भारतीय रिज़र्व बैंक
Reserve Bank of India

RBI/DoS/2026-27/450
DoS.CO.PPG.44/11.01.005/2026-27 July 31, 2026

Reserve Bank of India (Local Area Banks – Miscellaneous) Supervisory Directions, 2026

Table of Contents

In exercise of the powers conferred by Section 35-A of the Banking Regulation Act, 1949, and all other provisions / laws enabling the Reserve Bank of India ('RBI') in this regard, RBI being satisfied that it is necessary and expedient in the public interest so to do, hereby, issues Directions hereinafter specified.

Chapter I - Preliminary

A. Short Title and Commencement

1. These Directions shall be called the Reserve Bank of India (Local Area Banks – Miscellaneous) Supervisory Directions, 2026.

2. These Directions shall come into effect immediately upon issuance.

B. Applicability

3. These Directions shall be applicable to Local Area Banks (hereinafter collectively referred to as 'banks' and individually as 'bank').

C. Definitions

4. In Chapter VIII of these Directions, unless the context states otherwise, the terms therein shall bear the meanings assigned to them below, which are sourced from FSB Cyber Lexicon unless explicitly mentioned otherwise:

   (1) '*Audit Trail*' - A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to result.

   (*Source:* NIST SP 800-53r5 on Security and Privacy Controls for Information Systems and Organizations)

   (2) '*Cyber'* - Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.

   (3) '*Cybersecurity*' - Preservation of confidentiality, integrity, and availability of information and / or information systems through the cyber medium. In

addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

(4) '*Cyber Incident*' - A cyber event that adversely affects the cybersecurity of an information asset whether resulting from malicious activity or not.

(*Source:* Cyber incident definition is adapted from FSB Cyber Lexicon. By the definition, it includes cybersecurity as well as IT incident)

(5) '*Cyber Resilience*' - The ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing, and rapidly recovering from cyber incidents.

(6) *'Cyber-attack'* - Malicious attempt(s) to exploit vulnerabilities through the cyber medium to damage, disrupt, or gain unauthorised access to assets.

(7) *'Cyber Threat'* - A circumstance with the potential to exploit one or more vulnerabilities that adversely affects cybersecurity.

(8) *'De-militarized Zone (DMZ)'* - A perimeter network segment that is logically between internal and external networks.

(*Source:* NIST SP 800-82 Rev. 2)

(9) *'Distributed Denial of Service (DDoS)'* - A denial of service that is carried out using numerous sources simultaneously.

(10) '*Framework'* - A structured set of strategies, policies, processes, methods, and best practices that guides organisational activities, enables governance and control, and supports the achievement of defined objectives.

(*Source:* adapted from ISACA glossary and ISO 22340:2024)

(11) '*Information* Asset' - Any piece of data, device, or other component of the environment that supports information-related activities. Information Assets include information system, data, hardware, and software.

(*Source:* Information Asset definition is adapted from "Guidance on cyber resilience for financial market infrastructures" publication of Bank for International Settlements and International Organization of Securities Commissions of June 2016)

(12) '*Information System'* - Set of applications, services, information technology assets, or other information-handling components, which includes the operating environment and networks.

(13) *'Malware'* - Software designed with malicious intent containing features or capabilities that can potentially cause harm directly or indirectly to entities or their information systems.

(14) *'Penetration Testing'* - A test methodology in which assessors typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.

(15) *'Privileged User'* - A user who, by virtue of function, and / or role, has been allocated powers within an information system, which are significantly greater than those available to the majority of users.

(*Source:* adapted from ISO/IEC 24775-2:2021)

(16) '*Vulnerability'* - A weakness, susceptibility, or flaw of an asset or control that can be exploited by one or more threats.

(17) *'Vulnerability Assessment (VA)'* - Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.

5. All other expressions unless defined herein shall have the same meaning as have been assigned to them under the Reserve Bank of India Act, 1934, the Banking Regulation Act, 1949, the Companies Act, 2013, or any statutory modification or re-enactment thereto or other regulations issued by the RBI or

the Glossary of Terms published by the RBI, or as used in commercial parlance, as the case may be.

Chapter II - Fair Practices Code - Charging of Interest

6. The bank, in the interest of fairness and transparency, shall review its practices regarding mode of disbursal of loans, application of interest and other charges, charging of Equated Monthly Instalments (EMIs), and take corrective action, including system level changes, as may be necessary, to address unfair practices, some of which are briefly explained below:

   (1) Charging of interest from the date of sanction of loan or execution of loan agreement and not from the date of actual disbursement of funds to the customer. For loans disbursed by cheque, charging interest from the cheque date while handing over the cheque to the customer several days later.

   (2) Charging of EMIs on the sanctioned loan amount rather than on the actual disbursed amount, without the knowledge or consent of the borrower.

   (3) Any changes in the amortisation schedule originally provided in the Key Facts Statement (KFS), with each part-disbursement of loan, not being communicated to the borrowers.

   (4) In case of disbursal or repayment of loans during a month, charging interest for the entire month rather than charging interest only for the period for which the loan was outstanding.

   (5) Collecting one or more instalments in advance but reckoning the full loan amount for charging interest.

7. These and other such non-standard practices of charging interest are not in consonance with the spirit of fairness and transparency while dealing with customers. These are matters of serious concern to the RBI.

8. The bank may use online account transfers in lieu of cheques for loan disbursal.

Chapter III - Inoperative Accounts / Unclaimed Deposits

9. The bank shall take necessary steps to reduce the number of inoperative accounts and accounts pending for updation / periodic updation of 'Know Your Customer' (KYC) and make the process of updation / periodic updation of such accounts smoother and hassle free, including by enabling seamless updation of KYC through mobile / internet banking, non-home branches, and Video Customer Identification Process, in accordance with the relevant provisions of the Reserve Bank of India (Local Area Banks - Responsible Business Conduct) Directions, 2025.

10. The bank may facilitate the process of activation of accounts of beneficiaries of various Central / State government schemes like Direct Benefit Transfer (DBT) / Electronic Benefit Transfer (EBT) etc., and accounts pending for updation / periodic updation of KYC, by taking an empathetic view in such cases, since these accounts mostly pertain to the people from the underprivileged sections of the society.

11. The bank may organise special campaigns for facilitating activation of inoperative accounts and accounts pending for periodic updation of KYC.

12. The bank may also facilitate Aadhaar updation for its customers through its branches providing Aadhaar related services.

13. The Customer Service Committee of the Board shall monitor the progress in reduction of inoperative accounts and accounts pending for updation of KYC and the special efforts made by the bank in this regard.

14. The bank shall report the progress on reduction of inoperative accounts and accounts pending for updation of KYC on a quarterly basis to the Senior Supervisory Manager (SSM), RBI through DAKSH portal.

Chapter IV – Fraud Prevention Measures

From time to time, RBI has constituted various committees such as the Ghosh Committee, Gilani Committee, and Narang Committee, to examine different aspects relating to frauds and malpractices in banks and to recommend measures for their prevention and early detection. Based on the recommendations of these committees, RBI has, over the years, issued several guidelines to banks aimed at strengthening internal controls, enhanced monitoring in sensitive areas of banking operations, and curbing the occurrence of frauds. The key fraud preventive measures covered under these guidelines are outlined below.

A. Frauds due to Collusion of the bank Officials

15. In order to prevent / detect frauds due to collusion of the bank officials, the bank shall take the following measures:

    (1) ensure balancing of books at the stipulated intervals;

    (2) interact with the concurrent auditors and enquire about the problems faced by them in auditing certain branches and indicate to them in clear terms the expectations of the management from the auditors while auditing branches; and

    (3) immediately examine staff accountability and take appropriate action for the lapses / irregularities noticed.

B. Large Value Frauds

16. The bank shall take the following measures for prevention / detection of large value frauds:

    (1) Safeguards in respect of Letters of Credit and Bank Guarantee;

    (2) Management Audit System and its emphasis on analysis of existing control system, its adequacy, scope and need for periodical review;

    (3) Safe custody of critical items of bank stationery; and

    (4) A scheme to honour alert bank staff for timely detection of frauds.

C. Frauds by Deposit of Fake Title Deeds of Property

17. The bank officials shall follow the laid down procedures for verifying the genuineness of the documents submitted by the borrowers independently through their own advocates / solicitors. The documents sought to be submitted for creation of equitable mortgage / deposit as collateral security should be original and be verified through searches in the appropriate records of the Sub-Registrar of Assurances and Revenue and Municipal records up to or as near to the date of creation of security in the bank's favour as possible. The bank should obtain a certificate from the advocate / solicitor certifying the title to concerned property being original and not duplicate or fake and that the title is clear, marketable and free from encumbrances.

18. The bank shall be extra cautious while accepting sale deeds and other documents of properties as collateral securities. Necessary steps in this regard, may be detailed by the bank, in consultation with its Legal Department.

19. Furthermore, the bank may take the following measures:

    (1) The bank may insist on opening of bank accounts by owners of properties who offer the same as collateral security against loans given to third parties.

    (2) The bank should communicate with the owners of the property through registered letter to confirm proof of residence and their willingness to offer the security as collateral.

D. Safe Custody of Critical Documents

20. The bank shall exercise safeguards like maintenance of proper records, dual control, periodical balancing of books / verification, submission of control returns, and ensure their observations.

21. Blank Demand Drafts / Pay Orders and Mail Transfer forms should be treated as security items and the branches should take adequate safeguards against their pilferage. They should be held in joint custody and balanced daily.

22. The bank shall ensure that no unauthorised person has access to security items like blank cheques, drafts, fixed deposit receipts, pay orders, account opening forms, specimen signature cards / books, loose ledger sheets, and blank Letter of Credit forms.

23. The ledgers and other books of accounts, voucher bundles, and other items of Stationery should be stored properly.

E. Accounts opened by Employees

24. The bank shall make it incumbent on the part of the staff members to intimate in writing about the accounts opened by them with another branch of the bank or another bank. Accordingly, necessary amendments to the Officers' Conduct Regulations as also the Standing Orders to the workmen employees may be issued in consultation with Indian Banks Association (IBA).

F. Other Instructions

25. Wherever there is a prima-facie case against the loan dealing officials of the bank, appropriate action in terms of Central Vigilance Commission guidelines, for their inclusion in the list of officers with doubtful integrity, should be initiated by the bank in consultation with the Central Bureau of Investigation.

26. The officers posted in the Vigilance Department of the bank, preferably at the Head Office, should hold meetings with the investigating authorities at periodical intervals which should be minutised and action be taken within a time frame agreed to at the meetings.

Chapter V - Protected Disclosure Scheme

27. The bank shall take necessary action for implementing the Protected Disclosure Scheme. The salient features of the Scheme are as under:

A. Scope and Coverage

28. The complaints under the Scheme would cover the areas such as corruption, misuse of office, criminal offences, suspected / actual fraud, failure to comply with existing rules and regulations such as the Reserve Bank of India Act, 1934 and the Banking Regulation Act 1949, and acts resulting in financial loss / operational risk or loss of reputation, detrimental to depositors' interest / public interest.

29. Under the Scheme, employees of the bank, customers, stake holders, NGOs and members of public can lodge complaints.

30. Anonymous / pseudonymous complaints will not be covered under the Scheme and such complaints will not be entertained.

31. RBI will be the Nodal Agency to receive complaints under the Scheme. RBI would keep the identity of the complainant secret, except in cases where complaint turns out to be vexatious or frivolous and action has to be initiated against the complainant as mentioned below:

    (1) The institution against which complaint has been made can take action against complainants in cases where motivated / vexatious complaints are made under the Scheme, after being advised by RBI. An opportunity of hearing will, however, be given by the bank to the complainant before taking such action.

    (2) Final action taken by RBI on the complaint will be intimated to the complainant.

B. Procedure for Lodging the Complaint under the Scheme

32. The complaint should be sent in a closed / secured envelope.

33. The envelope should be addressed to *The Chief General Manager, Reserve Bank of India, Department of Supervision, Fraud Monitoring Group, 2nd Floor, Maker Tower-E, Cuffe Parade, Mumbai 400 005.* The envelope should be superscribed *'Complaint under Protected Disclosure Scheme for Banks'*.

34. The complainant should give his / her name and address in the beginning or end of the complaint or in an attached letter. In case of an employee making such complaint, details such as name, designation, department, institution and place of posting should be furnished.

35. Complaints can also be made through e-mail also giving full details as specified above.

36. The complainant should ensure that the issue raised by him involves dishonest intention / moral angle. They should study all the relevant facts and understand their significance. They should also make an effort, if possible, to resolve the issue through internal channels in order to avoid making the complaint.

37. The text of the complaint should be carefully drafted so as not to give any details or clue to complainant's identity. The details of the complaint should be specific and verifiable.

38. In order to protect the identity of the complainant, RBI will not issue any acknowledgement of receipt of the complaint and the complainants are advised not to enter into any further correspondence with the RBI in their own interest. RBI assures that, subject to the facts of the case being verifiable, it would take necessary action, as provided under the scheme. If any further clarification is required, RBI will get in touch with the complainant.

39. If the complaint is accompanied by particulars of the person making the complaint, the RBI shall take the following steps:

    (1) If necessary, it would ascertain from the complainant whether they were the person who made the complaint or not.

(2) The identity of the complainant will not be revealed unless the complainant himself has made the details of the complaint either public or disclosed his identity to any other authority.

(3) The identity of the complainant will be concealed, RBI will make discreet inquiries to ascertain if there is any basis for proceeding further with the complaint.

(4) Either as a result of the discreet enquiry, or on the basis of complaint itself without any enquiry, if RBI is of the opinion that the matter requires to be investigated further, RBI may consider calling for the comments / response from the Chairman / MD & CEO of the concerned bank.

(5) After obtaining the response of the concerned bank and / or on the basis of an independent scrutiny conducted / ordered by RBI, if RBI is of the opinion that the allegations are substantiated, then RBI shall recommend appropriate action to the concerned bank. These shall, inter alia, include the following:

(i) Appropriate action to be initiated against the concerned official.

(ii) Appropriate administrative steps for recovery of the loss caused to the bank as a result of the corrupt act or mis-use of office, or any other offence covered by the Scheme.

(iii) Recommend to the appropriate authority / agency for initiation of criminal proceedings, if warranted by the facts and circumstances of the cases.

(iv) Recommend taking corrective measures to prevent recurrence of such events in future.

(v) Consider initiating any other action that it deems fit keeping in view the facts of the case.

(6) If any person is aggrieved by any action on the ground that he is victimized due to filing of the complaint or disclosure, he may file an application before

the RBI seeking redressal in the matter. RBI will take such action, as deemed fit. In case the complainant is an employee of the bank, RBI may give suitable directions to the concerned bank, preventing initiation of any adverse personnel action against the complainant.

(7) Either on the basis of application of the complainant or on the basis of information gathered, if the RBI is of the opinion that either the complainant or the witnesses in the case need protection, the RBI shall issue appropriate directions to the concerned bank.

(8) The system described herein shall be in addition to the existing grievances redressal mechanism in place. However, secrecy of identity shall be observed, only if the complaint is received under the scheme.

(9) In case RBI finds that the complaint is motivated or vexatious, RBI shall be at liberty to take appropriate steps.

(10) In the event of the identity of the informant being disclosed in spite of RBI's directions to the contrary, then RBI shall be authorised to initiate appropriate action as per extant regulations against the person or agency making such disclosure. RBI may also direct such person or agency to suitably compensate the complainant.

C. Protected Disclosure Policy

40. The bank shall frame a 'Protected Disclosure Scheme' duly approved by its Board, keeping in view the broad framework given above. The policy should clearly lay down norms for protection of identity of employees making disclosures under the scheme and safeguarding them from any adverse personnel action. The role and responsibilities of the Board may also be well defined in dealing with the complaints received under the scheme. The Board, or a Board Committee may be made responsible for monitoring the implementation of the scheme. The bank may factor suggestions of the unions / associations of officers / employees before framing such a policy. Suitable mechanism should be put in place to make newly recruited employees of the bank aware of the existence of such a scheme in the bank.

Chapter VI – Vigilance

41. The bank shall put in place a system of internal vigilance machinery as per the guidelines furnished below with the approval of the Board, in order to uniformly address issues arising out of lapses in the functioning of the bank especially relating to corruption, malpractices, and frauds, for timely and appropriate action:

A. Preamble

42. Vigilance is an inseparable part of management. It promotes clean business transactions, professionalism, productivity, promptness and transparent practices and ensures putting in place systems and procedures to curb opportunities for corruption which results in improving efficiency and effectiveness of the personnel as well as the organization. These factors make it mandatory to have a dedicated vigilance setup in the banking industry. The following guidelines aim at structuring efficient and effective vigilance system in banks in the larger interest of all concerned stakeholders.

B. Introduction

43. Anti-corruption measures taken by the bank are a responsibility of the disciplinary authority identified in the bank and it has the over-all responsibility of looking into the acts of misconduct alleged against, or committed by, the employees within its control and to take appropriate punitive action. It is also required to take appropriate preventive measures so as to prevent commission of misconducts / malpractices by the employees under its control and jurisdiction. The designated Officer (similar to Chief Vigilance Officers in case of Public Sector Banks) acts as a Special Assistant / Advisor to the CEO of the bank in the discharge of these functions. They also act as a liaison officer between the bank and the Police / Serious Fraud Investigation Officer / other law enforcement authorities.

C. Vigilance Angle

44. Vigilance angle will be applicable in case of following acts:

(1) Demanding and / or accepting gratification other than legal remuneration in respect of an official act or for using his influence with any other official;

(2) Obtaining valuable thing, without consideration or with inadequate consideration from a person with whom he has or is likely to have official dealings or his subordinates have official dealings or where he can exert influence;

(3) Obtaining for himself or for any other person any valuable thing or pecuniary advantage by corrupt or illegal means or by abusing his position as an employee;

(4) Possession of assets disproportionate to their known sources of income; and

(5) Cases of misappropriation, forgery or cheating or other similar criminal offences.

45. In case of other irregularities like gross or wilful negligence; recklessness in decision making; blatant violations of systems and procedures; exercise of discretion in excess, where no ostensible organisational interest is evident; failure to keep the controlling authority / superiors informed in time; the disciplinary authority with the help of the Chief of Internal Vigilance (CIV) should carefully study the case and weigh the circumstances to arrive at a conclusion whether there is reasonable ground to doubt the integrity of the officer concerned.

D. Chief of Internal Vigilance

46. The bank shall designate an officer of suitable seniority as CIV who will head the Internal Vigilance Division of the bank. Vigilance functions to be performed by the CIV would be wide ranging and include collecting intelligence about the corrupt practices committed, or likely to be committed, by the employees of the bank; investigating or causing an investigation to be made into verifiable allegations reported to him; processing investigation reports for further consideration of the disciplinary authority concerned; referring the matters to the CEO of the bank for advice wherever necessary; and taking steps to prevent commission of improper practices / misconducts. Thus, the CIVs' functions can broadly be divided into three parts, viz. (i) Preventive vigilance; (ii) Punitive vigilance; and (iii) Surveillance and detection.

D.1 Appointment

47. The basis for appointment of CIV should be experience, track record, proven integrity, and ability to inspire confidence among personnel in the bank.

D.2 Tenure

48. The normal tenure of a CIV should be three years extendable up to a further period of two years. But if a CIV has to shift from one bank to another without completing the approved tenure in the previous bank, the principle of overall tenure of six years will apply.

D.3 Association with Sensitive Matters

49. The vigilance functionaries should not be a party to processing and decision-making processes or be involved in other administrative transactions of such nature, which are likely to have clear vigilance sensitivity. While it may not be difficult for full-time vigilance functionaries to comply with this requirement, the compliance of these instructions could be achieved in respect of part-time vigilance functionaries by confining their duties, other than those connected with vigilance work, as far as possible, to such items of work that are either free from vigilance angle or preferably serve as input to vigilance activities such as inspection and audit.

D.4 Submission of Reports and Returns - Review

50. CIV should invariably review all pending matters, such as investigation reports, disciplinary cases, and other vigilance complaints / cases in the first week of every month and take necessary steps for expediting action on those matters. The CIV would arrange periodic meetings to be taken by the CEO for reviewing the vigilance activities undertaken by the bank. CIV would also be required to furnish a report on the vigilance activities in the bank to the Board / Local Governing Council on a periodic basis.

E. Preventive Vigilance

51. The CIV may take the following measures on preventive vigilance:

(1) undertake a study of existing procedure and practices prevailing in the bank with a view to modifying those procedures or practices which provide a scope for corruption, and also to find out the causes of delay, the points at which it occurs and devise suitable steps to minimize delays at different stages;

(2) undertake a review of the regulatory functions with a view to see whether all of them are strictly necessary and whether the manner of discharge of those functions and exercise of powers of control are capable of improvement;

(3) devise adequate methods of control over exercise of discretion so as to ensure that discretionary powers are not exercised arbitrarily but in a transparent and fair manner; and

(4) identify the areas in his organisation which are prone to corruption and to ensure that the officers of proven integrity only are posted in those areas;

F. Staff Rotation and Mandatory Leave

52. The bank should identify sensitive positions and frame specific Board approved internal policy on staff matters such as rotation of staff in general and in respect of sensitive desks in particular. The bank may, while framing such policy, include the minimum period for staff rotation and mandatory leave that would apply to the staff at all levels. The bank shall also refer to Reserve Bank of India (Local Area Banks – Miscellaneous) Directions, 2025.

G. Complaints

53. Receipt of information about corruption, malpractice or misconduct on the part of employees, from whatever source, would be termed as a complaint. Information about corruption, malpractice or misconduct on the part of employees may flow to the administrative authority / the Police / Serious Fraud Investigation Officer / RBI from any of the following sources:

(1) Complaints received from employees of the bank or from the public;

(2) Departmental inspection reports and stock verification surveys;

(3) Scrutiny of annual property statements;

(4) Scrutiny of transactions reported under the Conduct Rules;

(5) Reports of irregularities in accounts detected in the routine audit of accounts, e.g., tampering with records, over-payments, and misappropriation of money or material;

(6) Audit reports of the accounts of the bank;

(7) Complaints and allegations appearing in the press;

(8) Source information, if received verbally from an identifiable source, to be reduced in writing; and

(9) Intelligence gathered by agencies like Central Bureau of Investigation and local bodies.

54. In addition, the CIV may also devise and adopt appropriate methods to collect information about any malpractice and misconduct among the employees. Anonymous / pseudonymous complaints received by the CIV may be dealt with on merit.

H. Investigation Agency for Conducting Investigations

55. As soon as a decision has been taken to investigate the allegations contained in a complaint, the bank shall decide whether the allegations should be inquired into departmentally or whether a police investigation is necessary. Instructions as to with which agency the complaint is to be lodged, are contained in the Reserve Bank of India (Local Area Banks – Fraud Risk Management) Directions, 2026.

I. Review of Cases entrusted to Investigating Agencies

56. No review should ordinarily be made by the administrative authority of a case registered by the Police. If, however, there are special reasons for discussion / review, the Police should invariably be associated with it.

J. Action against Persons making False Complaints

57. If a complaint against an employee is found to be malicious, vexatious or unfounded, it should be seriously considered whether action should be taken against the complainant for making a false complaint.

K. Liaison with Agencies

58. The CIV should closely liaise and co-operate with the Police / Serious Fraud Investigation Office (SFIO) during the course of an inquiry and investigation and the processing of individual cases, as both the Police / SFIO and the CIV, receive information about the activities of the officer from diverse sources. Such information may be cross checked at appropriate intervals to keep Police / SFIO fully apprised with the latest developments through periodical meetings between the CIV and Police / SFIO.

Chapter VII - Network Management

59. The bank shall enable its public facing IT infrastructure to handle Internet Protocol Version 6 (IPv6) traffic.

Chapter VIII - Cyber Security controls for Third party ATM Switch Application Service Providers

60. The bank shall ensure that the following cybersecurity controls given in this Chapter are implemented and maintained by third-party Automated Teller Machine (ATM) Switch Application Service Providers (ASPs) where the bank manages its ATM Switch ecosystem through their shared services. Further the bank shall share regulatory instructions (including circulars / advisories / alerts) issued from time to time, as applicable to the ATM switch ecosystem with the ASPs for necessary compliance.

A. Preventing Access of Unauthorised Software

61. The ASP shall have a mechanism to control installation of software / applications centrally / otherwise on its information systems including end-user Personal Computers (PCs), laptops, workstations, servers, mobile devices, and cloud environments and mechanism to block / prevent and identify installation and running of unauthorised software / applications on such devices / systems.

62. The ASP shall continuously monitor the release of patches by various vendors / Original Equipment Manufacturers (OEMs), advisories issued by CERT-In and other similar agencies and expeditiously apply the security patches as per the patch management policy of the ASP. Where a patch / series of patches is / are released by the OEM / manufacturer / vendor to mitigate critical vulnerabilities that are actively exploited or widely reported, the ASP shall have a mechanism to deploy such patches expeditiously, in accordance with its emergency patch management process.

63. The ASP shall put in place a policy specifying the justification for exceptions, duration of exceptions, process for granting exceptions, approving authority, and periodic review of granted exceptions by officers, at senior levels, who are equipped to understand the business and technical context of such exceptions.

B. Environmental Controls

64. The ASP shall put in place appropriate controls for securing the physical location of critical assets from natural and man-made threats.

65. The ASP shall put in place mechanisms for monitoring of breaches of environmental controls including temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), and access logs.

C. Network Management and Security

66. The ASP shall prepare and maintain an up-to-date network architecture diagram at the organisation level including wired / wireless networks.

67. The ASP shall maintain an up to date / centralised inventory of authorised devices connected to the ASP's network (within / outside ASP's premises) and authorised devices enabling the ASP's network. The ASP may consider implementing solutions to automate network discovery and management.

68. The ASP shall implement mechanism to identify authorised hardware / mobile devices such as laptops, mobile phones, and tablets, in the network and ensure that they are provided connectivity only when they meet the security requirements prescribed by the ASP.

69. The ASP shall ensure that all the network devices are configured appropriately. The ASP shall periodically assess whether the configurations are appropriate to the desired level of network security.

70. The default passwords of all the network devices / systems of the ASP shall be changed after installation.

71. The ASP shall design the infrastructure with adequate network segregation controls.

72. The ASP shall have mechanism to automatically identify unauthorised device connections to the ASP's network and block such connections.

73. The ASP shall ensure that boundary defences are multi-layered with properly configured firewalls, proxies, DMZ perimeter networks, and network-based Intrusion Prevention System (IPS) and Intrusion Detection System (IDS).

Additionally, the ASP shall establish robust mechanism for real-time filtering of inbound and outbound network traffic.

74. The ASP shall establish Standard Operating Procedures (SOPs) for all major IT activities including for connecting devices to the network.

75. The ASP shall put in place mechanism to detect and remedy any unusual activities in systems, servers, network devices, and endpoints.

76. The ASP shall define firewall rules to block unidentified outbound connections, reverse Transmission Control Protocol (TCP) shells, and other potential backdoor connections.

D. Secure Configuration

77. The ASP shall document and apply baseline security requirements / configurations to all categories of devices including endpoints / workstations, mobile devices, operating systems, databases, applications, network devices, security devices, and security systems, throughout the lifecycle (from conception to deployment) and carry out reviews periodically.

78. The ASP shall periodically evaluate the configuration of all such devices including firewall, network switches, and security devices and patch levels for all systems in the ASP's IT ecosystem.

79. The ASP shall disable remote connections from outside machines to the network hosting the ATM Switch infrastructure.

80. The ASP shall enable Internet Protocol (IP) table to restrict access to the clients and servers in Society for Worldwide Interbank Financial Telecommunication (SWIFT) and ATM Switch environment only to authorised systems.

81. The ASP shall ensure software integrity of the ATM Switch related applications.

E. Application Security Life Cycle

82. The ASP shall incorporate / ensure information security across all stages of application life cycle.

83. The ASP shall implement secure coding practices for internally / collaboratively developed applications.

84. The ASP shall properly segregate the development, test, and production environments. The ASP shall ensure to appropriately mask the data used for development and testing.

85. The ASP shall ensure that the software / application development process is guided by threat modelling, adheres to secure coding practices, includes security testing aligned with global standards, and ensures a secure deployment.

86. The ASP shall ensure adequate evaluation of adoption of new technologies for existing / evolving security threats. Such technologies shall be introduced for critical systems after IT and security team of the ASP reach reasonable level of comfort and maturity.

87. The ASP shall certify any new products and updates, upgrades as having been developed following secure coding practices. The application architecture shall be tested to safeguard the confidentiality and integrity of data being stored, processed, and transmitted. An assurance to this effect shall be shared with the bank / RBI as and when requested.

88. In respect of critical business applications, the ASP shall conduct source code audits by professionally competent personnel / service providers. They shall provide assurance to the bank that the application is free from embedded malicious / fraudulent code.

89. The ASP shall ensure that software / application development practices address the vulnerabilities based on best practices, baselines such as Open Web Application Security Project (OWASP) proactively and adopt principle of defence-in-depth to provide layered security mechanism.

F. Patch / Vulnerability and Change Management

90. The ASP shall adopt a documented, risk-based strategy for maintaining an inventory of IT components that require patching, identifying all applicable

patches, and applying them in a timely manner to minimise both the number of vulnerable systems and the duration of exposure.

91. The ASP shall manage changes to business applications, supporting technology, service components, and facilities through robust configuration management processes and configuration baselines to ensure the integrity of such changes.

92. The ASP shall periodically conduct application security testing of web / mobile applications throughout their lifecycle (pre-implementation, post implementation, and after changes) in an environment closely resembling or a replica of the production environment.

93. As part of its threat mitigation strategy, the ASP shall determine the root cause of any detected incident and implement necessary patches to address the vulnerabilities.

94. The ASP shall evaluate the access device configurations and patch levels periodically to ensure that all access points, nodes between (i) different Virtual Local Area Networks (VLANs) in the DC, (ii) Local Area Network (LAN) / Wide Area Network (WAN) interfaces, (iii) ASP's network to external network and interconnections with partner, vendor and service provider networks are securely configured.

95. The ASP shall have a robust change management process in place to record / monitor all the changes that are moved / pushed into the production environment. Such a change management process must clearly mention the test cases, chain of approving authority for the particular change, deployment plan, and rollback plan.

G. User Access Control / Management

96. The ASP shall provide secure access to its assets / services from within / outside its network by protecting data / information at rest (e.g., using encryption, if supported by the device) and in-transit [e.g., using technologies such as Virtual Private Network (VPN) or other secure protocols].

97. The ASP shall protect user access credentials such as logon user-id, authentication information and tokens, access profiles, against leakage / attacks.

98. The ASP shall implement controls to minimise invalid logon counts and deactivate dormant accounts.

99. The ASP shall implement centralised authentication and authorisation system through an Identity and Access Management solution for accessing and administering applications, operating systems, databases, network and security devices/systems, point of connectivity (local / remote) including enforcement of strong password policy, two-factor / multi-factor authentication depending on risk assessment, securing privileged accesses following the principle of least privileges and separation of duties.

100. The ASP shall ensure to provide access to critical servers, network and security devices / systems through Privileged User Management Systems / Identity and Access Management (IAM) systems.

101. The ASP shall monitor any abnormal change in pattern of logon.

102. The ASP shall put in place a mechanism to monitor the database security events, backend access to the databases to ensure access to the database is restricted and the activities carried out through the backend are logged and reviewed.

103. The ASP shall not use trivial and / or default passwords.

H. Data Leak Prevention Strategy

104. The ASP shall develop a comprehensive data loss / leakage prevention strategy to safeguard sensitive (including confidential) business and customer data / information. This shall include protecting data processed in end point devices, data in transmission, as well as data stored in servers and other digital stores, whether online or offline.

I. Audit Logs

105. The ASP shall ensure to capture audit logs pertaining to user actions in a system. Such arrangements shall facilitate forensic auditing, if need be.

106. The ASP shall implement and periodically validate settings for capturing appropriate logs and audit trails for each device, system software, and application software, ensuring that such logs include the minimum information required to uniquely identify each log, such as date, timestamp, source addresses, destination addresses, and other relevant elements of each packet, event, and / or transaction.

107. The ASP shall ensure to generate and capture logs from devices / applications / databases.

108. The ASP shall set an alert mechanism to monitor any change in the log settings.

109. The ASP shall manage and analyse audit logs to detect, respond, understand or recover from any unauthorised activity or attack.

J. Incident Response and Management

110. The ASP shall have a mechanism and resources to take appropriate action in case of any cyber incident. The ASP shall have a written incident response procedure including the roles of staff / outsourced staff handling such incidents. The response strategies shall consider readiness to meet various incident scenarios based on situational awareness, potential / post impact, and consistent communication and co-ordination with stakeholders, specifically with the bank, during response.

111. The ASP's BCP and DR capabilities shall be designed to effectively support resilience objectives and enable rapid recovery and secure resumption of critical operations including key cybersecurity controls post cyber-attacks / other incidents aligned with recovery time objectives while ensuring security of processes and data.

112. The ASP is responsible for meeting the requirements prescribed for incident management and Business Continuity Plan (BCP) / DR even if their IT infrastructure, systems, and applications, are managed by third-party vendors / service providers. The ASP shall have necessary arrangements, including a documented procedure for such purpose. This shall include, among other things,

informing the bank about any cyber incident occurring in respect of the bank on a timely basis to mitigate the risk at the earliest as well as to meet extant regulatory requirements.

K. Advanced Real-time Threat Defence and Management

113. The ASP shall build a robust defence against the installation, spread, and execution of malicious code at multiple points in its environment.

114. The ASP shall implement anti-malware, antivirus protection including behavioural detection capabilities across all relevant devices and environments, such as endpoints (including PCs, laptops, and mobile devices), servers (operating systems, databases, and applications), Web / Internet gateways, email-gateways, Wireless networks, and Short Message Service (SMS) servers. The ASP shall also implement tools and processes for centralised management and monitoring of these measures.

L. Vulnerability assessment and Penetration Test

115. The ASP shall periodically conduct Vulnerability Assessment / Penetration Testing (VA / PT) of applications, servers, and network components.

116. The ASP's risk management / treatment framework shall ensure that the vulnerabilities detected are remediated promptly to avoid exploitation of such vulnerabilities.

117. The ASP shall ensure to share the VA / PT report(s) and compliance to its findings with the bank / RBI as and when requested.

M. Forensics

118. The ASP shall have support / arrangement for network forensics / forensic investigation / DDOS mitigation services on stand-by.

N. Setting up of Cyber Security Operation Centre

119. The ASP shall set up a Cyber Security Operations Centre (CSOC). The CSOC, among other things, shall ensure to

(1) seamlessly collect the logs relevant to the IT ecosystem;

(2) store, process, and correlate the logs through appropriate Security Information and Event Management (SIEM) solution for continuous surveillance; and

(3) regularly update on the latest nature of emerging cyber threats.

O. Compliance with Various Standards

120. The ASP shall comply with the relevant standards including Payment Card Industry Data Security Standard (PCI-DSS) and Payment Card Industry - Software Security Framework (PCI-SSF), as applicable to the IT ecosystem.

Chapter IX - Repeal and Other Provisions

A. Repeal and Saving

121. With the issue of these Directions, the existing Directions, instructions, and guidelines relating to areas covered in these Directions as applicable to Local Area Banks stand repealed, as communicated vide circular no. DoS.CO.PPG.66/11.01.005/2026-27 dated July 31, 2026. The Directions, instructions and guidelines repealed prior to the issuance of these Directions shall continue to remain repealed.

122. Notwithstanding such repeal, any action taken or purported to have been taken, or initiated under the repealed Directions, instructions, or guidelines shall continue to be governed by the provisions thereof. All approvals or acknowledgments granted under these repealed lists shall be deemed as governed by these Directions. Further, the repeal of these directions, instructions, or guidelines shall not in any way prejudicially affect:

(1) any right, obligation or liability acquired, accrued, or incurred thereunder;

(2) any penalty, forfeiture, or punishment incurred in respect of any contravention committed thereunder;

(3) any investigation, legal proceeding, or remedy in respect of any such right, privilege, obligation, liability, penalty, forfeiture, or punishment as aforesaid; and any such investigation, legal proceedings or remedy may be instituted, continued, or enforced and any such penalty, forfeiture or punishment may be imposed as if those directions, instructions, or guidelines had not been repealed.

B. Application of Other Laws Not Barred

123. The provisions of these Directions shall be in addition to, and not in derogation of the provisions of any other laws, rules, regulations, or directions, for the time being in force.

C. Interpretations

124. For the purposes of giving effect to the provisions of these Directions or for removing any difficulties in their application or interpretation, RBI may, if it deems necessary, issue such clarifications as it considers appropriate in respect of any matter covered herein. The interpretation of any provision of these Directions by RBI shall be final and binding on all concerned entities.

(Tarun Singh)
Chief General Manager