
- Cost of investigation,
- Compensation to customers
- Reputational damage
- Regulatory penalties.
- Costs of recovering from disruptions
- Investment loss.

S18. Ans.(b)

Sol. Essential mitigation strategies for business continuity:



1. Application whitelisting	to control the execution of unauthorized software
2. Patching applications	to remediate known security vulnerabilities
3. Configuring Microsoft Office macro settings	to block untrusted macros
4. Application hardening	to protect against vulnerable functionality
5. Restricting administrative privileges	to limit powerful access to systems
6. Patching operating systems	to remediate known security vulnerabilities
7. Multifactor authentication	to protect against risky activities and credential theft
8. Daily backups	to maintain the availability of uninfected critical data.

S19. Ans.(b)

Sol. Technologies currently being **developed and tested range from a new generation of more sophisticated EMV and NFC cards to providing services through mobiles, wearables, and social media networks.** Cryptocurrencies and alternative forms of e-cash are emerging, which do not require a traditional paper-oriented payments system by using technologies that enable such smart cards to transfer value through the Internet.

Advancements in technology and shifts in consumer preferences driven by SMAC (social media, mobility, analytics, cloud computing) **have brought on opportunities and challenges in terms of utility/efficiency, product complexity, and deployment architecture**.

Information technology has brought significant changes in the banking industry, leading to increased efficiency, innovation, and effective delivery systems. **The new generation of tech-savvy personnel is being recruited by banks to leverage their skills in technology for maximizing productivity and excellence in customer service.**

Hence, Statement I, III and IV are correct.

S20. Ans.(c)

Sol. Following are the feature of chatbots: -

- Chatbots are software applications that simulate conversations with real people through written or spoken human speech.
- They can be deployed for customer service, as standalone applications, or on a website.
- Chatbots are driven by artificial intelligence, voice recognition, and natural language processing.
- Some real-life examples of chatbots are virtual assistants such as Google Now, Apple's Siri, and Microsoft's Cortana.
- There are some challenges in the ability of chatbots to parse human speech having inherent complexities in elements of speech such as metaphors and similes.
- Despite these limitations, chatbots are becoming increasingly sophisticated, responsive, and more natural.

S21. Ans.(a)

Sol. Differences between Digital Currency and Cryptocurrency

Although cryptocurrency is a type of digital currency, there are some key differences between the two, including:

1. ***Structure:*** Digital currencies are centralized, while cryptocurrencies are decentralized.
2. ***Anonymity:*** Digital currencies require the user to be identified, while cryptocurrencies are partially anonymous, protecting the identity.
3. ***Transparency:*** Digital currencies are not transparent, while cryptocurrencies are transparent, as all the revenue streams are placed in a public chain.
4. ***Legal aspects:*** Many countries have legal frameworks for digital currencies, while cryptocurrencies have yet to be defined officially in many countries.

Thus, only options I and IV are true.

S22. Ans.(d)

Sol. Robotic Process Automation (RPA) – It is a technology that uses software robots or bots to automate repetitive and rule-based tasks typically performed by humans

- RPA is the practice of automating routine business practices with software robots.
- RPA uses artificial intelligence to build software robots that automate tasks that once required human intervention.
- RPA is often applied to repetitive and mundane tasks so that employees can focus on more complex banking operations that require human interaction and decision-making.
- Some major advantages of RPA are 24x7 working without fatigue, time and cost savings, zero typos or copy/paste mistakes, and compliance.
- Banks can build a Virtual Workforce by adopting RPA integrated with artificial intelligence to automate processes through the deployment of custom applications.
- RPA is being used in banking activities like KYC, customer onboarding, loan origination, etc.

S23. Ans.(a)

Sol.

1. **Artificial Intelligence (AI)**
   - AI is an area of computer science that emphasizes the creation of intelligent machines and software that work and react like humans.
   - AI has the potential to transform customer experiences and establish entirely new business models in banking.
   - Key components of AI are machine learning, computer vision, natural language progression, and natural language generation.

2. **Robotic Process Automation (RPA)**
   - RPA is the practice of automating routine business practices with software robots.
   - RPA uses artificial intelligence to build software robots that automate tasks that once required human intervention.
   - RPA is often applied to repetitive and mundane tasks so that employees can focus on more complex banking operations that require human interaction and decision-making.
3. **Chatbots**
   - Chatbots are software applications that simulate conversations with real people through written or spoken human speech.
   - They can be deployed for customer service, as standalone applications, or on a website.
   - Chatbots are driven by artificial intelligence, voice recognition, and natural language processing.
4. **Blockchain Technology**
   - Blockchain is a distributed ledger technology (DLT) that stores groups of transactions known as “blocks” and then links and sequences the list of transactions using cryptography
   - Blockchain technology can be used in banking activities like secure document management, reporting, payments, treasury & securities, and trade finance.

S24. Ans.(a)

Sol. INFORMATION SYSTEM AUDIT (IS AUDIT)

The use of technology in accounting has transformed the way financial transactions are conducted, particularly in the banking industry where the majority of transactions take place. **The automation of manual processes has resulted in significant improvements in efficiency, speed, and cost-effectiveness, while also reducing the likelihood of fraudulent activities.**

Objective: -

- **The objective of an audit does not change depending on whether it is a manual or a computerized environment, and only the approach of the audit changes.**
- IS audit is a process of collecting and evaluating evidence to determine whether a computer system could safeguard its assets (hardware, software, and data) by adopting adequate security and control measures, maintaining data integrity, achieving the goals of an organization effectively, and resulting in the efficient use of resources.
- Control is defined as a system that prevents, detects, or corrects undesirable events.

Benefits of IS Audit

- IS audit assesses the strengths and weaknesses of an information system.
- It also assesses if an information system translates itself into an effective tool to meet business goals.
- Security features and controls in computerized information systems could be improved based on the suggestions made during the course of an IS audit.

S25. Ans.(c)

Sol. Phishing: Phishing emails are sent in large batches, often with a generic greeting from a bank. **The email might contain a forged link that leads to a fake website or a message that shows a sense of urgency to get personal information.** The intention is to trick the recipient into providing personal information, such as account number, card number, PIN, etc. Here are some precautions to take:

Vishing: Vishing is a phone-based version of phishing where the scammer calls and asks for personal details**. They might claim to be updating their customer database, and threaten to suspend the account if the details are not provided. Here are some precautions to take**

Smishing: Smishing is similar to phishing, but it uses text messages instead of email. **The text might contain an URL or phone number and usually asks for immediate attention. Here are some precautions to take:**

S26. Ans.(c)

Sol. The modus operandi of cyber fraud comprises the following steps:

1. **Reconnaissance and Compromise**
   Criminals conduct research and gather information about the target organization during the early reconnaissance period. They search for IP addresses and domain names, check for security holes in the network, and use phishing emails to find the email addresses of high-ranking members of an organization or weak employees. The attackers patiently wait for months to complete these tasks.
2. **Obtain Credentials**
   After gaining access to the network, hackers aim to gain further access privileges to penetrate the network. Attackers can gain administrator-level access by using numerous tools that assist them in stealing credentials.
3. **Send Fraudulent Messages**
   Attackers can implant malware into vital systems and submit fraudulent payment instructions using a fake operator or approver.
4. **Hide/Cover Up Evidence**
   Attackers must destroy proof of their operations to hide their conduct after fraudulent payments have been made. They use a variety of tools and strategies to remove or change records, as well as corrupt systems, to confound forensic investigators.

S27. Ans.(c)

Sol. Cybersecurity Awareness

- Cybersecurity knowledge should be relevant to each employee's position
- Developing a cybersecurity awareness program requires delivering the right training to each team
- Identity theft and network hacks happen when employees unintentionally download malicious code or click dubious links
- Social engineering like phishing is the most common cause of Cybercrime
- Data breach costs have significantly increased
- Firms with strong cybersecurity cultures are better equipped to identify and respond to potential threats, reduce cyber incidents, and improve their ability to recover from a cyber attack
- Comprehensive, hands-on training may help employees become more aware of potential hazards
- Effective cybersecurity training can establish excellent cybersecurity hygiene

S28. Ans.(b)

Sol. Ransomware*:* A type of malicious software that blocks access to a victim's data or threatens to publish it unless a ransom is paid.

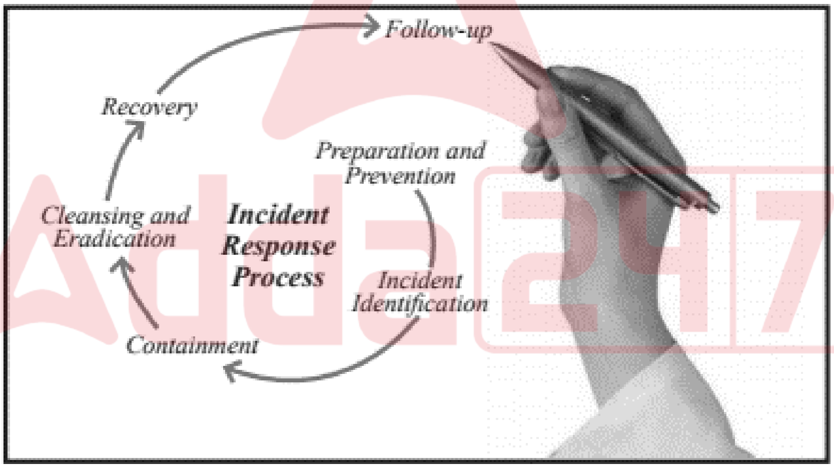
Malware: Malicious software code that intruders use to deceive individuals into believing that traditional security is protecting them during online banking transactions.

Viruses*:* Malicious software programs that harm computers by stealing user credentials, destroying data, or performing other malicious actions.

S29. Ans.(b)

Sol. In response to the increasing number of cyber-attacks, banks must develop a robust Cyber Incident Response (CIR) plan consisting of both proactive and responsive capabilities to stay ahead of the cybersecurity curve

1. ***Preparation:*** Banks must prepare for potential cyber incidents by identifying their critical assets, creating an incident response team, and developing an incident response plan.
2. ***Detection:*** Banks must have monitoring capabilities to detect potential cyber incidents as early as possible to minimize damage.
3. ***Analysis:*** Banks must have the ability to quickly analyze the incident and determine its scope and severity
4. ***Containment:*** Banks must contain the incident by isolating the affected systems and preventing the attacker from further infiltrating the network.
5. ***Eradication:*** Banks must eliminate the attacker's presence from the network, ensuring that all malware and other malicious code are removed.
6. ***Recovery:*** Banks must restore their systems and data to their pre-incident state and resume normal operations as quickly as possible


Follow-up
Recovery
Preparation and Prevention
Cleansing and Eradication
Incident Response Process
Incident Identification
Containment

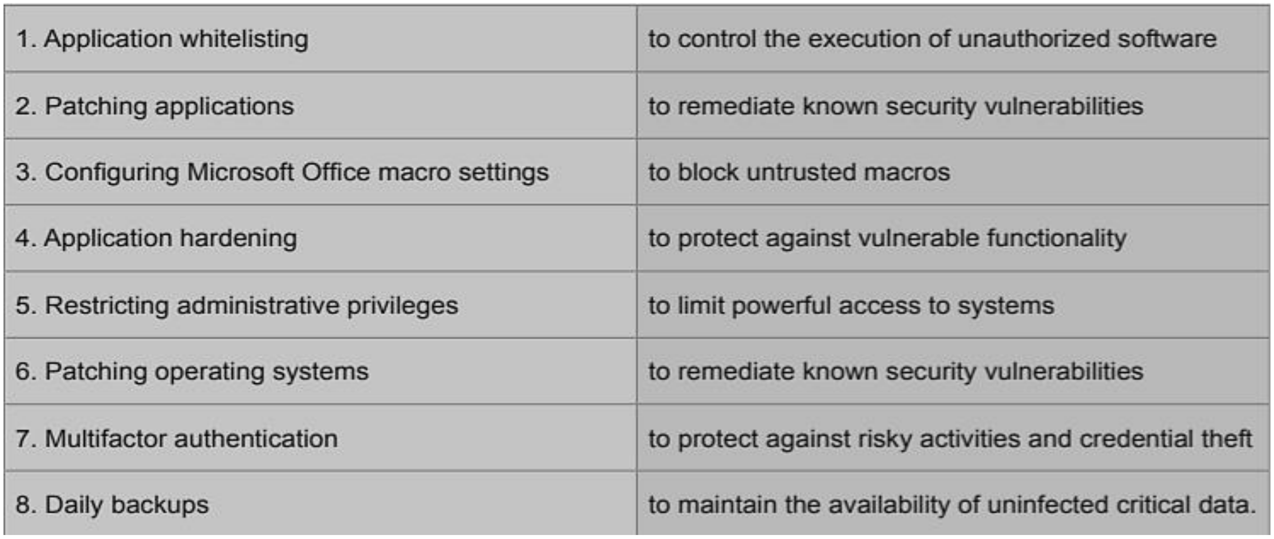
S30. Ans.(b)

Sol. Network Behaviour Anomaly Detection (NBAD)

- NBAD provides one approach to network security threat detection.
- It is a **complementary technology** to systems that detect security threats based on packet signatures.
- NBAD-based systems are particularly helpful in detecting security threat vectors in two instances where signature-based systems cannot.
- An NBAD program tracks critical network characteristics in real-time and generates an alarm if a strange event or trend is detected that could indicate the presence of a threat.
- NBAD technology/techniques are **applied in a number of network and security monitoring domains including log analysis, packet inspection systems, flow monitoring systems, and route analytics.**

S31. Ans.(a)

Sol. Essential Mitigation Strategies for Business Continuity.



1. Application whitelisting	to control the execution of unauthorized software
2. Patching applications	to remediate known security vulnerabilities
3. Configuring Microsoft Office macro settings	to block untrusted macros
4. Application hardening	to protect against vulnerable functionality
5. Restricting administrative privileges	to limit powerful access to systems
6. Patching operating systems	to remediate known security vulnerabilities
7. Multifactor authentication	to protect against risky activities and credential theft
8. Daily backups	to maintain the availability of uninfected critical data.

S32. Ans.(d)

Sol. Security Information and Event Management (SIEM)

- A platform for detecting, analyzing, and responding to security threats of the next generation.
- SIEM software analyses events against rules and analytics engines and indexes them for search in milliseconds.
- Consolidation of multiple data points, custom dashboards, and alert workflow management, and integration with other products.
- Provides security teams with both insight into and a record of the events taking place in an IT environment

Hence, All the statements are correct.

S33. Ans.(c)

Sol. Difference between e-RUPI and UPI

- e-RUPI is a one-time cashless and contactless payment mechanism, whereas UPI is an application used for receipt or payment of money.
- The Reserve Bank of India operates e-RUPI, whereas the National Payments Corporation of India operates UPI.
- e-RUPI vouchers can be redeemed at service providers' counters, whereas UPI is used for receipt or payment of money.

S34. Ans.(a)

Sol. Fintech or Financial technology refers to the use of technology to deliver financial solutions. It includes both established financial institutions and technologically enabled financial innovations such as start-ups and big techs. Fintech aims to improve and automate the delivery and utilization of financial services.

I. Elements of Fintech Ecosystem

The Fintech ecosystem (FE) consists of five elements that synergize to stimulate the economy, enhance customer experience, and promote social inclusion. These elements include start-ups, technology firms, government, customers, and traditional financial institutions like banks.

II. Fintech Products and Services

Fintech products and services are currently in use, which include peer-to-peer (P2P) lending platforms, crowdfunding, blockchain technology, distributed ledger technology, big data, smart contracts, Robo advisors, E-aggregators, and others. These products and services are used to connect lenders and borrowers, information seekers, and providers, with or without a nodal intermediation agency.

III. Impact of Fintech on the Financial Landscape

Fintech can alter the financial services and financial inclusion landscape fundamentally. It can contribute to the creation of a new financial system that is more inclusive, cost-effective, and robust by enabling innovations and controlling risks. The Fintech movement can transform the financial landscape, allowing consumers to choose from a broader range of options at competitive prices while also allowing financial institutions to improve efficiency through lower operational costs.

IV. Benefits of Fintech

Fintech simplifies financial transactions for consumers or businesses, making them more accessible and affordable. It can lower costs while also improving access and quality of financial services. Technological advancements fundamentally alter people's access to financial services and increase financial inclusion. Fintech products and services offer several benefits for Banks, such as:

S35. Ans.(a)

Sol. e-RUPI

e-RUPI is an innovative digital payment solution launched on 2nd August 2021 by the National Payments Corporation of India (NPCI). It is a seamless one-time payment mechanism that can be redeemed by beneficiaries at merchants without using a digital payment app, card, or Internet banking.

FinTech

Fintech or Financial technology refers to the use of technology to deliver financial solutions. It includes both established financial institutions and technologically enabled financial innovations such as start-ups and big techs. Fintech aims to improve and automate the delivery and utilization of financial services.

RegTech

RegTech or regulatory technology refers to technological solutions that streamline and improve regulatory processes. RegTech is a technology system that assists a bank or any financial institution in managing regulatory compliance. RegTech products are available in a wide range of shapes and sizes.

SupTech

SupTech or supervisory technology offers technological solutions that assist financial supervisory authorities in managing regulatory compliance. Supervisory agencies manage risk in the financial sector and also implement regulations

S36. Ans.(d)

Sol. Management Information Systems (MIS)

Management Information Systems (MIS) are computer-based information systems that transform data into meaningful information for managerial decision-making. In the banking industry, MIS has become essential for efficient operations and decision-making.

Importance of MIS

- MIS places emphasis on the availability and timeliness of data and information.
- It transforms data into meaningful information for decision-making.
- It helps in analysing customer data and assists management in making decisions scientifically in areas such as marketing and product development.

S37. Ans.(c)

Sol. OPEN BANKING

- Open banking is a new form of innovation in the financial industry that enables third-party financial service providers to access consumer banking data from banks and non-bank financial organizations through APIs.
- It can provide consumers, financial institutions, and third-party service providers with open access to banking, transactional, and other financial data
- It is also known as "open bank data" and is driven by networks instead of centralization.
- Open banking is driven by APIs that allow third-party providers to use shared data from banks and other financial organizations.
- Open banking is a major driver of innovation and change in the banking business. It allows consumers to obtain a more accurate picture of their personal financial situation before taking on debt.

S38. Ans.(d)

Sol. Stakeholders in an e-RUPI Ecosystem

1) **Issuer Bank (Issuer):** Bank who shall initiate the request to create e-RUPI.
2) Sponsor: Corporate, State, and Union Government department, a business customer of the Bank who shall request the Bank to create e-RUPIs.
3) **e-RUPI beneficiary:** Person for whom the e-RUPI is issued, who may not be a bank account holder.
4) **Designated Merchant:** Specific voucher acceptance points where e-RUPI can be redeemed/used.
5) **Acquiring Bank (Acquirer):** Bank provides facility/capability to the designated merchants to accept the e-RUPI (String/QR) for redemption.