

बाह्य परिपत्र सं. 32/डॉस - 07 /2020

06 फरवरी 2020



संदर्भ सं. राबैं. पॉल. प्रका. 3182/जे-1/2019-20

प्रबंध निदेशक/ मुख्य कार्यकारी अधिकारी

सभी राज्य सहकारी बैंक/

सभी जिला मध्यवर्ती सहकारी बैंक

महोदय / महोदया

**ग्रामीण सहकारी बैंकों (आरसीबी) के लिए व्यापक साइबर सुरक्षा फ्रेमवर्क -
समयबद्ध कार्यान्वयन के लिए क्रमिक पद्धति**

कृपया 16 मार्च 2018 के हमारे परिपत्र राबैं. डॉस. प्रका. पॉल. सं. 4811/जे-1 / 2017-18 का संदर्भ लें जिसके माध्यम से बैंकों में साइबर सुरक्षा फ्रेमवर्क के कार्यान्वयन से संबंधित दिशानिर्देश जारी किए गए थे. आगे और परीक्षण के बाद साइबर सुरक्षा फ्रेमवर्क के कार्यान्वयन की क्रमिक पद्धति तैयार की गई है.

2. ग्रामीण सहकारी बैंकों को उनके डिजिटल स्तर और भुगतान प्रणाली के परिदृश्य के साथ उनके पारस्परिक जुड़ाव के आधार पर चार स्तरों में श्रेणीकृत किया गया है. इन स्तरों को निम्नानुसार परिभाषित किया गया है:

स्तर	मानदंड	विनियामक निर्धारण	अभ्युक्ति
स्तर I	सभी आरसीबी	अनुबंध-1 में निर्धारित स्तर I के नियंत्रण	नियंत्रणों के अतिरिक्त, बैंक साइबर सुरक्षा के वल्नरेबिलिटी सूचकांक (वीआईसीएस-विक्स) टूल (अनुबंध 1अ) का प्रयोग करते हुए साइबर सुरक्षा को लेकर अपनी तैयारी का परीक्षण कर सकते हैं.
स्तर II	वे सभी आरसीबी, जो केंद्रीय भुगतान प्रणाली के	अनुबंध-1 में निर्धारित स्तर I के नियंत्रण के	अतिरिक्त नियंत्रणों में शामिल हैं: डाटा की क्षति

राष्ट्रीय कृषि और ग्रामीण विकास बैंक

National Bank for Agriculture and Rural Development

पर्यवेक्षण विभाग

प्लॉट नं. सी-24, 'जी' ब्लॉक, बांद्रा - कुर्ला कॉम्प्लेक्स बांद्रा (पूर्व), मुंबई - 400 051. • टेलि.: +91 22 2653 0017 • फैक्स : +91 22 2653 0103 • ई-मेल : dos@nabard.org

Department of Supervision

Plot No. C-24, 'G' Block, Bandra-Kurla Complex, Bandra (E), Mumbai - 400 051. • Tel.: +91 22 2653 0017 • Fax : +91 22 2653 0103 • E-mail : dos@nabard.org

**नाबार्ड**

स्तर	मानदंड	विनियामक निर्धारण	अभ्युक्ति
	उप-सदस्य हैं और निम्नलिखित मानदंडों में से कम-से-कम किसी एक को पूरा करते हैं: 1. अपने ग्राहकों को इंटरनेट बैंकिंग सुविधा (व्यू-आधारित और ट्रांजैक्शन- आधारित में से कोई भी) देते हैं. 2. एप्लिकेशन (स्मार्ट फोन का उपयोग) के माध्यम से मोबाइल बैंकिंग सेवा देते हैं. 3. सीटीएस/ आईएमपीएस/ यूपीआई के प्रत्यक्ष सदस्य हैं.	साथ-साथ अनुबंध-II में निर्धारित स्तर II के नियंत्रण	को रोकने की रणनीति, फिशिंग के विरुद्ध नियंत्रण और महत्वपूर्ण एप्लीकेशनों के वीए/पीटी.
स्तर III	वे आरसीबी जो निम्नलिखित मानदंडों में से कम-से-कम किसी एक को पूरा करते हैं: 1. सीपीएस के प्रत्यक्ष सदस्य हैं. 2. जिनके पास अपना एटीएम स्विच है. 3. जिनके पास स्विफ्ट (SWIFT) इंटरफेस है.	स्तर I और II के नियंत्रण के साथ-साथ अनुबंध-III में निर्धारित स्तर III के नियंत्रण	अतिरिक्त नियंत्रणों में शामिल हैं: उन्नत तात्कालिक खतरे से सुरक्षा और उसका प्रबंधन, ट्रांजैक्शन का जोखिम-आधारित अनुप्रवर्तन.
स्तर IV	वे आरसीबी जो सीपीएस के प्रत्यक्ष सदस्य/ उप-सदस्य हैं और जो निम्नलिखित मानदंडों में से	स्तर I, II और III के नियंत्रण के साथ-साथ अनुबंध-IV में निर्धारित स्तर IV के नियंत्रण	अतिरिक्त नियंत्रणों में शामिल हैं: साइबर सुरक्षा परिचालन केंद्र (सी-एसओसी) (अपना स्वयं का

स्तर	मानदंड	विनियामक निर्धारण	अभ्युक्ति
	<p>कम-से-कम किसी एक को पूरा करते हैं:</p> <p>1. जिनके पास अपना एटीएम स्विच है और जिनके पास स्विफ्ट (SWIFT) इंटरफेस है.</p> <p>2. जो डाटा सेंटर होस्ट करते हैं या अपने स्वयं के अथवा अपनी सहायक संस्थाओं के माध्यम से अन्य बैंकों को सॉफ्टवेयर सपोर्ट देते हैं.</p>		<p>अथवा सेवा-प्रदाताओं के माध्यम से) की स्थापना, और उच्चतर उत्तरदायित्व की सूचना प्रौद्योगिकी (आईटी) और सूचना सुरक्षा (आईएस) गवर्नेंस फ्रेमवर्क की स्थापना, परिपत्र जारी होने की तारीख से छह माह के भीतर.</p>

3. निदेशक बोर्ड अंतिम रूप से बैंक की सूचना सुरक्षा के लिए उत्तरदायी है और वह प्रभावी सूचना प्रौद्योगिकी (आईटी) और सूचना सुरक्षा (आईएस) गवर्नेंस सुनिश्चित करने में अग्रसक्रिय भूमिका निभाएगा. शीर्ष प्रबंध तंत्र की प्रमुख भूमिका होगी बोर्ड द्वारा अनुमोदित साइबर सुरक्षा नीति को कार्यान्वित करना, साइबर सुरक्षा के लिए आवश्यक सांगठनिक प्रक्रियाएँ स्थापित करना और पर्याप्त साइबर सुरक्षा सुनिश्चित करने के लिए आवश्यक संसाधन उपलब्ध कराना.

4. ग्रामीण सहकारी बैंक ऊपर दी गई तालिका में उल्लिखित मानदंडों के आधार पर स्व-मूल्यांकन कर, यह निर्धारित करेंगे कि वे किस स्तर के लिए उपयुक्त हैं और इसकी सूचना इस परिपत्र के जारी होने के 45 दिन के भीतर नाबार्ड के संबन्धित क्षेत्रीय कार्यालय को देंगे.

5. सभी ग्रामीण सहकारी बैंक इस परिपत्र के जारी होने से तीन महीने के भीतर **अनुबंध I** में निर्धारित नियंत्रण अपेक्षाओं का अनुपालन करेंगे. इसी प्रकार, स्तर II, III और IV के ग्रामीण सहकारी बैंक क्रमशः **अनुबंध II, III और IV** में निर्धारित नियंत्रण अपेक्षाओं को लागू करेंगे.

6. ग्रामीण सहकारी बैंक स्वयं किए गए जोखिम और क्षमता आकलन के आधार पर सुरक्षा उपायों के उच्चतर स्तर को अपना सकते हैं। इसके अलावा, यदि किसी ग्रामीण सहकारी बैंक ने, चाहे उसकी आस्तियों की राशि कितनी भी क्यों न हो, साइबर सुरक्षा के ऐसे फ्रेमवर्क को अपनाया है जो उनके उपयुक्त स्तर से ऊपर के स्तर का है, तो उत्कृष्ट पद्धति के रूप में यह वांछनीय है कि वह विद्यमान गवर्नेंस संरचना को बनाए रखे।

7. साइबर सुरक्षा नियंत्रणों की स्थापना के लिए साइबर सुरक्षा फ्रेमवर्क हेतु वल्लरेबिलिटी सूचकांक (विव्स) का उपयोग मार्गदर्शक टूल के रूप में किया जा सकता है।

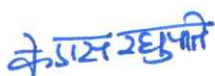
8. साइबर सुरक्षा फ्रेमवर्क के कार्यान्वयन की प्राथमिक ज़िम्मेदारी बैंक की ही है। राज्य सहकारी (रास) बैंकों के साथ आईटी प्लेटफॉर्म शेयर करने वाले जिला मध्यवर्ती सहकारी (जिमस) बैंक अपने रास बैंक के परामर्श से हमारे परिपत्र में जारी सभी निर्धारित साइबर सुरक्षा नियंत्रणों की समीक्षा कर सकते हैं। साइबर सुरक्षा फ्रेमवर्क के परिप्रेक्ष्य में रास बैंकों और जिमस बैंकों की भूमिकाओं और दायित्वों का प्रलेखीकरण रास बैंक और जिमस बैंक, दोनों स्तरों पर मेन्टेन किया जा सकता है।

9. जैसा कि 16 मार्च 2018 के हमारे परिपत्र में निर्दिष्ट किया गया है, सभी ग्रामीण सहकारी बैंकों को साइबर सुरक्षा से जुड़ी सभी घटनाएँ, चाहे वे सफल हुई हों या कोशिश भर रही हों, सीएसआईटीई कक्ष, नाबार्ड को ई-मेल (csite@nabard.org) द्वारा तुरंत रिपोर्ट करना है और उसकी एक प्रति नाबार्ड के संबन्धित क्षेत्रीय कार्यालय को परांकित करनी है। यदि साइबर सुरक्षा से जुड़ी कोई घटना न हुई हो / खतरा न देखा गया हो तो तिमाही शून्य रिपोर्ट भेजी जानी चाहिए।

10. इस परिपत्र की एक प्रति निदेशक बोर्ड की आगामी बैठक में रखी जा सकती है।

11. कृपया पावती दें।

भवदीय



(के एस रघुपति)

मुख्य महाप्रबंधक

संलग्न: यथोक्त।

Baseline Cyber Security and Resilience Requirements - Level I

The following controls shall be implemented:

1. Inventory Management of Business IT Assets

- 1.1 The bank should maintain an up-to-date Inventory Register of Business IT Assets containing the following details, as a minimum requirement:
 - a. Detail of the IT Asset (viz., hardware/software/network devices, key personnel, services, etc.)
 - b. Details of systems where customer data are stored.
 - c. Associated business applications, if any.
 - d. Criticality of the IT asset (for example, High/Medium/Low).
- 1.2 Classify data/information based on sensitivity criteria of the information.
- 1.3 Appropriately manage and provide protection within and outside RCB/network, keeping in mind how the data/information is stored, transmitted, processed, accessed and put to use within/outside the RCB's network, and level of risk they are exposed to depending on the sensitivity of the data/information.

2. Board approved Cyber Security Policy

All RCBs should immediately put in place a Cyber Security policy, duly approved by their Board/Administrator, giving a framework and the strategy containing a suitable approach to check cyber threats depending on the level of complexity of business and acceptable levels of risk. It shall be ensured that the cyber security policy deals with the following broad aspects, keeping in view the level of technology adoption and digital products offered to the customers:

2.1 Cyber Security Policy should be distinct from the IT policy/IS Policy of the RCBs so that it highlights the risks from cyber threats and the measures to address/reduce these risks. While identifying and assessing the inherent risks, RCBs should keep in view the technologies adopted, delivery channels, digital products being offered, internal and external threats etc. and rate each of these risks as Low, Medium, High and Very High.

2.2 IT Architecture/Framework should be security compliant:

The IT architecture/framework which includes network, server, database and application, end user systems, etc. should take care of security measures at all times and this should be reviewed by the Board or IT Sub-committee of the Board periodically. For this purpose, RCBs may carry out the following steps:



- a) Identify weak/vulnerable areas in IT systems and processes,
- b) Allow restricted access to networks, databases and applications wherever permitted, through well-defined processes and approvals including rationale for permitting such access,
- c) Assess the cost of impact in case of breaches/failures in these areas and put in place suitable Cyber Security system to address them,
- d) Specify and document clearly the responsibility for each of above steps.

A proper record should be kept of the entire process to enable supervisory assessment.

2.3 Cyber Crisis Management Plan: Since cyber risk is different from many other risks, the traditional BCP/DR (Business Continuity Plan/Disaster Recovery) arrangements may not be adequate and hence needs to be revisited keeping in view the nature of cyber risk. The Government of India organisation, CERT-In (Computer Emergency Response Team – India, a Government entity) has been taking important initiatives in strengthening Cyber Security by providing proactive/reactive services and guidelines, threat intelligence and assessment of preparedness of various agencies in different sectors, including the financial sector. CERT-In also has come out with National Cyber Crisis Management Plan and Cyber Security Assessment Framework. RCBs may refer to CERT-In/NCIIPC/RBI/IDRBT guidelines as reference material for their guidance.

2.4 Cyber Intrusions: RCBs should promptly detect any cyber intrusions (unauthorised entries) so as to respond/recover/contain impact of cyber-attacks. Among other things, RCBs, especially those offering services such as internet banking, mobile banking, mobile wallet, RTGS/NEFT/IMPS, SWIFT, debit cards, credit cards, etc. should take necessary detective and corrective measures/steps to address various types of cyber threats viz. denial of service (DoS), distributed denial of services (DDoS), ransomware/crypto ware, destructive malware, business email frauds including spam, email phishing, spear phishing, whaling, vishing frauds, drive-by downloads, browser gateway fraud, ghost administrator exploits, identity frauds, memory update frauds, password related frauds, etc.

3. Preventing access of unauthorised software

- 3.1 Maintain an up-to-date and preferably centralised inventory of authorised software(s)/approved applications/software/libraries, etc.
- 3.2 Put in place a mechanism to control installation of software/applications on end-user PCs, laptops, workstations, servers, mobile devices, etc. Also, put in place a mechanism to block/prevent and



identify installation and running of unauthorised software/applications on such devices/systems.

- 3.3 The web browser settings should be set to auto update and consider disabling scripts like JavaScript, Java and ActiveX controls when they are not in use.
- 3.4 Internet usage, if any, should be restricted to identified standalone computer(s) in the branch of an RCB which are strictly separate from the systems identified for running day to day business.

4. Environmental Controls

- 4.1 Put in place appropriate controls for securing physical location of critical assets (as identified by the RCB under its inventory of IT assets), providing protection from natural and man-made threats.
- 4.2 Put in place mechanisms for monitoring of breaches/compromises of environmental controls relating to temperature, water, smoke, access alarms, service availability alerts (power supply, telecommunication, servers), access logs, etc. Appropriate physical security measures shall be taken to protect the critical assets of the RCB.

5. Network Management and Security

- 5.1 Ensure that all the network devices are configured appropriately and periodically assessed to ensure that such configurations are securely maintained.
- 5.2 The default passwords of all the network devices/systems should be changed after installation.
- 5.3 Put in appropriate controls to secure wireless local area networks, wireless access points, wireless client access systems.
- 5.4 Critical infrastructure of RCB (viz., NEFT, RTGS, SWIFT, CBS, ATM infrastructure) should be designed with adequate network separation controls.
- 5.5 Conduct security review of PCs/terminals used for accessing corporate Internet Banking applications of sponsor banks (SCBs/State Co-operative Banks), CBS servers and network perimeter through a qualified information security auditor.
- 5.6 There should be a robust password management policy in place, with specific emphasis for sensitive activities like accessing critical systems, putting through financial transactions. Usage of trivial passwords shall be avoided. [An illustrative but not exhaustive list of practices that should be strictly avoided are: For example, XYZ bank having password as xyz@123; network/server/security solution devices with passwords as device/solution_name123/device_name/ solution@123; hard coding of passwords in plain text in thick clients or storage of passwords in plain text in the databases.



6. Secure Configuration

- 6.1 The firewall configurations should be set to the highest security level and evaluation of critical device (such as firewall, network switches, security devices, etc.) configurations should be done periodically.
- 6.2 Systems such as Network, application, database and servers should be used dedicatedly for the purpose for which they have been set up.
- 6.3 Disable remote connections from outside machines to the network hosting critical payment infrastructure (Ex: RTGS/NEFT, ATM Switch, SWIFT Interface). Disable Remote Desktop Protocol (RDP) on all critical systems.

7. Anti-virus and Patch Management

- 7.1 Put in place systems and processes to identify, track, manage and monitor the status of patches to servers, operating system and application software running at the systems used by the RCB officials (end-users).
- 7.2 Implement and update antivirus protection for all servers and applicable end points preferably through a centralised system.

8. User Access Control/Management

- 8.1 Disallow administrative rights on end-user workstations/PCs/laptops and provide access rights on a 'need to know' and 'need to do' basis.
- 8.2 Passwords should be set as complex and lengthy and users should not use same passwords for all the applications/systems/devices.
- 8.3 Remote Desktop Protocol (RDP) which allows others to access the computer remotely over a network or over the internet should be always disabled. In extreme circumstances if RDP has to be used it should be enabled only with the approval of the CISO (see para 17) of the RCB and a record of such permissions with reasons and complete details may be maintained. Logs for such remote access shall be enabled and monitored for suspicious activities.
- 8.4 Implement appropriate (e.g. centralised) systems and controls to allow, manage, log and monitor privileged/super user/administrative access to critical systems (servers/databases, applications, network devices etc.)
- 8.5 RCBs shall put in place two factor authentication for accessing their CBS and applications connecting to the CBS with the 2nd factor being **dynamic** in nature. (Eg: 2nd factor should not be a static password and must not be associated with the PC/terminal used for putting through payment transactions).

9. Secure mail and messaging systems

- 9.1 Implement bank specific email domains (example, XYZ bank with mail domain xyz.in) with anti-phishing and anti-malware, DMARC controls enforced in the email solution.



- 9.2 Implement secure mail and messaging systems, including those used by RCB's partners & vendors, that include measures to prevent email spoofing, identical mail domains, protection of attachments, malicious links, etc.
- 9.3 Document and implement email server specific controls.

10. Removable Media

- 10.1 As a default rule, use of removable devices and media should not be permitted in the banking environment unless specifically authorised for defined use and duration of use.
- 10.2 Secure the usage of removable media on workstations/PCs/Laptops, etc. and secure erasure/deletion of data on such media after use.
- 10.3 Get the removable media scanned for malware/anti-virus prior to providing read/write access.

11. User/Employee/Management Awareness

- 11.1 Communicate to users/employees, vendors & partners security policies covering secure and acceptable use of RCB's network/assets including customer information/data, educating them about cyber security risks and protection measures at their level.
- 11.2 Conduct awareness/training for staff on basic information security controls (Do's and Don'ts), incident reporting, etc.
- 11.3 Board members may be kept updated on basic tenets/principles of IT risk/cyber security risk at least once a year.
- 11.4 The end-users should be made aware to never open or download an email attachment from unknown sources.
- 11.5 Educate employees to strictly avoid clicking any links received via email (to prevent phishing attacks).

12. Customer Education and Awareness

- 12.1 Improve and maintain customer awareness and education with regard to cyber security risks.
- 12.2 Educate the customers on keeping their card, PIN, etc. secure and not to share with any third party.

13. Backup and Restoration

Take periodic back up of the important data and store this data 'off line' (i.e., transferring important files to a storage device that can be detached from a computer/system after copying all the files).

14. Data Leak Prevention Strategy

- 14.1 Develop and implement a comprehensive data loss/leakage prevention strategy to safeguard sensitive (including confidential) business and customer data/information.



14.2 Similar arrangements need to be ensured at vendor managed facilities as well.

15. Vendor/Outsourcing Risk Management

RCBs may adhere to the guidelines on sharing of Information Technology resources issued by RBI vide their circular RBI/2013-14/216 dated 30 August 2013. In addition to the above, the following are to be included:

- 15.1 RCBs shall be accountable for ensuring appropriate management and assurance on security risks in outsourced vendor arrangements. RCBs shall carefully evaluate the need for outsourcing critical processes and selection of vendor/partner based on comprehensive risk assessment. RCBs shall regularly conduct effective due diligence, oversight and management of third party vendors/service providers and partners.
- 15.2 RCBs shall be required to be thoroughly satisfied about the credentials of vendor/third-party personnel accessing and managing the RCB's critical assets. Background checks, non-disclosure and security policy compliance agreements shall be mandated for all third party service providers.
- 15.3 The bank shall be required to necessarily enter into agreement with the service provider that, among other things, provides for right to audit by the RCB. The outsourcing agreements should include clauses to recognise the right of the Reserve Bank of India/NABARD to cause an inspection to be made of a service provider of the RCB and allow the Reserve Bank of India or NABARD or persons authorised by it to access the bank's documents, records of transactions, logs and other necessary information given to, stored or processed by the service provider within a reasonable time.
- 15.4 All the outsourcing Service Level Agreements (SLAs) signed with the vendors must clearly mention the responsibility of the RCB and vendor in case of any failure of services.
- 15.5 All the existing outsourcing SLAs may be reviewed and vetted for inclusion of conditions indicated at 15.3 and 15.4 above. If the SLAs are found not complying with the same there is a need to revise the SLA by adding a suitable addendum to the SLA with mutual consent.
- 15.6 The agreements must clearly mention the grievance redressal mechanism to resolve customer complaints.
- 15.7 Vendors' service level agreements shall be periodically reviewed for performance in security controls.

16. Supervisory Reporting Framework - Reporting of Cyber Incidents

Put in place an effective mechanism to report the cyber security incidents in a timely manner and take appropriate action to mitigate the incident. RCBs shall also report all unusual cyber security incidents to CERT-In and IB-CART.



17. Chief Information Security Officer (CISO)

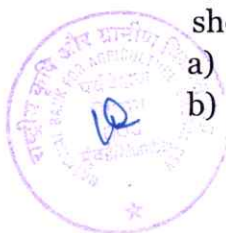
A senior level official (GM/DGM) should be designated as Chief Information Security Officer (CISO), responsible for articulating and enforcing the policies that the RCB uses to protect its information assets apart from coordinating the cyber security related issues/implementation within the organisation as well as relevant external agencies. The CISO shall be primarily responsible for ensuring compliance to various instructions issued on information/cyber security by NABARD/RBI. The following may be noted in this regard:

- a) The CISO should report directly to the top executive overseeing the risk management function or in his absence to the CEO directly.
- b) The CISO should have a reasonable minimum term.
- c) The CISO should place a separate review of cyber security arrangements/preparedness of the RCB before the Board on a quarterly basis.
- d) The CISO will be responsible for bringing to the notice of the Board about the vulnerabilities and cyber security risks that the RCB is exposed to.
- e) The CISO, by virtue of his role as member secretary of information security and/or related committees(s), if any, may assess, inter alia, current/emerging cyber threats to banking (including payment systems) sector and ensure that the RCB's preparedness in these aspects are invariably discussed in such committee(s).
- f) The CISO shall be an invitee to the IT Strategy Committee and IT Steering Committee. The CISO may also be a member of (or invited to) committees on operational risk where IT/IS risk is also discussed.
- g) The CISO's office shall be adequately staffed with technically competent people, if necessary, through recruitment of specialist officers, commensurate with the business volume, extent of technology adoption and complexity.

18. IT Steering Committee

An IT Steering Committee shall be formed with representatives from the IT, HR, legal and business sectors. Its role is to assist the Executive Management in implementing IT strategy that has been approved by the IT Sub Committee of the Board. The IT Steering committee/Board should appraise/report to the IT Sub-Committee periodically. The committee should focus on implementation. Its functions, inter-alia, include:

- a) Defining project priorities and assessing strategic fit for IT proposals.
- b) Reviewing, approving and funding initiatives, after assessing value-addition to business process.



19. Information Security Committee

Since IT/cyber security affects all aspects of an organisation, in order to consider IT/cyber security from a RCB-wide perspective a steering committee of executives should be formed with formal terms of reference. The CISO would be the member secretary of the Committee. The Information Security Committee may include, among others, the Chief Executive Officer (CEO) or designee and two senior management officials well versed in the subject. The Committee shall meet at least on a quarterly basis. Major responsibilities of the Information Security Committee, inter-alia, include:

- a) Developing and facilitating the implementation of information security policies, standards and procedures to ensure that all identified risks are managed within a RCB's risk appetite.
- b) Supporting the development and implementation of a RCB-wide information security management programme.

20. Audit Committee of Board (ACB)

Please refer to our circular NB.DoS. HO. Pol/ 1H-872 /J-1/2003-04 dated 19 August 2003 on setting up of Audit Committee (ACB) at the Board level. In addition to its prescribed role as per extant instructions, the ACB shall also be responsible for the following:

- a) Performance of IS Audit and Evaluation of significant IS Audit issues – The ACB should devote appropriate and sufficient time to IS Audit findings identified and members of ACB need to review critical issues highlighted and provide appropriate guidance to the RCB's management.
- b) Monitor the compliance in respect of the information security reviews/VA-PT audits under various scope conducted by internal as well as external auditors/consultants to ensure that open issues are closed on a timely basis and sustenance of the compliance is adhered to.

21. RCBs may assess their preparedness on Level I controls on a periodic basis and use the Vulnerability Index for Cyber security Framework (VICS) tool as a guidance for the same. **VICS may be administered and findings may be placed before the IT Sub Committee and the Board.**



Annexure-IA

The Vulnerability Index for Cyber Security Framework (VICS) is a self-assessment tool to be administered by a bank to assess the existing level of baseline cyber security framework within the organisation. The controls specified in VICS are based on the Cyber Security framework specified for Level I (Annexure I) in the circular, and are only indicative in nature. Banks are encouraged to adopt and implement more stringent controls and strengthen the Cyber security posture of the organisation.

VICS covers four major areas viz. a) Baseline Cyber Security Framework (CSF), b) Policy strength, c) Vendor management and d) Cyber Security Crisis Management Plan through 30 major topics.

Scoring:

Grade	Score	VICS implication for the Bank
A	> 75% in each of the categories OR 75% overall	i. indicates that the bank has taken purposeful steps and adopted best practices in strengthening its security posture. ii. The bank may adopt the remaining controls depending on the products and services offered by it at the earliest.
B	< 75% and > 50% in each of the categories OR < 75% and > 50% overall provided the score is >50% in at least three categories	i. indicates that the bank is on the way to strengthening its cyber security posture but will have to overcome staff/knowledge and policy constraints in achieving its goals in CSF. ii. The bank may develop a time bound plan to achieve more than 75% compliance in all categories.
C	< 50% in two or more than two categories OR < 50% overall	i. Cyber Security and understanding are a serious concern in the Bank. The bank is highly prone to threats/incidents due to lack of basic CSF controls ii. Bank may need to seek professional consultancy in doing a gap assessment on CSF as prescribed in our circulars dated 16 March 2018 and 06 February 2020 to comply with Level I controls.

Note: Banks have to achieve Level I controls within three months of issue of this circular irrespective of marks scored. VICS is only an assessment tool to help banks in self-assessment. (Please see Appendix-A for VICS tool)



Level II - Baseline Cyber Security and Resilience Requirements (in addition to the requirements given in Annexure-I)

In addition to controls indicated at Annexure-I, the following controls shall be implemented:

1. Network Management and Security

- 1.1 Maintain an up-to-date/centralised inventory of authorised devices connected to RCB's network (within/outside RCB's premises) and related network devices in the RCB's network.
- 1.2 Boundary defences should be multi-layered with properly configured firewalls, proxies, De-Militarized Zone (DMZ) perimeter networks, and network-based Intrusion Prevention System (IPS)/Intrusion Detection System (IDS). Mechanism to filter both inbound and outbound traffic shall be put in place.
- 1.3 LAN segments for in-house/onsite ATM and CBS/branch network should be different.

2. Secure Configuration

Document and apply baseline security requirements/configurations to all categories of devices (end-points/workstations, mobile devices, operating systems, databases, applications, network devices, security devices, security systems, etc.), throughout the lifecycle (from conception to deployment) and carry out reviews periodically.

3. Application Security Life Cycle (ASLC)

- 3.1 The development/test and production environments need to be properly segregated. The data used for development and testing should be appropriately masked.
- 3.2 Software/Application development approach should incorporate secure coding principles, security testing (based on global standards) and secure rollout.

4. Change Management

RCBs should have a robust change management process in place to record/monitor all the changes that are moved/pushed into production environment. Changes to business applications, supporting technology, service components and facilities should be managed using robust configuration management processes that ensure integrity of any changes thereto.



5. Periodic Testing

- 5.1 Periodically conduct Vulnerability Assessment/Penetration Testing (VA/PT) of internet facing web/mobile applications, servers and network components throughout their lifecycle (pre-implementation, post implementation, after changes, etc.). VA of critical applications and those on DMZ shall be conducted at least once in every 6 months. PT shall be conducted at least once in a year.
- 5.2 RCBs having CBS on a shared infrastructure of an Application Service Provider (CBS-ASP) shall get their CBS application including the infrastructure hosting it subjected to VA/PT through the CBS-ASP.
- 5.3 Application security testing of web/mobile applications should be conducted before going live and after every major change(s) in the applications.
- 5.4 The vulnerabilities detected are to be remedied promptly in terms of the RCB's risk management/treatment framework so as to avoid exploitation of such vulnerabilities.
- 5.5 Penetration testing of public facing systems as well as other critical applications are to be carried out by professionally qualified teams. Findings of VA/PT and the follow up actions necessitated are to be monitored closely by the Information Security/Information Technology Audit team as well as Top Management.

6. User Access Control/Management

Provide secure access to the RCB's assets/services from within/outside RCB's 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 VPN or other standard secure protocols, etc.)

7. Authentication Framework for Customers

- 7.1 RCBs should have adequate checks and balances to ensure (including security of customer access credentials held with them) that transactions are put only through the genuine/authorised applications and that authentication methodology is robust, secure and centralised.
- 7.2 Implement authentication framework/mechanism to securely verify and identify the applications of RCB to customers (Example, with digital certificate).

8. Anti-Phishing

Subscribe to Anti-phishing/anti-rogue application services from external service providers for identifying and taking down phishing websites/rogue applications.



9. User/Employee/Management Awareness

- 9.1 Encourage them to report suspicious behaviour incidents to the incident management team.
- 9.2 Make cyber security awareness programs mandatory for new recruits and web-based quiz and training for lower, middle and upper management every year.
- 9.3 Board members may be sensitised on various technological developments and cyber security related developments periodically.

10. Audit Logs

- 10.1 Capture the audit logs pertaining to user actions in a system. Such arrangements should facilitate forensic auditing, if need be.
- 10.2 An alert mechanism should be set to monitor any change in the log settings.

11. Incident Response and Management

- 11.1 Put in place an effective Incident Response programme. RCBs must have a mechanism/resources to take appropriate action in case of any cyber security incident. They must have written incident response procedures including the roles of staff/outsourced staff handling such incidents.
- 11.2 RCBs are responsible for meeting the requirements prescribed for incident management and BCP/DR even if their IT infrastructure, systems, applications, etc., are managed by third party vendors/service providers.



Level III - Baseline Cyber Security and Resilience Requirements (in addition to the requirements given in Annexures-I & II)

1. Network Management and Security

- 1.1 Put in place mechanism to detect and remedy any unusual activities in systems, servers, network devices and endpoints.
- 1.2 Firewall rules shall be defined to block unidentified outbound connections, reverse TCP shells and other potential backdoor connections.

2. Secure Configuration

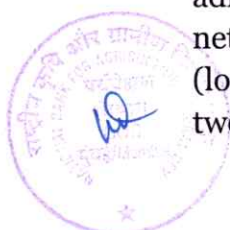
- 2.1 Enable IP table to restrict access to the clients and servers in SWIFT and ATM Switch environment only to authorised systems.
- 2.2 Ensure the software integrity of the ATM Switch/SWIFT related applications.
- 2.3 Disable PowerShell in servers where not required and disable PowerShell in Desktop systems.
- 2.4 Restrict default shares including IPC share (inter-process communication share)

3. Application Security Life Cycle (ASLC)

- 3.1 In respect of critical business applications, RCBs may conduct source code audits by professionally competent personnel/service providers or have assurance from application providers/OEMs that the application is free from embedded malicious/fraudulent code.
- 3.2 Besides business functionalities, security requirements relating to system access control, authentication, transaction authorization, data integrity, system activity logging, audit trail, session management, security event tracking and exception handling are required to be clearly specified at the initial and ongoing stages of system development/acquisition/implementation.
- 3.3 Ensure that software/application development practices adopt principle of defence-in-depth to provide layered security mechanism.
- 3.4 Ensure that adoption of new technologies is adequately evaluated for existing/evolving security threats and that the IT/security team of the RCB achieve reasonable level of comfort and maturity with such technologies before introducing them for critical systems of the RCB.

4. User Access Control

- 4.1 Implement a centralised authentication and authorisation system through an Identity and Access Management solution for accessing and administering critical applications, operating systems, databases, network and security devices/systems, point of connectivity (local/remote, etc.) including enforcement of strong password policy, two-factor/multi-factor authentication, securing privileged accesses



following the principle of least privileges and separation of duties. This shall be implemented by the bank either with the in-house team managing the infrastructure or through the service provider if their infrastructure is hosted at a shared location at the service provider's end.

- 4.2 Implement centralised policies through Active Directory or Endpoint management systems to whitelist/blacklist/restrict removable media use.

5. Advanced Real-time Threat Defence and Management

- 5.1 Build a robust defence against the installation, spread, and execution of malicious code at multiple points in the enterprise.
- 5.2 Implement whitelisting of internet websites/systems.

6. Maintenance, Monitoring, and Analysis of Audit Logs

- 6.1 Consult all the stakeholders before finalising the scope, frequency and storage of log collection.
- 6.2 Manage and analyse audit logs in a systematic manner so as to detect, respond, understand or recover from an attack.
- 6.3 Implement and periodically validate settings for capturing of appropriate logs/audit trails of each device, system software and application software, ensuring that logs include minimum information to uniquely identify the log for example by including a date, timestamp, source addresses, destination addresses.

7. Incident Response and Management

- 7.1 RCB's BCP/DR capabilities shall adequately and effectively support the RCB's cyber resilience objectives and should be so designed to enable the RCB to recover rapidly from cyber-attacks/other incidents and safely resume critical operations aligned with recovery time objectives while ensuring security of processes and data is protected.
- 7.2 RCBs shall have necessary arrangements, including a documented procedure, with such third party vendors/service providers for such purpose. This shall include, among other things, to get informed about any cyber security incident occurring in respect of the bank on timely basis to mitigate the risk early as well as to meet extant regulatory requirements.
- 7.3 Have a mechanism to dynamically incorporate lessons learnt to continually improve the response strategies. Response strategies shall consider readiness to meet various incident scenarios based on situational awareness and potential/post impact, consistent communication and co-ordination with stakeholders during response.

8. Risk based transaction monitoring

(This control shall be applicable to those banks who are direct members of CPS as well as having their own ATM Switch interface or SWIFT interface)

Risk based transaction monitoring or surveillance process shall be implemented as part of fraud risk management system across all delivery channels.



Level IV - Baseline Cyber Security and Resilience Requirements (in addition to the requirements given in Annexures-I, II & III)

1. Arrangement for continuous surveillance - Setting up of Cyber Security Operation Centre (C-SOC)

RCBs are mandated that a C-SOC (Cyber Security Operations Centre) be set up at the earliest, if not yet done. It is also essential that this Centre ensures continuous surveillance and keeps itself regularly updated on the latest nature of emerging cyber threats.

1.1 Expectations from C-SOC

- i. Ability to protect critical business and customer data/information, demonstrate compliance with relevant internal guidelines, country regulations and laws.
- ii. Ability to provide real-time/near-real time information on and insight into the security posture of the RCB.
- iii. Ability to effectively and efficiently manage security operations by preparing for and responding to cyber risks/threats, facilitate continuity and recovery.
- iv. Ability to know who did what, when, how and preservation of evidence.
- v. Integration of various log types and logging options into a Security Information and Event Management (SIEM) system, ticketing/workflow/case management, unstructured data/big data, reporting/dashboard, use cases/rule design (customised based on risk and compliance requirements/drivers, etc.), etc.
- vi. C-SOC should be able to monitor the logs of various network activities and should have the capability to escalate any abnormal/undesirable activities.
- vii. Key Responsibilities of C-SOC could include:
 - a) Monitor, analyse and escalate security incidents
 - b) Develop Response - protect, detect, respond, recover
 - c) Conduct Incident Management and Forensic Analysis
 - d) Co-ordination with relevant stakeholders within the RCB/external agencies.

1.2 Steps for setting up C-SOC – Technological Aspects

- i. First step is to arrive at a suitable and cost effective technology framework designed and implemented to ensure proactive monitoring capabilities aligned with the banking technology risk profile and business and regulatory requirements. Clear understanding of the service delivery architecture deployed by the RCB will enable identification of the location for the sensors to collect the logs that are



required to carry out the analysis and investigation. SIEM is able to meet this requirement to some extent but a holistic approach to problem identification and solution is required.

- ii. Second step is to have a security analytics engine which can process the logs within reasonable time frame and come out with possible recommendations with options for further deep dive investigations.
- iii. Third step is to look at deep packet inspection approaches.
- iv. Fourth step is to have tools and technologies for malware detection and analysis as well as imaging solutions for data to address the forensics requirements.
- v. It is to be noted that the solution architecture deployed for the above has to address performance and scalability requirements in addition to high availability requirements. Some of the aspects to be considered are:
 - a) Staffing of C-SOC - is it required to be 24x7x365, in shifts, business hours only, etc.
 - b) Model used - Finding staff with required skills/managed security service provider with required skill set.
 - c) Metrics to measure performance of C-SOC.
 - d) Ensuring scalability and continuity of staff through appropriate capacity planning initiatives.

2. Participation in Cyber Drills

RCBs shall participate in cyber drills conducted under the aegis of Cert-IN, IDRBT, etc.

3. Incident Response and Management

- 3.1 RCBs shall ensure incident response capabilities in all interconnected systems and networks including those of vendors and partners and readiness demonstrated through collaborative and co-ordinated resilience testing that meet the RCB's recovery time objectives.
- 3.2 Implement a policy & framework for aligning Security Operation Centre, Incident Response and Digital forensics to reduce the business downtime/to bounce back to normalcy.

4. Forensics and Metrics

- 4.1 Develop a comprehensive set of metrics that provides for prospective and retrospective measures, like key performance indicators and key risk indicators. Some illustrative metrics include coverage of anti-malware software and their updation percentage, patch latency, extent of user awareness training, vulnerability related metrics, number of open vulnerabilities, IS/security audit observations, etc.
- 4.2 Have support/arrangement for network forensics/forensic investigation/distributed denial-of-service (DDOS) mitigation services on stand-by.



5. IT Strategy and Policy

- 5.1 The Board approved Cyber Security Policy may invariably include IT-related strategy and policies covering areas such as:
- a) Existing and proposed hardware and networking architecture for the RCB and its rationale.
 - b) Standards for hardware or software prescribed by the proposed architecture.
 - c) Strategy for outsourcing, in-sourcing, procuring off-the-shelf software and in-house development.
 - d) IT Department's Organisational Structure.
 - e) Desired number and level of IT expertise or competencies in RCB's human resources, plan to bridge the gap (if any) and requirements relating to training and development.
 - f) Strategy for keeping abreast with technology developments and to update systems as and when required.
 - g) Strategy for independent assessment, evaluation and monitoring of IT risks, findings of IT/IS/Cyber security related audits.

6. IT and IS Governance Framework

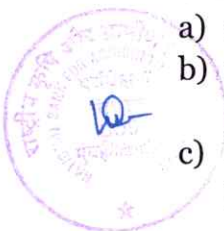
a) Security Team/Function

RCBs shall form a separate cyber security function/group to focus exclusively on cyber security management. The organisation of the cyber security function should be commensurate with the nature and size of activities of the RCB including factors such as technologies adopted, delivery channels, digital products being offered, internal and external threats, etc. The cyber security function should be adequately resourced in terms of the number of staff, level of skills and tools or techniques like risk assessment, security architecture, vulnerability assessment, forensic assessment, etc.

b) IT Strategy Committee

RCBs may consider setting up a Board level IT Strategy Committee with a minimum of two directors as members, one of whom should be a professional director. At least two members of the IT Strategy Committee would need to be technically competent while at least one member would need to have substantial expertise in managing/guiding technology initiatives. Roles and responsibilities of IT Strategy Committee/Board include:

- a) approving IT strategy and policy documents.
- b) ensuring that the management has put an effective strategic planning process in place.
- c) Ensuring that the IT organizational structure complements the business model and its direction.



- d) Ensuring IT investments represent a balance of risks and benefits and that budgets are acceptable.
- e) Reviewing IT performance measurement and contribution of IT to businesses.

c) IT Steering Committee

The IT Steering Committee with representatives from the IT, HR, legal and business sectors shall assist the Executive Management in implementing IT strategy that has been approved by the IT Strategy Committee of the Board. It includes prioritization of IT-enabled investment, reviewing the status of projects (including resource conflict), monitoring service levels and improvements, IT service delivery and projects. The IT Steering committee/Board should appraise/report to the IT Strategy Committee periodically. The committee should focus on implementation. In addition to the functions of the IT strategy Committee indicated at para 18 of Annexure I, the other functions of the Committee shall, inter-alia, include:

- a) Ensuring that all critical projects have a component for “project risk management”.
- b) Sponsoring or assisting in governance, risk and control framework, and also directing and monitoring key IT Governance processes.
- c) Provide direction relating to technology standards and practices.
- d) Ensure that vulnerability assessments of new technology is performed.
- e) Verify compliance with technology standards and guidelines.
- f) Ensure compliance to regulatory and statutory requirements.
- g) Provide direction to IT architecture design and ensure that the IT architecture reflects the need for legal and regulatory compliance, the ethical use of information and business continuity.

d) Chief Information Security Officer (CISO)

In addition to the functions of CISO laid down in para 17 of Annexure I, it may be ensured that:

- a) The CISO should have the requisite technical background and expertise.
- b) The RCB's Board should be able to objectively measure steps to assess the effectiveness of the CISO's office.
- c) The CISO's office shall be adequately staffed with technically competent people, if necessary, through recruitment of specialist officers, commensurate with the business volume, extent of technology adoption and complexity.



- d) The CISO shall not have any direct reporting relationship with the CIO/CTO and shall not be given any business targets.

e) Information Security Committee

The Information Security Committee will also ensure the following in addition to the functions indicated at para 19 of Annexure I:

- a) Approving and monitoring major cyber security projects and the status of cyber security plans and budgets, establishing priorities, approving standards and procedures
- b) Reviewing the position of security incidents and various information security assessments and monitoring activities across the RCB.
- c) Reviewing the status of security awareness programmes.
- d) Assessing new developments or issues relating to information/cyber security.
- e) Reporting to the Board of Directors on cyber security activities.
- f) Minutes of the Information Security Committee meetings should be maintained to document the committee's activities and decisions and a review on information/cyber security needs to be escalated to the Board on a quarterly basis.



Name of the Bank :
Vulnerability Index of Cyber Security Framework (VICS)

Appendix-A

Sl. no	Category	Topic	Questionnaire	Select Yes / No	Marks obtained	Max marks
		Cyber Security Framework (CSF)				
1	CSF	Business assets and IT asset inventory register	(a) Whether IT Assets have been documented in a separate Inventory Register	Select	0	2
			(b) Whether documented IT assets have been classified based on their sensitivity?	Select	0	1
			(c) Whether the IT assets and sensitivity classification is updated and reviewed periodically?	Select	0	2
			Total		0	5
2	CSF	Preventing access to unauthorised software	(a) Whether the bank has centralised authorised software inventory/ Register?	Select	0	1
			(b) Whether the bank has a mechanism to block installation of unauthorised software	Select	0	1
			(c) Whether Javascripts, java Activex controls disabled when not in use?	Select	0	1
			(d) Whether the bank has ensured that internet usage is limited to stand alone PCs	Select	0	2
			Total		0	5
3	CSF	Environment controls	(a) Whether Fire alarms installed	Select	0	1
			(b) Whether Earthing checked ?	Select	0	1
			(c) Whether Fire extinguisher maintained?	Select	0	1
			(d) Whether Water alarms installed?	Select	0	1
			(e) Whether Smoke alarms installed?	Select	0	1
			Total		0	5



Vulnerability Index of Cyber Security Framework (VICS)

Sl. no	Category	Topic	Questionnaire	Select Yes / No	Marks obtained	Max marks
4	CSF	Network management	(a) Whether Network devices have been configured?	Select	0	1
			(b) Whether Updation of Network devices done on regular basis?	Select	0	1
			(c) Whether secure Password management system in place?	Select	0	1
			(d) whether security review of terminals used to access corporate internet banking applications of sponsor bank is done through a qualified IS auditor?	Select	0	1
			(e) whether there is a documented mechanism to review all the above?	Select	0	1
			Total		0	5
5	CSF	AntiVirus and patch management	(a) Whether Antivirus installed in all Servers/ PCs / endpoints?	Select	0	1
			(c) Whether updation of Antivirus done regularly	Select	0	2
			(c) Whether register for patch updation maintained?	Select	0	2
			Total		0	5
6	CSF	User Access Control	(a) Whether user rights have been defined for each category of users?	Select	0	1
			(b) Whether Admin rights disallowed to end users?	Select	0	1
			(c) Whether Remote Desktop Protocol (RDP) disabled?	Select	0	1
			(d) Does the bank have a two factor authentication (2FA) for CBS and other critical applications with second factor being dynamic?	Select	0	2
			Total		0	5
7	CSF	Removable media	Whether removable media disallowed in all PCs used by the end-users?	Select	0	3
			Whether register for PCs having access to Removable media is maintained separately?	Select	0	2
			Total		0	5



Vulnerability Index of Cyber Security Framework (VICS)

Sl. no	Category	Topic	Questionnaire	Select Yes / No	Marks obtained	Max marks
8	CSF	Secure Configuration	(a) Are the Networks, applications, database and servers used only for the purpose for which they were acquired?	Select	0	3
			(b) Whether firewall settings are updated and set to highest security level?	Select	0	2
			Total		0	5
9	CSF	Gap analysis of Cyber Security Framework	(a) Whether Gap analysis of Cyber Security Framework (Availability vs Requirement) based on IT assets carried out?	Select	0	5
			Total		0	5
10	CSF	Vulnerability Assessment and Penetration Testing	(a) Whether Board approved VAPT policy is available?	Select	0	2
			(b) Whether critical devices / DMZs tested every six months?	Select	0	1
			(c) Whether VAPT is conducted on Web applications, mobile applications, servers, network components throughout lifecycle?	Select	0	2
			Total		0	5
11	CSF	Secure mail and messaging	(a) Whether bank specific domain email system in place?	Select	0	2
			(b) Whether anti phishing, anti malware, DMARC controls enforced with email solution?	Select	0	1
			(c) Whether email server specific controls have been documented?	Select	0	1
			(d) Whether measures have been taken to prevent email spoofing?	Select	0	1
			Total		0	5
		Marks in the category			0	55



Vulnerability Index of Cyber Security Framework (VICS)

Sl. no	Category	Topic	Questionnaire	Select Yes / No	Marks obtained	Max marks
		Strength of Policy Framework				
12	Policy	Board approved Information Security (IS) Policy	(a) Whether Board approved IS policy is available?	Select	0	1
			(b) Whether guidelines are framed for implementing IS policy?	Select	0	2
			(c) Whether the policy is reviewed annually?	Select	0	2
			Total		0	5
13	Policy	Board approved distinct Cyber Security Policy	(a) Whether Board approved Cyber Security policy is available?	Select	0	2
			(b) Whether implementation strategy for Cyber Security policy is documented?	Select	0	2
			(c) Whether the policy is reviewed annually?	Select	0	1
			Total		0	5
14	Policy	Governance Mechanism - Committees	(a) Whether IT Sub-Committee of the Board is constituted?	Select	0	1
			(b) Whether the proceedings / findings of the Sub-Committee are placed before the Board?	Select	0	2
			(d) whether IT Steering Committee set up?	Select	0	2
			(e) Does the IT steering Committee review progress in implementation of IT strategy etc?	Select	0	1
15		Audit Committee of Board	(a) Does the Audit Committee of the Board review IS audit findings?	Select	0	2
			(b) Does Audit Committee of Board monitor Information security review, VAPT reports, and ensure compliance and closure of issues?	Select	0	2
			Total		0	10



Vulnerability Index of Cyber Security Framework (VICS)

Sl. no	Category	Topic	Questionnaire	Select Yes / No	Marks obtained	Max marks
16	Policy	Chief Information Security Officer (CISO) appointed	(a) Whether the bank has appointed CISO?	Select	0	2
			(b) Whether CISO is from senior management? [GM and above for RRBs and StCBs & DGM or above for DCCBs]	Select	0	2
			(c) Whether role of CISO is defined in Cyber security policy?	Select	0	1
			Total		0	5
17	Policy	Organisational Arrangements	(a) Whether dedicated department or team set-up for cyber security?	Select	0	2
			(b) Whether hierarchy has been defined in the bank for cyber security measures with roles and responsibilities for each person?	Select	0	1
			(c) Whether accountabilities have been fixed in case of threat observed / occurrence of incident?	Select	0	2
			Total		0	5
18	Policy	Conduct of awareness programmes / trainings on Cyber security	(a) Whether awareness programmes conducted for all staff on cyber security?	Select	0	2
			(b) Whether any document prepared and distributed among staff on measures to be taken by them on cyber security?	Select		2
			(c) Whether Bank has taken steps to educate its customers?	Select	0	1
			Total		0	5
19	Policy	CSF training of Top management / Board of Directors	(a) Whether CEO has attended any training programme on Cyber Security Framework?	Select	0	2
			(b) Whether atleast three Board members have attended any programme on Cyber Security?	Select	0	3
			Total		0	5
		Marks in the category			0	40



Vulnerability Index of Cyber Security Framework (VICS)

Sl. no	Category	Topic	Questionnaire	Select Yes / No	Marks obtained	Max marks
		Vendor Management				
20		Inventory of third party vendors	(a) Whether a list of third party IT vendors is maintained?	Select	0	1
			(b) Whether contracts have been signed between the bank and all the vendors?	Select	0	2
			(c) Whether the Service Level Agreements are reviewed and updated?	Select	0	2
			Total		0	5
21		Framework for management oversight and due dilligence	(a) Whether Bank has framed guidelines with roles and responsibilities defined for the vendor in case of cyber security incidents?	Select	0	1
			(b) Whether meeting between the vendor and Bank take place at regular intervals to discuss about cyber security related issues and developments?	Select	0	1
			(c) whether the guidelines for vendor management are being used by management / IT sub-committee?	Select	0	1
			Total		0	3
22		Addressing security in SLA	(a) Whether SLA has provisions for updating latest security requirements ?	Select	0	2
			(b) Whether roles and responsibilities for vendor and bank are defined in SLA in case of incident?	Select	0	1
			(c) Whether accountabilities have been fixed in case of inaction / failure of service?	Select	0	1
			(d) Whether time-frame has been indicated for implementing solutions and ensuring uptime?	Select	0	1
			(e) Do the outsourcing agreements include clauses to recognise the right of RBI / NABARD to inspect bank's documents, records, transactions, logs processed by the service provider?	Select		1
			(f) Whether there is a Grievance redressal mechanism to resolve customer complaints?	Select		1
			Total		0	7



Vulnerability Index of Cyber Security Framework (VICS)

Sl. no	Category	Topic	Questionnaire	Select Yes / No	Marks obtained	Max marks
23		Compliance with legal and regulatory compliances	(a) Whether regulatory compliances on network, DC/DR security standards are indicated in the SLA?	Select	0	2
			(b) Whether the right to audit by the bank has been included in the SLA	Select		2
			(c) Whether the SLA was checked by legal department or law officer for compliance?	Select		1
			Total		0	5
24		Dependence on Vendor staff	(a) Whether IT staff of bank has full control of the system and does not take support of vendor staff for managing day to day activities?	Select	0	3
			(b) Whether Admin rights are available strictly with Bank staff only and not shared with vendor?	Select	0	2
			Total		0	5
25		Managing Change of Vendor driven services	(a) Whether steps laid down for smooth transition from one system to the other without hampering business continuity?	Select	0	2.5
			(b) Whether steps laid down for smooth transition without hampering cyber security ?	Select	0	2.5
			Total		0	5
		Marks in the category			0	30
		Cyber Crisis Management Plan (CCMP)				
26		Is the CCMP a part of overall Board approved Cyber Security policy?	(a) Whether CCMP part of Board approved Cyber Security Policy?	Select	0	3
			(b) Whether CCMP reviewed annually?	Select	0	2
			Total		0	5
27		Responsibilities and procedures in CCMP	(a) Whether roles and responsibilities of staff in the hierarchy, in case of an incident, have been documented?	Select	0	1
			(b) Whether the procedures to be implemented for CCMP have been documented?	Select	0	1
			(c) Whether dedicated bank staff are available to manage in case of a cyber crisis?	Select	0	1
			(d) Whether the key personnel/s is/are aware of their roles and responsibilities?	Select	0	1
			(e) Whether accountabilities / penalties have been fixed ?	Select	0	1
			Total		0	5



Vulnerability Index of Cyber Security Framework (VICS)

Sl. no	Category	Topic	Questionnaire	Select Yes / No	Marks obtained	Max marks
28		Collection of evidence and metrics	(a) Whether documentation of threats received / events occurred are maintained by the bank?	Select	0	2
			(b) Whether the bank has documented and maintained the source, root cause of such incidents?	Select	0	2
			(c) Whether the above are placed before the Board for information?	Select	0	1
			Total			5
29		Reporting events to higher authorities	(a) Whether information on cyber threats / attacks reviewed by the bank?	Select	0	2
			(b) Whether core staff is aware that incidents have to be reported to NABARD within 06 hours of occurrence with preliminary details in given format?	Select	0	2
			(c) whether follow up action taken to prevent future incidents?	Select	0	1
			Total		0	5
30		Detection and correction measures	(a) Whether any mechanism has been put in place for detection of breaches / incidents?	Select	0	1
			(b) Whether any register is maintained on steps to be followed in case of detection of such threats / events?	Select	0	1
			(c) Whether the action taken against these threats are recorded and maintained?	Select	0	1.5
			(d) Whether the details of breaches/ incidents, action taken, compliance and closure placed before the Board?	Select	0	1.5
			Total		0	5
		Marks in the category			0	25
		Grand total			0	150
		Rating				

