



CAIIB CRASH COURSE

JUNE 2025

ABM



MODULE D SPECIAL MCQS



23 MAY 2025



08:00 PM



KIRTI Ma'am
Coupon Code- **KRT23**

1. Under the RBI guidelines, which of the following is a responsibility of the Chief Vigilance Officer (CVO) in private sector and foreign banks?

- (a) Monitoring employee performance**
- (b) Developing marketing strategies**
- (c) Conducting internal audits**
- (d) Implementing anti-fraud measures**



[Jaiib.caiib](https://www.instagram.com/jaiib.caiib/)



JAIIB CAIIB

Baba



Telegram - @caiib_group

According to the RBI guidelines, the Chief Vigilance Officer (CVO) in private sector and foreign banks is responsible for implementing anti-fraud measures.

The CVO plays a crucial role in overseeing and coordinating the bank's efforts to prevent, detect, and investigate fraudulent activities within the organization.

They work closely with various departments to develop and implement effective measures to safeguard the bank's assets and maintain integrity in banking operations.



[Jaiib.caiib](https://www.instagram.com/jaiib.caiib/)



JAIIB CAIIB

Baba



Telegram - @caiib_group



2. According to the _____ Act, companies are required to disclose their financial statements to the public.

- (a) Companies Act, 2013
- (b) Banking Regulation Act, 1949
- (c) Income Tax Act, 1961
- (d) Securities and Exchange Board of India (SEBI) Act, 1992



Jaiib.caiib



JAIIB CAIIB
Baba



Telegram - @caiib_group



3. As per the _____ guidelines, banks are required to disclose information about their non-performing assets (NPAs) and provisioning policies.

- (a) Basel III
- (b) Reserve Bank of India (RBI)
- (c) Indian Banks' Association (IBA)
- (d) National Stock Exchange (NSE)



[Jaiib.caiib](https://www.instagram.com/jaiib.caiib/)



JAIIB CAIIB

Baba



Telegram - [@caiib_group](https://t.me/caiib_group)



4. What is the purpose of a Compliance Policy in an organization?

- (a) To facilitate tax evasion and unethical practices.
- (b) To restrict business operations and hinder growth.
- (c) To ensure adherence to laws, regulations, and internal policies.
- (d) To bypass regulatory authorities and gain unfair advantages.



Jaiib.caiib



JAIIB CAIIB

Baba



Telegram - @caiib_group

- The purpose of a Compliance Policy in an organization is to ensure adherence to laws, regulations, and internal policies.
- It serves as a framework that guides employees and the organization as a whole in conducting business ethically and within the boundaries set by regulatory authorities.
- A Compliance Policy helps prevent legal and reputational risks, ensures transparency, and promotes trust with stakeholders.



[Jaiib.caiib](https://www.instagram.com/jaiib.caiib/)



JAIIB CAIIB

Baba



Telegram - [@caiib_group](https://t.me/caiib_group)



5. Which of the following activities is within the scope of the compliance function?

- (a) Developing marketing campaigns and strategies.
- (b) Conducting background checks on potential employees.
- (c) Setting sales targets and monitoring sales performance.
- (d) Ensuring data privacy and protection.



Jaiib.caiib



JAIIB CAIIB
Baba



Telegram - @caiib_group



- The compliance function is responsible for ensuring that the organization adheres to relevant laws and regulations, including data privacy and protection requirements.
- This involves implementing safeguards, policies, and procedures to safeguard sensitive information, ensuring compliance with data protection laws, and addressing data breaches or incidents.
- While marketing, employee background checks, and sales monitoring are important activities within an organization, they do not typically fall within the scope of the compliance function.



6. ABC Bank has recently implemented a new compliance policy to ensure adherence to anti-money laundering (AML) regulations. The policy requires the bank's employees to conduct enhanced due diligence (EDD) for high-risk customers. However, one of the relationship managers, Mr. Sharma, is not fully aware of the new policy and continues to onboard high-risk customers without performing EDD. What action should the bank take to address this situation?

- (a) Issue a verbal warning to Mr. Sharma and provide him with training on the new compliance policy.
- (b) Temporarily suspend Mr. Sharma's responsibilities and assign him a different role within the bank.
- (c) Terminate Mr. Sharma's employment due to non-compliance with the bank's policy.
- (d) Ignore the issue since Mr. Sharma is a seasoned employee and has a good track record.



7. Which of the following is an essential component of the Compliance Structure at the Corporate Office?

- (a) Compliance Committee
- (b) Compliance Officer
- (c) Compliance Manual
- (d) Compliance Training Program



- **The Compliance Committee is an essential component of the Compliance Structure at the Corporate Office.**
- **The committee consists of key stakeholders, such as senior management representatives and subject matter experts.**
- **Its primary responsibility is to oversee and guide the organization's compliance efforts.**
- **The Compliance Committee ensures the effective implementation of compliance policies, reviews compliance reports, and provides guidance on emerging regulatory requirements.**



8. A bank has recently experienced a significant increase in fraudulent transactions conducted through its online banking platform. On further investigation, it was discovered that the bank's internal control system did not have appropriate authentication measures in place, allowing unauthorized individuals to gain access to customer accounts. This situation highlights the importance of:

- (a) Risk assessment
- (b) Information security policies
- (c) Internal control monitoring
- (d) Training and awareness programs



- **Information security policies define the rules and procedures for protecting sensitive data and ensuring the secure operation of systems.**
- **In this case, the lack of appropriate authentication measures in the bank's internal control system allowed unauthorized individuals to access customer accounts and conduct fraudulent transactions.**
- **By implementing robust information security policies, including secure authentication methods, the bank could have mitigated the risk of unauthorized access and fraudulent activities..**



9. Statement I: The Operations Department is responsible for overseeing the production and delivery of goods or services.

Statement II: The Research and Development Department is responsible for conducting market research and developing new products or technologies.

Statement III: The Legal Department is responsible for ensuring compliance with laws and regulations.

- (a) Only statement I is correct.**
- (b) Only statements II and III are correct.**
- (c) Only statements I and III are correct.**
- (d) All statements are correct.**



10. Which of the following strategies is effective in reducing control risk?

- (a) Increasing the complexity of control procedures to minimize errors.
- (b) Implementing segregation of duties to ensure checks and balances.
- (c) Reducing the frequency of internal audits to save costs.
- (d) Relying solely on automated controls for transaction processing.



- **Segregation of duties is an important internal control principle that involves dividing responsibilities for key functions among different individuals to reduce the risk of errors or fraud going undetected.**
- **By implementing segregation of duties, organizations create checks and balances in their operations, ensuring that no single individual has complete control over a transaction from initiation to completion.**
- **This reduces the likelihood of errors or fraudulent activities occurring without detection. Therefore, option (b) is the correct answer as it describes an effective strategy for reducing control risk.**



11. Which of the following is a key benefit of implementing a robust loan review mechanism or credit audit?

- (a) Increase in loan delinquency rates
- (b) Decrease in non-performing assets (NPAs)
- (c) Reduction in loan origination process time
- (d) Higher profitability through aggressive lending practices



- **Implementing a robust loan review mechanism or credit audit helps in decreasing non-performing assets (NPAs).**
- **NPAs are loans or advances that have stopped generating interest income or principal repayment due to default or non-payment by the borrower.**
- **A thorough credit audit process helps identify potential risks and weaknesses in the loan portfolio, allowing timely remedial actions to be taken, such as restructuring or recovery efforts, thus reducing NPAs.**
- **Increasing loan delinquency rates, reducing loan origination process time, and pursuing aggressive lending practices may have negative consequences, such as higher credit risk and a potential increase in NPAs.**
-



12. Compliance risk arises due to _____ of regulatory and legal requirements and _____ by the organization.

- (a) non-compliance, misinterpretation**
- (b) compliance, violations**
- (c) violations, misinterpretation**
- (d) non-compliance, adherence**



13. Statement I: Credit audit involves a detailed examination of the credit approval process, credit monitoring, and recovery mechanisms of a financial institution.

Statement II: The objective of credit audit is to ensure compliance with regulatory guidelines and internal credit policies.

Statement III: Credit audit primarily focuses on evaluating the profitability and financial performance of the borrowers.

- (a) Only statements I and II are correct.**
- (b) Only statements I and III are correct.**
- (c) Only statements II and III are correct.**
- (d) All statements I, II, and III are correct.**



14. PQR Bank has implemented stringent measures to prevent money laundering and comply with anti-money laundering regulations. As an AML officer, you have identified a suspicious transaction in which a customer is involved. What should be your immediate action?

- (a) Freeze the customer's account and initiate an internal investigation.**
- (b) Inform the customer about the suspicious transaction and request an explanation.**
- (c) Report the suspicious transaction to the relevant regulatory authorities.**
- (d) Monitor the customer's account for further suspicious activities without taking immediate action.**



[Jaiib.caiib](https://www.instagram.com/jaiib.caiib/)



[JAIIB CAIIB](#)

Baba



[Telegram - @caiib_group](#)



- When a suspicious transaction is identified, immediate action is crucial to ensure good compliance with anti-money laundering regulations. Reporting the suspicious transaction to the relevant regulatory authorities is the appropriate course of action.
- These authorities have the expertise and jurisdiction to investigate such activities and take necessary legal actions, if required.
- By promptly reporting the suspicious transaction, the bank demonstrates its commitment to combating money laundering and cooperating with regulatory bodies.



15. In the GRC framework, risk _____ is the process of identifying, assessing, and prioritizing risks, while risk evaluation involves developing strategies to manage and mitigate those risks.

- (a) monitoring
- (b) assessment
- (c) identification
- (d) evaluation



[Jaiib.caiib](https://www.instagram.com/jaiib.caiib/)



[JAIIB CAIIB
Baba](https://www.youtube.com/@JAIIB-CAIIB-Baba)



[Telegram - @caiib_group](https://t.me/@caiib_group)



16. ABC Corporation, a manufacturing company, is considering implementing an integrated GRC approach. They are evaluating the potential benefits to justify the investment. Which of the following benefits is a strategic advantage of an integrated GRC approach?

- (a) Improved stakeholder confidence and reputation**
- (b) Cost savings through reduced insurance premiums**
- (c) Streamlined internal communication and collaboration**
- (d) Enhanced decision-making through data analytics**



- An integrated GRC approach provides several benefits, including improved stakeholder confidence and reputation (option a).
- By implementing effective governance, risk management, and compliance measures, organizations can demonstrate their commitment to ethical conduct, regulatory compliance, and overall sound business practices, thereby enhancing stakeholder confidence and reputation.
- While options b, c, and d are also potential benefits of an integrated GRC approach, they are more operational in nature.
- Cost savings through reduced insurance premiums (option b) can be achieved by effectively managing risks and demonstrating lower risk exposure.
- Streamlined internal communication and collaboration (option c) can enhance operational efficiency, and enhanced decision-making through data analytics (option d) can be facilitated by integrated GRC systems that provide access to relevant data and insights.



Jaiib.caiib



JAIIB CAIIB

Baba



Telegram - @caiib_group

17. LMN Corporation wants to establish a robust whistle-blower policy that encourages reporting of unethical practices and provides protection to whistle-blowers. Which of the following components should be included in the policy?

- (a) Establishing a dedicated whistle-blower committee to investigate reported cases.**
- (b) Penalizing whistle-blowers for reporting false allegations.**
- (c) Promising full confidentiality without any exceptions.**
- (d) Offering protection against retaliation for the whistle-blowers.**



- **A robust whistle-blower policy should include mechanisms for investigating reported cases.**
- **Establishing a dedicated whistle-blower committee ensures that reported cases are thoroughly examined and appropriate actions are taken.**
- **Penalizing whistle-blowers for reporting false allegations may discourage reporting and go against the spirit of protection.**
- **Promising full confidentiality without any exceptions is unrealistic as there may be circumstances where disclosure of identity becomes necessary for investigation or legal purposes.**
- **Lastly, offering protection against retaliation is crucial to encourage whistle-blowers to come forward without fear of adverse consequences.**



[Jaiib.caiib](https://www.instagram.com/jaiib.caiib/)



JAIIB CAIIB

Baba



Telegram - [@caiib_group](https://t.me/caiib_group)

18. ABC Non-Banking Financial Company (NBFC) has recently achieved significant growth and now falls under the purview of scale-based regulation. As per the transition path, which regulatory framework will ABC NBFC be subjected to?

- (a) Current regulatory framework**
- (b) Revised regulatory framework**
- (c) Scale-based regulatory framework**
- (d) No regulatory framework**



19. for the compliance function in NBFC-UL/ML, the compliance function should be independent and _____ from the operational and business _____.

- (a) distinct, functions
- (b) isolated, areas
- (c) separated, units
- (d) differentiated, divisions



20. Statement I: Non-Banking Financial Companies in the Upper Layer (NBFC-UL) and Middle Layer (NBFC-ML) are required to establish a compliance function.

Statement II: The compliance function in NBFC-UL and NBFC-ML should be independent and separate from other functions within the organization.

Statement III: The Chief Compliance Officer (CCO) is responsible for ensuring compliance with applicable laws, regulations, and internal policies in both NBFC-UL and NBFC-ML.

- (a) Only statement I is true.**
- (b) Only statements I and II are true.**
- (c) Only statements II and III are true.**
- (d) All statements are true.**



(a)Base Layer

- non-deposit taking NBFCs below the asset size of 1000 crore and
- NBFCs undertaking the following activities:
 - (i) NBFC-Peer to Peer Lending Platform (NBFC-P2P),
 - (ii) NBFC-Account Aggregator (NBFC-AA),
 - (iii) Non-Operative Financial Holding Company (NOFHC)
 - (iv) NBFCs not availing public funds and not having any customer interface.

(b) Middle Layer

- all deposit taking NBFCs (NBFC-Ds), irrespective of asset size,
- non-deposit taking NBFCs with asset size of 1000 crore and above and
- NBFCs undertaking the following activities
 - (i) Standalone Primary Dealers (SPDs),
 - (ii) Infrastructure Debt Fund - Non-Banking Financial Companies (IDF-NBFCs),
 - (iii) Core Investment Companies (CICs),
 - (iv) Housing Finance Companies (HFCs)
 - (v) Infrastructure Finance Companies (NBFC-IFCs).



Jaiib.caiib



JAIIB CAIIB

Baba



Telegram - @caiib_group

(c) Upper Layer

The Upper Layer comprises of those NBFCs which are specifically identified by the Reserve Bank as warranting enhanced regulatory requirement based on a set of parameters and scoring.

The top ten eligible NBFCs in terms of their asset size shall always reside in the upper layer, irrespective of any other factor.

Upper Layer shall be populated with NBFCs, identified by way of a parametric scoring methodology, comprising of quantitative and qualitative parameters/ supervisory judgment.

The quantitative and qualitative parameters shall have weightage of 70% and 30% respectively.

Scoring methodology for identification of an NBFC as NBFC-UL shall be based on the set of NBFCs fulfilling the following criteria:

- (a) Top 50 NBFCs (excluding top ten NBFCs based on asset size, which automatically fall in the Upper Layer) based on their total exposure including credit equivalent of off-balance sheet exposure.
- (b) NBFCs designated as NBFC-UL in the previous year.
- (c) NBFCs added to the set by supervisors using supervisory judgment.

(d) Top Layer

The Top Layer will ideally remain empty. This layer can get populated if the Reserve Bank is of the opinion that there is a substantial increase in the potential systemic risk from specific NBFCs in the Upper Layer. Such NBFCs shall move to the Top Layer from the Upper Layer.



Jaiib.caiib



JAIIB CAIIB

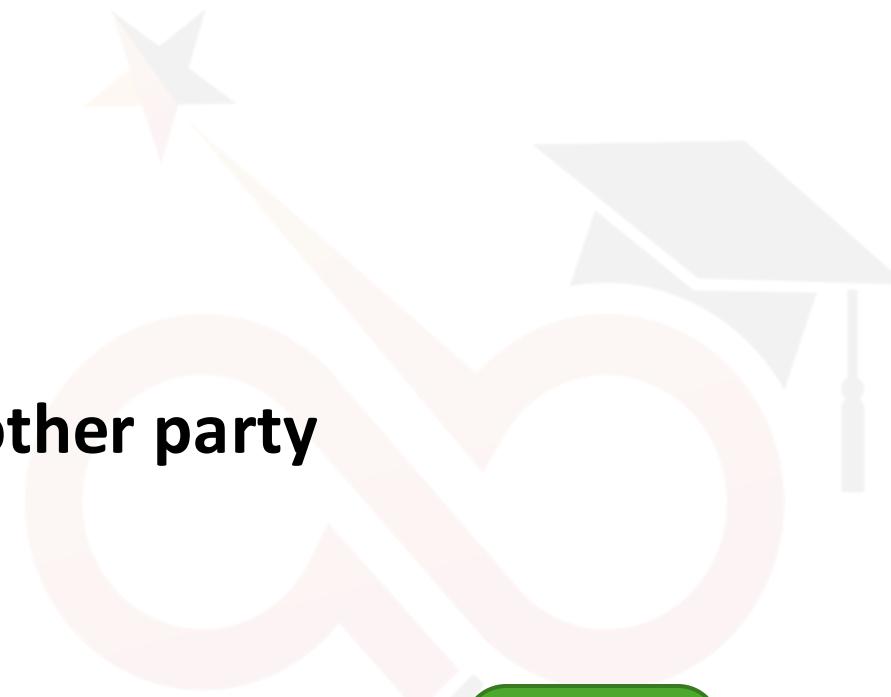
Baba



Telegram - @caiib_group

21. Which of the following elements is NOT typically present in the definition of fraud?

- (a) Intent**
- (b) Unintentional act**
- (c) Deception**
- (d) Financial loss to another party**



[Jaiib.caiib](https://www.instagram.com/jaiib.caiib/)



[JAIIB CAIIB](https://www.youtube.com/@JAIIB-CAIIB-Baba)

Baba



[Telegram - @caiib_group](https://t.me/@caiib_group)

22. Fraud is an _____ act or omission carried out by a person with the intent to deceive others and to _____ unfair advantages.

- (a) Unintentional, gain
- (b) Intentional, obtain
- (c) Accidental, acquire
- (d) Inadvertent, secure



Jaiib.caiib



JAIIB CAIIB

Baba



Telegram - @caiib_group

23. Which of the following best describes phishing in the context of cyber fraud in the banking sector?

- (a) Manipulating financial markets for personal gain**
- (b) Intercepting and altering communication between parties**
- (c) Using deceptive emails or websites to trick individuals into revealing sensitive information**
- (d) Exploiting software vulnerabilities to gain unauthorized access**



[Jaiib.caiib](https://www.instagram.com/jaiib.caiib/)



JAIIB CAIIB

Baba



Telegram - @caiib_group

24. Statement I: The Vigilance Officer in a bank is responsible for conducting investigations and initiating disciplinary action against employees involved in misconduct.

Statement II: Whistleblowers who report incidents of fraud or corruption in banks are protected under the Whistleblower Protection Act, 2011.

Statement III: The Reserve Bank of India (RBI) is responsible for appointing Vigilance Officers in all banks operating in India.

- (a) Only statement I is correct.**
- (b) Only statements II and III are correct.**
- (c) Only statements I and II are correct.**
- (d) All statements I, II, and III are correct.**



25. Statement I: Distributed denial of service (DDoS) attack is to overwhelm the resources of a target system and cause it to stop functioning, denying access to its users.

Statement II: In a MitM attack, attackers break this assumption, placing themselves in between the user and the target server.

Statement III : Social engineering attacks work by psychologically manipulating users into performing actions desirable to an attacker, or divulging sensitive information.

- (a) Only statement I is correct.**
- (b) Only statements II and III are correct.**
- (c) Only statements I and II are correct.**
- (d) All statements I, II, and III are correct.**



26. Which of the following is incorrect?

- a. Social engineering attacks include Phishing, Spear phishing and Smishing
- b. Ransomware prevents access to the data of the victim and threatens to delete or publish it unless a ransom is paid.
- c. Both are correct
- d. None of these



27. Which of the following is correct as per Public Interest Disclosure and Protection of Informers Resolution (PIDPI)?

- (a) CVC is authorised as the Designated Agency to receive written complaints or disclosure on any allegation of corruption or of misuse of office by any employee of the Central Government etc.
- (b) Anonymous complaints shall not be acted upon;
- (c) The identity of the complainant will not be revealed unless the complainant himself has disclosed his identity;
- (d) All are correct



28. Which of the following is incorrect about SBR for NBFC –UL?

- a. NBFC-UL shall be mandatorily listed within 5 years of identification as NBFC-UL.
- b. NBFC-UL shall be required to report to the supervisors in case any Independent Director is removed/ resigns before completion of his normal tenure
- c. In order that the Board is able to focus on risk management, NBFCs shall constitute a Risk Management Committee (RMC) either at the Board or executive level.
- d. All are correct



29. Statement I: Business risk, annihilation risk and strategic risk are non-financial risk.

Statement II : A business risk is a factor that may have a negative impact on the operation or profitability of the business

Statement III: Compliance failure can severely damage reputation, brand and market value leading to liquidity risk and associate effect on running of the organisation.

- (a) Only statement I is correct.**
- (b) Only statements II and III are correct.**
- (c) Only statements I and II are correct.**
- (d) All statements I, II, and III are correct.**



[Jaiib.caiib](https://www.instagram.com/jaiib.caiib/)



[JAIIB CAIIB](https://www.youtube.com/@JAIIB_CAIIB)

Baba



[Telegram - @caiib_group](https://t.me/@caiib_group)

30. Which of the following is not correct about scope of compliance function?

- a. Regulatory Compliance to guidelines issued by the Regulators such as RBI, SEBI, IRDA, etc.
- b. Code of Conduct to be abided based on the guidelines issued by organisations like IBA, BCSBI, FEDAI/FIMDDA, etc.
- c. Internal Compliances/Process Compliances/Policy Compliances as prescribed by the SEBI
- d. All are correct



31. Which of the following is incorrect about role and responsibility of CCO?

1. The CCO shall be appointed for a minimum fixed tenure of not less than 5 years.
2. The CCO should not be more than 60 years;
3. The CCO shall have an overall experience of at least 15 years in the banking or financial services, out of which minimum 10 years shall be in the Audit/Finance/Compliance/Legal/ Risk Management functions;
4. The CCO shall have direct reporting lines to the MD & CEO and/or Board/Board Committee (ACB) of the bank.

a. 1 to 4

b. 1 to 3

c. 1,2 & 4

d. 1, 3a& 4



32. Which of the following duties and responsibilities of the CCO as Head of Compliance Function is/ are wrong ?

- a. To provide clarification on any compliance related issues.
- b. To conduct assessment of the compliance risk (at least twice a year) and to develop a risk oriented activity plan for compliance assessment.
- c. To periodically report on compliance failures/breaches to the Board/ACB and circulating to the concerned functional heads
- d. To monitor and periodically test compliance by performing sufficient and representative compliance testing. The results of the compliance testing should be placed to Board/ACB/MD & CEO.



33. _____ means that CCO shall not be given any responsibility which brings elements of conflict of interest, especially the role relating to business.

- a. Dual Role
- b. Dual Hagging
- c. Dual Hatting
- d. Dual Ranking



Jaiib.caiib



JAIIB CAIIB

Baba



Telegram - @caiib_group

34. Which of the following is incorrect?

1. RBIA is not about auditing risks but about auditing the management of risk.
2. The processes used to assess risks, to decide on the responses to them, to monitor the responses and to report to the board.
3. Its focus is on the processes applied by the management team:
4. The responses to group risks.

- a. 1 to 4
- b. 1 to 3
- c. 1,2 & 4
- d. 1, 3 & 4



35. Match the following?

1. Accounting Standard 5 – i. Employee Benefits
2. Accounting Standard 9 – ii. Revenue Recognition
3. Accounting Standard 15 – iii. Net Profit or Loss for the Period
4. Accounting Standard 17 – iv. Segment Reporting

a. 1 – iii, 2- ii, 3 – I, 4- iv

b. 1 – ii, 2- i, 3 – iii, 4- iv

c. 1 – i, 2- ii, 3 – iii, 4- iv

d. 1 – iii, 2- iv, 3 – I, 4- ii



Q.36. Which of the following statement accurately describe the requirement for compliance certificate by overseas branches?

- a. Ensure that the overseas branches are using updated and reviewed policies, not more than a three ago, specifically in respect of KYC-AML policy as well as compliance policy.**
- b. Ensure that the compliance officers at overseas branches are conducting an independent compliance testing and submit the report periodically, currently at monthly intervals.**
- c. Compliance certificate must be sent from Chief executive of the centre to compliance dept & international dept HO within 5 days of the end of each month**
- d. All are correct**



Q.37. Which of the following is incorrect about pre packaged insolvency resolution process for MSME?

- a. The pre-pack framework is applicable to MSMEs default value up to Rs. 1 crore, beyond which, IBC or other resolution mechanisms can continue to be used.**
- b. In case of a default by an MSME and if a minimum of 75% creditors vote in favour, the financial creditors can initiate the PIRP and file an application with the adjudicating authority for the same.**
- c. 120 days from the date of commencement is the time frame given for completion of the entire PIR process. Also, within 90 days of date of commencement, the Resolution Personal has to submit the resolution plan to the adjudicating authority**
- d. All are correct**



38 As per which section of BR Act, 1949, RBI can impose penalty based on the deficiencies in regulatory compliance and is not intended to pronounce upon the validity of any transaction or agreement entered into by the banks with their customers?

1. 46(4)(i)
2. 46 (4) (ii)
3. 51(1)

- a. 1 to 3
- b. 1 & 2
- c. 1 & 3
- d. 2 & 3



JAIIB CAIIB

Baba



Telegram - @caib_group



39. _____ is a risk that gives negative publicity regarding Bank's business practices, health, and soundness of operations which may lead to lack of confidence with the Bank resulting in loss of business, revenue or may involve the Bank in litigation.

- a. Operational Risk
- b. Legal Risk
- c. Reputation risk
- d. Annihilation risk



40. ____ is a factor that may have a negative impact on the operation or profitability of a given organisation.

- a. Strategic Risk
- b. Operational Risk
- c. Business Risk
- d. None of these



[Jaiib.caiib](https://www.instagram.com/jaiib.caiib/)



[JAIIB CAIIB](#)

Baba



Telegram - [@caiib_group](https://t.me/caiib_group)



41. Which of the following is incorrectly matched:

- (a) Statutory Compliance : Banking Regulation Act, Reserve bank of India Act, Foreign Exchange Management act, Prevention of Money Laundering Act, etc.
- (b) Regulatory Compliance : guidelines issued by RBI, SEBI, IRDA, etc.
- (c) Code of Conduct : abided based on the guidelines issued by organisations like IBA, BCSBI, FEDAI/FIMDDA, etc.
- (d) Listing Agreement : In case of bank wishing to list its securities on money market



42. What is the NPA classification to NBFCs in Base Layer by Mar 31, 2025?

- a. 90 days
- b. 120 days
- c. 150 days
- d. 180 days



Jaiib.caiib



JAIIB CAIIB

Baba



Telegram - @caiib_group

43. Which of the following current NOF is not correct:

- a. NBFC-ICC : current is 2 cr and by Mar 31, 2025 is 5 cr
- b. NBFC – MFI : current is 3 cr and by Mar 31, 2025 is 7 cr
- c. NBFC- Factor: current is 5 cr and by Mar 31, 2025 is 7 cr
- d. For all these NBFC current NOF is 10cr



44. What is the current revised limit as per Tier 1 for NBFC- ML incase of single borrower?

- a. 10%
- b. 25%
- c. 50%
- d. 40%



Jaiib.caiib



JAIIB CAIIB

Baba



Telegram - @caiib_group

45. Which of the following is incorrect about transition of NBFC?

- (a) Within 3 months of being advised by the RBI regarding its inclusion in the NBFC-UL, the NBFC shall put in place a Board approved policy for adoption of the enhanced regulatory framework
- (b) The Board shall ensure that the stipulations prescribed for the NBFC-UL are adhered to within a maximum time-period of 12 months from the date of advice regarding classification as a NBFCUL from the Reserve Bank.
- (c) The period of 3 months provided for charting out the plan for implementation shall be subsumed within the 24-months' time-period referred to above.
- (d) All are correct



46. In case of non-compliance the possibility of regulatory action of closing down business is which risk?

- (a) Operational**
- (b) Regulatory**
- (c) Annihilation**
- (d) Legal**



[Jaiib.caiib](https://www.instagram.com/jaiib.caiib/)



JAIIB CAIIB

Baba



Telegram - @caiib_group



47. _____ of the following is not a part of the GRC concept.

- (a) Risk
- (b) Regulation
- (c) Compliance
- (d) Governance



[Jaiib.caiib](https://www.instagram.com/jaiib.caiib/)



[JAIIB CAIIB](https://www.youtube.com/@JAIIB_CAIIB)

Baba



Telegram - [@caiib_group](https://t.me/@caiib_group)



48. Which of the following option is correct?

- (a) The individuals which raise ethical concerns to others, inside or outside the organization are known as whistle blowers.
- (b) The individuals which raise ethical concerns to others, inside or outside the organization are known as entrepreneur.
- (c) The individuals which raise ethical concerns to others, inside or outside the organization are known as social impact management.
- (d) None of these



Whistleblowing process

- A. The whistle-blower can raise the concern in writing or verbally to the ombudsperson/CVO. The complaint can be sent through email or verbally through the telephone. However, even for verbal complain a written draft is prepared by ombudsperson/CVO.**
- B. All complaints received by ombudsperson/CVO or the audit committee which is constituted by ombudsperson/CVO shall check whether any breach of the code of conduct has happened or not. In case of the review by the audit committee, if any illegal activity has happened committee can recommend that its whistleblowing at work complaint or not. The ombudsperson/CVO or audit committee will respond to the concern within 2 days of receiving the complaint.**
- C. The person who is a whistle-blower may or may not disclose his/her identity**



D. Even in case of whistle-blower has not revealed the identity, the complaint will be taken with utmost seriousness. This is to be noted that any false allegations on any employee by other employees, vendor or contractor or any other stakeholder will result in strict disciplinary action as per the rules framed under the whistleblowing policy in the workplace.

E. Once the investigation is given to the Audit Committee by the CVO/Ombudsman the audit committee will perform tasks

F. The final report must contain all the details and documentation deemed fit or necessary.

G. The whistleblowing process allows the whistle-blower in the company can raise their concern to their manager or head of the department. However, they can also contact the following mentioned persons: (a) Human resource (b) Head of the department (c) Legal department (d) Compliance Head (e) CEO/CVO (f) Management committee members'



49 _____ bank fraud involves having personal information stolen through the use of a fake website.

- (a) Microelectronic fraud
- (b) Cheque book fraud
- (c) Credit card fraud
- (d) Identity theft



[Jaiib.caiib](https://www.instagram.com/jaiib.caiib/)



[JAIIB CAIIB
Baba](https://www.youtube.com/@JAIIB-CAIIB-Baba)



[Telegram - @caiib_group](https://t.me/@caiib_group)



- The Objective of a **Distributed denial of service (DDoS) attack** is to overwhelm the resources of a target system and cause it to stop functioning, denying access to its users. DDoS attacks are often used in combination with other cyber threats.
- **Social engineering attacks** : work by psychologically manipulating users into performing actions desirable to an attacker, or divulging sensitive information. These include Phishing, Spear phishing and Homograph attacks.
- **Man-in-the-middle attack (MitM)** : When users or devices access a remote system over the internet, they assume they are communicating directly with the server of the target system. In a MitM attack, attackers break this assumption, placing themselves in between the user and the target server. Once the attacker has intercepted communications, they may be able to compromise a user's credentials, steal sensitive data and return different responses to the user. MitM attacks include Session hijacking . The server believes it is corresponding with the client and continues the session. Then, there are other MitM attacks including **Replay attack, IP spoofing Eavesdropping attacks.**



- **Malware and spyware attack:** Users may be asked to take an action, such as clicking a link or opening an attachment. In other cases, malware uses vulnerabilities in browsers or operating systems to install themselves without the user's knowledge or consent. Once malware is installed, it can monitor user activities, send confidential data to the attacker, assist the attacker in penetrating other targets within the network, and even cause the user's device to participate in a botnet leveraged by the attacker for malicious intent.

Malware and spyware attacks include:

Trojan virus

- Tricks a user into thinking it is harmless file. Trojan can launch an attack on a system and can establish a backdoor, which attackers can use.

Ransomware

- Prevents access to the data of the victim and threatens to delete or publish it unless a ransom is paid.



[Jaiib.caiib](https://www.instagram.com/jaiib.caiib/)



JAIIB CAIIB

Baba



Telegram - @caiib_group

Malvertising

- **Online advertising controlled by hackers, which contains malicious code that infects a user's computer when they click, or even just view the advertisement.**
Malvertising has been found on many leading online publications
- **Password attacks** : A hacker can gain access to the password information of an individual by 'sniffing' the connection to the network, using social engineering, guessing, or gaining access to a password database. An attacker can 'guess' a password in a random or systematic way.
- **Advanced persistent threats (APT) :** When an individual or group gains unauthorised access to a network and remains undiscovered for an extended period of time, attackers may exfiltrate sensitive data, deliberately avoiding detection by the organisation's security staff.



**50. The Whistle-Blower policy preamble contains the following.
_____ of them should be the most important.**

- (a) Anonymity of the informant will be maintained**
- (b) Appropriate and disciplinary action will be taken after investigation and on confirmation of the information**
- (c) The authenticity of the information will be confirmed and there will be no reprisal for reporting the information**
- (d) None of the above**



[Jaiib.caiib](https://www.instagram.com/jaiib.caiib/)



JAIIB CAIIB

Baba



Telegram - @caiib_group



Trending Now

Bilingual*



CAIIB MAHACOMBO

Clear in 1st Attempt



ambitious **baba**.com

BUY NOW