दि दमण एवं दीव राज्य सहकारी बैंक लिमिटेड
THE DAMAN & DIU STATE CO-OPERATIVE BANK LTD.
(RBI LICENSE No. Dos. RO (AH). REG/LIC.S-2187/04.36.000/2023-24 dtd.07-March-2024)
INFORMATION TECHNOLOGY DEPARTMENT
Head Office: H. No. 14/54,1st Floor, Dilip Nagar, Nani Daman-396210
Ph. No: 0260 2255984, 2255985 | Email: it@ddscbl.bank.in

IT/82/Cyber Security Audit/2025-26/08/ 1448 Date: 17-03-2026

QUOTATION NOTICE

Sub: - Quotation Inviting Notice for Conduct Cyber Security Audit for F.Y. 2025-26.

Ref: Vide Note 01: IT/82/CYBER SECUIRTY AUDIT/2025-26/08 dated 13.03.2026.

Quotation is hereby invited by the "The Daman and Diu State Co Operative Bank Ltd., Daman for the Conduct Cyber Security Audit for F.Y. 2025-26.

WORK SCOPE

Sr No	Particular
1	**Conduct Cyber Security Audit for F.Y. 2025-26** • Conduct a comprehensive assessment of the bank's Cyber Security Controls against mandatory and recommended requirements defined under NABARD Circular **EC No. 307/DoS-25/2024** for Conduct of Information Technology/Cyber Security Audit (Ref No: NB.HO. DoS.CSITE/ 3300 /CS-01 /2024-25) • Provide Necessary Support and guidance to the bank in addressing identified gaps, including quarterly compliance support to ensure adherence to applicable regulatory requirement.

TERMS AND CONDITIONS

1. The Rate should be quoted inclusive of all taxes, No Extra charges will be paid on the rates quoted.
2. The rate should be quoted only for specific scope of work as per the list of requirement.

3. The Sealed quotation should be super scribed by words "**Quotation for the Conduct Cyber Security Audit for FY 2025-26 for the "The Daman and Diu State Co Operative Bank Ltd, Nani Daman"** and sealed quotation should be sent to the The Daman and Diu State Co Operative Bank Ltd, Head Office, H.No.14/54,1st Floor, Dilip Nagar, Nani Daman-396210.
4. Quotation should reach at above address on or before 24.03.2026 at 05:00 PM.
5. The terms and conditions will be specified in the quotation.
6. The undersigned has the right to accept or reject the quotation.

General Manager (IT)

The Daman & Diu State Co-Operative Bank Ltd.

NABAR

EC No. 307/DoS-25/2024

Ref. No. **NB.HO.DoS.CSITE/ 3300 / CS-01 /2024-25**

17 December 2024

1. The Chairman, all Regional Rural Banks
2. The Managing Director/Chief Executive Officer, all State Central Cooperative Banks
3. The Managing Director/Chief Executive Officer, all District Central Cooperative Banks

Madam/Dear Sir

Conduct of Information Technology/Cyber Security Audit

As you may be aware, there has been an increasing number of cyber incidents and attacks that require all systems to be alert and vigilant regarding potential threats. This is primarily due to the existence of vulnerabilities in software, applications, websites and configurations of IT infrastructure. Moreover, due to application of emerging technologies such as Artificial Intelligence/ Machine Learning, Internet of Things, etc. threat vectors are evolving and becoming more complex.

2. In the circumstances, as advised by the Ministry of Electronics and Information Technology (MeitY), Government of India, we advise as under:

(i) In order to take preventive measures and minimize the security risk & exposures, all Supervised Entities of NABARD (viz. State Cooperative Banks, District Central Cooperative Banks and Regional Rural Banks) should get their IT infrastructure, websites and applications (including APIs) audited on a regular basis or whenever there are any changes/updates in infrastructure or websites/applications.

(ii) Audits should be conducted against comprehensive frameworks and should follow MeitY/CERT-In Guidelines released/updated from time to time (enclosed). The list of empanelled agencies who can do the cyber security audit is available at: https://www.cert-in.org.in/PDF/Empanel org.pdf.

3. You are, accordingly, advised to immediately put in place a system of regular conduct of cyber security audit through CERT-In empanelled agencies strictly as per the MeitY/CERT-In guidelines atleast on an annual basis or whenever there are any changes/updates in infrastructure or websites/ applications, in consultation with the Board of Directors of your bank.

4. In case of third party hosting service provider, the instructions given at para F of the guidelines may be followed which provide that in case a services/website is hosted on a webserver owned by another organization, the webserver system, its operating system and webhosting application software including backend database application software, if any, are under the control of the organization hosting the website (i.e. owning the webserver) and it is the responsibility of webserver owner to take care of information security auditing of these, as the organization owning the website contents does not have any access or control over these assets. However, since the data/software related to the website are under the control of the organization owning the contents of the website, their responsibility is limited to get these audited by a CERT-In empanelled information security auditing organization. In such cases, compliance may be obtained from the third-party hosting service provider.

5. The copies of Audit Reports along with information in the enclosed format may please be submitted to NABARD at csite@nabard.org on a quarterly basis by the last working day of the quarter to enable us to keep MeitY, Govt of India timely informed of the same.

Please acknowledge.

Yours faithfully

Sd/-

(Sudhir Kumar Roy)
Chief General Manager

Encl. : As above

NABARD

FORMAT

Report for the quarter ended _____ (to be submitted by last working day of the last month of the quarter)

1. Name of the Supervised Entity (SE):_____
2. Cyber security audit conducted on _____ (copy of report enclosed)
3. Name of third-party hosting service provider: _____
4. Name of the agency which had conducted cyber security audit: _____
5. Whether agency at 4. empanelled by CERT-In: _____
6. Type of audit, audit scope, methodology/standards :
7. Summary:

Sr No	Particulars	SE's comments
7.1	Major recommendations mentioned in audit report	
7.2	Status of action taken/closure status in respect of each such recommendation	
7.3	Significant cyber security audit recommendations (outlining the overall major recommendations which interalia include policy enhancement, access control improvements, third party risk management, incident response preparedness, training and awareness, etc.)	
7.4	Whether fully/partly complied with CERT-In/MeitY guidelines	
7.5	Whether fully/partly complied with Cyber Security Framework Guidelines of RBI/NABARD	
