BGB
बिहार का अपना बैंक

बिहार ग्रामीण बैंक
BIHAR GRAMIN BANK
(Scheduled Bank Owned by Government)

निरीक्षण एवं अंकेक्षण विभाग

Application for Selection of IS Auditor for IS Audit of Bank (FY 2025-26)

Applications are being invited from Cert IN Certified (NABARD Empanelled) IS Auditor (Firms/Companies) for allocation of IS Audit of the Bank. Firm/Company may be selected on the basis of L-1 rate. The Firm/Company can submit their Application/bid (Technical and Financial) through GEM Portal. The last date for receipt of application is 14 days from the Date of Advertisement. The Bank reserves the right to reject any or all applications without assigning any reason.

S.d.
General Manager- IAD
Bihar Gramin Bank, Head Office,
Shri Vishnu Commercial Complex,
NH-30, New Bypass, Asochak,
Patna-800030, PH/फ़ो-0612-2385418,
Email/ईमेल-hoiad@bgb.bank.in

Scope and Applicability

This Policy applies to Bihar Gramin Bank Employees, contractors, consultants, temporary staff and other individuals, even if affiliated with Third Parties, who have access to Bihar Gramin Bank's Information/data/Information Processing Facilities.

The scope of IS Audit covers the whole information infrastructure/cyber space used by the Bank related to people, process and system viz. system planning, organizing, acquisition, monitoring, implementation, delivery and support to end users.

Accordingly, the scope of the audit will also include the adequacy and effectiveness of internal control systems and processes for the use and protection of the information infrastructure as detailed under:

a)	Data	It's representativeness for business and its Integrity.
b)	Application Systems	It's functionality, controls and change Management
c)	Technology	The standardization, risks, investments and Returns.
d)	Facilities	In terms of infrastructure, maintenance and security.
e)	People	In terms of establishing segregation of duties And organizational structure, adequacy and competence.

The Policy consists of Risk Assessment Methodology in performance of technology-related products/services/delivery channels and compliance of laid down systems and procedures in order to avoid potential operational risks.

Accordingly, the following areas/functions are proposed to be covered in the proposal IS Audit for FY 2025 – 2026.

a. At least 38 branches, 26 Regional Offices and Head Office of the Bank.
b. Application Software including bank's intranet web & data transfer mechanism servers, DMS, application which has been developed internally on a separate Server.
c. Outsourced activities/services & control, mainly related to ISP, Anti – Virus, Network Support, AMC & SLA, etc.
d. BGB Website, which is outsourced but covered under IS Audit of the bank.
e. CTS/NACH Training Centers, etc.
f. Digital Signatures.
g. Business Continuity Plans & DR Drills.
h. VAPT wherever required.
i. Cyber related domain as perceived by IS Auditor.

NOTE:-

This is to be clarified that the CBS (Core banking Solution) Server is located in the premises of our Sponsor Bank in at a different localities situated distantly for the bank's operational area.

IS Audit including VA/PT of CBS is done separately by sponsor bank under their own supervision and control. Thus, the remaining part as an end user falls under the purview of the bank (BGB), although the bank is doing complete access on data.

IS Audits shall consist of following audits / assessments:

a) Operational / IS Audit of Branches

The audit of IT operations at the branches covering Environmental and operational aspects as defined in Risk Based Internal Audit (RBIA) Policy.

b) Information Systems Audits of Assets at Critical Locations

The IS Audit should put in place the suitable audit types for various tasks such as:

Audit Domain	Audit Objective	High level Audit Scope	Audit Frequency
Vulnerability Assessment / Penetration Testing / Device Level Audit	Comprehensive evaluation of computer systems, applications and network infrastructure deployed at critical locations	Vulnerability Assessment / Penetration Testing (Code Obfuscation, Secure review of application architecture, Business logic flaws), Device Level Audit of Servers and Security Devices. Audit of SOC Devices.	Quarterly

Audit Domain	Audit Objective	High level Audit Scope	Audit Frequency
External Attack / Penetration Testing of web facing applications	Review of Vulnerabilities for Internet facing applications that could be exploited by external attackers.	External Attack / Penetration Testing of web facing applications.	Quarterly

IT Application Management	Review the Application Management activity at the bank to seek assurance that adequate degree of controls are in place for authentication, authorization, data processing, data storage, data transfer	1. To include Audit of DMS server. New in house developed- Document Management System. 2. Secure integration with other systems and applications for data exchange and transfer. 3. Incident Management including Service Level Management 4. Critical IT Applications 5. Regulatory and Software License compliance. 6. Capacity Planning 7. Review AMC and Support Contracts (SLA) for Validity and Scope.	Half-Yearly

Other Audit Assignments	Perform other Audit tasks as per the requirements of the Bank	1. Vendor Audit (Outsourced Vendors- ISP Routers) 2. Perform IS and IT Security Audits based on requirements of Ministry of Finance GOI, RBI, NPCI,NCIIPC, SEBI and others. 3. Carrying out the audit of the software/ packages at pre implementation level or before any major upgrade or version change. In respect of procured software systems audit shall be conducted after it is deployed in the Bank's environment.	As per requirement