HOOGHLY DISTRICT CENTRAL CO-OPERATIVE BANK LTD.

GSTN : 19AACFH9855Q1ZE

Netaji Subhas Road : P.O. Chinsurah
Dist. Hooghly : Pin – 712 101
Phone : (033) 2680 2949 / 9131 / 2408 / 6573 / 9303 (FAX)
E-mail : hooghlydccb@hooghlydccb.com

Memo No. 3878 / 2022-23 Dated 08.03.2023

Notice Inviting E- Tender

E-Tender (BOTH TECHNICAL AND COMMERCIAL) as detailed below, for **conducting Comprehensive Information Systems & Information Technology Audit,** from different eligible chartered firms are invited for this Bank. **Interested firms** must be submit the quotations through E-Tender in requisite format ***only in the Bank Website : hooghlydccb.com/tender*** by **30/03/2023 within 11.59 PM** positively. The Bank reserves the right to itself to cancel any or all the quotations without assigning any reasons thereto. The Bank does not bind itself to accept the lowest rate :-

Sl No	Particulars	Total Amount (IN INR) WITH GST, Taxes	Work Location
01.	CONDUCTING INFORMATION SYSTEMS (IS), INFORMATION TECHNOLOGY (IT) AUDIT AND COMPREHENSIVE AUDIT OF OTHER INTEGRATED APPLICATIONS FOR THE YEAR 2022-23 BY CHARTERED FIRM HAVING CISA CERTIFIED PARTNER AND ALSO CERTIFIED AMONGST ANY TWO OF CISSP / CCNA / CISM / OSCP as per ANNEXURE I		21 Branches and Head Office of the Bank

The Scope of work is broadly as under:

Sr No	Business Area		Major Aspects to be covered
1	Information System	Management Control	To ensure proper controls are in place in the area of System development, data management, security management, operations management and quality assurance management. Industry Best Practices are observed wherever possible.
2	Information System	Information Security	Security features including user management. Evaluation of controls prescribed by Bank's Information Security Policy and Business Continuity Policy.
3	Information System	Application controls	- Evaluation of system documentation and user manuals and interface with menus, submenus and reports - Evaluation of safeguarding of assets, data integrity, efficiency and effectiveness of the system - Special emphasis on Sufficiency / accuracy of all types of reports, Backups and recovery procedures, Audit trails, Version control, patch management, rollover, Setting of various parameters, Generation of exception reports and their coverage - Evaluation of existence and effectiveness of the controls, input, communications, processing, database
4	Information System	System Generated Transactions	Evaluate the Correctness, Completeness, Confidentiality Integrity & Availability of System Generated Entries, GL etc.
5	Information System	SLA	Compliance with Service Level Agreement (SLA) for Core Banking System. To ensure Monitoring of Service Level Agreements being done by the vendors and the Bank

PTO

HOOGHLY DISTRICT CENTRAL CO-OPERATIVE BANK LTD.

GSTN : 19AACFH9855Q1ZE

Netaji Subhas Road : P.O. Chinsurah
Dist. Hooghly : Pin – 712 101
Phone : (033) 2680 2949 / 9131 / 2408 / 6573 / 9303 (FAX)
E-mail : hooghlydccb@hooghlydccb.com

6	Information System	Bulk Transaction Posting Utilities	Correctness, Completeness, Confidentiality, Integrity, Availability of transactions posted through bulk transaction posting utilities e.g., Trickle Feed Utility etc.
7	Information System	Change Management	□ Evaluation of the Procedures adopted by the bank for the Business Process Re-engineering and controls thereof with a special emphasis on the processes reengineered since 01/04/2014 Gap Analysis for the Processes Reengineered □ Evaluation of Change management process
8	Information System	Interfaces- Internal & External	Review process and controls over interface of BANCS@24 CBS application, including validation of interface files and handling of rejections, with the other applications
9	Information System	Core Banking System Control Reports generation	Identify module wise modifications required to achieve the above.
10	Information System	Disaster recovery Plan	□ Ascertain Disaster Recovery Plan, its adequacy, components, awareness, related provisions in software, testing, training needs, recovery alternative and suggest changes/ modifications, if any. □ Evaluation and review of Recovery Time Objective (RTO), RPO (Recovery Point Objective)
11	Information System	Review of hardware and software to suggest measures, if any, for better control	□ Maintenance, monitoring, effective and efficient usage of resources Access to Operating System (OS), Version control, OS security and compliance with essential and desired functionality for Transaction Processing and its support in areas of RDBMS. □ Terms and conditions specified in Annual Maintenance Contracts of Hardware and Software to safeguard Bank's interest □ Evaluation of Minimum Base Line Security documents and their implementation. □ Evaluation of exceptions and their conformity to business requirements.
12	Information System	Audit of other areas	Procedures/ guidelines w.r.t practice as regards generation/ maintenance of records, access control and methods adopted for checking and verification of accounting procedure and control. Any other area/ aspect relevant to the assignment with mutual understanding
13	Information System	Manual Interventions	In addition, the auditor will be required to verify 1. The risk that is posed by the manual interventions that are allowed in all the applications. This will be examined for the need to keep this and restrict it or the need to eliminate it. This decision will be conveyed by the auditor based on the critical nature of the manual control and availability of the system control to manage. 2. Possibility of any wrong figures/ misrepresentation or misstatement in financial statement due to system generated

JOGHLY DISTRICT CENTRAL CO-OPERATIVE BANK LTD.

GSTN : 19AACFH9855Q1ZE

Netaji Subhas Road : P.O. Chinsurah
Dist. Hooghly : Pin – 712 101
Phone : (033) 2680 2949 / 9131 / 2408 / 6573 / 9303 (FAX)
E-mail : hooghlydccb@hooghlydccb.com

The selected bidder will be required to provide the services of professionals for auditing information systems audit and other applications. Name of few applications is given below:

S. No	Business Application
1	Core Banking Solution
2	e-banking Solution
3	Treasury
4	Alert System
5	Anti-Money Laundering (AML)
6	GST Module- Income Expenditure
7	ADF/ADEPT/CIMS/SLBC/MIS reports
8	NPA Module
9	CTS-Inward/Outward
10	ALM / FTP
11	Door Step Banking- FI
12	C-KYC
13	PFMS
14	NACH
15	Switch Services for AGS- EFT, UPI, IMPS, PoS
16	Loan Origination System (LOS)
17	Early Warning System (EWS)
18	NEFT/ RTGS with SFMS (STP) 24x7
19	e-Mail System
20	Bank's Website
21	Security Operations Centre (SOC)
22	FI Application
23	Payment Gateway-Bill Desk
24	Salary Module
25	HO Module - Asset & Inventory
26	Mail Server operations
27	Attendance Systems – operations (MATRIX – COSEC)
28	Other software – operations (Mail Server, JAAGO Data Services)
29	IT Asset Management

Terms and conditions:

1. The Financial Bids only for the eligible firms will be considered after scrutiny of Technical Bids comprising the last THREE (03) years Audit Reports, Income Tax Returns, GEM Registration and GST Certificate. Vendors failing to submit any of the documents as per TECHNICAL bids will be treated as cancelled. Non-Disclosure Agreement to be signed between the selected Firm and the Bank.
2. **Delivery of Product**
   The above job must be completed in respect of all, such as visiting, auditing, submission of reports etc. within 20 (TWENTY) Business Working Days to the locations as noted above from the date of placement of work order. Vehicle will be arranged by the Bank for visiting the branches for the purpose of Audit, accompanied by the officers from the CBS & System Cell, H.O., only within the area of operation i.e. movement restricted within Hooghly District only.

PTO

JOGHLY DISTRICT CENTRAL CO-OPERATIVE BANK LTD.

GSTN : 19AACFH9855Q1ZE

Netaji Subhas Road : P.O. Chinsurah
Dist. Hooghly : Pin – 712 101
Phone : (033) 2680 2949 / 9131 / 2408 / 6573 / 9303 (FAX)
E-mail : hooghlydccb@hooghlydccb.com

3. **Terms of payment:**
100% after completion of work of audit as mentioned above and as certified by our System Manager and Branch Managers of this Bank. The payment will be made from Head Office of this Bank. NO ADVANCE WILL BE ALLOWED.

4. **Bank Guarantee:**
The SUCCESSFUL bidder will be required to submit Non Interest bearing Security deposit in the form of Bank Guarantee, favoring Hooghly District Central Cooperative Bank equal to the 5% of purchase order value. Security Deposit should be valid for the entire contract period of 12 months.

5. Validity: Quoted rate should be valid for 30(THIRTY) days from the date of opening of quotation.

The Bank reserves the right to accept and / or reject any or all the quotations without assigning any reason thereto and the Bank's decision shall be binding and final.

Quotations will be opened **on 31/03/2023 at 11.30 A.M** tentatively. Vendor's representation is solicited.

08/3/23

Enclosure : Annexure I

Chief Executive Officer
Hooghly District Central Cooperative Bank Ltd.

Memo No. 3878 / 1 (38) / 2022 - 23 Dated :08.03.2023

Copy forwarded for information and taking necessary action to

1. The Special Officer, Hooghly District Central Cooperative Bank Ltd.
2. The Deputy General Manager I, H.O. Hooghly DCCB Ltd.
3. The Deputy General Manager II (Accounts)(In Charge), H.O. Hooghly DCCB Ltd.
4. The Grade I Officer (All), H.O. Hooghly DCCB Ltd.
5. The Grade II Officer (All). H.O. Hooghly DCCB Ltd.
6. The Branch Manager / The Accountant (All Branch), Hooghly DCCB Ltd.
7. The System Manger, H.O. Hooghly DCCB Ltd.
8. Loans Section / Accounts Section / System & CBS Cell, H.O. Hooghly DCCB Ltd.

08/3/2023

Chief Executive Officer
Hooghly District Central Cooperative Bank Ltd.

ANEX, I

नाबार्ड

EC No. 32 **/DoS-** 07 **/2020** **06 February 2020**

Ref. No. NB.DoS.Pol.HO/3182 **/J-**1 **/2019-20**

The Managing Directors/Chief Executive Officers of
All the State Cooperative Banks/
All District Central Cooperative Banks

Dear Sir/Madam

Comprehensive Cyber Security Framework for Rural Cooperative Banks (RCBs) - A Graded Approach for time bound implementation

Please refer to our Circular NB.DoS.HO.Pol.No./4811/J-1/2017-18 dated 16 March 2018, issuing guidelines for implementing Cyber Security Framework (CSF) in Banks. On further examination a graded approach to implementation of the CSF has been formulated.

2. The RCBs have been categorised into four levels based on their digital depth and interconnectedness to the payment systems landscape. The levels are defined as below:

Level	Criteria	Regulatory Prescription	Remarks
Level I	All RCBs	Level I controls prescribed in **Annexure-I**	In addition to the controls, the banks may test their preparedness on cyber security by administering the Vulnerability Index on Cyber Security (VICS) tool **Annexure-IA**
Level II	All RCBs, which are sub-members of Central Payment System (CPS) and satisfying at least one of the criteria given below: 1. offers internet banking facility to its customers (either view or transaction based)	Level II controls given in **Annexure-II, in addition to** Level I controls.	Additional controls include Data Loss Prevention Strategy, Anti-Phishing, VA/PT of critical applications.

HOOGHLY DISTRICT CENTRAL CO-OP. BANK LTD. Regd.-32 HG Date-29-4-66 Hooghly

Level	Criteria	Regulatory Prescription	Remarks
	2. provides Mobile Banking facility through application (Smart phone usage) 3. is a direct Member of CTS/IMPS/UPI.		
Level III	RCBs having at least one of the criteria given below: 1. Direct members of CPS 2. having their own ATM Switch 3. having SWIFT interface	Level III controls given in **Annexure-III**, **in addition to** Level I and II controls.	Additional controls include Advanced Real-time Threat Defence and Management, Risk based transaction monitoring.
Level IV	RCBs which are members/sub-members of CPS and satisfy at least one of the criteria given below: 1. having their own ATM Switch **and** having SWIFT interface 2. hosting data centre or providing software support to other banks on their own or through their wholly owned subsidiaries	Level IV controls given in **Annexure-IV**, **in addition to** Level I, II and III controls	Additional controls include setting up of a Cyber Security Operation Center (C-SOC) (either on their own or through service providers), Information Technology (IT) and Information Security (IS) Governance Framework with higher responsibilities to be put in place within six months of issue of circular.

3. The Board of Directors is ultimately responsible for the information security of the bank and shall play a proactive role in ensuring an effective IT (Information Technology) and IS (Information Security) governance. The major role of top management involves implementing the Board approved cyber security policy, establishing necessary organisational processes for cyber security and providing necessary resources for ensuring adequate cyber security.

4. RCBs shall undertake a self-assessment of the level in which they fit into based on the criteria given in the table above and report the same to the NABARD Regional Offices concerned within 45 days from the date of issuance of this circular.

5. All RCBs shall comply with the control requirements prescribed in **Annexure-I** within three months from the date of issuance of this circular. Similarly, Level II, III and IV RCBs are required to implement additional controls prescribed in **Annexures-II, III and IV** respectively.

नाबार्ड

6. RCBs may adopt higher level of security measures based on their own assessment of risk and capabilities. Further, if an RCB, irrespective of its asset size already has a cyber security framework higher than the self-assessed level in which it fits, then, as a matter of best practice, it is desirable that it continues with the existing governance structure.

7. The Vulnerability Index for Cyber Security Framework (VICS) may be used as a guidance tool for establishing cyber security controls.

8. The primary responsibility of implementing cyber security framework rests with the bank itself. The District Central Cooperative Banks (DCCBs) sharing IT platform with the State Cooperative Banks (StCBs) may review all the prescribed cyber security controls issued in our circulars in consultation with the StCBs. Documentation of the roles and responsibilities of the StCBs and the DCCBs vis-a-vis cyber security framework may be maintained at both DCCB and StCB level.

9. As indicated in our circular dated 16 March 2018, RCBs should report immediately on occurrence, all cyber security incidents (whether they were successful or mere attempts) to CSITE cell, NABARD by email (csite@nabard.org) with a copy endorsed to concerned Regional Office of NABARD. A quarterly NIL report shall be submitted in case no cyber security incidents/threats were observed during the quarter.

10. A copy of this circular may be placed before the Board of Directors in its ensuing meeting.

11. Please acknowledge receipt.

Yours faithfully

(K S Raghupathi)
Chief General Manager

Encl: As above.

HOOGHLY DISTRICT CENTRAL CO-OP. BANK LTD.
Regd.-32 HG
Date-29.4.66
Hooghly

Annexure-I

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.

HOOGHLY DISTRICT CENTRAL CO-OP. BANK LTD. Regd.-32 HG Date-29-4-66 Hooghly

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)**

Annexure-II

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.

HOOGHLY DISTRICT CENTRAL CO-OP BANK LTD. Regd.-32 HG Date-29-4-66 Hooghly

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.

HOOGHLY DISTRICT CENTRAL CO-OP. BANK LTD. Regd.-32 HG Date-29-4-66 Hooghly

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.

HOOGHLY DISTRICT CENTRAL CO-OP. BANK LTD. Regd.-32 HG Date-29-4-66 Hooghly

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 :

Appendix-A

Vulnerability Index of Cyber Security Framework (VICS)

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

HOOGHLY DISTRICT CENTRAL CO-OP. BANK LTD. Regd. 32 HG Date-29-4-66 Hooghly

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

HOOGHLY DISTRICT CENTRAL CO-OP. BANK LTD. Regd -32 HG Date-29-4-66 Hooghly

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

HOOGHLY DISTRICT CENTRAL CO-OP BANK LTD. Regd.-32 HG Date-29-4-66 Hooghly

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**

HOOGHLY DISTRICT CENTRAL CO-OP BANK LTD. Regd.-32 HG Date-29-4-66 Hooghly

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 / occurence 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

HOOGHLY DISTRICT CENTRAL CO-OP. Regd. 32 HG Date 29.4.86 Hooghly

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				

HOOGHLY DISTRICT CENTRAL CO-OP BANK LTD. Regd.-32 HG Date-29-4-66 Hooghly

REPORT ON INFORMATION SYSTEM AUDIT

Sl. No.				AREA OF OPERATION	AUDITOR`S OBSERVATION & COMMENTS
I				**Segregation of Duties**	
I	A			**Are duties segregated between the data processing function and users?**	
		a		Does the organizational structure provide for separation of functions between:	
			i	Transaction initiation & authorization?	
			ii	Console operations and data-entry?	
			iii	Programme team and Custody of System Documentation (including programmes), confidential data, etc.?	
		b		Does the Data Bank Administrator (DBA) / IS Manager reports to higher authorities about day-to-day as well as non-routine activities?	
		c		Are data processing personnel restricted from having asset custodianship functions, and access to assets, particularly liquid assets?	
I	B			**Are the duties segregated within the IS functions?**	
		a		Does a current organization chart exists which defines the organizational structure within IS department/Computer Cell?	
		b		Do current job descriptions exist for all personnel associated with IS department/Computer Cell?	
		c		Are new employees provided with orientation upon recruitment?	
		d		Have IS department/Computer Cell employees been provided with formal and on-the-job training to maintain knowledge, skills and ability in Information Technology and control-requirements?	
		e		Is there a separation between Data Base Administration and other data processing functions?	
I	C			**Precautions regarding personnel involved in IS functions :**	
		a		Are employees who constitute a potential threat transferred or suspended immediately?	
		b		Are references verified before an employee is recruited?	
		c		Is the IS personnel (including DBA) required to take regular vacations, and are their duties reassigned during the vacation period?	

HOOGHLY DISTRICT CENTRAL CO-OP BANK LTD. Regd.-32 HG Date-29-4-66 Hooghly

REPORT ON INFORMATION SYSTEM AUDIT

Sl. No.				AREA OF OPERATION	AUDITOR`S OBSERVATION & COMMENTS
II				**Access Controls**	
II	A			**Access controls: is access to the main processor (i.e. system-console or server) adequately controlled?**	
		a		Does the computer room have adequate physical barriers to prevent unauthorized access to the system console / server?	
		b		Are combination locks, security badges or other means used to restrict access to the computer server room, back-up storage library and documentation library?	
		c		Does the computer room have adequate physical barriers to prevent unauthorized access to the system console / server?	
		d		Does the location of off-line storage of data, transaction journals and critical reports are safeguarded against unauthorized access	
II	B			**Access controls: if access to programmes and data including Data Centre / Disaster Recovery Centre is primarily controlled through passwords? Are procedures adequate?**	
		a		Are password administrations facilities in Operating System (OS) and in Application packages are in vogue?	
		b		Is a security package in use, or any other security facilities in O.S. and App. Packages is being explored?	
		c		Is suitable security software installed and updated regularly in all systems for protecting software systems against virus, spyware, spam ware and other malicious programs?	
		d		Are various levels of passwords established for different transaction types, files and programmes?	
		e		Are various levels of passwords required based on the usability, confidentiality and significance of information?	
		f		Are passwords periodically changed? How often passwords are changed?	
		g		Are all modifications to authorization tables and access privileges recorded and reviewed?	
		h		Are all Systems / Database logs validated by the Solution/Service provider at periodical intervals?	

HOOGHLY DISTRICT CENTRAL CO-OP. BANK LTD. Regd.-32 HG Date-29-4-66 Hooghly

REPORT ON INFORMATION SYSTEM AUDIT

Sl. No.				AREA OF OPERATION	AUDITOR`S OBSERVATION & COMMENTS
		i		Are log-in IDs of terminated employees immediately disabled on the system?	
		j		Are users prohibited from selecting passwords that contain their names, or the passwords, which are very easy to guess?	
		k		If the DBA/password administrator assigns passwords first time, are delivery procedures appropriate to assure that an employee's password is not intercepted?	
		l		Does that employee change the password immediately after he receives from the DBA?	
II	C			**Access controls: if access to programmes and data files is primarily controlled through physical restrictions in terminals, are procedures adequate?**	
		a		Does the layout of the area where terminals are located prevent unauthorized access to equipment?	
		b		Do the location of terminals used for either data entry or inquiry, restrict access to authorized personnel when the system is in operation?	
II	D			**Access controls: Are the programming activities properly controlled?**	
		a		Do the procedures and system - mechanisms prevent programmers from accessing production data, object programmes and other automated procedures during the testing and debugging process?	
		b		Are programmers required to work on a separate computer system (i.e. other than production system)?	
		c		Is all live data removed from the computer system and secured in a separate library at the time software or hardware maintenance activities take place?	
		d		Does production software (i.e. programmes in use) protected from unauthorized access (i.e. use of a restricted facilities)?	
		e		Is all testing activity restricted to non-production programmes and data?	
		f		Do the procedures used FOR INCORPORATING NEW OR ALTERED PROGRAMMES IN PRODUCTION SYSTEMS, prevent unauthorized access to other programmes?	

REPORT ON INFORMATION SYSTEM AUDIT

Sl. No.				AREA OF OPERATION	AUDITOR`S OBSERVATION & COMMENTS
II	E			**Access controls: is system-activity appropriately monitored?**	
		a		Does the computer system maintain a log of access activity?	
		b		Are invalid access attempts reported to, and investigated by management, DBA, and Computer Auditors?	
		c		Is the system capable of distinguishing activity source by terminal identification?	
		d		Is the system capable of identifying authorized individuals by multi-level passwords?	
		e		Are all entries by personnel restricted or secured areas recorded?	
II	F			**Access controls: is hardware and software maintenance properly monitored/ controlled?**	
				Do supervisory activities ensure that all hardware and software-maintenance is:	
			i	Identified?	
			ii	Authorized?	
			iii	Recorded?	
			iv	Reviewed?	
			v	Monitored?	
II	G			**Access controls: is the operating system properly controlled?**	
		a		Are the operating system options / configuration settings properly documented?	
		b		Is the operating system free of extensive modifications?	
		c		Are the modifications in operating system configuration-settings subject to the same controls as application programmes?	
		d		Does the data processing department have a system-software programmer on staff?	
		e		Are the patches/ upgrades / updates applied regularly on operating systems and other system applications?	
II	H			**Access controls: Distribution of Reports**	
		a		Do the procedures for receipt and distribution of computer-outputs ensure that access to information is authorized?	
		b		Is a report distribution list used, for this purpose?	
		c		Do the waste disposal procedures include the destruction of obsolete reports, which contain sensitive data?	

Sl. No.				AREA OF OPERATION	AUDITOR`S OBSERVATION & COMMENTS
II	I			**Access controls: is access to blank cheques, demand drafts and other critical documents controlled?**	
		a		Are these documents issued (internally to the concerned employee/s) on the basis of run schedules only?	
		b		Are these documents kept locked in a secure location when unattended?	
		c		Are records of supply of these forms maintained?	
		d		Are records of ACCESS TO supplies of these forms maintained?	
		e		Are these documents periodically inventoried?	
		f		Are the documents pre-printed?	
		g		Are the documents pre-numbered or sequentially numbered and accounted for?	
II	J			**Access controls: is there other access controls in place in the following areas?**	
		a		Are all computer language-compilers removed from the production system, (and at the location of software development site, protected from unauthorized access)?	
		b		If the computer system uses an interpreter of the language, have adequate measures been taken to prevent the illegal interrupt of programme execution or alteration of programme logic by computer operators?	
		c		Are report-generation packages secured from the update capabilities (especially from modifying the contents of the reports generated)?	
		d		Do the reports generated clearly identify their source?	
		e		Is the availability of utilities, which can be used to alter or copy data and programmes restricted and controlled?	
III				**Authorization**	
III	A			**Authorization: does the senior management or a committee authorize the following IS-related functions?**	
		a		IS Personnel Policy?	
		b		Hardware Policy?	
		c		Software Policy	
		d		Software Development Policy?	
		e		Programming Methodology?	
		f		IS Security Policy?	
		g		Documentation Policy?	As per documented IT Policy
Sl. No.				**AREA OF OPERATION**	**AUDITOR`S OBSERVATION & COMMENTS**

HOOGHLY DISTRICT CENTRAL CO-OP. BANK LTD. Regd.-32 HG Date-29-4-66 Hooghly

		h		Information Policy?	
		i		Priorities of IS-related activities?	
		j		Major system / design /equipment changes?	
		k		Manpower allocations by project?	
		l		Procedures for security and control measures?	
		m		Research and Development studies?	
		n		IS budgets?	
		o		IS long-range plans?	
III	B			**Authorization: are only authorized transactions processed, and unauthorized transactions (if any) identified?**	
		a		Are clerks / computer-operators provided an approval-form to assure authorization (in addition to on-line authorization), in order to process the transactions?	
		b		Does the computer system verify authorization for transactions entered on-line, through terminal identification? (i.e. a data-entry terminal cannot be used simultaneously as authorization terminal).	
		c		Are individuals held accountable for all transaction-activities through the use of transaction - logs?	
		d		Do the transaction logs contain the log in-id, the source (i.e. terminal #), Voucher #, Date & time of transactional for ALL the transactions during on-line data-entry?	
		e		Are permanent records of ALL the live programmes and data on the computer system (in the following areas), maintained by System Administrator as well as Branch Manager?	
			i	Production (i.e. live) files and directories?	
			ii	Production programme libraries?	
			iii	Production environment parameter settings (e.g. O.S. and DBMS configuration settings)?	
III	C			**Authorization: are written standards developed / prepared to provide management's general and specific authorization for various IS-related activities?**	
		a		Is a written manual of systems and procedures available for all computer operations, and does it provide a definition and explanation of management's general and specific authorization to process transactions?	
		b		Are there written standards for:	
		c		Hardware selection?	

REPORT ON INFORMATION SYSTEM AUDIT

Sl. No.				AREA OF OPERATION	AUDITOR`S OBSERVATION & COMMENTS
		d		System Software selection?	
		e		Application package selection?	
		f		Network component selection?	
		g		System design and development?	
		h		Programming standards?	
		i		Testing?	
		j		Programme approval standards?	
		k		Implementation (including procedures for putting a programme/system into production)?	
		l		Software Change Management Procedures?	
III	D			**Authorization: is system development properly controlled?**	
		a		Is a formal System Development approach used? (Please specify):	
		b		Does management make a clear distinction between production (i.e. live) and development programmes?	
		c		Is "prototyping" done?	
		d		Do the procedures for system design, including the acquisition of software packages require active participation by representatives of users, accounting, internal audit, and computer auditors (I.S. auditors), as appropriate?	
		e		Does each system have a written (in detail) specification, which are reviewed and approved by management, and applicable users before preparation of the detailed systems design specifications to assure implementation of an acceptable quality standards?	
III	E			**Authorization: are new systems adequately tested?**	
		a		Do software-testing a joint effort of programmers, system developers and users?	
Sl. No.				**AREA OF OPERATION**	**AUDITOR`S OBSERVATION & COMMENTS**
		b		Does system testing include testing of both, the manual and computerized phases of the system?	
		c		Is test data developed to specifically test the functioning of programmed control procedures?	
		d		During parallel testing, is consideration given to whether errors exist in the populated data, to test programmed controls?	
		e		Is documentation of system tests (data and results) retained for future use, which will be required in case of later system modifications?	
		f		Are test results reviewed and approved by user / management personnel before authorizing the transfer of programmes into the live environment?	

HOOGHLY DISTRICT CENTRAL CO-OP BANK LTD. Regd. 32 HG Date-29-4-66 Hooghly

		g		Do final testing procedures provide user, management, IS-staff with a clear identification of the programme version used to perform the test?	
		h		Are programmers prohibited from using live data files to test programmes?	
III	F			**Authorization: Is system conversion adequately planned and controlled?**	
		a		Are formal, written conversion procedures prepared?	
		b		Is formal approval by system development steering - committee / management and IS auditor obtained, of IS related activities including a review of changes from original design specifications, review of system test results, review of input and output controls, and review of documentation prior to putting a new system into production?	
		c		Are these written conversion procedures approved by management, internal audit, IS auditing, user departments and accounting personnel as appropriate?	
		d		Are all master file / table and transaction file / table conversions controlled to prevent unauthorized changes, to provide accurate and complete results, and to ensure data integrity?	
		e		Do programme transfer - procedures ensure that only those programmes, which were used for the final test, are transferred to the live environment?	
III	G			**Authorization: Are programme changes authorized?**	
		a		Do policies and procedures for initiating changes to programmes and other forms of processing logic ensure that management authorizes all changes?	
		b		Do policies, procedures and mechanisms ensure that personnel responsible for application programme perform no changes to the operating system configuration?	
Sl. No.				**AREA OF OPERATION**	**AUDITOR`S OBSERVATION & COMMENTS**
		c		Is a log maintained of all changes requested that identify the person initiating the change, the date initiated and the date implemented?	
		d		Does this log also identify the specific programme (s) and / or operating procedures affected by the change?	
III	H			**Authorization: are programme changes monitored and controlled?**	
		a		Do procedures ensure that all changes to the system are documented?	
		b		Are programme modifications made ONLY TO COPIES OF current production programmes rather than the programmes themselves?	
		c		Does a responsible official INDEPENDENT OF	

HOOGHLY DISTRICT CENTRAL CO-OP. BANK LTD. Regd.-32 HG Date-29-4-66 Hooghly

				PROGRAMME authorize operations personnel to put a modified programme into production?	
		d		Are source programmes supplied when programme changes are authorized for putting into live operation?	
		e		Is the following documentation obtained / prepared before and after each change, and retained as a permanent record?	
			i	Files / directories in the system?	
			ii	Production library directories?	
			iii	Programme source listings?	
			iv	Operation procedures' listings?	
			v	Systems flowcharts?	
			vi	Data flow diagrams?	
			vii	Entity Relationship (ER) diagrams?	
			viii	Are operations' procedures updated to reflect system changes?	
			ix	Do system administrators of all transfers to production libraries (i.e. live environment) maintain logs?	
		f		If patching techniques are used:	
			i	Are they allowed only in emergencies?	
			ii	Are they allowed only after supervisory approval?	
			iii	Are records of patches maintained, including appropriate approvals, records of the instructions / routines altered, the name of the person making the changes and the reason for the changes?	

HOOGHLY DISTRICT CENTRAL CO-OP. BANK LTD.
Regd.-32 HG
Date-29-4-66
Hooghly

Sl. No.				AREA OF OPERATION	AUDITOR`S OBSERVATION & COMMENTS
IV				**Supervision and Review**	
IV	A			**Supervision and review: are IS related activities subject to review by management?**	
		a		Is management knowledgeable about the activities performed by the computer system and the methods used for operation and maintenance of the system?	
		b		Are logs of computer processing and balancing activities available, and reviewed by Management at least on half-yearly basis.	
		c		Are logs the basis for preparation of performance statistics to be reviewed by management?	
		d		Are logs the basis for charging computer expenses to user departments, (if applicable)?	
		e		Is the system log file / table properly controlled to prevent unauthorized changes?	
		g		Is computer processing scheduled, either manually or through automated techniques, and regularly compared to machine utilization reports and / or console logs?	
		h		Does the processing schedule include periodic (i.e. daily, fortnightly, month-end, quarterly, six-monthly, yearly, exceptional etc.) processing-requirements?	
		i		Are significant variations from scheduled processing investigated?	
IV	B			**Supervision and review: does the management periodically review access - authorization?**	
		a		Are authorization levels for terminal users and points of transaction / operation organization periodically reviewed?	
		b		Do supervisory or managerial personnel routinely review the logs and reports of invalid access attempts?	
IV	C			**Supervision and review: are computer operations well documented and organized in an orderly fashion?**	
		a		Is computer operations staff (including DBAs / System Administrators, and computer auditors) adequately trained to the extent necessary to perform all their tasks in a systematic manner (without relying upon external personnel)?	

HOOGHLY DISTRICT CENTRAL CO-OP. BANK LTD. Regd.-32 HG Date-29-4-66 Hooghly

		b		Do computer processes detect or prevent the initiation of processing steps, which are OUT OF SEQUENCE?	

HOOGHLY DISTRICT CENTRAL CO-OP. BANK LTD.
Regd.-32 HG
Date-29-4-66
Hooghly

Sl. No.				AREA OF OPERATION	AUDITOR`S OBSERVATION & COMMENTS
		c		Are hardware maintenance boundaries contractually defined with each vendor when the bank (or even a branch / office within a bank) uses hardware from more than one manufacture?	
		d		Is a record of all Hardware problems (including UPS) properly maintained in a register?	
		e		Is a record of all Software problems properly maintained in a register?	
		f		Is preventive maintenance routinely performed? How frequently?	
		g		Is a record of such maintenance prepared and reviewed?	
IV	D			**Supervision and review: has management established documentation standards to allow for maintenance and supervision of IS-related activities in the following areas:**	
		a		Information Systems setup documentation?	
		b		Systems documentation?	
		c		Programmes documentation?	
		d		Operations documentation?	
		e		User documentation (e.g. user profile and the kind of operations he is allowed to perform)?	
		f		Do supervisors review "Users" and "Technical" manuals to make sure that prescribed documentation standards are adhered to?	
		g		Are "documentation standards" and "change procedures" adequate to ensure that documentation is maintained in a correct and consistent manner?	
IV	E			**Supervision and review: does adequate and up-to-date system-documentation exist (for every system) including the following:**	
		a		Systems narrative?	
		b		Systems flowcharts?	
		c		Broad input-design?	
		d		Broad Database design?	
		e		Broad (context-level) DFDs i.e. Data Flow Diagrams?	
		f		Data element definitions?	
		g		Codes Design?	
		h		Dialogue Design?	
		i		Broad Procedure-Design?	
Sl. No.				AREA OF OPERATION	AUDITOR`S OBSERVATION & COMMENTS
		j		Held Design?	

HOOGHLY DISTRICT CENTRAL CO-OP. BANK LTD. Regd.-32 HG Date-29-4-66 Hooghly

		k		Broad Output Design (Report and Screen Design)?	
		l		Data capture procedures?	
		m		Backup and recovery procedures?	
		n		System changes?	
IV	**F**			**Supervision and review: does adequate and up-to-date documentation exist including the following:**	
		a		Detailed System Flowcharts?	
		b		Narrative description of each major programme module, subsystem?	
		c		In-detail programme-flowcharts?	
		d		In-detail DFDs (Data Flow Diagrams)?	
		e		Decision tables?	
		f		In Detail database design?	
		g		In detail ER diagram?	
		h		List of constants, codes and tables used?	
		i		**Source programme listing?**	
			i	Operating System (OS) Commands listings?	
			ii	Specimen vouchers?	
			iii	Specimen data-entry (and other interface) screens?	
			iv	Specimen reports?	
			v	Programme changes?	
			vi	Changes in ANY COMPONENT of the system?	
IV	**G**			**Supervision and review: are computer jobs streams supported by computer set-up and run instructions including**	
		a		Set-up instructions and device assignments?	
		b		Identity of input and output data tables/files?	
		c		Parameters of Job Control Language /OS Commands?	
		d		Normal console/server-messages for each run?	
		e		List of error and halt messages, probable causes, programmed and machines halts, and required action?	
		f		Restart and recovery procedures?	
		g		Estimated run times and maximum run time (for every major job /major task)?	
		h		Form (and distribution) of printed and other outputs?	
		i		End of job instructions?	
		j		Output and destination and retention instructions?	

HOOGHLY DISTRICT CENTRAL CO-OP BANK LTD.
Regd.-32 HG
Date-29-4-86
Hooghly

Sl. No.				AREA OF OPERATION	AUDITOR`S OBSERVATION & COMMENTS
IV	H			**Supervision and review: are procedures for input and output documented?**	
		a		Are input procedures documented to describe all tasks necessary for the control of transactions processed by the system including:	
			i	Input receipt?	
			ii	Data entry?	
			iii	Error correction?	
			iv	Source document control?	
			v	Permanent record retention?	
		b		Are procedures documented for the generation, verification and distribution of computer output including:	
			i	Output reports generation?	
			ii	Report balancing and reconciliation?	
			iii	Report distribution?	
			iv	System inquiries?	
		c		Are control totals produced by the system to allow balancing with input control totals including:	
			i	Batch number?	
			ii	Amount totals of significant fields?	
			iii	Hash totals of significant fields?	
			iv	Transaction or record counts?	
			v	Ending number of master file records?	
			vi	Total number of master file / table records?	
V				**Security and Recovery**	
V	A			**Security and recovery: has the potential risk of events, which could cause short-term or sustained loss of computer processing capability been identified?**	
		a		Has the maximum time period for which loss of computer processing could be tolerated without serious disruption to the business been identified (separately for every business-operation based on nature and criticality of that business operation)?	
		b		Has the effect of loss at differing times i.e. start of day, peak business-hours time, end of week, end of month, end of year, etc) been addressed?	
		c		Have the effects of daily operating practices, customer reaction and exposure to loss been considered?	
		d		Has the effect of loss of individual components of the system (Hardware components, network components, system and application, Software components, data, documentation, people, etc.) been isolated?	

HOOGHLY DISTRICT CENTRAL CO-OP. BANK LTD. Regd.-32 HG Date-29-4-66 Hooghly

Sl. No.				AREA OF OPERATION	AUDITOR`S OBSERVATION & COMMENTS
V	B			**Security and recovery: has information systems activities related insurance coverage been considered for the following risks**	
		a		Equipment destruction?	
		b		Programme of Software destruction?	
		c		Loss of Data?	
		d		Business interruption?	
		e		Errors of omission?	
		f		Fidelity insurance on IS personnel?	
		g		Payment for use of alternative equipment?	
V	C			**Security and recovery: do the plans and procedures exist to prevent a short-term or partial failure in a controlled manner?**	
		a		Does the environment for the computer systems conform to manufacturer's specification for elect, humidity, temp & air particle tolerance?	
		b		Does the physical location of computer equipment discourage access or interruption by unauthorised personnel and reduce vulnerability to environmental effects and natural disasters?	
		c		Does on-premises backup storage area provide reasonable protection against accidental damage or destruction of data, programmes and documentation?	
		d		Does the bank have written policies and procedures for backup and recovery of all data and programs stored on magnetic media to assure sufficient backup exists to restore them if they are destroyed?	
Sl. No.				**AREA OF OPERATION**	**AUDITOR`S OBSERVATION & COMMENTS**
V	D			**Do the plans and procedures exist to recover from a short-term or partial system failure in a controlled manner?**	
		a		Do procedures exist for recovery in an orderly manner in the event of processing interruptions resulting from such occurrences as equipment malfunction, power fluctuations, software errors or loss of on-line data?	
		b		Is there procedure for continuation of processing in the absence of key individuals?	
		c		Are programmes which have backup data included in the routinely run application software so that the backup procedure will not be a DBA's or operator's choice?	
		d		Is at least one current copy of the supervisory and application programme library maintained in the nearby magnetic-storage library as immediate	

HOOGHLY DISTRICT CENTRAL CO-OP BANK LTD. Regd -32 HG Date-29-4-66 Hooghly

				backup?	
		e		Are error recovery procedures for short-term failure tested periodically to ensure control of process?	
		f		How frequently?	
		g		Are computer operator's duties rotated periodically, to have internal controls and also ensure availability of trained staff?	
		h		Is the "Maker-Checker" principle used in Software development activities also?	
V	E			**Security and recovery: are backup procedures adequate?**	
		a		Are current copies of the following maintained off-site?	
			i	Operating Systems?	
			ii	Source programmes	
			iii	Runtime (executable) codes?	
			iv	Master data?	1.
			v	Transaction data necessary for recovery?	
			vi	Programme documentation?	
			vii	Operating instructions?	
			viii	Critical forms and supplies?	
			ix	Disaster Recovery plan?	
			x	System documentation?	
Sl. No.				**AREA OF OPERATION**	**AUDITOR`S OBSERVATION & COMMENTS**
V	F			**Security and recovery: are the arrangements with vendors adequate?**	
		a		Are vendors responsible for reliable hardware and software support to avoid the possibility of processing interruption due to lack of support?	
		b		Do remedial equipment - maintenance arrangements provide for response to problems in sufficient time to prevent business disruption?	
		c		What is the average response time after registering the complaint?	
		d		Does the equipment maintenance vendor maintain an inventory of replacement components (which are frequently required for local service)?	
V	G			**Security and recovery: is the disaster recovery planning adequate?**	
		a		Is there a detailed disaster recovery planning explaining procedures and steps necessary for recovery after the disaster?	
		b		Is a copy of the plan stored off premises or in a location where it would not be destroyed in the	

HOOGHLY DISTRICT CENTRAL CO-OP. BANK LTD. Regd.-32 HG Date-29-4-66 Hooghly

				backup?	
		e		Are error recovery procedures for short-term failure tested periodically to ensure control of process?	
		f		How frequently?	
		g		Are computer operator's duties rotated periodically, to have internal controls and also ensure availability of trained staff?	
		h		Is the "Maker-Checker" principle used in Software development activities also?	
V	E			**Security and recovery: are backup procedures adequate?**	
		a		Are current copies of the following maintained off-site?	
			i	Operating Systems?	
			ii	Source programmes	
			iii	Runtime (executable) codes?	
			iv	Master data?	1.
			v	Transaction data necessary for recovery?	
			vi	Programme documentation?	
			vii	Operating instructions?	
			viii	Critical forms and supplies?	
			ix	Disaster Recovery plan?	
			x	System documentation?	
Sl. No.				**AREA OF OPERATION**	**AUDITOR`S OBSERVATION & COMMENTS**
V	F			**Security and recovery: are the arrangements with vendors adequate?**	
		a		Are vendors responsible for reliable hardware and software support to avoid the possibility of processing interruption due to lack of support?	
		b		Do remedial equipment - maintenance arrangements provide for response to problems in sufficient time to prevent business disruption?	
		c		What is the average response time after registering the complaint?	
		d		Does the equipment maintenance vendor maintain an inventory of replacement components (which are frequently required for local service)?	
V	G			**Security and recovery: is the disaster recovery planning adequate?**	
		a		Is there a detailed disaster recovery planning explaining procedures and steps necessary for recovery after the disaster?	
		b		Is a copy of the plan stored off premises or in a location where it would not be destroyed in the	

HOOGHLY DISTRICT CENTRAL CO-OP. BANK LTD. Regd.-32 HG Date-29-4-66 Hooghly

				event of a disaster?	
		c		Have backup alternatives been considered (i.e. hot site, cold site, warm site, reciprocal arrangements, etc.)?	
		d		Are alternative computer equipment arrangements tested periodically to ensure that the plan functions?	
		e		Has the disaster recovery plan been tested?	
		f		How frequently?	
V	H			**Security and recovery: is other recovery - considerations adequate?**	
		a		Do documented operating procedures permit continuation of computer processing in the event of permanent loss of key operations personnel?	
Sl. No.				**AREA OF OPERATION**	**AUDITOR`S OBSERVATION & COMMENTS**
		b		Does the documentation of the system permit maintenance by alternate support personnel in the event of loss of key programmers?	
		c		Does the Disaster Recovery Plan (DRP) include the provision for continuation of business operations in the event of any (minor or major) disaster?	
		d		Is the bank (i.e. every computerized branch and office) in compliance with the regulatory / statutory requirements, with respect to retention of data, generate reports which is in the machine-readable form?	

HOOGHLY DISTRICT CENTRAL CO-OP BANK LTD
Regd.-32 HG
Date-29-4-66
Hooghly