आज़ादी का अमृत महोत्सव

राष्ट्रीय आवास बैंक
NATIONAL HOUSING BANK

HO/Audit/DAK/ 2023/00164

Date: 10-08-2023

<<<Vendor Name>>>

<<<Address>>>

Madam/Dear Sir,

Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June)

In reference to the RFP REF NO- NHB(ND)/AD/A-1162/2019 dated February 03, 2020, Corrigendum dated February 21, 2020, & the notification published on the website of the Bank dated April 28, 2020, for Empanelment of IS & Cyber Security Auditors for a period of five years till year 2023-2024, National Housing Bank (NHB) invites sealed commercial quotations from Empanelled Information Security & Cyber Security Auditors to conduct Information Security & Cyber Security Audit for the entire IT Infrastructure, Systems, Applications, portals, CSOC and Cyber Security Framework of the Bank for the Year 2022-23 (July-June). Necessary '**Requirement Proposal**' (RP) document including Scope of Work and Other Terms & Format for Commercial Bid are enclosed herewith.

Please take note of the following points while submitting your quotations -

- The quotation must contain the price inclusive of all levies/charges, and taxes. The Empanelled IS & Cyber Security Auditors must give the price Bid as per the specified format given along with the '**Requirement Proposal**' (RP) document at **Annexure A.** Prices and other terms offered by Bidders must be valid for an acceptance period of six months from the date of opening of Commercial Bid.
- **The quotation should be accompanied by self-declaration(s) duly signed by the Authorized Signatory (s) of the company/firm with respect to the Minimum Eligibility Criteria (MEC) Sl. No. 3, 4,5, 6 & 7 as defined in the aforesaid Request for Proposal (RFP) and the Corrigendum thereafter.**
- The quotation should be signed by the Authorized Signatory (s) of the company. It should be enclosed in a non-window sealed cover, superscripted as **"Commercial Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June)"** and must reach at the following address-

एचओ/ लेखापरीक्षा/डाक/2023/00164

दिनांक: 10-08-2023

<<<विक्रेता का नाम>>>

<<<पता>>>

महोदया /महोदय,

वर्ष 2022-23 (जुलाई-जून) के लिए सूचना सुरक्षा एवं साइबर सुरक्षा लेखा परीक्षा करने हेतु कोटेशन

कृपया दिनांकित 03 फरवरी, 2020 के आरएफपी संदर्भ सं. रा. आ. बैंक (नदि)/एडी / ए-1162/2019 तथा दिनांक 21 फरवरी, 2020 का शुद्धिपत्र एवं दिनांक 28 अप्रैल, 2020 की बैंक की वेबसाइट पर प्रकाशित अधिसूचना का संदर्भ लें, जिसमें वर्ष 2023-2024 तक पांच वर्ष की अवधि के लिए आईएस एवं साइबर सुरक्षा लेखा परीक्षकों के पैनलबद्धता हेतु राष्ट्रीय आवास बैंक (रा. आ. बैंक) वर्ष 2022-23 (जुलाई-जून) के लिए बैंक की संपूर्ण आईटी आधारभूत संरचना प्रणाली एप्लिकेशन, पोर्टल, सीएसओसी तथा साइबर सुरक्षा ढांचा हेतु सूचना सुरक्षा और साइबर सुरक्षा लेखा परीक्षा आयोजित करने के लिए पैनलबद्ध सूचना सुरक्षा एवं साइबर सुरक्षा लेखा परीक्षकों से मुहरबंद वाणिज्यिक कोटेशन आमंत्रित करता है। अनिवार्य '**आवश्यकता प्रस्ताव**' दस्तावेज जिसमें कार्य क्षेत्र एवं वाणिज्यिक बोली हेतु अन्य नियम तथा प्रारूप शामिल हैं, इस पत्र के साथ संलग्न हैं।

कृपया अपनी कोटेशन प्रस्तुत करते समय निम्नलिखित बातों का ध्यान रखें-

- कोटेशन में सभी लेवी / प्रभार एवं करों सहित मूल्य शामिल होना चाहिए। पैनलबद्ध आईएस तथा साइबर सुरक्षा लेखा परीक्षकों को **अनुलग्नक 'क'** में **'आवश्यकता प्रस्ताव'** दस्तावेज के साथ ही दिए गए विनिर्दिष्ट प्रारूप के अनुसार मूल्य बोली देनी होगी बोलीदाताओं द्वारा प्रस्तावित मूल्य एवं अन्य शर्तें वाणिज्यिक बोली खोलने की तिथि से छः महीने की स्वीकृति अवधि हेतु वैध होनी चाहिए।
- **कोटेशन पूर्वोक्त प्रस्ताव हेतु अनुरोध (आरएफपी) तथा शुद्धिपत्र में यथा परिभाषित न्यूनतम पात्रता मानदंड (एमईसी) क्र.सं. 3, 4, 5, 6 और 7 के संबंध में कंपनी/फर्म के प्राधिकृत हस्ताक्षरकर्ता (ओं) द्वारा स्व घोषणा (ओं) के साथ विधिवत हस्ताक्षरित होनी चाहिए। कोटेशन कंपनी के प्राधिकृत प्रतिनिधि द्वारा हस्ताक्षरित होनी चाहिए।**
- कोटेशन को नॉन-विडो मुहरबंद लिफाफे में संलग्न कर उस पर **"वर्ष 2022-23 (जुलाई-जून) के लिए सूचना सुरक्षा तथा साइबर सुरक्षा लेखा परीक्षा करने हेतु वाणिज्यिक कोटेशन"** लिख कर निम्नलिखित पते पर भेंजे-

The General Manager,
Audit Department, National Housing Bank,
4th Floor, Core 5A, India Habitat Centre,
Lodhi Road, New Delhi- 110003

The envelope should indicate on the cover the name and address of the company along with contact number and email address. Quotations not sealed properly shall not be considered and will stand rejected without recourse.

The quotation must reach the above address by 25-08-2023 (Friday), before 6:00 p.m. The quotation must be received by NHB at the address specified, not later than the last date of submission of quotation /commercial Bid as indicated above. Any Bid received by NHB after the deadline for submission of Bids prescribed by NHB will be rejected and returned unopened.

The bidder may seek queries/ clarification, if any, regarding the Bid document(s) via emails on the email IDs provided in this Bid document **on or before 18-08-2023 (Friday), before 6:00 p.m**.

The Authorised Representative of companies/firm may contact Audit Department, National Housing Bank between **10:00 am to 6:00 p.m**. at Head Office on Monday to Friday, excluding public holidays, for any query/clarification.

The Bank reserves the right to reject or accept any quotation and/or reject any or all quotations without assigning any reason.

Yours faithfully,

(Rita Bhattacharya)
General Manager

राष्ट्रीय आवास बैंक, नई दिल्ली * NATIONAL HOUSING BANK, NEW DELHI *
ले. प. वि.
Audit. Deptt.

Encl: As Above

महाप्रबंधक,

लेखा परीक्षा विभाग, राष्ट्रीय आवास बैंक,

चौथी मंजिल, कोर 5ए भारत पर्यावास केंद्र,

लोधी रोड, नई दिल्ली- 110003

लिफाफे के कवर पर संपर्क नंबर एवं ईमेल पते के साथ कंपनी का नाम और पता लिखा होना चाहिए। ठीक से मुहरबंद नहीं की गई कोटेशन पर विचार नहीं किया जाएगा तथा उन्हें बिना कोई कारण बताए रद्द कर दिया जाएगा।

कोटेशन 25-08-2023 (शुक्रवार) को सायं 6.00 बजे से पूर्व उपरोक्त पते पर पहुंच जानी चाहिए। रा. आ. बैंक को कोटेशन जैसा कि ऊपर बताया गया है कोटेशन/ वाणिज्यिक बोली जमा करने की अंतिम तिथि से पहले विनिर्दिष्ट पते पर पहुंच जानी चाहिए। रा. आ. बैंक द्वारा निर्धारित बोली जमा करने की समय सीमा के बाद रा. आ. बैंक द्वारा प्राप्त किसी भी बोली को अस्वीकार कर दिया जाएगा एवं बोली को बिना खोले वापस कर दिया जाएगा।

बोलीदाता **दिनांक 18-08-2023 (शुक्रवार) को शाम 6:00 बजे से पहले** तक बोली दस्तावेज में प्रदान की गई ईमेल आईडी पर ईमेल के माध्यम से बोली दस्तावेज के संबंध में प्रश्न / स्पष्टीकरण, यदि कोई हो पर जानकारी प्राप्त कर सकता है।

कंपनियों के प्राधिकृत प्रतिनिधि, किसी भी प्रश्न/ स्पष्टीकरण हेतु सार्वजनिक अवकाश को छोड़कर सोमवार से शुक्रवार को सुबह **10:00 बजे से शाम 6:00 बजे** के बीच लेखा परीक्षा विभाग, राष्ट्रीय आवास बैंक से संपर्क कर सकते हैं।

बैंक किसी भी कोटेशन को बिना कोई कारण बताये रद्द या स्वीकार करने और / या सभी कोटेशनों को रद्द करने का अधिकार रखता है।

भवदीया,

(रीता भट्टाचार्य)

महाप्रबंधक

संलग्नः यथोपरि

For Undertaking Information Security & Cyber Security Audit for the Year 2022-2023 (July-June)

"Requirement Proposal (RP)"

1. PROJECT

(i) Most of the functions of National Housing Bank (NHB) have been computerized and have been brought under the single ERP platform (SAP). There has been great reliance on IT systems on day-to-day operations of the Bank. This has increased the criticality of the IT & IS infrastructure of the Bank.

(ii) NHB proposes to undertake Information Security Audit (ISA), Vulnerability Assessment and Penetration Testing (VAPT) & Cyber Security Audit (CSA) of its IT Infrastructure Systems, Applications and Web facing applications/ portals as per the activities delineated hereunder in Scope of Work, with a view to check the resilience of the extant infrastructure, enhance the security measures and to adopt best international practices and standards in due course. The ISA & CSA should be conducted in accordance with the guidelines of ISO 27001, RBI, CERT-In, NCIIPC, Govt. of India, OWASP, Information Technology Act 2000 – 2008 (*and amendments thereafter*) and other international standard guidelines for the same.

(iii) The audits are to be carried out as per the said frequency: -

S. No.	Type of Audit	Frequency of Audit	Related Period
1.	Information Security Audit & Cyber Security Audit	Annually	July 2022- June 2023
2.	VAPT	Quarterly	July 2023– June 2024

2. BRIEF OVERVIEW OF BANK'S IT INFRASTRUCTURE

NHB under its MPLS WAN architecture has four LAN segments at its Delhi Office, one in DR site & one LAN each at Regional offices. All the offices are interconnected through MPLS connectivity with Any-to-Any connectivity. DC, DR site and Mumbai offices are having redundant last mile from the service provider with 32 Mbps and 16 Mbps bandwidth respectively. The offices are connected to the MPLS cloud through last mile of 2 Mbps which is delivered through Wireless and Fibre Link. In addition to this NHB has a dedicated LAN at Delhi to run RBI-NDS application through MPLS from two different service providers. Separate MPLS link is also available at Mumbai Regional Office for the NDS application.

NHB has SSL, VPN Gateway to enable its employees to connect to IT services hosted in its Data Centre. Bank has its Disaster Recovery Site at Navi Mumbai which is fully operational DR Site consisting of SAP System & File Servers. Both Data Centre and DR Site are in real time sync with maximum gap of up to 15 minutes

2A. Wide Area Network (MPLS)

Presently NHB has MPLS connectivity between New Delhi, DR Site & Regional Offices (ROs) as under. MPLS services are in managed mode.

S. No.	Location	Bandwidth
1	New Delhi	32 Mbps
2	DR Site	32 Mbps
3	Mumbai Office	16 Mbps
4	ROs	2 Mbps

Presently Bank has 15 nos. of ROs at Ahmedabad, Bengaluru, Bhopal, Bhubaneswar, Chandigarh, Chennai, Delhi, Guwahati, Hyderabad, Jaipur, Lucknow, Kolkata, Mumbai, Patna and Raipur.

2B. Local Area Network

At New Delhi and Mumbai offices the LAN is based on Layer 2 switches. The switches used at the locations are unmanaged. All switches are property of NHB and are under Warranty/AMC with respective vendors.

- At DC, Delhi and DR Site Navi Mumbai has deployed Cisco series switches
- At DC, Delhi has installed Cisco Series Firewall and DR Site Navi Mumbai has installed Sophos firewall.
- Other offices are connected to Head office over MPLS. The offices access Bank's hosted IT services over MPLS. MPLS network as well as the premises MPLS equipment is managed by present MPLS connectivity provider.

2C. Applications/ Internet/ Intranet etc.

- Bank has setup domain controller (DC) & ADC for managing its environment.
- Bank has implemented SAP ERP system for most of its business operations.
- For mailing solution, Bank has currently subscribed to O365 suite for its users.
- Internet dedicated bandwidth from two different service providers is available at Delhi. The bandwidths are used for Internet browsing and other web-based services.
- NHB at its Delhi office has implemented proxy server with web caching, web content filtering integrated with Active Directory at DC for user authentication and controlling user Internet access. In addition to this Bank has implemented Cisco ASA firewall and Antivirus solution for security.
- NHB has SSL VPN Gateway to enable its emp1oyees to connect to IT services hosted in its Data Centre.
- Bank uses services like Cogencis, Refinitiv at its Treasury Department to keep a tab on developments happening in financial and treasury market.

2D. Infrastructure at Head Office, New Delhi

SERVERS	NUMBERS
Servers- on Windows 2012/2016 platform - including SQL Server/ Outlook/SAP Servers and others	74

PCs	PLATFORM	NUMBERS
1. Client Machines on LAN	Windows Vista/7/Windows 8/10	197
2. Laptops/Mobile Computers	Windows 7/8/10	154

DR Site, Navi Mumbai

SERVERS	NUMBERS
Servers- on Windows 2012/2016 platform- including SQL Server	15

PCs	PLATFORM	NUMBERS
1. Client Machines on LAN	Windows Vista/7/Windows 8/10	2
2. Laptops/Mobile Computers	Windows 7/8/10	1

**Please Note that aforesaid list is subject to change.*

3. PROJECT SCOPE OF WORK

(i) ISA & CSA will cover the IT Infrastructure, Systems, Applications and web facing applications / portals of the Bank's head office at Delhi and Regional office at Mumbai, including CSOC, Cyber Security Framework. Further, the Bank has its Regional Offices at Ahmedabad, Bengaluru, Bhopal, Bhubaneswar, Chandigarh, Chennai, Delhi, Guwahati, Hyderabad, Jaipur, Lucknow, Kolkata, Mumbai, Patna and Raipur, which are connected to the centralized Data Centre located at Head Office. **Some more regional offices are expected to be set up during the period of audit (i.e. FY 2023-2024 (July -June) , which shall also be connected to the centralized Data Centre located at Head Office.** ISA & CSA will cover the access control mechanism implemented for these offices also.

(ii) ISA & CSA are to be conducted in following three phases:
- **PHASE – I EVALUATION**
- **PHASE – II COMMUNICATION**
- **PHASE – III REVIEW & CERTIFICATION/FINAL COMPLIANCE REPORT**

The activities covered under each phase are appended below and all these activities are collectively referred to as the "**Project Scope of Work**"

PHASE – I EVALUATION

1. Risk assessment and identification of security needs.

a. Evaluation of security needs of the current IT infrastructure of NHB-

- Network and the devices in use, Firewall Rule Base Review;
- Operating Systems – Setup, Configuration, Tuning, License Audit, etc.
- Database, Systems and Applications (Web facing and non-Web facing) – Setup, configuration, Tuning, Database Audit, etc.
- Cyber Security Set-up.
- Pre-Audit / Verification of KRI returns within the timelines prescribed by the Bank.
- Pre-Audit / Verification of Public facing applications and databases returns within prescribed timelines.
- Pre-Audit / Verification of Cyber Security Incident Summary within prescribed timelines and any other such returns, required to be submitted to Reserve Bank of India (RBI), within prescribed timelines.

b. Evaluation of the extant design of Security Architecture-

- Evaluation of the extant security architecture, change recommendations /new designs/layouts, and documentation of the security architecture so as to conform to the RBI Guidelines, International Standards and Industry wide accepted best practices.
- Coverage of review of Bank's inventory for identifying inventory having reached beyond End of life/ End of support.
  Coverage of review of endpoints and servers for unauthorized/ unlicensed Software installation.
- Evaluation of the risk posture of the Bank based on, but not limited to, threats, vulnerabilities observed during IS Audit, quarterly VAPT exercise, red team exercise, and also based on Bank's security posture for protection of its information assets.
- Conduct Red Teams exercise on half-yearly basis to identify the vulnerabilities and the business risk, assess the efficacy of the defences and check the mitigating controls already in place by simulating the objectives and actions of an attacker.

c. Evaluation of the System implementation in the Bank-

- Evaluation of the current Operational Procedure and Security Policy for processes that have been computerized. Recommending and framing Operation Procedure and Security Policy for these processes. Special emphasis is to be laid on evaluation of the security aspects of systems and applications such as SAP, CRAMIS, PMAY-CLSS, GRIDS, ADF and other web-facing applications, other software etc. implemented in the Bank.

- Evaluation of implementation and maintenance of access controls based on the instructions from the information resource owner and in accordance with applicable policies, directives, and standards.
- IS & Cyber Security Auditor must interact with all Head of the Departments (HODs) in the Bank to obtain their views/feedback towards Information Security & Cyber Security measures taken by the Bank and evaluate the gaps (*if any*) based on their feedback.

d. Evaluation of Web Facing Applications and Portals-

- Evaluation of web application configuration and testing reporting of gaps/vulnerabilities/improvements (if any). Suggesting solutions/mitigating strategies to tackle the same.
- To carry Software Audit of Bank's internal applications for vulnerabilities and portals developed in-house as also newly implemented applications during Audit Period Details will be provided at the time of commencement of Audit/testing.
- To test the resilience level of Bank's web facing interfaces by conducting audit as per latest OWASP attack guidelines and Vulnerability Assessment and Penetration Testing (VAPT). The objective of the assessment is to determine the effectiveness of the security of organizations infrastructure and its ability to withstand an intrusion attempt. This may be achieved by conducting both reconnaissance and a comprehensive penetration test. This will provide good insight as to what an attacker can discover about the network and applications to exploit them. The security assessment should use the industry standard penetration test methodologies (like OSSTMM) and scanning techniques and will focus on applications/web-applications. The application tests should cover but not limited to OWASP Top 10 attacks and SANS TOP 25 Most Dangerous Software Errors. The details of Bank's web-facing applications/portals are as under:
    - ✓ SAP Employee Portal
    - ✓ GRIDS
    - ✓ CRAMIS
    - ✓ PMAY-CLSS Portal
    - ✓ RESIDEX
    - ✓ Automated Data Flow (ADF)
    - ✓ HFR
    - ✓ NHB Website
    - ✓ HRMS Portal
    - ✓ Some more applications may be added during the course of Audit.

- Evaluation of Cyber Security Framework, Policy, CSOC in lines with the guidelines as indicated in the RFP

e. Evaluation of Bank's Cyber Security Preparedness Indicators as mentioned in the Cyber Security Framework as per their assigned periodicity and provide its

report on the same, based on the periodicity of the indicators. The Cyber Security Preparedness Indicators Matrix is enclosed at **Annexure I.**

2. Detailing the Security Gaps

- Audit of Business Continuity Plan & Disaster Recovery Plan.
- Site Audit of DC & DR Sites
- Audit of all Outsourced activities and services
- Evaluation of Capacity Planning of Critical Infrastructure, recommendation of plugging the Gaps in infrastructure.
- Documentation of the security gaps i.e., vulnerability, security flaws, loopholes, etc. observed during the course of the review of the IT infrastructure of the Bank.
- Documentation of recommendations for addressing these security gaps and categorization of identified security gaps based in their criticality, resource/effort requirement to address them.
- Chart a roadmap for the Bank to ensure compliance and address these security gaps.
- A preliminary report documenting the major findings of the ISA & CSA is to be furnished at the end of this phase.

3. Addressing the Security Gaps

- Recommending fixes & solutions addressing the Security flaws, gaps, loopholes, shortfalls, vulnerabilities in deployment of applications/systems, web-facing applications which can be fixed immediately.
- Recommendations of fixes for system vulnerabilities in design or otherwise for application systems, web and network infrastructure.
- Advising the Bank regarding detailed processes to apply software patches available through OEM to overcome security loopholes / flaws.
- Suggest changes/modifications in the Security Policies and Security Architecture including Network, applications and web facing applications / portals of NHB to address the same.

4. Conducting Cyber Audit

As per the standard and latest industry practices and guidelines as indicated in the RFP.

PHASE – II COMMUNICATION

1. User Training

Imparting IT & cyber security awareness training for Bank's employees and on-site staff handling Bank's IT infrastructure in form of lecture, seminar/webinar, interactions, and presentations on quarterly basis. The training material will

also be shared with the Bank. The training shall be carried out at Delhi in 2/3 sessions at various operational levels, in a single /two days.

2. Reports of ISA & CSA Findings

The reports of the ISA & CSA findings will include the risk areas which are to be categorized in High Risk, Medium Risk, and Low Risk categories. The possible solutions for addressing the risk areas are to be clearly indicated in the report to facilitate Gap Closer activities.

PHASE – III REVIEW & CERTIFICATION/FINAL COMPLIANCE REPORT

1. Review

An exercise to review the compliance with the findings and recommendations of ISA & CSA has to be undertaken by the selected empanelled auditor. This exercise would be undertaken after 1-2 months of completion of the ISA & CSA. This exercise would encompass evaluation of the general/overall level of compliance undertaken by the Bank

2. Certification / final compliance report for the findings of the ISA & CSA

On completion of the compliance review, the selected empanelled auditor has to provide an ISA & CSA compliance document/report to that effect.

4. PROJECT DELIVERABLES

There are five major deliverables in the project-

1. ISA & CSA including OWASP Audit
2. Vulnerability Assessment, Analysis and Resolution
3. ISA & CSA Reports
4. Training Programs & Training Material for NHB officials
5. To provide Certificate/report/compliance report for the ISA & CSA &VAPT

These are described in the following sub-sections below-

4.1. Information Security Audit & Cyber Security Audit

(Type - Services)

Under this project the bidder/ selected empanelled auditor will provide services for:

- Risk assessment and identification of security needs.
- Evaluation of the current IT infrastructure of NHB, Network and the devices in use, Operating Systems, Database and Application packages,

Web facing applications/portals and Operational Procedures, Cyber infrastructure/applications.

- Identification of vulnerability, security flaws, gaps and loopholes.
- Evaluation of the extant design of Security Architecture, recommendation of changes/new design/layouts and document the security architecture so as to conform to the ISO 27001 guidelines, RBI Guidelines, OWASP attack guidelines, OSSTMM, International Standards and Industry wide accepted practices, CERT-In , Information Technology Act 2000 - 2008 (& amendments thereafter) ;
- The Security Architecture Design includes the Head Office and the Regional Offices combined i.e., including the interconnection between the two offices and the interfaces used by various applications on the NHB network.
- To undertake configuration of Security Architecture including Network and Applications of NHB to address the same.
- Evaluate the current Operational Procedure and Security Policy for processes that have been computerized. Recommending and framing Operational Procedure and Security policy for these processes.
- Evaluation of the SAP implementation in the Bank. The business processes implementation on SAP needs to be assessed for their security aspects and recommendation for suitability amendments may be given, if required.
- Review of all Application Programming Interfaces (APIs) in the production for vulnerabilities.
- Coverage of secure configuration review of, but not limited to, Bank's security solutions, OS, applications, servers, and network devices.
- Evaluating the implementation and effectiveness of security controls and applicable directions as mentioned in Bank's policies, plans, procedures, cyber security preparedness indicators related to information and cyber security.
- Evaluating the compliance related to advisories and alerts issued by various cyber security agencies such as CERT-In, RBI, NCIIPC and IDRBT etc.
- Evaluating the effectiveness of IT asset inventory management, data classification management, Patch/ vulnerability management, user access management, incident response management and IT change management in the Bank.
- To undertake Source code audit of Bank's public facing applications.
- To undertake the Information security review of APIs in production environment.
- To ensure that DAKSH usage, the process of user creation & maintenance, and role assignment is reviewed regularly.

4.2. Vulnerability Assessment, Analysis and Resolution

(Type – Documentation & Service)

- Under this project the bidder/ selected empanelled auditor will provide services for assessment and will provide recommendations for addressing the vulnerabilities.
- Documenting the vulnerabilities, security flaws, gaps and loopholes.

- Identifying the vulnerabilities in deployment of applications/systems and recommending fixes for system vulnerabilities in design or otherwise for application systems and network infrastructure.
- Fixing/addressing shortfalls which can be addresses immediately.
- Recommendation for applying software patches available through OEM to overcome security loopholes/flaws.
- VAPT shall be carried out quarterly and the findings are to be shared with the concerned Departments within defined timeline.
- Verification of the closure/ compliance of VAPT Observations, 1 month post submission of the report in coordination with concerned Department(s).
- VAPT of Bank's internal applications throughout their lifecycle (pre-implementation, post implementation, after major changes).
- Bidder /Auditor will be responsible to conduct pre deployment VAPT of any application during the contract period, in coordination with the bank and as per requirement of Bank. The list of application under IS Audit/VAPT scope will be kept updated accordingly.
- The penetration testing exercise should be carried out like offensive security certified professionals so that the robustness of IT security infrastructure of the Bank can be assessed.
- VAPT Reports should mention the date of occurrence of VAPT exercise.
- Coverage of quarterly review of all critical security patches and security updates, but not limited to, endpoints, OS, browsers, Servers, VMWare, Firewall, network devices, security solutions, antivirus, and other application-level patches (SAP/ related banking software, etc.)
- Cover user access review for Bank's applications, SAP/ related banking software, and Windows directory on quarterly basis.
- Cover the review of Business Continuity plan/policy and Business Continuity Document of the Bank.
- Check the effectiveness of email spoofing controls such as DKIM, SPF and DMARC through security testing during the VAPT exercise.

IS Auditors may provide suggestions/ probable solutions to mitigate the risks and threats in future w.r.t. IS Audit and VAPT observations.

Physical presence of IS Auditors *(preferably for at least 1 week)* required for validation of IS Audit and VAPT observations during Compliance Testing.

4.3. ISA & CSA Report

(Type - Documentation)

The ISA & CSA Report would comprise of three sub – reports:

I. **ISA & CSA Report: Detailed Findings:** The detailed findings of the ISA and CSA would be brought out in this report which will cover in details all aspects viz. identification of flaws/vulnerabilities, suggestion for solutions/corrective measures that are in line with the RBI guidelines, ISO

27001 and OWASP attack guidelines, future preventive measures as per the latest industry standards, action taken, along with suggested timeline for correction/improvement/implementation of solutions or recommendations provided etc. Two separate finding reports shall be submitted for ISA & CSA.

II. **ISA & CSA Report: Compliance Report:** This report would enclose compliance status on the findings of ISA Report and CSA Report furnished earlier.

III. **ISA & CSA Report: Knowledge Transfer:** Further, the selected empanelled auditor will also furnish a report capturing the experience gathered during the ISA & CSA. It will also cover in detail the knowledge transfer activity undertaken by the bidder/ selected empanelled auditor, the response received from the employees of the Bank and the bidder / selected empanelled auditor's assessment of the IT & Cyber security awareness and readiness of the Bank's employees.

4.4. Training Programs & Training Material for NHB officials

(Type - Documentation)

The bidder/ selected empanelled auditor will develop courseware, impart training, and provide training material for the NHB officials, NHB Administrators and other related users.

4.5. Provide Certification/Compliance Report for the ISA & CSA

(Type – Documentation & Services)

The bidder/selected empanelled auditor is to provide NHB a certification/compliance report each for ISA and for CSA (separately) and for VAPT

Documentation Format:

- All documents will be handed over in three copies, legible, neatly and robustly bound on A-4 size, good-quality paper.
- Soft copies of the document in MS Word format will also be submitted in CDs along with the hard copies (three hard copies of each documents/certificate).
- All documents will be in plain English or Hindi.

Further, the scope of ISA and CSA also includes evaluation of policy documents related to ITD and Information Security and Cyber Security and give recommendations for improvement (if any) and provide feedback after evaluation of Bank's IT infrastructure towards preparedness of ISO 27001 certification for Bank's Data Centre and DR Site.

The Bank has following five policies related to IT & Cyber Security:

1. Information Technology Policy & Guidelines
2. Information Security Policy
3. Policy of Procurement of Goods and Services
4. Disposal Policy
5. Cyber Security Framework

IS and Cyber Security Auditors may be assigned any additional task including forensic investigation of a cyber security incident or undertaking data migration audit, as per the requirement of the Bank beyond the scope of work. In such cases, the task is to be completed at the man-day rate quoted by the Auditor based on the assessed man-days required for completion of the task i.e. No. of days x Man Day Rate.

5. PROJECT SCHEDULE

Commercial bids would be called from the empanelled bidders and the L1 (lowest) bidder shall be selected for carrying out IS & Cyber Security Audit. The selected bidder shall depute their officials at the Bank's Head Office at Delhi and at Regional Office at Mumbai for conducting ISA & CSA within 15 days of placement of work order/service contract. The timeframe for completion of Phase - I of the project would be 4-6 weeks from acceptance of the work order and for Phase - II would be 2-3 weeks from the end of Phase I. An exercise to review the compliance with the findings and recommendations of ISA & CSA has to be undertaken in Phase - III. The exercise would be undertaken after 1-2 months of completion of ISA & CSA and certificate/compliance report is to be issued within a week of Audit Review. **The entire exercise (from commencement of audit to conclusion of audit) of ISA & CSA shall not exceed 6 months from beginning of the financial year 2023-24 (July-June) i.e. by 31-12-2023**. Furthermore, VAPT is to be conducted quarterly preferably in the beginning of each quarter and the findings of the same is to be shared within 30 days from the last day of the quarter. **The project will be treated as completed only after completion of all activities as given under the "Project Scope of Work" and providing all "Project Deliverables" to the Bank.**

5.1 DURATION OF CONTRACT

The contract shall be valid till completion of all activities as given under the "Project Scope of Work" and providing all "Project Deliverables" to the Bank, from the date of the work order/letter of award.

6. PENALTY

Penalty will be charged @ 2% of the total contract value per week on delay in submission of audit report & audit compliance report in phase – I, II and III respectively (For phase – I, delay will be counted after 8 weeks from the acceptance of work order & for phase – II after 16 weeks of from the acceptance of work order) with a maximum of 10% of the contract value. If the delay exceeds 5 weeks, contract may be cancelled, and the Bank may claim entire advance amount with interest from the selected bidder as also shall forfeit the EMD amount.

7. INSTRUCTION TO BIDDERS

7.1 General Instructions:

(i) All General Terms and Conditions of the RFP REF NO: NHB(ND)/AD/A-1162/2019 dated February 03, 2020 and corrigendum dated February 21, 2020 (herein after referred to as "**RFP**") will be applicable, unless specified otherwise by NHB.

(ii) The quotation must contain the price inclusive of all levies/charges, and taxes. The bidder must give the price Bid as per the format specified at **Annexure II**. Prices and other terms offered by bidders must be valid for an acceptance period of six months from the date of opening of Commercial Bid.

(iii) The quotation should be accompanied by self-declaration(s) duly signed by the Authorized Signatory (s) of the company with respect to the Minimum Eligibility Criteria (MEC) Sl. No. 3, 4,5, 6 & 7 as defined in aforesaid RFP and the Corrigendum thereafter.

(iv) The quotation should be signed by the Authorized Signatory (s) of the company. It should be enclosed in a non-window sealed cover, superscripted as **"Commercial Quotation for undertaking Information Security & Cyber Security Audit for the Year 2022-23 (July-June)"** and must reach at the following address-

The General Manager,
Audit Department, National Housing Bank,
4th Floor, Core 5A, India Habitat Centre,
Lodhi Road, New Delhi- 110003

(v) The envelope should indicate on the cover the name and address of the company along with contact number and email address. **Quotations not sealed properly shall not be considered and will stand rejected without recourse.**

(vi) The quotation must reach the above address **by 25-08-2023 (Friday), before 6:00 p.m.** The quotation must be received by the Bank at the address specified, not later than the last date of submission of quotation /Commercial Bid as indicated above. **Any Bid received by NHB after the deadline for submission of Bids prescribed by NHB will be rejected and returned unopened.**

(vii) The bidder may seek queries/ clarification, if any, regarding the Bid document(s) via emails on the email IDs provided in this Bid document on or before **18-08-2023 (Friday), before 6:00 p.m.** The Authorised Representative of companies may contact Audit Department, National Housing Bank between **10:00 am to 6:00 p.m**. at Head Office on Monday to Friday, excluding public holidays, for any query/clarification.

(viii) Bidders are required to direct all communications related to this quotation, through the nominated point of Contact Persons, mentioned below:

Atul Pal, Manager, Audit Department National Housing Bank, Head Office Core 5-A, 4th Floor, India Habitat Centre, Lodhi Road, New Delhi – 110003 Email: atul.pal@nhb.org.in Phone Number 011-39187324	Hardik Budh, Deputy Manager Audit Department National Housing Bank Head Office Core 5 A, 4th Floor, India Habitat Centre, Lodhi road, New Delhi, 110003 Email: hardik.budh@nhb.org.in Phone Number 011-39187267

(ix) The Bank reserves the right to reject or accept any quotation and/or all quotations without assigning any reason.

(x) All costs and expenses incurred by the bidders in any way associated with the development, preparation, and submission of responses, including but not limited to; the attendance at meetings, discussions, demonstrations, etc. and providing any additional information required by the Bank, will be borne entirely and exclusively by the bidder.

(xi) No binding legal relationship will exist between any of the bidders and the Bank until execution of a contractual agreement, except the pre-contract Integrity Pact to be submitted along with the Bid. Post evaluation and finalization of the Bids and identification of the successful bidder, the Integrity Pact will form part of the definitive agreement to be signed by the successful bidder. For the other bidders, the pre-contract Integrity Pact will be binding on them for any acts/omissions committed by the bidder in violation/breach of the said pre-contract Integrity Pact in relation to the Bid submitted.

(xii) Each bidder acknowledges and accepts that the Bank may in its absolute discretion apply selection criteria specified in the document for evaluation of proposals for selecting the eligible auditors.

(xiii) Every bidder will, by submitting his Bid in response to this RP, be deemed to have accepted the terms of the RFP, this RP and the Disclaimer.

- NHB may, in its absolute discretion, seek additional information or material from any bidder/s even after the RP closes and all such information and material provided must be taken to form part of that bidder's response.
- Bidders should provide details of their contact person, telephone, fax, email and full address(s) to ensure that replies to RP could be conveyed promptly.
- If the Bank, in its absolute discretion, deems that the originator of any query will gain an advantage by any response to such query, then the Bank reserves the right to communicate such response to all bidders.
- Queries / Clarification if any, may be taken up with the contact person/s detailed above before the deadline for submission of Bids between **10:00 am to 6:00 p.m**. on Monday to Friday, excluding public holidays.
- Bidder should not have been blacklisted/debarred from participation in the Bid process by any of the Govt. Departments/PSUs/Banks/Financial Institutes

in India and such order of debarment shall not be effective on date applying for the bid.

- The Bank will notify all short-listed bidders in writing or by mail or by publishing in its website as soon as practicable about the outcome of their RP. The Bank is not obliged to provide any reasons for any such acceptance or rejection.

7.2 Performance Bank Guarantee (PBG)

The successful bidder will be required to provide PBG in the form of bank guarantee from a scheduled commercial bank in the format as substantially prescribed in **Annexure-III** of the RP. The PBG should be valid till at least six months beyond the expiry of contract period or such other extended period as the Bank may decide. The PBG is required to protect the interest of the Bank against the risk of non-performance or default in RFP & RP Term/s, including non-compliance of applicable statutory provisions including labour laws and any other laws/rules/regulations, by the successful bidder. Default in successful implementation of the conditions of the contract, may warrant the invoking of PBG, and also if any act of the selected bidder results into imposition of Liquidated Damages/penalty, then the Bank reserves the right to invoke the PBG submitted by such bidder. The decision of the Bank as to non-performance or default in RFP & RP Term/s, including non-compliance of applicable statutory provisions etc., shall be final and binding on the successful bidder.

8. Acceptance of Work Order/Letter of Award

NHB will notify the successful Bidder in writing by issuing a letter of award/work order in duplicate. The successful Bidder has to return the duplicate copy to NHB within 7 working days from the date of the letter of award/work order duly accepted, and signed by Authorized Signatory in token of acceptance. However, NHB has a right to cancel the letter of award/work order, if the same is not accepted within the stipulated period.

9. SIGNING OF CONTRACT

The successful bidder(s) will sign a Service Level Agreement (SLA), and the Confidentiality cum Non-Disclosure Agreement (NDA) as per **Annexure IV & Annexure V** with NHB within 30 days of award of the service order or within such extended period as may be decided by the Bank. All expenses, stamp duty and other charges/ expenses in connection with the execution of the Agreement/s as a result of this RP /quotation process shall be borne by successful bidder. Copy of Board Resolution or Power of Attorney showing that the signatory has been duly authorized by the company to sign the acceptance letter /work order, service level contract, and non-disclosure agreement, should be submitted. Requisite KYC documents of the successful bidder (company) and the authorised signatory also should be submitted. The resultant contract shall be governed by Indian Laws.

10. BID OPENING AND EVALUATION

(i) The Bank will open the Commercial Bids, in the presence of bidder's representative who choose to attend. The date, time and venue of opening of commercial bids will be communicated separately. Any bids may be rejected, if the information provided by the bidder is either incomplete or is not in a specified format. Any interlineations', erasures or overwriting in any form will not be accepted in the Commercial Bid. There should be no hand-written material, corrections, or alterations in the Commercial Bid. L1 bidder (Lowest Bidder) will be considered for awarding the contract. In case of a tie, the Bank reserves the right to select the bidder based on marks scored during technical evaluation. If a bidder quotes NIL charges/consideration, the bid shall be treated as unresponsive and will not be considered.

(ii) **Pre-Bid Meeting:**

For the purpose of clarification of doubts of the bidders on issues related to this tender/RP, the Bank intends to hold a Pre-Bid meeting. The date and time of the meeting shall be intimated separately. The queries of all the bidders, in writing, should reach by e-mail or by post on or **before 18-08-2023 (Friday), before 6:00 p.m** on the address as mentioned in Clause 7.1 (viii) above. It may be noted that no query of any bidder shall be entertained after the Pre-Bid meeting. Clarifications on queries will be given in the Pre-Bid meeting itself. Only the authorized representatives of the bidders will be allowed to attend the Pre-Bid meeting.

(iii) **Period of Validity of Bids**

(a) Prices and other terms offered by bidders must be valid for a period of six months from the date of submission of Commercial Bid for acceptance by the Bank.

(b) In exceptional circumstances, the Bank may solicit the bidders' consent for extension of the period of validity. Any such request and response thereto shall be made in writing. The Bid security/EMD provided shall also be extended.

11. PAYMENT TERMS

11.1 Subsequent to the award of contract to the L1 bidder, following conditions are applicable for processing of payment.

- **30% of contract value** as advance Payment on acceptance of work order. Advance payment will be released only on submission of Performance Bank Guarantee of equal amount valid up to One year and six months (18 months).
- 10% on Submission of the ISA & CSA Report (2022-2023) and VAPT report for Quarter 1 (July 2023- Sept 2023).
- 10% on Submission of VAPT report for Quarter 2 (Oct 2023- Dec 2023)
- 10% on Submission of VAPT report for Quarter 3 (Jan 2024- March 2024)
- 10% on Submission of VAPT report for Quarter 4 (April 2024- June 2024)

- 30% on providing all deliverables as mentioned in RFP/RP/Bid Document and/or Work Order {including Final Compliance reports of ISA and CSA (2022-2023) and VAPT Reports (2023-2024)}.

(If the selected bidder does not submit PBG within one month of placement of work order, no advance amount shall be released and full payment will be done only after completion of the entire project).

11.2 **Payment in case of termination of contract**

Subject to the terms of the RFP & RP, in case the contract is terminated, payment towards services will be made on pro rata basis, for the period services have been delivered, after deducting applicable penalty and TDS/other applicable taxes.

12. Banned or Delisted Bidder

12.1 Bidders have to give a declaration that they have not been banned or delisted by any Government, Quasi Government agencies, PSUs or PSBs and its subsidiaries. If a Bidder has been banned by any Government, Quasi Government agencies, PSUs or PSBs and its subsidiaries, this fact must be clearly stated. If this declaration is not given, the Bid will be rejected as non-responsive. This declaration will be submitted along with the Commercial Bid.

12.2 Restriction on procurement from a bidder of a country which shares a land border with India:

(a) Any bidder from a country which shares a land border with India will be eligible to bid in this tender only if the bidder is registered with the Competent Authority i.e. the Registration Committee constituted by the Department for Promotion of Industry and Internal Trade (DPIIT).

However, such registration is not required for being eligible under this RP in case the bidders are from countries (even if sharing land border with India) to which Government of India has extended lines of credit or in which the Government of India is engaged in development projects, as per the updated list of such countries given on website of Ministry of External Affairs.

(b) **The bidder shall also submit a certificate as per the format enclosed as Annexure VI. If such certificate given by the successful bidder is found to be false, this would be a ground for immediate termination of the contract and for further legal action in accordance with law.**

12.3 For the purpose of this clause:

a) "Bidder "(including the term 'vendor', 'IS Auditor' or 'service provider' in certain contexts) means any person or firm or company, including any member of a consortium or joint venture (that is an association of several persons, or firms or companies), every artificial judicial person not falling in any of the descriptions of bidders stated hereinbefore, including any agency branch or office controlled by such person, participating in a procurement process.

b) "Bidder from a country which shares a land border with India" for the purpose of this Order means:-

(i) An entity incorporated, established or registered in such a country; or

(ii) A subsidiary or an entity incorporated, established or registered in such a country; or

(iii) An entity substantially controlled through entities incorporated, established or registered in such a country; or

(iv) An entity whose beneficial owner is situated in such a country; or

(v) An Indian (or other) agent of such an entity; or

(vi) A natural person who is a citizen of such a country; or

(vii) A consortium or joint venture where any member of the consortium or joint venture falls under any of the above.

c) The beneficial owner for the purpose of (b) above will be as under.

i. In case of company or Limited Liability Partnership, the beneficial owner is the natural person (s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means.

"Controlling ownership interest" means ownership of or entitlement to more than twenty-five per cent. Of shares or capital or profits of the company;

"Control" shall include the right to appoint majority of the directors or to control the management or policy decision including by virtue of their shareholding or management rights or shareholders agreement or voting agreement;

ii. In case of partnership firm, the beneficial owner is the natural person (s) who, whether acting alone or together, or through one or more juridical person, has ownership of entitlement to more than fifteen percent of capital or profits of the partnership;

iii. In case of an unincorporated association or body of individuals, the beneficial owner is the natural person (s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more

than fifteen percent of the property or capital or profits of such association or body of individuals;

iv. Where no natural person is identified under (i) or (ii) or (iii) above, the beneficial owner is the relevant natural person who holds the position of senior managing official;

v. In case of a trust, the identification of beneficial owner(s) shall include identification of the author of the trust, the trustee, the beneficiaries with fifteen percent or more interest in the trust and any other natural person exercising ultimate effective control over the trust through a chain of control ownership.

d) An Agent is a person employed to do any act for another, or to preset another in dealings with third person.

13. Pre-Contract Integrity Pact Clause (To be mentioned only in cases depending on the threshold fixed as per the policy of NHB)

13.1 A "Pre-Contract Integrity Pact" would be signed between the Bank and the bidder. This is a binding agreement between the Bank and bidder. Under this Pact, the bidder agree with NHB to carry out the assignment in a specified manner. **The format of Pre-Contract Integrity Pact will be as per Annexure VII.**

13.2 In this regard, NHB has appointed Shri Lov Verma, IAS (Retd.)- lov_56@yahoo.com and Shri Hare Krushna Das, IAS (Retd.) - E-mail: hkdash184@hotmail.com as independent external monitors for the Integrity Pact in consultation with the Central Vigilance Commission.

13.3 The following set of sanctions shall be enforced for any violation by a Bidder of its commitments or undertakings under the Integrity Pact:

(i) Denial or loss of contracts;
(ii) Forfeiture of the EMD/Bid security and the performance bond/PBG;
(iii) Liability for damages to the principal and the competing bidders; and
(iv) Debarment of the violator by NHB for an appropriate period of time.

13.4 The bidders are also advised to have a company code of conduct (clearly rejecting the use of bribes and other unethical behavior compliance program for the implementation of the code of conduct throughout the company.

14. In addition to the terms & conditions provided herein, all the terms & conditions of RFP, on basis of which auditors were empanelled as IS & Cyber Security Auditors of the Bank, shall be applicable for this Bid/contract under this RP. In case of any inconsistency or repugnancy between the provisions contained RFP and this

RP, the provisions of this RP shall prevail to the extent of such inconsistency or repugnancy and the same shall be binding on the bidders.

Note-

This RP is not exhaustive in describing the functions, activities, responsibilities and services for which Auditor will be responsible. The bidder, by participation in this tender, implicitly confirm that if any functions, activities, responsibilities or services which are either not specifically described in this RP or specifically described but has to undergo suitable changes/modifications due to regulatory/statutory changes and are termed necessary or appropriate by NHB for the proper performance of the contract, such functions, activities, responsibilities or services (with applicable changes, if any) will be deemed to be implied by and included within the scope of services under this RP and bidder's response to the same extent and in the same manner as if specifically described in this RP and bidder's response.

वर्ष 2022-2023 (जुलाई-जून) हेतु सूचना सुरक्षा और साइबर सुरक्षा लेखापरीक्षा करने के सम्बन्ध में

"आवश्यकता प्रस्ताव"

1. पररयोजना

(i) राष्ट्रीय आवास बैंक के अधिकांश कार्यों को कम्प्यूटरीकृत कर दिया गया है और उन्हें एकल ईआरपी प्लेटफॉर्म (एसएपी) के अंतर्गत व्यवस्थित किया गया है। बैंक के दिन-प्रतिदिन के कार्यों पर आईटी सिस्टम पर बहुत अधिक निर्भरता रही है। इससे बैंक की आईटी और आईएस अवसंरचना की महत्ता बढ़ गई है।

(ii) रा.आ.बैंक मौजूदा बुनियादी ढांचे के लोचता की जांच करने, सुरक्षा उपायों को बढ़ाने और उचित समय में सर्वोत्तम अंतरराष्ट्रीय प्रथाओं और मानकों को अपनाने की दृष्टि से कार्य के दायरे में नीचे दी गई गतिविधियों के अनुसार अपने आईटी इन्फ्रास्ट्रक्चर सिस्टम, एप्लिकेशन और वेब फेसिंग एप्लिकेशन / पोर्टल्स की सूचना सुरक्षा लेखा परीक्षा (आईएसए), सुभेद्यता मूल्यांकन और पेनेट्रेशन परीक्षण (वीएपीटी) और साइबर सुरक्षा लेखापरीक्षा (सीएसए) करने का प्रस्ताव आमंत्रित करता है। सूचना सुरक्षा लेखा परीक्षा (आईएसए) और साइबर सुरक्षा लेखा परीक्षा (सीएसए) आईएसओ 27001, आरबीआई, सीईआरटी-इन, एनसीआईआईपीसी, भारत सरकार, OWASP, सूचना प्रौद्योगिकी अधिनियम 2000 - 2008 (और उसके बाद संशोधन) और इसके लिए अन्य मानक अंतर्राष्ट्रीय दिशानिर्देश के अनुसार आयोजित की जानी चाहिए।

(iii) लेखा परीक्षा निम्नलिखित आवृत्ति के अनुसार किए जाने हैं:-

क्र. सं.	लेखा परीक्षा का प्रकार	लेखा परीक्षा की आवृत्ति	सम्बंधित अवधि
1.	सूचना सुरक्षा लेखा परीक्षा एवं साइबर सुरक्षा लेखा परीक्षा	वार्षिक	जुलाई 2022- जून 2023
2.	वीएपीटी	तिमाही	जुलाई 2023– जून 2024

2. बैंक की आईटी अवसंरचना का संक्षिप्त विवरण

अपने एमपीएलएस वैन आर्किटेक्चर के अंतर्गत राष्ट्रीय आवास बैंक के दिल्ली कार्यालय में चार लैन सेगमेंट हैं, एक डीआर साइट में और एक-एक लैन क्षेत्रीय/प्रतिनिधि कार्यालयों में हैं। सभी कार्यालय एमपीएलएस कनेक्टिविटी के माध्यम से एनी-टू-एनी कनेक्टिविटी के साथ जुड़े हुए हैं। डीसी, डीआर साइट और मुंबई कार्यालय क्रमशः 32 एमबीपीएस और 16 एमबीपीएस बैंडविड्थ के साथ सेवा प्रदाता से अतिरिक्त लास्ट माइल प्राप्त कर रहे हैं। प्रतिनिधि कार्यालय एमपीएलएस क्लाउड से 2 एमबीपीएस के लास्ट माइल के माध्यम से जुड़े हुए हैं जो वायरलेस और फाइबर लिंक के माध्यम से दिया जाता है। इसके अलावा राष्ट्रीय आवास बैंक के पास दो अलग-अलग सेवा प्रदाताओं से एमपीएलएस के माध्यम से आरबीआई-एनडीएस एप्लिकेशन चलाने के लिए दिल्ली में एक समर्पित लैन है। एनडीएस एप्लिकेशन के लिए मुंबई क्षेत्रीय कार्यालय में अलग एमपीएलएस लिंक भी उपलब्ध है।

रा.आ.बैंक के पास एसएसएल, वीपीएन गेटवे है जो अपने कर्मचारियों को अपने डेटा सेंटर में होस्ट की गई आईटी सेवाओं से जुड़ने में सक्षम बनाता नवी मुंबई में बैंक की आपदा रिकवरी साइट है जो पूरी तरह से चालू डीआर साइट है जिसमें एसएपी सिस्टम और फाइल सर्वर शामिल हैं। डाटा सेंटर और डीआर साइट दोनों वास्तविक समय में अधिकतम 15 मिनट के अंतराल के साथ तालमेल में हैं।

2क. वाइड एरिया नेटवर्क (एमपीएलएस)

वर्तमान में राष्ट्रीय आवास बैंक के पास नई दिल्ली, डीआर साइट, आरओ मुंबई और क्षेत्रीय कार्यालयों (आरओ) के बीच एमपीएलएस कनेक्टिविटी निम्न प्रकार से है। एमपीएलएस सेवाएं प्रबंधित मोड में हैं।

क्र. सं.	स्थान	बैंडविड्थ
1	नई दिल्ली	32 एमबीपीएस
2	डीआर साइट	32 एमबीपीएस
3	मुंबई कार्यालय	16 एमबीपीएस
4	आरओ और आरआरओ	2 एमबीपीएस

वर्तमान में बैंक के अहमदाबाद, बेंगलुरु, भोपाल, भुवनेश्वर, चंडीगढ़, चेन्नई, दिल्ली, गुवाहाटी, हैदराबाद, जयपुर, लखनऊ, कोलकाता, मुंबई, पटना और रायपुर में 15 आरओ हैं।

2ख. लोकल एरिया नेटवर्क

अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

2ग. एप्लीकेशन/इंटरनेट/इंट्रानेट आदि।

अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

2घ. प्रधान कार्यालय, नई दिल्ली में अवसंरचना

सर्वर	संख्या
सर्वर- विंडोज2012/2016 प्लेटफॉर्म पर - SQL सर्वर/आउटलुक/एसएपी सर्वर और अन्य सहित	74

कंप्यूटर	प्लेटफार्म	संख्या
1. लैन पर क्लाइंट मशीनें	विंडोज़ विस्टा/7/ विंडोज़ 8/10	197
2. लैपटॉप/मोबाइल कंप्यूटर	विंडोज़ 7/8/10	154

डीआर साइट, नवी मुंबई

सर्वर	संख्या
सर्वर- विंडोज 2012/2016 प्लेटफॉर्म पर - SQL सर्वरसहित	15

कंप्यूटर	प्लेटफार्म	संख्या
1. लैन पर क्लाइंट मशीनें	विंडोज़ विस्टा/7/ विंडोज़ 8/10	2
2. लैपटॉप/मोबाइल कंप्यूटर	विंडोज़ 7/8/10	1

* *कृपया ध्यान दें कि उपरोक्त सूची परिवर्तन के अधीन है।*

3. परियोजना हेतु कार्य क्षेत्र

अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

4. परियोजना डिलिवरबल्स

अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

5. परियोजना समयावधि

अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

6. दंड

अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

7. बोलीदाताओं को निर्देश

अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

8. अनुबंध पर हस्ताक्षर

अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

9. बोली खोलना एवं मूल्यांकन

अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

10. भुगतान की शर्तें

अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

11. प्रतिबंधित या असूचीबद्ध बोलीदाता

अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

12. अनुबंध-पूर्व सत्यनिष्ठा संधि खंड (केवल रा.आ.बैंक की नीति के अनुसार निर्धारित सीमा के आधार पर मामलों में उल्लेख किया जाना है)

अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

अनुलग्नक हेतु अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

किसी भी विवाद की स्थिति में दस्तावेज का अंग्रेजी संस्करण मान्य होगा।

Annexure I

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
Vulnerability Management										
End-Points										
1	Successful Endpoint Scanning (Coverage)- Internal	Total number of Endpoints in the environment	Endpoints that were not scanned	(Total number of Endpoints scanned/Total number of Endpoint)*100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the endpoint systems that are not part of internal VA scanning and resolve the issues accordingly. • Take approvals in case of exceptions with assistance of IT Department.
2	Compliant Endpoints	Total number of Endpoints scanned	Endpoints that were non compliant as per standards	Total Compliant Endpoints (No aged or overdue vulnerabilities)/Total endpoints*100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the number and reason for non-compliant endpoint systems and resolve specific issues • Take approvals in case of exceptions.
3	Remediated Vulnerabilities (Endpoints)- Internal	Total vulnerabilities present on all scanned endpoints	Aged vulnerabilities present on all scanned endpoints	(Vulnerabilities that were fixed on Endpoints/Total vulnerabilities present on endpoints)*100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the number and reason for non-remediated endpoint vulnerabilities as per Manage Engine Desktop Central report and apply patches/upgrades appropriately as per NHB Patch Management Procedure.
Servers										
4	Successful Server Scanning (Coverage) Internal	Total number of Internal Servers in the environment	Servers that were not scanned	(Total number of Internal Servers Scanned/Total number of Servers)*100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the servers that are not part of internal VA scanning and resolve the issues accordingly • Take approvals in case of exceptions or delayed actions.
5	Vulnerability Closure Rate (Servers)- Internal	% of servers (internal) patched within 30 days post security testing	Percentage of servers (internal) patched within lead time of 30 days post security testing	[(No. of internal servers that are patched within lead time of 30 days) / (Total No. of internal servers tested)] *100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the number and reason for servers that are still non-compliant after 30 days of testing and apply patches/upgrades appropriately as per NHB Patch Management Procedure • Take approvals in case of exceptions or delayed actions..
6	Compliant Vulnerabilities (Internal Facing Servers)- Internal	Total vulnerabilities identified on internally hosted servers	Aged vulnerabilities present on such servers	(Vulnerabilities fixed on the Internal Servers/Total vulnerabilities present on Internal Servers)*100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the number and reason for current vulnerable servers and apply patches/upgrades appropriately as per NHB Patch Management Procedure • Take approvals in case of exceptions or delayed actions
7	Successful Server Scanning (Coverage) External	Total number of external/ web-facing Servers in the environment	Servers that were not scanned	(Total number of external/ web-facing Servers Scanned/Total number of Servers)*100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the servers that are not part of VA scanning and resolve the issues accordingly • Take approvals in case of exceptions or delayed actions.
8	Vulnerability Closure Rate (Servers)- External	% of servers (external facing) patched within 30 days post security testing	Percentage of servers (external facing) patched within lead time of 30 days post security testing	[(No. of external facing servers that are patched within lead time of 30 days) / (Total No. of external facing servers tested)] *100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the number and reason for current vulnerable servers and apply patches/upgrades appropriately as per NHB Patch Management Procedure • Take approvals in case of exceptions or delayed actions
9	Compliant Vulnerabilities (External Facing Servers)- External	Total vulnerabilities identified on externally/DMZ/internet facing servers	Aged vulnerabilities present on such servers	(Vulnerabilities fixed on External facing Servers/Total vulnerabilities present on External facing Servers)*100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the number and reason for current vulnerable External servers and apply patches/upgrades appropriately as per NHB Patch Management Procedure . • Take approvals in case of exceptions or delayed actions
10	Compliant Servers	Total number of Servers scanned in the environment	Total servers that are non compliant as per standard	Total Compliant Servers (No aged or overdue vulnerabilities)/Total Servers*100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the number and reason for non-compliant servers • Take approvals in case of exceptions or delayed actions
11	Exception Tracking (for exclusion from vulnerability remediation)	Open Exceptions	Overdue / delay exceptions	1-2 (IP addresses) exceptions = Green 3-5 (IP addresses) exceptions = Amber >5 (IP addresses) exceptions = Red	up to 2	3 to 5	over 5	Quarterly	IT Department and Audit Department	• Identify the number and reason for exceptions approved • Analyse to assess if alternative solution/ control can be deployed and implement the same with due approvals.
Network Devices										
12	Successful Network Device Scanning (Coverage)- Internal	Total number of Network Devices in the environment	Network Devices that were not scanned	(Total number of Network Devices Scanned/Total number of Network Devices)*100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the Network devices that are not being managed and resolve the issues accordingly. • Take approvals in case of exceptions or delayed actions.

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
13	Compliant Network Devices	Total number of Network Devices scanned in the environment	Total network devices that are non compliant with standard	[Total compliant network devices (No aged or overdue vulnerabilities)/Total Network Devices]*100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the number and reason for non-compliant Network devices. • Take approvals in case of exceptions or delayed actions.
14	Network Device VAPT Closure Rate	% of network devices patched within 30 days post security testing	Percentage of network devices patched within lead time of 30 days post security testing	[(No. of network devices that are patched within lead time of 30 days) / (Total No. of network devices tested)] *100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the number and reason for Network Devices that are still non-compliant after 30 days of testing and apply patches/upgrades appropriately as per NHB Patch Management Procedure • Take approvals in case of exceptions or delayed actions.
15	Exception Tracking (for exclusion from vulnerability remediation)	Open Exceptions	Overdue / delay exceptions	1-2 (IP addresses) exceptions = Green 3-5 (IP addresses) exceptions = Amber >5 (IP addresses) exceptions = Red	up to 2	3 to 5	over 5	Quarterly	IT Department and Audit Department	• Identify the number and reason for exceptions approved • Analyse to assess if alternative solution/ control can be deployed and implement the same with due approvals.
Applications										
16	Application Security -Software Developement	All applications developed as per SDLC Process	Applications that deviate from SDLC Process /Exceptions	0 All applications as per SDLC model' = Green 1-5 applications not as per SDLC model' = Amber >5 applications not as per SDLC model' = Red	O	1 to 5	over 5	Quarterly		• Identify the Bank applications that deviate from Bank's Secure SDLC model and resolve the issues accordingly. • Define the timeline for resolving the specific issues • Take approvals in case of exceptions or delays in the testing.
17	Application Security Testing Compliance- Internal (Greybox/Whitebox)	All Internal Applications within scope for Application Security Testing - Quarterly as per calendar	Delayed/ Overdue application assessments	(Number of Application for which Security Assessment is completed /Total Number of application in scope)*100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the Internal Bank applications that are not being tested and resolve the issues accordingly. • Define the timeline for remaining applications • Take approvals in case of exceptions or delays in the testing.
18	Application Security Testing Compliance- External (Blackbox)	All Internet facing Applications within scope for Application Security Testing - Quarterly as per calendar	Delayed/ Overdue application assessments	(Number of Internet facing Applications for which Security Assessment is completed /Total Number of application in scope)*100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the External Bank applications that are not being tested and resolve the issues accordingly. • Define the timeline for remaining applications • Take approvals in case of exceptions or delays in the testing.
19	Application Security Testing Compliance- Observation Closure (Greybox/Whitebox/Blackbox)	All Applications in-scope for Greybox/Whitebox/Blackbox testing	Applications that were not fixed to address the findings raised during the last application security testing exercise	(Total Vulnerabilities closed within the timeline per application/Total Vulnerabilities identified in the application)*100	>=99%	>=95%	<95%	Quarterly (application wise)	IT Department and Audit Department	• Identify the number and reason for current Bank applications that still have open or pending status of vulnerabilities and apply patches/upgrades appropriately as per recommendations defined • Determine the timelines for closing the vulnerabilities at earliest • Take approvals in case of exceptions or delays in actions.
20	Application Security Testing Closure Rate	% of applications patched within 30 days post security testing	Percentage of applications patched within lead time of 30 days post security testing	[(No. of applications that are patched within lead time of 30 days) / (Total No. of applications tested)] *100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the number and reason for current Bank applications that still have open or pending status of vulnerabilities after 30 days of testing and apply patches/upgrades appropriately as per recommendations defined. • Determine the timelines for closing the vulnerabilities at earliest • Take approvals in case of exceptions or delays in actions.
21	Exception Tracking (for exclusion from vulnerability remediation)	Open Exceptions	Overdue / delay exceptions	1-2 (IP addresses) exceptions = Green 3-5 (IP addresses) exceptions = Amber >5 (IP addresses) exceptions = Red	up to 2	3 to 5	over 5	Quarterly	IT Department and Audit Department	• Identify the number and reason for exceptions approved • Analyse to assess if alternative solution/ control can be deployed and implement the same with due approvals.
VAPT										
22	Discovery Scan vs Inventory Accuracy	Total number of IP address in the environment	IP addresses that were not scanned or not part of inventory list	(No. of IP addresses found in Discovery Scan/Total number of IP addresses in Inventory List)*100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify and add the new IP's discovered in automated scanning and define the asset type and classification • Follow bank's Asset Management Procedure and template for new additions.

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
23	External VA (Coverage)	Total number of IP address in the environment	IP addresses that were not scanned	(Total number of IP addresses Scanned/Total number of IP addresses in environment)*100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the number and reason for IP addresses not covered in Vulnerability assessment and resolve issues accordingly. • Define the new time frame External VA of new IPs. • Take approvals in case of any exceptions or delayed actions
24	External PT (Coverage)	Total number of IP address in the environment	IP addresses that were not scanned	(Total number of IP addresses Scanned/Total number of IP addresses in environment)*100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the number and reason for IP addresses not covered in Penetration Testing and resolve issues accordingly. • Define the new time frame External PT of new IPs. • Take approvals in case of any exceptions or delayed actions
25	External VA Compliance- Observation Closure (Applications/Servers/Devices/Security Solution)	All observations (from devices/servers/applications/solutions) in scope for external VA	Observations that were not fixed during the last External VA exercise	(Total Vulnerabilities closed within the timeline/Total Vulnerabilities identified in the external VA exercise)*100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the number and reason for current applications, servers, network devices and endpoints that have current open observations from last VA • Define timeline and remediation for open observations. • Take approvals in case of exceptions or delayed actions.
26	External PT Compliance- Observation Closure (Applications/Servers/Devices/Security Solution)	All observations (from devices/servers/applications/solutions) in scope for external PT	Observations that were not fixed during the last External PT exercise	(Total Vulnerabilities closed within the timeline/Total Vulnerabilities identified in the external PT exercise)*100	>=99%	>=95%	<95%	Quarterly	IT Department and Audit Department	• Identify the number and reason for current applications, servers, network devices and endpoints that have current open observations from last PT • Define timeline and remediation for open observations. • Take approvals in case of exceptions or delayed actions.
27	Non-production (Test or Development) infra/application exposed on internet	No test or development infra or application instances is exposed on internet	Non-prod instance exposed on internet	1-2 non-prod IP addresses = Green 3-5 non-prod IP addresses = Amber >5 non-prod IP addresses = Red	up to 2	3 to 5	over 5	Quarterly	IT Department and Audit Department	• Identify the number and reason for current applications, servers, network devices and endpoints that are internet facing and apply proper security controls for their protection • Take approvals in case of exceptions or delayed actions.
Security Operations										
Firewall										
28	Firewall Rulebase Review	Total number of firewalls in the environment	Firewalls that are not in-scope for rulebase review	(Total number of firewall rulebase review performed/Total number of firewalls in environment)*100	>=99%	>=95%	<95%	Half yearly	IT Department	• Identify the number and reason for Firewalls not covered in Rule base Review • Take approvals in case of exceptions or delayed actions.
29	Firewall Rulebase Defects Remediation	Total number of firewalls rulebase where defects are identified	Firewalls where rulebase defect are still not remediated	(Total number of firewall rulebase where all defects are remediated/Total number of firewalls where defects are identified in rulebase)*100	>=99%	>=95%	<95%	Half yearly	IT Department	• Identify the number and reason for non remediated rulebase defects. '•Define resolution and time frame for closure. • Take approvals in case of exceptions or delayed actions.
30	Personal Firewall (Endpoints)	Total number of Endpoints in the environment	Number of endpoints where personal firewall is not enabled on malware protection software or at OS level	(Number of endpoints where personal firewall is enabled/Total number of endpoints in environment) *100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the number and reason for endpoints where personal firewall has not been enabled and resolve issues accordingly
31	Network Firewall (Coverage)	Total number of network segments in the environment	Number of network segments not protected with firewall	(Number of perimeter and internal network segments protected with firewalls/ Total Number of network segments) *100	>=99%	>=95%	<95%	Quarterly	IT Department	• Identify the number and reason for network segments covered under firewall and integrate accordingly. • Take approvals in case of exceptions or delayed actions.
32	Network Firewall (Zoning)	No access between firewall zones (UAT/Dev/ Prod)	Any access allowed between firewall zones	0 access allowed/No access allowed = Green 1-5 (IP address) full access allowed on a firewall = Amber >5 (IP address) full access allowed on a firewall = Red	0	1 to 5	over 5	Quarterly	IT Department	• Identify the number and reason for rules that allow access between firewall zones and optimize the allowed access accordingly specific to Bank's network requirement. • Take approvals in case of exceptions or delayed actions.
33	Firewall Rules - Non Secure Ports/Service (To be tracked once Firewall Rule exercise by InfoSec is over)	No non-secure port on firewalls to be opened without any business justification	Opening of non-secure port or service on firewalls	0 non-secure port /No non-secure port opened = Green 1-5 non-secure ports/service opened on a firewall = Amber >5 non-secure ports/service opened on a firewall = Red	0	1 to 5	over 5	Quarterly	IT Department	• Identify the number and reason for non secure ports opened and close the non required ports accordingly. • Take approvals in case of exceptions or delayed actions.

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
34	Firewall Rules - 'Any - Any' rule (To be tracked once Firewall Rule Review exercise is over) (Exception rules are tracked separately)	No 'Any' rule in source or destination IPor destination ports/services shall be opened	Rules allowing 'Any' in source IP or in destination IP or in destination ports in all the firewalls	0 'Any' rule on firewalls = Green 1-5 'Any' rule on firewalls = Amber >5 'Any' rule on firewalls = Red	0	1 to 5	over 5	Quarterly	IT Department	• Identify the number and reason for 'Any Any' Firewalls rules allowed in Rule base. • Optimize the firewall rule base and allow only particular subnet or IP addresses in case of allowing any any source, destination or service. • Take approvals in case of exceptions or delayed actions.
35	Firewall Rules Exception/Change Request (allowing non-secure ports/service or allowing 'Any' in source or destination for business need with change approval process for specific IP addresses only not on IP range)	No exceptional firewall rule created to allow unsecure ports/services or 'Any' rule in source or destination IP or services	Any exceptional firewall rule created	1-2 firewall rules change/exceptions = Green 3-5 firewall rules change/exceptions = Amber >5 firewall rules change/exceptions = Red	up to 2	3 to 5	over 5	Quarterly	IT Department	• Define the timeline for the exception period of allowing non-secure ports/service or allowing 'Any' in source or destination for business need with change approval process for specific IP addresses only not on IP range. • Document approval in duly filled Exception Management Template defined for Bank in case of exceptions and take necessary approvals.
Anti-virus and Anti-Malware										
36	Antivirus Compliance Monitoring-Endpoints	Total number of Endpoints in the environment	Endpoints on which antivirus is not getting updated properly (Current AV engine and signature files 2 Days Older(n-2))	(Total number of endpoint compliant (n-2)/Total number of Endpoints)*100	>=99%	>=95%	<95%	Quarterly	IT Department	• Identify the endpoint systems that are not compliant on Symantec AV and resolve the issues accordingly. • Take approvals in case of exceptions or delayed actions.
37	Antivirus Compliance monitoring - Servers	Total number of Wintel and Linux servers in the environment	Servers on which antivirus is not updated properly (Current AV engine and signature files 2 Days Older (n-2))	(Total number of Server compliant (n-2))/Total number of Servers)*100	>=99%	>=95%	<95%	Quarterly	IT Department	• Identify the servers that are not compliant on Symantec AV and resolve the issues accordingly. • Take approvals in case of exceptions or delayed actions.
38	Malware Detected and Auto-Cleaned (Endpoints)	Total number of malware detected and automatically cleaned/quarantined on endpoints	Number of malware detected but not automatically cleaned/quarantined by AV software	(Number of malware detected and cleaned or quarantined automatically on endpoints / Total number of malware detected on endpoints)*100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the number and reason for endpoint systems where auto clean action could not be completed and resolve issues accordingly • Take approvals in case of exceptions or delayed actions.
39	Malware Detected and Auto-Cleaned (Servers)	Total number of malware detected and automatically cleaned/quarantined on Servers	Number of malware detected but not automatically cleaned/quarantined by AV software	(Number of malware detected and cleaned or quarantined automatically on Servers / Total number of malware detected on servers)*100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the number and reason for servers where auto clean action could not be completed and resolve issues accordingly • Take approvals in case of exceptions or delayed actions.
40	Malware detected but not auto-cleaned by AV software (Endpoints)	All malware attacks successfully detected and cleaned automatically by AV software	Number of malware attacks that AV software not able to clean automatically	0 or All malware detected are auto-cleaned = Green 1-5 malware attack not auto-cleaned = Amber >5 malware attacks not auto-cleaned = Red	0	1 to 5	over 5	Monthly	IT Department	• Identify the number and reason for endpoints where auto clean action could not be completed and resolve issues accordingly • Take approvals in case of exceptions or delayed actions.
41	Malware detected but not auto-cleaned by AV software (Servers)	All malware attacks successfully detected and cleaned automatically by AV software	Number of malware attacks that AV software not able to clean automatically	0 or All malware detected are auto-cleaned = Green 1-5 malware attack not auto-cleaned = Amber >5 malware attacks not auto-cleaned = Red	0	1 to 5	over 5	Monthly	IT Department	• Identify the number and reason for servers where auto clean action could not be completed and resolve issues accordingly • Take approvals in case of exceptions or delayed actions.
42	Scheduled AV scan (Endpoints)	Total number of Endpoints for scheduled weekly scan	Number of Endpoints where scheduled weekly scans were not completed successfully	(Number of endpoints where scheduled scan were completed successfully / Total number endpoints for scheduled weekly scan)*100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the number and reason for endpoint systems where automated scheduled scan action could not be completed and resolve issues accordingly • Take approvals in case of exceptions or delayed actions
43	Scheduled AV scan (Servers)	Total number of Servers for scheduled weekly scan	Number of Servers where scheduled weekly scans were not completed successfully	(Number of servers where scheduled scan were completed successfully / Total number servers for scheduled weekly scan) *100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the number and reason for servers where automated scheduled scan action could not be completed and resolve issues accordingly • Take approvals in case of exceptions or delayed actions
44	Full Disk Encryption - Endpoints	Total number of Endpoints in the environment	Endpoints on which AV Full Disk Encryption agent is not installed or working properly	(Total number of endpoint compliant /Total number of Endpoint)*100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the number and reason for endpoint systems where AV Full Disk Encryption agent is not installed or working properly and resolve the issues accordingly. • Take approvals in case of exceptions or delayed actions.

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
DLP, WAF, SIEM and others										
45	DLP	Average time taken to escalate the incidents	Average time taken to escalate the incidents	[Sum of (Difference in time between incident Escalation Date and incident Trigger date) / (Total No. of incidents escalated)]	Less than 24hrs	>=24hrs to <36hrs	>=36hrs	Monthly	IT Department	• Identify the reason and apply control measures for time taken greater than 24hrs and optimize the process accordingly to reduce the number of hours .
46	DLP	% closure of incidents within 15 days	Percentage closure of incidents	[(No. of incidents closed within 15 working days)/ (Total no. of incidents reported)]*100	>=98%	>=95%	<95%	Monthly	IT Department	Identify the reason and apply control measures for time taken greater than 15 days to close the incidents and optimize the process accordingly to reduce the number of • days .
47	DLP	% false positive reduction	Percentage reduction in False positive	[Percentage of false positives identified in previous month- Percentage of false positives identified in current month)/ (Percentage. of false positive in the previous month)]*100	>=25%	>=15%	<15%	Monthly	IT Department	• Identify the number and reason for false positive incidents reported and configure the DLP system accordingly. • Take approvals in case of exceptions or delayed actions.
48	DLP	% of new policies introduced	Percentage of new policy introduced	[(No. of new policies introduced in this quarter)/(Total no. of policies in the system)]*100	>10%	>=5%	<5%	Quarterly	IT Department	Identify the number and reason for less policies introduced and optimize the policies accordingly incase the the percentage is less than 10 percent
49	DLP	System availability during the month	Percentage of hours DLP is available	[(System uptime in hours) /(Total hours in the month)]/ *100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the number and reason for unavailability of the DLP system in the month and identify the root cause to maintain the its availability • Take approvals in case of exceptions or delayed actions.
50	DLP	% of DLP agent installation on devices	Percentage of DLP agents installed on devices	[(No. of devices having DLP agents installed)/ (Total no. of devices onboarded in the system)] *100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the number and reason for systems where DLP agents are not installed and resolve issues accordingly . • Take approvals in case of exceptions or delayed actions.
51	DLP	% of DLP agent Reporting	Percentage of DLP agents reporting	[(No. of DLP agents reporting)/ (Total no. of machines in NHB environment)]*100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the number and reason for systems where DLP agents are not reporting and resolve issues accordingly. • Take approvals in case of exceptions or delayed actions with assistance from IS Department
52	Asset Inventory - Endpoints	Total number of Endpoints in the environment	Endpoints not appropriate with the inventory	(Total number of endpoint compliant /Total number of Endpoint) *100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the total endpoints that were not compliant with asset management template or with inappropriate asset information • Take necessary steps to identify the complete information on endpoint and follow Bank's Asset Management procedure
53	Asset Inventory - Servers	Total number of Servers in the environment	Serversnot appropriate with the inventory	(Total number of servers compliant with Asset agent/Total number of Servers) *100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the total servers that were not compliant with asset management template or with inappropriate asset information • Take necessary steps to identify the complete information on endpoint and follow Bank's Asset Management procedure
54	NAC Compliance	All endpoints subjected to a solution equivalent to 'NAC' to establish trusted network connection	Number of Endpoints that are not subjected to NAC before providing network connectivity	(Total number of endpoint compliant with NAC Agent/Total number of Endpoint)*100	>=99%	>=95%	<95%	Monthly	IT Department	Identify the number and reason for endpoints not subjected to NAC and resolve the specific issues accordingly.Take approvals in case of exceptions or delayed actions.
55	WAF - Application Onboarding	Total number of Web Applications in environment	Web Applications not integrated with WAF	(Total number of Applications compliant with WAF integration/Total number of Application)*100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the number and reason for endpoints not subjected to NAC and resolve the specific issues accordingly. • Take approvals in case of exceptions or delayed actions.
56	WAF - Prevention Mode	Total number of WAF appliances in the environment	WAF not configured to prevent malicious traffic or drop such packets	(Total number of WAF appliances configured in inline prevention mode/Total number of WAF appliances) *100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the number and reason for Bank applications not integrated with WAF prevention mode. • Resolve the specific issues and take approvals in case of exceptions or delayed actions.

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
57	WAF - Signatures Update	Total number of WAF appliances in the environment	WAF is not updated properly with latest signatures or customized signatures	(Total number of WAF appliance compliant with latest signatures (n-1)/Total number of WAF appliances) *100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the number and reason for WAF application/appliance not updated with latest signatures. • Download and upgrade the signatures • Resolve the specific issues and take approvals in case of exceptions or delayed actions
58	Network IPS (Prevention Mode)	Total number of NIPS in the environment	NIPS not configured to prevent malicious traffic or drop such packets	(Total number of NIPS configured in inline prevention mode/Total number of NIPS appliances) *100	>=99%	>=95%	<95%	Monthly	SOC	• Identify the number and reason for Bank's NIPS devices configured in Prevention mode. •Resolve the specific issues and take approvals in case of exceptions or delayed actions
59	Network IPS (Signature Update)	Total number of NIPS in the environment	NIPS is not updated properly with latest signatures or customized signatures	(Total number of NIPS compliant with latest signatures released by OEM (n-1)/Total number of NIPS appliances)*100	>=99%	>=95%	<95%	Monthly	SOC	• Identify the number and reason for Bank's NIPS devices not configured with latest signaures. • Resolve the specific issues with help of OEM guide and • take approvals in case of exceptions or delayed actions
60	Network Devices utilization (CPU, Memory, backplane, port throughput) - Spike/Peak		Number of times utilization for network devices has breached the utilization threshold of 70% for at least 5 minutes at a streach	1-2 times utilization spike on a device =Green 3-5 times utilization spike on a device = Amber >5 times utilization spike on a device =	1 to 2	3 to 5	over 5	Monthly	SOC	• Identify the number and reason for Bank's devices 70 % or more memory utilization and optimize the resources for efficient use. • Resolve the specific issues with help of OEM guide and take approvals in case of exceptions or delayed actions.
61	Network Devices utilization (CPU, Memory, backplane, port throughput) - Average/Consistent	No utilization (CPU, Memory, backplane, port throughput) for all network devices has breached the averaged threshold for 5 minutes	Number of times utilization for network devices has breached the threshold of 30% for at least 5 minutes at a streach	1-2 times utilization has breached on a device =Green 3-5 times utilization has breached on a device = Amber >5 times utilization has breached on a	1 to 2	3 to 5	over 5	Monthly	SOC	• Identify the number and reason for Bank's devices 30 % or more memory utilization and optimize the resources for efficient use. • Resolve the specific issues with help of OEM guide and take approvals in case of exceptions or delayed actions.
62	SOC/SIEM Integration-Servers	Total number of Servers in the environment	Number of servers not integrated with SIEM/SOC	(Total number of Servers compliant with SOC integration/Total number of Servers)*100	>=99%	>=95%	<95%	Monthly	SOC	• Identify the number and reason for Bank's servers that are not integrated. • Check for vendor guides for SIEM integration and apply configuration changes • Resolve the specific issues with help of OEM guide and take approvals in case of exceptions or delayed actions.
63	SOC/SIEM Integration-Network Devices	Total number of network devices in the environment	Number of network devices not integrated with SIEM/SOC	(Total number of Network Devices compliant with SOC integration/Total number of Network Devices) *100	>=99%	>=95%	<95%	Monthly	SOC	• Identify the number and reason for Network Devices that are not integrated. • Check for vendor guides for SIEM integration and apply configuration changes
64	SOC/SIEM Integration-Security Applications/Solutions/Tools	Total number of Security Solutions (IDAM,PIM, AV, Firewall, IPS, WAF, Proxy, VPN, DLP, NAC, TACACS, etc.) / devices in the environment	Number of Security Solution/ Devices not integrated with SIEM/SOC	[Total number of Security Solutions or Devices compliant with SOC integration /Total number of Security Solutions or Devices]*100	>=99%	>=95%	<95%	Monthly	SOC	• Identify the number and reason for Security solutions that are not integrated. • Check for vendor guides for SIEM integration and apply configuration changes • Resolve the specific issues with help of OEM guide and take approvals in case of exceptions or delayed actions.
65	SOC/SIEM Integration-Applications	Total number of IT applications in the environment	Number of applications not integrated with SIEM/SOC	[Total number of Applications compliant with SOC integration/Total number of Applications]*100	>=99%	>=95%	<95%	Monthly	SOC	• Identify the number and reason for Bank applications that are not integrated. • Check for vendor guides for SIEM integration and apply configuration changes • Resolve the specific issues with help of OEM guide and take approvals in case of exceptions or delayed actions.
66	SOC/SIEM Integration-Databases	Total number of databases in the environment	Number of databases not integrated with SIEM/SOC	[Total number of databases compliant with SOC integration/Total number of Databases in scope]*100	>=99%	>=95%	<95%	Monthly	SOC	• Identify the number and reason for Bank databases that are not integrated. • Check for vendor guides for SIEM integration and apply configuration changes • Resolve the specific issues with help of OEM guide and take approvals in case of exceptions or delayed actions.
67	SOC	% of critical threats patched on devices	Percentage of critical threats patched on devices	[(No. of critical threats patched on devices) / (No. of critical threats identified that are applicable to NHB environment)] *100	>=99%	>=95%	<95%	Monthly	SOC	• Identify the number and reason for non-patched critical threats and apply patches/upgrades appropriately as per NHB Patch Management Procedure • Take approvals in case of exceptions of non-remediated vulnerabilities or delayed actions

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
68	SOC	% of higher priority incidents (P1 and P2) closed within 2 hrs	Percentage of higher priority (P1 and P2) incidentsclosed within 2hrs	[(No. of higher priority(P1 and P2) incidents tickets closed with in 2 hours / Total No. of higher priority incidents tickets raised)] * 100	>=95%	>=90%	<90%	Monthly	SOC	• Identify the number of High Priority SOC incidents (S1 and S2) that were not closed within 2 hours. • Identify the chronology and root cause and apply effective controls to reduce the high percentage of such incidents..
69	SOC	% of P1, P2 priority incidents responded within 15 mins	Percentage of P1, P2 priority incidents responded towithin 15 min	[(No. of P1,P2 priority incidents responded within 15 mins) / (Total no. of P1,P2 priority incidents identified)]*100	>=95%	>=90%	<90%	Monthly	SOC	• Identify the number of High Priority SOC incidents (S1 and S2) that were not responded within 15 minutes. • Identify the chronology and root cause and apply effective controls to reduce the high percentage of such incidents
70	SOC	% of implementation of new use cases	Percentage of new use cases implemented	[(Total no. of new use cases implemented in the current month / Total no. of use cases implemented)] *100	>10%	>=5%	<5%	Quarterly	SOC	• Identify the number and reason for non-application of use cases in SOC. • Prepare and identify the appropriate use cases for bank's SOC and do necessary changes in assistance with IT and IS • Department.
71	Privilege Identity Management - Onboarding Compliance	Total Asset onboarding compliance score	Number of Servers, Network devices, applications and databases that are not integrated with PIM	[Total number of Servers, Devices, Databases, Applications compliant with PIM integrations/Total number of Servers, Devices, Databases, Applications in scope for PIM integration]*100	>=99%	>=95%	<95%	Monthly	SOC	• Identify the reason and number of Servers, Network devices, applications and databases that are not integrated with PIM • Identify the root causes and take appropriate steps for the integration. • Take approvals in case of exceptions or delayed actions.
72	Privilege Identity Management - Bypassing PIM authentication	Total number of times servers were accessed via PIM	Number of times servers were accessed bypassing PIM	[Total number of times servers are accessed via PIM/ Total number of times servers are accessed]*100	>=99%	>=95%	<95%	Monthly	SOC	• Identify the Number of times servers were accessed bypassing PIM. • Reduce the number of accesses by applying necessary access controls. • Take approvals in case of exceptions or delayed actions.
73	Privilege Identity Management - Service Tickets	Total number of Service tickets (S1/S2/S3) that were opened/logged and closed within SLA during the period	Number of service tickets that were not timely processed or closed	[Total number of service requests processed and closed within SLA/ Total number of service requests raised for PIM during the period]*100	>=99%	>=95%	<95%	Monthly	SOC	• Identify the number of Service Tickets (S1 ,S2 and S3) that were not responded or closed within defined time. • Identify the chronology and root cause and apply effective controls to reduce the high percentage of such incidents.
74	Privilege Identity Management	% of service id in use	Percentage of Service IDs in use	{(No. of Service ID in use)/(No. of service IDs configured in PIM)}*100)	>=95%	>=90%	<90%	Monthly	SOC	• Identify the number and reason for Privileged ID that are configured and not in use. • Remove such ID's and maintain proper records for such ID's.
75	Privilege Identity Management	% of service request and change request processed within Defined SLA (SLA not Defined yet)	Percentage of Service request and change request processed within 24 hrs	[(No. of SR/CR processed within 24 hrs)/(No. of CR/SR raised for PIM)]*100	>=95%	>=90%	<90%	Monthly	SOC	• Identify the number of Service requests and change requests for Privilege Id's that were not responded or closed within defined time. • Identify the chronology and root cause and apply effective controls to reduce the high percentage of such requests.
76	Privilege Identity Management	% of Active User account	Percentage of Active User Account	([(No. of Active user account)/(No. of user account configured in PIM)]*100)	>=95%	>=90%	<90%	Monthly	SOC	• Identify the number and reason for Privileged ID that are configured and not in use . •Remove such ID's and maintain proper records for such ID's.
77	IDAM - Service Tickets	Total number of Service tickets (S1/S2/S3) that were opened/logged and closed within SLA during the period	Number of service tickets that were not timely processed or closed	[Total number of service requests processed and closed within SLA/ Total number of service requests raised for IDAM during the period]*100	>=99%	>=95%	<95%	Monthly	SOC	• Identify the number of IDAM Service Tickets (S1 and S2) that were not responded or closed within defined time. • Identify the chronology and root cause and apply effective controls to reduce the high percentage of such incidents..
Incident Management										
78	All Suspected data leakage events closure rate - DLP	Total events identified in the month from DLP log review	Overdue/ Delayed events identified from DLP	(Total number of DLP Events or Incidents closed within timeline/Total number of DLP Events or Incident Reported)*100	>=99%	>=95%	<95%	Monthly	CISO Office/ SOC	• Identify the number of DLP incidents that were not responded or closed within defined time. • Identify the chronology and root cause and apply effective controls to reduce the high percentage of such incidents. • Take approvals in case of exceptions or delayed actions.
79	All Suspected data leakage events detection and response rate - DLP Timeline - within 24 hours	Total events identified in the month from DLP log review	Overdue/ Delayed events identified from DLP	(Total number of DLP Events or Incidents detected and responded within timeline/Total number of DLP Events or Incident Reported)*100	>=99%	>=95%	<95%	Monthly	CISO Office/ SOC	• Identify the number of DLP incidents that were not responded or closed within defined time of 24 hours. • Identify the chronology and root cause and apply effective controls to reduce the high percentage of such incidents. • Take approvals in case of exceptions or delayed actions.

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
80	Cyber Security (SOC) Incident Detection Rate	Total security events/incidents identified or reported in the month (e.g. Malware infections, Phishing compromises, sensitive data breach, etc.)	Overdue/ Delayed security events or incidents	(Total number of Cybersecurity events or incidents detected and responded within SLA/Total number of Cyber events or Incident Occurred)*100	>=99%	>=95%	<95%	Monthly	CISO Office/ SOC	• Identify the number of Cyber SOC incidents that were not detected and responded within defined time • Identify the chronology and root cause and apply effective controls to reduce the high percentage of such incidents. • Take approvals in case of exceptions or delayed actions.
81	Cyber Security (SOC) Incident ClosureRate	Total security events/incidents identified or reported and successfully closed in the month (e.g. Malware infections, Phishing compromises, sensitive data breach, etc.)	Overdue/ Delayed security events or incidents	(Total number of Cybersecurity events or incidents closed within SLA/Total number of Cyber events or Incident Occurred)*100	>=99%	>=95%	<95%	Monthly	CISO Office/ SOC	• Identify the number of Cyber SOC incidents that were not closed within defined time. • Identify the chronology and root cause and apply effective controls to reduce the high percentage of such incidents. • Take approvals in case of exceptions or delayed actions.
82	Cyber Incident Reporting to RBI (within timeline)	Number of security incidents occurred/reported in a Month (e.g. Phishing/Sensitive Data Breach/Financial Loss occurred due to Security Incident etc.)	Number of security incidents (e.g. Phishing/Sensitive Data Breach/Financial Loss occurred due to Security Incident etc.) not timely reported in the Month	(Total number of Incidents reported to RBI within defined timeline/Total number of Incident Identified during the month)*100	100%	>=98%	<98%	Monthly	CISO Office/ SOC	• Identify the number of Cyber SOC incidents that were not reported to RBI within defined time • Identify the chronology and root cause and apply effective controls to reduce the high percentage of such incidents. • Take approvals in case of exceptions or delayed actions.
83	Cyber Incident Reporting to RBI (all incidents as mandated by RBI)	Number of security incidents occurred/reported in a Month (e.g. Phishing/Sensitive Data Breach/Financial Loss occurred due to Security Incident etc.)	Number of security incidents (e.g. Phishing/Sensitive Data Breach/Financial Loss occurred due to Security Incident etc.) not reported in the Month	(Total number of Incidents reported to RBI and CERT-IN/Total number of Incident Identified during the month)*100	100%	>=98%	<98%	Monthly	CISO Office/ SOC	• Identify all the number of Cyber SOC incidents that were not reported to RBI and CERT-In within defined time • Identify the chronology and root cause and apply effective controls to reduce the high percentage of such incidents. • Take approvals in case of exceptions or delayed actions.
84	Darknet Security Incidents	Number of darknet security incidents occurred/reported in a month	Number of darknet security incidents not timely actioned upon in the month	(Total number of darkent Incidents timely actioned upon/Total number of darknet incidents reported in the	>=99%	>=95%	<95%	Monthly	CISO Office/ SOC	• Identify the number of Darknet incidents that were not detected and responded within defined time. • Identify the root cause and apply effective controls to
85	Internet facing applications security incidents reported by external parties/partners	Number of malware detection/security incidents on internet facing web applications occurred/reported in a month by external parties	Number of malware detection/security incidents on internet facing web applications not timely actioned upon in the month	(Total number of malware detection/security incidents on internet facing web applications timely actioned upon/Total number of internet facing web application security incidents reported in the month)*100	>=99%	>=95%	<95%	Monthly	CISO Office/ SOC	• Identify the number of Internet facing application incidents that were not closed within defined time. • Identify the chronology and root cause and apply effective controls to reduce the high percentage of such incidents. • Take approvals in case of exceptions or delayed actions.
86	Security Forensics Investigation Incidents	All Forensic Investigation incidents are closed	Number of forensic investigation incidents not timely actioned upon in the month/Delayed	(Total number of forensic investigation Incidents timely actioned upon/Total number of forensic investigation incidents reported in the month)*100	>=99%	>=95%	<95%	Monthly	CISO Office/ SOC	• Identify the number of security forensic investigation incidents that were not closed within defined time. • Identify the chronology and root cause and apply effective controls to reduce the high percentage of such incidents. • Take approvals in case of exceptions or delayed actions.
87	IT asset stolen or lost related incidents	No IT assets/laptops stolen or lost reported in a month	Number of IT assets/laptops stolen or lost reported in a month	0 asset or No asset lost = Green 1-5 assets lost/stolen reported = Amber >5 assets lost/stolen reported = Red	0	1 to 5	over 5	Monthly	IT Department/CISO Office/ SOC	• Identify the number and reason for stolen or lost IT assets. • Take appropriate actions for reporting of lost assets with the assistance of IT Head.
88	System Uptime - DLP	System availability during the month	Unavailability of DLP in hours during the month	System uptime in hours/ Total hours in month*100	>=99%	>=95%	<95%	Monthly	IT Department/CISO Office/ SOC	• Identify the number and reason for unavailability of the DLP system in the month and identify the root cause to maintain the its availability • Take approvals in case of any config changes or exceptions required.
89	System Uptime - SIEM	System availability during the month	Unavailability of SIEM in hours during the month	System uptime in hours/ Total hours in month*100	>=99%	>=95%	<95%	Monthly	IT Department/CISO Office/ SOC	• Identify the number and reason for unavailability of the SIEM system in the month and identify the root cause to maintain the its availability • Take approvals in case of any config changes or exceptions required.
90	True vs False positive detections - DLP (in %age)	Total number of False Positive alerts triggered on the tool vs true positive detections	Alerts triggered on tool which create noise in a month	False Positive is less than 50% of True Positive = Green False Positive is between 51% to 90% of True Positive = Amber False Positive is over 91% of True Positive = Red	<=50%	51%<91%	>91%	Monthly	IT Department/CISO Office/ SOC	• Identify the number and reason for false positive incidents reported and configure the DLP system accordingly. • Take approvals in case of exceptions or delayed actions.

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
91	True vs False positive detections - SIEM (in %age)	Total number of False Positive alerts triggered on the tool vs true positive detections	Alerts triggered on tool which create noise in a month	False Positive is less than 50% of True Positive = Green False Positive is between 51% to 90% of True Positive = Amber False Positive is over 91% of True Positive = Red	<=50%	51%<91%	>91%	Monthly	CISO Office/ SOC	• Identify the number and reason for false positive incidents reported and configure the SIEM system accordingly for optimized performance and reduced false positives • Take approvals in case of exceptions or delayed actions.
92	Logs Monitoring on SIEM (in terms of number of logging cyclefor integrated devices)	Devices/Systems sending logs as per cycle to SIEM	Loss of logs /Log stoppage during 5 cycles	Log stoppage upto 30 cycles = Green Log stoppage between 31 to 60 cycles = Amber Log stoppage over 61 cycles = Red	<=30	31<61	>61	Monthly	CISO Office/ SOC	• Identify the systems with log stoppage above 30 cycles. • Identify the root cause and take approvals in case of exceptions or delayed actions.
InfoSec BAU Activities										
93	Role Based Access Review - User Access Certification Activity for all Business Functions/IT Systems in scope	All user access present on applications within scope of Role Based Access Review	Unauthorized/ Redundant/ Old access on applications within scope of Role Based Access Review	=Total number of Accesses certified / Total number of Accesses in scope for review*100	>=99%	>=95%	<95%	Half yearly	IT Department	• Identify the reason and number of user accesses on applications not timely reviewed and certified. • Identify the root cause and delete all unauthorized accesses immediately. • Maintain and review the access record periodically.
94	Role Based Access Review - Applications in scope	All applications within scope of Role Based Access Review	Number of applications not timely reviewed and certified	=Total number of applications timely reviewed and certified / Total number of applications in scope for review*100	>=99%	>=95%	<95%	Half yearly	IT Department	• Identify the reason and number of Number of applications not timely reviewed and certified. • Identify the root cause and delete all unauthorized accesses immediately.
95	Role Based Access Review - Access Revocation	All access to be revoked from in-scope applications as part of Role Based Access Review	Number of access not timely revoked after review and certification	=Total number of access timely revoked from in-scope applications/ Total number of access privileges identified to be revoked*100	>=99%	>=95%	<95%	Half yearly	IT Department	• Identify the reason and number of access not timely revoked after review and certified • Identify the root cause and delete all unauthorized accesses immediately. • Maintain and review the access record periodically. • Take approvals in case of exceptions or delayed actions.
96	Third Party Risk Assessments - Suppliers assessment conducted (Onsite/Offsite)	All suppliers in scope of assessment	Delayed/ Overdue supplier assessments	=Total number of TPRA timely conducted / Total number of vendors in scope for assessment*100	>=99%	>=95%	<95%	Monthly	Audit Department	• Identify the number and reason for third party Delayed/ Overdue supplier assessments. • Take appropriate steps and measures for conducting risks assessments of all third-party suppliers. • Take approvals in case of exceptions or delayed actions.
97	Third Party Risk Assessments - Suppliers assessment extended (Onsite/Offsite)	All suppliers in scope of assessment	Delayed/ Overdue supplier assessments	0 assessment extended/all assessments were timely completed= Green 1-5 assessments extended = Amber >5 assessments extended = Red	0	1 to 5	over 5	Monthly	Audit Department	• Identify the number and reason for third party Delayed/ Overdue supplier assessments. • Enforce mandatory controls and measure as per Bank's Cyber Sec policy • Take appropriate steps and measures for conducting risks assessments of all third party suppliers. • Take approvals in case of exceptions or delayed actions.
98	Third Party Risk Assessments- Finding Closure	All findings due for closure from suppliers in scope	Delayed/ Overdue finding closure from supplier assessments	=Total number of TPRA Observation closed within Timeframe / Total number of observations identified*100	>=99%	>=95%	<95%	Monthly	Audit Department	• Identify the number and reason for non-closure of TPRA observations that were not closed within defined time. • Take approvals in case of exceptions or delayed actions.
99	Third Party Risk Assessments - New Risks of existing supplier	All suppliers in scope of assessment	Any new risks identified in assessment of an existing supplier	0 new risk or No new risk identified = Green 1-5 new risks identified = Amber >5 new risks identified = Red	0	1 to 5	over 5	Monthly	Audit Department	• Identify the number and reason for detection of new risks of existing supplier. • Enforce mandatory controls and measure as per Bank's Cyber Sec policy. • Take approvals in case of exceptions or delayed actions.
100	Third Party Risk Assessments - Risk Extension	All findings due from suppliers in scope	Number of risks getting extended during the period	0 risk extended= Green 1-5 risks extended = Amber >5 risks extended = Red	0	1 to 5	over 5	Monthly	Audit Department	• Identify the number and reason for risk extension of third-party supplier. • Enforce mandatory controls and measure as per Bank's Cyber Sec policy . • Take approvals in case of exceptions or delayed actions.

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
101	Third Party Risk Assessments - RFI/RFP/Contracts Reviewed	All RFI/RFP/Vendor Contracts to bereviewed	Delay in reviewing RFI/RFP/Vendor Contracts	=Total number of RFI, RFP, Vendor contracts timely reviewed within the period / Total number of RFI, RFP, Vendor contracts to be reviewed within the period*100	>=99%	>=95%	<95%	Monthly	Audit Department	• Identify the number and reason for delayed RFI/RFP/Contracts review. • Enforce mandatory controls and measure as per Bank's Cyber Sec policy. • Take approvals in case of exceptions or delayed actions.
102	Security Risks identified during the month	No security risks identified last month	Any security risk identified last month	Only count of risks with severity level needs to be provided				Monthly	CISO Office/ SOC	•
103	Security Risks remediated during the month	Total number of risks closed or remediated last month	Risks not closed within defined timeline	=Total number of Risk closed within last month / Total number of risks tobe closed last month identified*100	>=99%	>=95%	<95%	Monthly	CISO Office/ SOC	• Identify the number and security risks that were not closed. • Identify the factors for non closure and take approvals in case of exceptions or delayed actions.
104	Secure Configuration Reviews(security solutions, OS, applications, servers and network devices)	All configurations security standards(MBSS) are available	Services/Solutions that do not have configurations security standards(MBSS)	=Total number of configurations security standards(MBSS) that were reviewed within defined timeline/ Total number of configurations security standards(MBSS) to be reviewed*100	>=99%	>=95%	<95%	Annually	CISO Office/ IT Department/SOC	• Identify the number and reason for security configurations(MBSS)not reviewed. • Resolve the issues accordingly • Take approvals in case of exceptions or delayed actions.
105	Policies and Procedure review	All Information and Cyber Security Policies and Procedures	Policies and/or Procedure that missed timely review and update	=Total number of policies and procedure that were reviewed within defined timeline/ Total number of policies and procedures to be reviewed*100	>=99%	>=95%	<95%	Annually	CISO Office	• Identify the number and reason for policies and procedures not reviewed. • Resolve the issues accordingly • Take approvals in case of exceptions or delayed actions.
106	Annual User Awareness - Cyber Security Awareness Training	Total number of employees assigned to undergo security awareness training	Number of employees not undergone the annual refresher training	=Total number of employees successfully completed Awareness Trainings within timeframe / Total number of employees scheduled for awareness training*100	>=99%	>=95%	<95%	Annually	Audit Department/ CISO Office	• Identify the number and reason for Bank employees that did not participate or complete in Cyber security awareness training. • Enforce appropriate controls and resolve the issues accordingly • Take approvals in case of exceptions or delayed actions.
107	Annual User Awareness - Cyber Security Awareness Training - Vendors	Total number of vendor employees assigned to undergo security awareness training	Number of Vendor employees not undergone the annual refresher training	=Total number of successfully completed Awareness Trainings within timeframe / Total number of scheduled for awareness training*100	>=99%	>=95%	<95%	Annually	IT Department/CISO Office	• Identify the number and reason for Vendor users that did not participate or complete in Cyber security awareness training. • Enforce appropriate controls and resolve the issues accordingly • Take approvals in case of exceptions or delayed actions.
108	Phishing simulation tests conducted	Percentage of employees vulnerable (clicked and submitted credentials) to the phishing simulation tests conducted.	Total Number of phishing email send vs number of users clicked and submitted the response/PII data	=Total number of users not felling into Phishing trap (not submitted any PII or sensitive data) / Total number of phishing emails sent*100	>=99%	>=95%	<95%	Half Yearly	IT Department/CISO Office	Identify the number and reason for users that failed in phishing simulation tests . Enforce appropriate controls and traning for failed user and resolve the issues accordingly .Take approvals in case of exceptions or delayed actions.
109	Phishing awareness training conducted	Total number of users assigned to undergo phishing awareness training	Number of users not undergone the phishing awareness training	=Total number of users successfully completed Phishing Awareness Trainings within timeframe / Total number of users scheduled for awareness training*100	>=99%	>=95%	<95%	Half Yearly	IT Department/CISO Office	• Identify the number and reason for users that did not participate in phishing awareness training • Enforce appropriate controls and resolve the issues accordingly. • Take approvals in case of exceptions or delayed actions.
Audit Management										
110	ISMS Audit Review	Total Number of Issues reported in the Audit	Open Issues that are delayed / overdue.	(Total number of audit observations closed within timeline/ Total number of audit issues observed or identified)*100	>=99%	>=95%	<95%	Monthly	Audit Department	• Identify the number and reason for ISMS audit observations that are currently open and Resolve the issues accordingly . • Take approvals in case of exceptions or delayed actions.
111	Internal Audit	Total Number of Issues reported in the Internal Audits for which remediation is in progress.	Open Issues that are delayed / overdue.	(Total number of audit observations closed within timeline/ Total number of audit issues observed or identified)*100	>=99%	>=95%	<95%	Monthly	Audit Department	• Identify the number and reason for audit observations from internal audit that are currently open and Resolve the issues accordingly. • Take approvals in case of exceptions or delayed actions.

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
112	Other External/Regulatory Cyber Security Audits	Total Number of Issues reported in otheraudits / reviews for which remediation isin progress.	Open Issues that are delayed / overdue.	(Total number of audit observations closed within timeline/ Total number of audit issues observed or identified)*100	>=99%	>=95%	<95%	Monthly	Audit Department	• Identify the number and reason for audit observations from external audit that are currently open and Resolve the issues accordingly. • Take approvals in case of exceptions or delayed actions.
113	Audit Observations reported	No audit observations from any auditduring the month	Number of audit observations that were reportedduring the month	0 or no audit observation = Green 1-5 audit observations = Amber >5 audit observations = Red	0	1 to 5	over 5	Monthly	Audit Department	• Identify the number and reason for audit observations that were not reported within defined time line. • Identify and define necessary action items. • Take approvals in case of exceptions or delayed actions.
114	Audit Observations closed	Total number of audit observations to beclosed during last month	Audit observations that are still open	(Total number of audit observations closed within timeline/ Total number of audit issues identified to be closed during last month)*100	>=99%	>=95%	<95%	Monthly	Audit Department	• Identify the number and reason for audit observations that are currently open. • Identify and define necessary action items. • Take approvals in case of exceptions or delayed actions.
115	Audit Observations closure extended	All audit observations closed within timeline	Number of audit observations closure timeline extended	0 or no audit observation extended = Green 1-5 audit observations extended = Amber >5 audit observations extended = Red	0	1 to 5	over 5	Monthly	Audit Department	• Identify the number and reason for audit observations that exceeded defined timeline. • Identify the chronology, root cause and define necessary action items. • Take approvals in case of exceptions or delayed actions.
Change and Exception Management										
116	Change Management- Emergency Changes	No emergency change raised and implemented during the period	Any emergency change raised and implemented during period	0 emergency changes = Green 1-5 emergency changes = Amber >5 emergency changes = Red	0	1 to 5	over 5	Monthly	IT Department	• Identify the number and reason for emergency approved changes. • Enforce the appropriate control measures to avoid emergency changes and follow Banks change management procedure
117	Change Management- Security Changes	Total number of security changes timely reviewed, approved and successfully implemented	Security related changes that were raised but not successfully implemented/executed because of reasons like implementation failure, rollback, delay in approvals on the tool, etc.	(Total number of Security Changes successfully implemented/ Total number of Security Change requests raised in a month)*100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the number and reason for emergency approved changes. • Enforce the appropriate control measures to avoid emergency changes and follow Banks change management procedure
118	Change Management - InfoSec approval	Total number of change requests timely reviewed and approved by InfoSec	Change Requests that were not timely reviewed and approved by InfoSec	(Total number of Change Requests timely reviewed and approved by InfoSec/ Total number of Change Request raised for which InfoSec approval was required) *100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the number and reason for un-timely approved changes • Enforce the appropriate control measures to avoid untimely approval of and follow Banks change management procedure for assistance
119	Change Management - Without InfoSec approval	Total number of change requests executed during the period for which InfoSec approval was mandated	Change Requests that were executed without InfoSec approval (no approval was sought at all)	0 or all change requests executed after getting InfoSec approval = Green 1-5 change requests executed without InfoSec approval = Amber >5 change requests executed without InfoSec approval = Red	0	1 to 5	over 5	Monthly	IT Department	• Identify the number and reason for non-approved changes done and not revoked within defined timeline • Enforce the appropriate control measures to avoid such changes and follow Banks change management procedure for assistance
120	Change Management - Post Facto InfoSec approval	Total number of changes requests executed during the period for which InfoSec approval was mandated but was not taken	Change Requests that were executed without InfoSec approval (but approval was sought post facto after execution)	0 change requests with post facto approval = Green 1-5 change requests with post facto approval = Amber >5 change requests with post facto approval = Red	0	1 to 5	over 5	Monthly	IT Department	• Identify the number and reason for changes done before approval grant and not revoked within defined timeline. • Enforce the appropriate control measures to avoid such changes and follow Banks change management procedure for assistance
121	Change Management - Temporary Changes	Total number of temporary changes that were revoked within defined timeline or after expiry of the period for which change was executed	Number of temporary changes that were not revoked within defined timeline/period for which change was executed	0 temporary change requests to be revoked = Green 1-5 temporary change requests not revoked = Amber >5 temporary change requests not revoked = Red	0	1 to 5	over 5	Monthly	IT Department	• Identify the number and reason for temporary changes not revoked within defined timeline. • Enforce the appropriate control measures to avoid such changes and follow Banks change management procedure for assistance
122	Exception Tracking (for waiver in compliance with any information security policy/control/password related exceptions)	All security policies and controls should be complied with without any exceptions	Number of exceptions granted in a month	0 exception = Green 1-5 exceptions = Amber >5 exceptions = Red	0	1 to 5	over 5	Monthly	IT Department	• Identify the number and reason for exceptions granted and minimize the risks associated with it accordingly. • Document approval in duly filled Exception Management Template defined for Bank in case of exceptions and take necessary approvals.
123	Exception Revocation during the month	All security policies and controls should be complied with without any exceptions	Number of exceptions revoked in a month	(Total number of Exceptions actually revoked last month/ Total number of Exceptions to be revoked last month)*100	>99%	>95%	<95%	Monthly	IT Department	• Identify the number and reason for exceptions still pending and minimize the risks associated with it accordingly by defining timelines of revocation at the earliest.

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
124	Password Policy	All user accounts on AD/systems/network devices/applications/databases followingpassword policy	Number of user accounts on accounts on AD/systems/network devices/ applications/databases not following password policy	(Total number of user accounts in compliance with password policy/ Total number of user accounts on Ad or applications or systems or devices or databases)*100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the number and reason for User accounts where password policy is not followed. Enforce measures as perBank's Password policy.
125	System Accounts with interactive Login enabled	All systems/service accounts with interactive login rights disabled	Number of system/services accounts with interactive login enabled	(Total number of system or services accounts with interactive login disabled/ Total number of system or service accounts)*100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the number and reason for systems where interactive login ID is enabled. • Identify the User ID's that have access and maintain the record incase approved from management. • Define specific timelines for access allowed.
126	Local Admin Rights on Endpoints	No user shall have local administratorrights on the endpoint	Local Administrator rights assigned to a user	(Total number of endpoints where no local administrator rights are given to any user/ Total number of endpoints in the environment)*100	100%	>99%	<99%	Monthly	IT Department	• Identify the number and reason for systems where local user rights is enabled. • Identify the User ID's that have access and maintain the record in case approved from management. • Define specific timelines for access allowed.
127	Removable Media on Endpoints	All removable media drives/ports (CD/DVD/USB) shall be disabled on endpoints	Removable media drives/ports (CD/DVD/USB) are enabled on any endpoints	(Total number of endpoints where removable media ports are disabled on all endpoints/ Total number of endpoints in the environment)*100	>=99%	>=95%	<95%	Monthly	IT Department	• Identify the number and reason for systems where removable media is enabled • Identify the User ID's that have access and maintain the record incase approved from management. • Define specific timelines for access allowed.
Software Governance										
128	Software Governance Metrics - Unauthorized/Freeware/Shareware	All systems to be installed with authorized and approved software	Unauthorized/Unlicensed/Freeware/ Shareware Software installation on systems	[Total number of systems (endpoints/servers) found installed with all authorized licensed software / Total number of systems (endpoints/servers)]*100	>=99%	>=95%	<95%	Monthly	IT Department and SOC	• Identify the number and reason for unauthorized softwares installed. • Get the latest licensed software versions and upgrade accordingly. • Take approvals in case of exceptions or delayed actions.
129	Software Governance Metrics-End of Life/End of Support	Percentage of software system including operating systems for servers, virtual instances, OS for network devices, databases, OS of end points having reached beyond End of Life/End of Support.	No of Licensed and Supported software in production vs Number of software system reached beyond End of Life/End of Support.	[Total number of Software Licenses that are within support from OEM and has not reached EoL or EoS / Total number of Softwares in use]*100	>=99%	>=95%	<95%	Monthly	IT Department and SOC	• Identify the number and reason for high percentage of software system including operating systems for servers, virtual instances, OS for network devices, databases, OS of end points having reached beyond End of Life/End of Support. • Take necessary approvals and upgrade to the latest licensed versions available. • Take approvals in case of exceptions or delayed actions.
Disaster Recovery										
130	Disaster Recovery - Readiness	Total number of InfoSec platforms/services having DR readiness	Number of InfoSec platforms/services without DR readiness	(Total number of InfoSec platforms with DR readiness/ Total number of InfoSec platform and services)*100	>=99%	>=95%	<95%	Half yearly	IT Department and CISO Office	• Identify the reason and no. of platform/services that have been excluded from testing DR readiness and resolve the issues accordingly. • Identify the alternate timelines for conducting tests. • Take approvals in case of exceptions or delayed actions.
131	Disaster Recovery - Drill and Testing	Total number of DR drills and tests conducted successfully for InfoSec platforms/services, as per defined frequency	Number of DR drills/tests not conducted successfully for InfoSec platforms/services within defined frequency	(Total number of DR drills conducted successfully within defined timeframe/ Total number of DR drills to be conducted within defined timeframe)*100	>=99%	>=95%	<95%	Half yearly	IT Department and CISO Office	• Identify the reason and no. of platform/services where DR drills/tests have been excluded and resolve the issues accordingly. • Identify the alternate timelines for conducting tests. • Take approvals in case of exceptions or delayed actions.

Color	Definition	Timelines for Resolution
Green	The metric denotes high effectiveness/efficiency	NA
Amber	The metric denotes partial effectiveness/efficiency and requires attention	Within 15-30 Days
Red	The metric denotes non effectiveness/efficiency and requires immediate attention	Within 7 Days

Annexure II

Format for Commercial Bid
(*to be submitted along with a covering letter)*

Table 1

S. No.	Particulars	Amount (in ₹)*
1.	For Undertaking Information Security Audit *(including Software Audit)* & Cyber Security Audit for Year 2022-23 (July -June) and VAPT as defined in scope of work for Year 2023-24 (July -June)	
Total		

Table 2

S. No.	Particulars	Man Day Rate(in ₹)*
1.	For any additional task assigned including forensic investigation of a cyber security incident as per the requirement of the Bank beyond the scope of work.	
2.	For any additional task assigned such as data migration audit as per the requirement of the Bank beyond the scope of work	
Total		

Bidders are requested to note the following-

a) The bidder must submit the commercial bid in the above format. Incomplete formats will result in rejection of the proposal.
b) *The quoted price/cost must include all applicable taxes, duties, levies & charges.
c) The Commercial Bid to be signed by the Authorized Signatory of the Company.
d) Bids/price to be quoted in Indian Rupee only
e) For computation of financial score, Total Amount (in ₹) as given in Table 1 will only be taken into consideration.
f) The contract will be awarded to the L1 (Lowest) Bidder. In case of a tie, the Bank reserves the right to select the Vendor/Bidder based on marks scored during technical evaluation.
g) If a firm quotes NIL charges/consideration, the bid shall be treated as unresponsive and will not be considered.
h) IS and Cyber Security Auditors may be assigned any additional task including forensic investigation of a cyber security incident or to undertake data migration audit ,as per the requirement of the Bank beyond the scope of work. In such cases, the task is to be completed at the man-day rate quoted by the Auditor based on the assessed man-days required for completion of the task i.e.No. of days x Man Day Rate

Note: *Providing Commercial Proposal/Bid in other than this format may result in rejection of the Bid. Any interlineations', erasures or overwriting in any form will not be accepted in the Commercial Bid. There should be no hand-written material, corrections, or alterations in the Commercial Bid.*

Authorized Signatory(s)
(Name & Designation, Seal of the Company)
Date-

Annexure III

(Format of Bank Guarantee)

(To be executed on a non- judicial stamp paper)

To

National Housing Bank

_____,

In consideration of the National Housing Bank (hereinafter referred to as "NHB", which expression shall, unless repugnant to the context or meaning, thereof include its successors, representatives and assignees), having awarded in favour of M/s. _____ having its registered office at _____ (hereinafter referred to as "the IS Auditor ", which expression shall unless repugnant to the context or meaning thereof include its successors, administrators, representatives and assignees), a contract to provide _____ on terms and conditions set out in the Request for Proposal dated _____ & Requirement Proposal for undertaking _____ dated _____ (collectively referred as "the RFP")the Service Level Agreement dated _____ ("the SLA") (hereinafter the RFP and the SLA are together referred to as "the Contract"), and the IS Auditor having agreed to provide a performance bank guarantee for the faithful performance of the services as per the terms of the "Contract" including the warranty obligations /liabilities under the Contract of equivalent value amounting to _____ (Rupees _____Only), which is ___ % of the value of the Contract, to NHB in the form of a bank guarantee,

We, _____ (Name) _____(Address) (hereinafter referred to as "the Bank", which expression shall, unless repugnant to the context or meaning thereof, include its successors, administrators, representatives and assignees) at the request of the IS Auditor do hereby irrevocably guarantee for an amount of Rs. _____ (Rupees._____) (hereinafter referred to as the "Guaranteed Amount") and undertake to pay NHB the Guaranteed Amount merely on demand, without any previous notice from NHB, without any demur or protest and without referring to any other source, any and all monies payable by the IS Auditor by reason of any breach by the said IS Auditor of any of the terms and conditions of the said Contract including non-execution of the Contract at any time till _____ (day /month/ year). Any such demand made by NHB on the Bank shall be conclusive and binding, absolute and unequivocal not withstanding any disputes raised/pending before any court, tribunal, arbitration or any other authority by and between the IS Auditor and NHB. The Bank agrees that the guarantee herein contained shall continue to be enforceable till the sum due to NHB under this bank guarantee is fully paid and claims satisfied or till NHB discharges this bank guarantee. Unless a demand for claim under this bank guarantee is made on the Bank in writing on or before _____, the Bank shall be discharged from all liabilities under this bank guarantee thereafter.

NHB shall have the fullest liberty without affecting in any way the liability of the Bank under this bank guarantee, from time to time, to extend the time of performance by the IS Auditor. The Bank shall not be released from its liabilities under these presents by any exercise of NHB of the liberty with reference to the matter aforesaid.

NHB shall have the fullest liberty, without affecting this bank guarantee to postpone from time to time the exercise of any powers vested in them or of any right which they might have against the IS Auditor and to exercise the same at any time in any manner, and either to enforce or to forbear to enforce any covenants, contained or implied in the Contract between NHB and the IS Auditor or any other course or remedy or security available to NHB and the Bank shall not be released of its obligations/ liabilities under these presents by any exercise by NHB of his liberty with reference to the matters aforesaid or any of them or by reasons of any other act or forbearance or other acts of omission or commission on part of NHB or any other indulgence shown by NHB or by any other matter or thing whatsoever which under law would, but for this provision, have the effect of relieving the bank guarantee. The Bank further undertakes not to revoke this bank guarantee during its currency without the previous consent of NHB in writing.

The Bank further agrees that the decision of NHB as to the failure on the part of the IS Auditor to fulfil their obligations as aforesaid and/or as to the amount payable by the Bank to NHB hereunder shall be final, conclusive and binding on the Bank.

The Bank also agrees that NHB shall be entitled at his option to enforce this bank guarantee against the Bank as a principal debtor, in the first instance notwithstanding any other security or bank guarantee that it may have in relation to the IS Auditor's liabilities.

This bank guarantee will not be discharged due to the change in the constitution of the Bank or the IS Auditor(s).

Notwithstanding anything contained herein:

(a) our liability under this bank guarantee shall not exceed Rs. _____ (Rupees _____in words);

(b) this bank guarantee shall be valid up to _____; and

(c) We are liable to pay the Guaranteed Amount or any part thereof under this bank guarantee only and only if you serve upon us a written claim or demand on or before _____.

(Signature)

Designation/Staff Code No.

Bank's seal

Attorney as per power of Attorney No. Dated

Annexure IV

(To be executed on a non- judicial stamp paper)

Service Level Agreement

THIS SERVICE LEVEL AGREEMENT (hereinafter referred to "this **Agreement**") is made on this _____ day of the month of _____, 202_, by____ and between,

National Housing Bank, a body corporate established under the National Housing Bank Act, 1987, having its Head Office at Core 5A, 3rd -5th floors, India Habitat Centre, Lodhi Road, New Delhi-110003 (hereinafter called "**NHB**",) which expression shall include wherever the context so permits, its successors and assigns ; AND

_____, a company registered under the Companies Act, 1956, having its registered office at _____ (hereinafter called the **"IS Auditor")**, which expression shall include wherever the context so permits, its successors and permitted assigns.

(Hereinafter NHB and the IS Auditor are collectively referred to as "the Parties" and individually as "the Party")

WHEREAS

(A) NHB, vide Request for Proposals for Empanelment of Information & Cyber Security Auditor having RFP Reference No. – NHB(ND)/AD/A- 1162/2019 dated February 03,2020 has invited bids for shortlisting and empanelment of Auditors for undertaking Information Security Audit (ISA), Vulnerability Assessment and Penetration Testing (VAPT) & Cyber Security Audit (CSA) of its IT Infrastructure Systems, Applications and Web facing applications/ portals as per the activities delineated hereunder in Scope of Work, with a view to check the resilience of the extant infrastructure, enhance the security measures and to adopt best international practices and standards in due course. The ISA & CSA to be conducted in accordance with the guidelines of ISO 27001, RBI, CERT-In, NCIIPC, Govt. of India, OWASP, Information Technology Act 2000 and other international standard guidelines for the same.

(B) The said Request for Proposals including Corrigendum/Clarification, if any, issued hereinafter collectively referred to the "**RFP"** (attached hereto as **Appendix-** I)

(C) The bid submitted by the IS Auditor for empanelment pursuant to the RFP were considered and they were shortlisted for empanelment after evaluation of Technical Bid.

(D) Subsequent to the empanelment of the Information & Cyber Security Auditors, NHB has sought commercial quotes from the empanelled auditors vide Requirement Proposal with reference No. _____ dated _____ for Undertaking Information Security & Cyber Security Audit for the Year 2022-2023 (July-June). The said Requirement Proposal hereinafter referred to as "RP".

(E) The IS Auditor have been selected as successful bidder and NHB has issued letter of award/work order vide letter No._____ dated _____"LoA" (attached hereto as **Appendix-** II).

(F) The IS Auditor has accepted and agreed to provide the Services in accordance with terms and conditions of RFP, RP and the LoA.

(G) In terms of the RFP, RP NHB and the IS Auditor have agreed to enter into this Agreement in the manner hereinafter appearing:

NOW THEREFORE the Parties hereby agree as follows:

1. GENERAL PROVISIONS

1.1 Definitions

Unless the context otherwise requires, the following terms whenever used in this Agreement have the following meanings:

(a) "Applicable Law" means the laws and any other instruments having the force of law in India, as they may be issued and in force from time to time.

(b) " Contract" or "this Contract" means and shall construe this Agreement;

(c) "Deliverables" means and includes the major deliverables as specified in Clause _____ of the RFP& RP.

(d) "Effective Date" means the date on which this Agreement comes into force and effect pursuant to Clause 2.1 hereof.

(e) "Personnel" means persons hired/to be hired by the IS Auditor as employees and assigned to the performance of the Services or any part thereof.

(f) "Project" means collectively the Services and the Deliverables to be provided as detailed in the RFP & RP.

(g) "Services" or "Scope of Work" means and includes the scope of work to be performed by the IS Auditor as described/set out in Clause _____ of the RFP & RP.

(h) "Third Party" means any person or entity other than NHB and the IS Auditor.

1.2 Principles of Interpretation

In this Agreement, unless the context otherwise requires:

a) All capitalized terms unless specifically defined in this Agreement shall have the meaning given to them in the RFP& RP.

b) Words and abbreviations, which have well known technical or trade/commercial meanings are used in this Agreement in accordance with such meanings;

c) The RFP, RP, LoA and the NDA along with the Appendices/ Attachments hereto, shall form part and parcel of this Agreement and shall be read together for all purpose and effect.

d) In case of any inconsistency or repugnancy between the provisions contained RFP,RP, LoA and this Agreement, unless the context otherwise requires, the opinion of NHB shall prevail to the extent of such inconsistency or repugnancy and the same shall be binding on the IS Auditor.

1.3 Purpose

1.3.1 It is hereby agreed that the IS Auditor shall provide the Services to NHB as set out in the RFP till the completion of the Project. The objective of the Project is to make _____.

1.3.2 Performance of the Scope of Work

The IS Auditor shall perform all the services as set out in the Scope of Work and complete the Deliverables within the prescribed timelines in terms of the RFP and the entire assignment shall be completed within the Term of this Contract.

1.3.3 Term/Period of Contract

The contract shall be valid till completion of all activities as given under the "Project Scope of Work" and providing all "Project Deliverables" to the Bank, from the date of the work order/letter of award issued to the IS auditor, unless the period is extended in accordance with this agreement.

1.3.4 Contract Price

The entire assignment to be performed under this Contract is fixed price contract and the IS Auditor shall be paid the total price consideration of Rs. _____ (Rupees _____) (**"Contract Price**") for the satisfactory performance/execution of the entire assignment under the Project. The Contract Price shall be paid by NHB as per the payment terms agreed at Clause 4.2 of this Agreement.

1.4 Relation between the Parties

Nothing contained herein shall be construed as establishing a relationship of master and servant or of principal and agent as between NHB and the IS Auditor. The IS Auditor, subject to this Agreement, has complete charge of personnel to be engaged by the IS Auditor for performing the Services and shall be fully responsible for the works to be performed by them or on their behalf hereunder and also for the quality of the work done by their personnel.

1.5 Language

This Contract has been executed in the English language, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this Contract.

1.6 Headings

The headings shall not limit, alter or affect the meaning of this Contract.

1.7 Notices

1.7.1 Any notice, request or consent required or permitted to be given or made pursuant to this Contract shall be in writing. Any such notice, request or consent shall be deemed to have been given or made when delivered in person to an authorized representative of the Party to whom the communication is addressed, or when sent by registered mail, telex, telegram or facsimile to such Party at the following address:

For NHB:

Attention:_____

Fax:_____

For the IS Auditor:

Attention:_____

Fax:_____

1.7.2 Notice will be deemed to be effective as follows

(a) In the case of personal delivery or registered mail, on delivery;
(b) In case of telegrams, ninety six (96) hours following confirmed transmission; and
(c) In the case of facsimiles, seventy two (72) hours following confirmed transmission.

1.7.3 A Party may change its address for notice hereunder by giving the other Party notice of such change pursuant to this Clause.

1.8 Location

The Services shall be performed at Delhi or at such location required/ approved by NHB.

1.9 Authority of IS Auditor

The IS Auditor hereby authorize _____ to act on their behalf in exercising the entire IS Auditor's rights and obligations towards NHB under this Contract, including without limitation for signing letters/communications, execution of agreements, for receiving instructions and payments from NHB.

1.10 Taxes and Duties

The IS Auditor and their personnel shall pay the taxes (excluding GST), duties, fees, levies and other impositions levied under the existing, amended or enacted laws during the tenure of this Agreement and NHB shall perform such duties in regard to the deduction of such taxes as may be lawfully imposed from the payments to be made to the IS Auditor.

2.0 COMMENCEMENT, COMPLETION, MODIFICATION AND TERMINATION OF CONTRACT

2.1 Effectiveness of Contract

This Agreement deemed to have taken effect from the date of acceptance of the letter of award (LoA) by the IS Auditor i.e. w.e.f. …….

2.2 Commencement of Services

The IS Auditor shall begin carrying out the Services immediately viz. from the date of acceptance of LoA, or on such date as the Parties may agree in writing.

2.3 Expiration of Contract

Unless terminated earlier pursuant to Clause-2.8 hereof, this Contract shall expire on the expiry of the Term as stated on Clause 1.3.3 herein unless the Term is extended in accordance with the Clause 2.6.4.

2.4 Entire Agreement

This Contract contains all covenants, stipulations and provisions agreed by the Parties. No representative of either Party has authority to make, and the Parties shall not be bound by or be liable for, any statement, representation, promise or agreement not set forth herein.

2.5 Modification

Modification of the terms and conditions of this Contract, including any modification of the scope of the Services/Scope of Work, may only be made by written agreement between the Parties and shall not be effective until the consent of the Parties has been obtained, however, each Party shall give due consideration to any proposals for modification made by the other Party.

2.6 Force Majeure

2.6.1 Definition

In the event of either Party being rendered unable by Force Majeure to perform any obligation required to be performed by them under the Contract, the relative obligation of the Party affected by such Force Majeure shall be suspended for the period during which such cause lasts.

The term "Force Majeure" as employed herein shall mean acts of God, War, Civil Riots, Fire, Flood and Acts and Regulations of respective government of the two Parties directly affecting the performance of the Contract.

Upon the occurrence of such cause and upon its termination, the Party alleging that it has been rendered unable as aforesaid thereby, shall notify the other Party in writing, the beginning of the cause amounting to Force Majeure as also the ending of the said cause by giving notice to the other Party within 72 hours of the ending of the cause respectively. If the deliveries are suspended by Force Majeure conditions lasting for more than 2 (two) months, NHB shall have the option of canceling this Contract in whole or part at its discretion without any liability on its part.

Time for performance of the relative obligation suspended by Force Majeure shall then stand extended by the period for which such cause lasts.

2.6.2 No Breach of Contract

The failure of a Party to fulfill any of its obligations hereunder shall not be considered to be a breach of or default under this Contract in so far as such inability arises from an event of Force Majeure, provided that the Party affected by such an event has taken all reasonable precautions, due care and reasonable alternative measures, all with the objective of carrying out the terms and conditions of this Contract.

2.6.3 Measures to be taken

(a) A Party affected by an event of Force Majeure shall take all reasonable measures to remove such Party's inability to fulfill its obligations hereunder with a minimum of delay.

(b) A Party affected by an event of Force Majeure shall notify the other Party such event as soon as possible, and in any event not later than fourteen (14) days following the occurrence of such event, providing evidence of the nature and cause of such event, and shall similarly give notice of the restoration of normal conditions as soon as possible.

(c) The Parties shall take all reasonable measures to minimize the consequences of any event of Force Majeure.

2.6.4 **Extension of Time**

Any period within which a Party shall, pursuant to this Contract, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action as a result of Force Majeure.

2.6.5 **Consultation**

Not later than thirty (30) days after the Party, as the result of an event of Force Majeure, has become unable to perform a material portion of the Services, the Parties shall consult with each other with a view to agreeing on appropriate measures to be taken in the circumstances.

2.7 Suspension

NHB may, by written notice of suspension to the IS Auditor, suspend all payments to the IS Auditor hereunder if NHB is not satisfied with the performance of the IS Auditor or if the IS Auditor fails to perform any of their obligations under this Contract, including the carrying out of services, provided that such notice of suspension (i) shall specify the nature of the failure, and (ii) shall request the IS Auditor to provide remedy for such failure within a period not exceeding thirty (30) days after receipt by the IS Auditor of such notice of suspension and shall invoke contract performance guarantee.

2.8 Termination

2.8.1 **By NHB**

NHB may by not less than fifteen (15) calendar days written notice of termination to the IS Auditor, (except in the event listed in paragraph (g) below, for which there shall be a written notice of not less than sixty (60) days) such notice to be given after the occurrence of any of the events specified in paragraphs (a) to (f) of this Clause-2.8.l, terminate this Contract:

(a) If the IS Auditor fails to remedy a failure in the performance of their obligations hereunder, as specified in a notice of suspension pursuant to Clause-2.7 here-in-above, within thirty (30) days of receipt of such notice of suspension or within such further period as NHB may have subsequently approved in writing;

(b) If the IS Auditor becomes insolvent or bankrupt or enters into an agreement with its creditors for relief of debt or take advance of any law for the benefit of debtors or goes into liquidation receivership whether compulsory or voluntary;

(c) If the IS Auditor fails to comply with any final decision reached/award passed as a result of arbitration proceedings pursuant to Clause-8 hereof;

(d) If the IS Auditor submits to NHB a statement which has a material effect on the rights, obligations or interests of NHB and which the IS Auditor knows to be false;

(e) If, as a result of Force Majeure, the IS Auditor is unable to perform a material portion of the Services for a period of not less than sixty (60) days; or

(f) In the event it comes to the notice of NHB that any of the representations and/or warranties made by the IS Auditor either in the Bid Documents or in the subsequent correspondences are found to be false and/or the IS Auditor/its personnel are found to be involved in any fraudulent or criminal act;

(g) If NHB, in its sole discretion and for any reason whatsoever, decides to terminate this Contract.

2.8.2 **Cessation of Rights and Obligations**

Upon termination of this Contract pursuant to Clause- 2.8.1 hereof or upon expiration of this Contract pursuant to Clause-2.3 hereof, all rights and obligations of the Parties hereunder shall cease, except:

(a) Such rights and obligations as may have accrued on the date of termination or expiration,
(b) The obligation of confidentiality set forth in Clause-3.7 hereof,
(c) Any right which a Party may have under the Applicable Law.

2.8.3 **Cessation of Services**

Upon termination of this Contract by notice pursuant to clauses-2.8.1 hereof, the IS Auditor shall, immediately upon dispatch or receipt of such notice, take all necessary steps to bring the Services to a close in a prompt and orderly manner and shall make every reasonable effort to keep expenditures for this purpose to a minimum.

2.8.4 **Payment in case of termination of contract**

Subject to the terms of the RFP & RP , in case the Contract is terminated, payment towards services will be made on pro rata basis, for the services already delivered, after deducting applicable penalty and TDS/other applicable taxes.

3.0 OBLIGATIONS OF THE IS AUDITOR

3.1 Standard of Performance

The IS Auditor shall perform the Services and carry out their obligations hereunder with all due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used with professional engineering and consulting standards recognized by professional bodies, and

shall observe sound management, technical and engineering practices, and employ appropriate advanced technology, safe and effective equipment, machinery, materials and methods. The IS Auditor shall always act, in respect of any matter relating to this Contract or to the Services, as faithful advisers to NHB, and shall at all times support and safeguard NHB's legitimate interests in any dealings with third parties.

3.2 Law Governing contract

The IS Auditor shall perform the assignment in accordance with the applicable Law and shall take all practicable steps to ensure that the Personnel of the IS Auditor comply with the Applicable Law.

3.3 Conflict of Interest

The IS Auditor shall hold NHB's interest paramount, without any consideration for future work, and strictly avoid conflict with other assignments or their corporate interests.

3.4 IS Auditor Not to Benefit from Commissions/Discounts etc.

The payment of the IS Auditor by NHB shall constitute the IS Auditor's only payment in connection with this Contract or the Services, and the IS Auditor shall not accept for their own benefit any trade commission, discount, or similar payment in connection with activities pursuant to this Contract or to the Services or in the discharge of their obligations under the Contract, and the IS Auditor shall use their best efforts to ensure that its Personnel similarly shall not receive any such additional payment.

3.5 IS Auditor and Affiliates not to be otherwise interested in /benefited from the Project

The IS Auditor agrees that, during the term of this Contract and after its termination, the IS Auditor shall not create any work/ opportunity for itself and for any of its affiliates from this Project/ assignment and/or derive any financial benefits directly or otherwise, other than what is agreed to be paid as professional fee as mentioned at Clause 4.2 for this assignment.

3.6 Prohibition of Conflicting Activities

The IS Auditor and its affiliates shall not engage, either directly or indirectly, in any business or professional activities which would conflict with the activities assigned to them under this Contract. The IS Auditor and its affiliates hired to provide services for the proposed assignment will be disqualified from services related to the initial assignment for the same Project subsequently.

3.7 Confidentiality

The IS Auditor and its Personnel shall not, either during the term or after the expiration of this Contract, disclose any proprietary or confidential

information relating to the Project, the Services, this Agreement or NHB's business or operations without the prior written consent of NHB.

A separate non-disclosure cum confidentiality agreement ("NDA") will be signed between the IS Auditor and NHB, if required.

3.8 Insurance to be taken out by the IS Auditor

The IS Auditor shall take out and maintain at their own cost, appropriate insurance against all the risks, and for all the coverage, like workers compensation, employment liability insurance for all the staff on the assignment, comprehensive general liability insurance, including contractual liability coverage adequate to cover the indemnity of obligation against all damages, costs, and charges and expenses for injury to any person or damage to any property arising out of, or in connection with, the services which result from the fault of the IS Auditor or their staff on the assignment

3.9 Liability of the IS Auditor

The IS Auditor shall be liable to NHB for the performance of the Services in accordance with the provisions of this Contract and for any loss suffered by NHB as a result of a default of the IS Auditor in such performance, subject to the following limitations:

(a) The IS Auditor shall not be liable for any damage or injury caused by or arising out of any act, neglect, default or omission of any persons other than the IS Auditor and its Personnel; and
(b) The IS Auditor shall not be liable for any loss or damage caused by or arising out of circumstances over which the IS Auditor had no control.

3.10 Indemnification of NHB by the IS Auditor

The IS Auditor shall indemnify NHB and shall always keep NHB, its employees, personnel, officers and directors, both during and after the term of this Agreement, fully and effectively indemnified against all losses, damage, injuries, deaths, expenses, actions, proceedings, demands, costs and claims, including legal fees and expenses, suffered by NHB or any Third Party, where such loss, damage, injury is the result of (i) any wrongful action, negligence or breach of contract by the IS Auditor or its personnel; and/or (ii) any negligence or gross misconduct attributable to the IS Auditor or its personnel; and/or (iii) any claim made by employees who are deployed by the IS Auditor against NHB; and/or (iv) any claim arising out of employment, non-payment of remuneration and non-provision of benefits in accordance with the statues/various labour laws by the IS Auditor to its employees; and/or (v) any or all Deliverables or Services infringing any patent, trademarks, copyrights or such other Intellectual Property Rights; and/or (vi) any breach of the confidentiality obligations mentioned under clause 3.7 and /or NDA.

3.11 Limitation of Liability

(i) The IS Auditor's aggregate liability, in connection with the obligations undertaken as a part of this Project, whether arising under this Project regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), other than the circumstances mentioned in the sub-clause (ii) below, shall be limited to _____ times of the total contract value.

(ii) The IS Auditor's liability in case of claims against NHB resulting from infringement of patents, trademarks, copyrights or such other Intellectual Property Rights or breach of confidentiality obligations committed by the IS Auditor shall be actual and unlimited.

(iii) Under no circumstances, NHB shall be liable to the IS Auditor for direct, indirect, incidental, consequential, special or exemplary damages arising from termination of this Agreement, even if he has been advised of the possibility of such damages.

3.12 IS Auditor's Actions Requiring Owner's Prior Approval

The IS Auditor shall not enter into a sub contract for the performance of any part of the Services, without the prior approval of NHB in writing. However, the IS Auditor can hire the services of Personnel to carry out any part of the services. The IS Auditor shall remain fully liable for the performance of the services by its personnel pursuant to this Contract.

3.13 Reporting Obligations

The IS Auditor shall submit to NHB the reports and documents within the timelines set forth in the Offer Letter, including any supporting data required by NHB.

3.14 Documents prepared by the IS Auditor to be the Property of NHB:

All software, algorithms, reports and other documents prepared/developed by the IS Auditor in performing the Services shall become and remain the property of NHB, and the IS Auditor shall, not later than upon termination or expiration of this Contract, deliver all such documents to NHB, together with a detailed inventory thereof. The IS Auditor may retain a copy of such documents and shall not use them for purposes unrelated to this Contract without the prior written approval of NHB.

3.15 IS Auditor's Personnel

The IS Auditor shall ensure that personnel/employees engaged by him in the project/contract, have appropriate qualifications and competence as stipulated under the RFP and are in all respects acceptable to NHB. The IS Auditor will do its utmost to ensure that the personnel identified by the IS

Auditor to work under this Agreement completes the Term. If any such personnel resigns from his job and leaves the IS Auditor, the IS Auditor will provide NHB with another personnel of equivalent knowledge, skill and experience acceptable to NHB as his substitute.

The IS Auditor shall strictly comply with all applicable labour laws and such other laws in relation to the services to be provided and the personnel engaged by the IS Auditor and he shall be solely responsible for all acts of the said personnel so enrolled and there shall and will not be any privity of contract for any purpose and to any intent between NHB and said personnel so engaged by the IS Auditor.

The IS Auditor shall be responsible for making appropriate deductions in respect of income tax and any other statutory deductions under applicable laws in respect of its personnel/employees engaged by the IS Auditor under this Agreement. The IS Auditor agrees to indemnify NHB in respect of any claims that may be made by statutory authorities against NHB in respect of contributions relating to the personnel/employees engaged by the IS Auditor for performing the work under this Agreement. NHB is authorized to make such tax deduction at source as may be necessary as per law/rules in force in respect of payments made to the IS Auditor.

3.16 Non-Compete

The IS Auditor will neither approach nor make any proposal for work for any employee of NHB directly or indirectly during the validity of this Agreement and for one year from the date of termination of this Agreement.

3.17 Change in Ownership or Constitution:

The IS Auditor will inform NHB immediately about any change in its ownership or its constitution. The IS Auditor will ensure that the NHB's interest will be protected with utmost care. If NHB is not satisfied with the change of ownership or constitution of the IS Auditor and/or with the new owner, NHB shall have the right of termination and in that event, the payment, if any, upon termination may be made as provided in clause 2.8.4.

3.18 **Monitoring**

The SLA parameters shall be monitored on continuous basis. If the performance is not satisfactory at any given point in time during the contract period and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of NHB, then NHB will have the right to take appropriate actions including termination of the contract.

3.19 **Rights to Visit**

All records of the IS Auditor relating to any matters covered by the RFP shall be made available to NHB including its authorized personnel at any time, as

often as NHB deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data.

NHB, including its regulatory authorities like Reserve Bank of India shall have the right to verify, through their officials or such other persons as may be authorized, the progress of the project at the site of the IS Auditor or at the place where the services are being rendered by the IS Auditor.

NHB and its authorized representatives, including regulator like Reserve Bank of India shall have the right to visit any of the IS Auditor's premises to ensure that data provided by NHB is not misused. The IS Auditor will have to cooperate with the authorized representative/s of NHB or the Reserve Bank of India, as the case may be and will have to provide all information/ documents required by NHB/RBI.

3.20 **Audit**

The IS Auditor shall allow and grant NHB, its authorized personnel, its auditors (internal and external) and/or the Reserve Bank of India/ other regulatory & statutory authorities, and their authorized personnel, unrestricted right to inspect and/ or audit its books and accounts, to provide copies of any audit or review reports and findings made on the IS Auditor, directly related to the Services.

In case any of the Services are further outsourced/ assigned/ subcontracted to other IS Auditors in terms of the RFP, it will be the responsibility of the IS Auditor to ensure that the authorities /officials as mentioned above are allowed access to all the related places, for inspection and/ or audit.

3.21 **Contingency Plans**

The IS Auditor shall arrange and ensure proper Data Recovery Mechanism, Attrition Plan and other contingency plans to meet any unexpected obstruction to the IS Auditor or any employees or sub-contractors of the IS Auditor in rendering the Services or any part of the same under this Agreement to NHB.

3.22 **Transition Requirement**

In the event of failure of the IS Auditor to render the Services or in the event of termination of the Agreement or expiry of term or otherwise, without prejudice to any other right, NHB at its sole discretion may make alternate arrangement for getting the Services contracted with another IS Auditor. In such case, upon receiving notice from NHB, the IS Auditor shall continue to provide the Services as per the terms of the Contract until the new IS Auditor completely takes over the work. During the transition phase, the existing IS Auditor shall render all reasonable assistance to the new IS Auditor within such period prescribed by NHB.

4.0 OBLIGATIONS OF NHB

4.1 Support:

NHB will provide the support as required necessary by it including giving access to the relevant and limited data maintained in its system to the IS Auditor for carrying out the assignment under the Contract.

4.2 Consideration & Payment Terms

In consideration of the Services performed by the IS Auditor under this Agreement, NHB shall make to the IS Auditor such payments and in such manner as specified in the RFP, RP and/or the LoA.

The IS Auditor shall submit the bills to NHB of firms printed bill forms indicating the work done by him during the period for which payment is sought. NHB shall make payments to the IS Auditor as per the payment schedule given in the RFP & or RP. But if the progress is not satisfactory and according to agreed work program/schedule the payment may be withheld.

4.3 Non-Solicitation:

NHB agrees not to make an offer for employment to any personnel provided/deployed by the IS Auditor under this Agreement, and, not to accept any application for employment from him/her, while he is under the term of this Agreement, and, for up to twelve (12) months from the date of last assignment of the work under this Agreement with NHB.

5.0 FAIRNESS AND GOOD FAITH

5.1 Good Faith

The Parties undertake to act in all fairness and good faith in respect to each other's rights under this Contract and to adopt all reasonable measures to ensure the realization of the objectives of this Contract

6.0 UNDERTAKINGS:

The IS Auditor hereby further undertakes:

(i) That the IS Auditor has gone through all the required/relevant and extant instructions/ circulars of Government of India, Reserve Bank of India and /or any other concerned authority, GFR issued by Ministry of Finance, guidelines of CVC and provisions of the manual/relevant instructions of NHB, as applicable to the scope/area of its work/operation under this Agreement and the advice/services to be rendered by it as the IS Auditor and it complies/will comply with all such requirements.

(ii) That the IS Auditor has the necessary expertise to work and execute the Project as per the scope of work set out in detail in the RFP & the RP and it has the capability to deliver efficient and effective advice/services to NHB.

It shall carry out the assignment under this Agreement with due diligence and with the highest standard of professionalism and business ethics.

(iii) That being the IS Auditor of NHB for a consideration, it shall be accountable for (a) any improper discharge of the assignment under this Agreement and/or (b) any deviant conduct keeping in view the norms of ethical business and professionalism.

(iv) That NHB shall have every right at its discretion to enforce such accountability in case of any improper discharge of contractual obligations and/or any advice/service rendered in the views of NHB is found to be grossly faulty/negligent/deficient and/or any deviant conduct by the IS Auditor and as a consequence of it, NHB can, irrespective of anything stated herein, terminate this Agreement by giving 15 days prior notice, including to withhold/retain the dues payable to the IS Auditor by NHB under this Agreement and appropriate/adjust the same for the losses, if any, suffered by NHB without requiring NHB to prove the actual loss.

(v) That the IS Auditor shall not do anything that will be of any conflict of interest to the IS Auditor while discharging the obligations under this Agreement and it shall bring to the notice/knowledge of NHB beforehand any possible instance of conflict of interest while rendering any advice or service. Further, the IS Auditor shall not receive any remuneration in connection with the assignment except as provided in this Agreement. The IS Auditor and/or any of its affiliates shall not engage in consulting or other activities that will be in conflict with the obligations under this Agreement.

(vi) That the IS Auditor has not been hired for any assignment that would be in conflict with its prior or current obligations to NHB or that may place the IS Auditor in a position of being unable to carry out the assignment in the best interest of NHB.

(vii) That the IS Auditor shall act at all times in the interest of NHB and render advice/service with highest professional integrity and shall cooperate fully with any legitimately provided/constituted investigative body, conducting inquiry into processing or execution of the consultancy contract/any other matter related with discharge of the contractual obligations by the IS Auditor.

7.0 SEVERABILITY:

Each clause of this Agreement is enforceable independently. Should any clause of this Agreement become not enforceable due to any reason, it will not affect the enforceability of the other clauses.

8.0 SETTLEMENT OF DISPUTES

In the event of any dispute or difference arising out of, in relation to, or in connection with this Agreement, or the breach thereof, shall be settled amicably through mutual discussions. If, however, the parties are not able to settle them amicably without undue delay, the same shall be settled by the process of arbitration in accordance with the provisions of the Arbitration & Conciliation Act, 1996 (as amended from time to time). The venue of such arbitration shall be at New Delhi and the proceedings shall be conducted in English. The arbitration tribunal shall consist of Sole i.e. 1(one) Arbitrator to be appointed jointly by the Parties within thirty (30) days from the date of first recommendation for appointment of arbitrator in written form one Party to the other. If the Parties fail to agree on appointment of such Sole Arbitrator, arbitral tribunal consisting of Sole Arbitrator shall be appointed in accordance with the provisions of the Arbitration and Conciliation Act, 1996. The award of arbitrator made in pursuance thereof shall be final and binding on the Parties. All costs and expenses of such arbitration shall be borne equally by the Parties at the first instance which however subject to the provisions of the said Act.

Notwithstanding, it is agreed that the IS Auditor shall continue the remaining work for the assignment under this Agreement during the pendency of arbitration proceedings unless otherwise directed in writing by NHB or unless the matter is such that the work cannot possibly be continued until the decision of the arbitrator, as the case may be, is obtained.

9.0 JURISDICTION AND APPLICABLE LAW

This agreement including all matters connected with this Agreement, shall be governed by the laws of India (both substantive and procedural) for the time being in force and shall be subjected to exclusive jurisdiction of the Courts at New Delhi.

IN WITNESS WHEREOF, the Parties hereto have caused this Agreement signed in their respective names on the day and year first above written at New Delhi.

FOR AND ON BEHALF OF NATIONAL HOUSING BANK

By _____

Authorized Representative

FOR AND ON BEHALF OF [IS AUDITOR]

By _____

Authorized Representative

WITNESSES:

1.

(Name and address)

2.

(Name and address)

Annexure V

CONFIDENTIALITY –CUM- NON-DISCLOSURE AGREEMENT

(To be executed on a non- judicial stamp paper)

This Confidentiality –cum-Non Disclosure Agreement is entered into at New Delhi on this ……..day ……..of _____, 202__, by and between;

_____, a ……. incorporated _____, having its Registered Office at …… (hereinafter referred to as "the IS Auditor"), which expression shall include wherever the context so permits, its successors and permitted assigns;

and

The National Housing Bank, a bank constituted under the National Housing Bank Act,1987 (Central act No. 53 of 1987) having its Head Office at Core-5A,5th Floor, India Habitat Centre, Lodhi Road, New Delhi-110003; (herein after referred to as "NHB"), which expression shall include wherever the context so permits, its successors and permitted assigns:

WHEREAS the IS Auditor & NHB would be having discussions and negotiations concerning _____ ("Purpose") between them as per the Service Level Agreement dated …… (hereinafter referred to as "SLA"). In the course of such discussions & negotiations, it is anticipated that either party may disclose or deliver to the other party certain of its trade secrets or confidential or proprietary information for the purpose of enabling the other party to evaluate the feasibility of such a business relationship. The parties have entered into this Agreement, in order to assure the confidentiality of such trade secrets and confidential & proprietary information in accordance with the terms of this Agreement. As used in this Agreement, the party disclosing Proprietary Information (as defined below) is referred to as "the **Disclosing Party"** & will include its affiliates and subsidiaries, the party receiving such Proprietary Information is referred to as "the **Recipient/Receiving Party"**, and will include its affiliates & subsidiaries and its personnel.

Now this Agreement witnesses: -

1. **Proprietary Information:** As used in this Agreement, the term Proprietary information shall mean as all trade secrets or confidential or Proprietary information designated as such in writing by the Disclosing Party, whether by letter or by the use of an appropriate prominently placed Proprietary stamp or legend, prior to or at the time such trade secret or confidential or Proprietary information is disclosed by the Disclosing Party to the

Recipient/Receiving Party. Notwithstanding the foregoing, information which is orally or visually disclosed to the Recipient/Receiving Party by the Disclosing party or is disclosed in writing unaccompanied by a covering letter, proprietary stamp or legend, shall constitute proprietary information if the disclosing party , within 10(ten) days after such disclosure, delivers to the Recipient/Receiving Party a written document or documents describing such Proprietary Information and referencing the place and date of such oral ,visual or written disclosure and the names of the employees or officers of the Recipient/ Receiving party to whom such disclosure was made.

2. **Confidentiality:**
   a) Each party shall keep secret and treat in strictest confidence all confidential information it has received about the other party or its customers and will not use the confidential information otherwise than for the purpose of performing its obligations under this Agreement in accordance with its terms and so far this may be required for the proper exercise of the Parties respective rights and obligations under this Agreement.

   b) The term confidential information shall mean and include all written or oral information (including information received from third parties that the Disclosing Party is obligated to treat as confidential) that is (i) clearly identified in writing at the time of disclosure as confidential and in case of oral or visual disclosure, or (ii) that a reasonable person at the time of disclosure reasonably would assume, under the circumstances, to be confidential. Confidential Information shall also mean, software programs, technical data, methodologies, know how, processes, designs, customer names, prospective customer's names, customer information and business information of the Disclosing Party.

   c) Confidential information does not include information which:
      (i) is publicly available at the time of its disclosure; or
      (ii) becomes publicly available following disclosure; or
      (iii) is already known to or was in the possession of Recipient/Receiving party prior to disclosure under this Agreement; or
      (iv) is disclosed to the Recipient/Receiving party from a third party, which party is not bound by any obligation of confidentiality; or
      (v) is or has been independently developed by the Recipient/Receiving party without using the confidential information.
      (vi) is disclosed with the prior consent of the Disclosing Party.

3. **Non –Disclosure of Proprietary Information:** For the period during the agreement or its renewal, the Recipient/Receiving Party will:
   a) Use such Proprietary Information only for the purpose for which it was disclosed and without written authorization of the Disclosing Party

shall not use or exploit such Proprietary Information for its own benefit or the benefit of others.

b) Protect the Proprietary Information against disclosure to third parties in the same manner and with the reasonable degree of care, with which it protects its own confidential information of similar importance and
c) Limit disclosure of Proprietary Information received under this Agreement to persons within its organization and to those 3rd party contractors performing tasks that would otherwise customarily or routinely be performed by its employees, who have a need to know such Proprietary Information in the course of performance of their duties and who are bound to protect the confidentiality of such Proprietary Information.

4. **Limit on Obligations:** The obligations of the Recipient/ Receiving Party specified in clause 3 above shall not apply and the Recipient/ Receiving Party shall have no further obligations, with respect to any Proprietary Information to the extent that such Proprietary information:
   a) is generally known to the public at the time of disclosure or becomes generally known without any wrongful act on the part of the Recipient/ Receiving Party;
   b) is in the Recipient's/ Receiving Party's possession at the time of disclosure otherwise than as a result of the Recipient's/ Receiving Party's breach of an obligation of confidentiality owed to the Disclosing Party;
   c) becomes known to the Recipient/ Receiving Party through disclosure by any other source, other than the Disclosing party, having the legal right to disclose such Proprietary Information.
   d) is independently developed by the Recipient/ Receiving Party without reference to or reliance upon the Proprietary Information; or
   e) is required to be disclosed by the Recipient/ Receiving Party to comply with applicable laws or governmental regulation, provided that the Recipient/ Receiving Party provides prior written notice of such disclosure to the Disclosing Party and take reasonable and lawful actions for such disclosure.

5. **Return of Documents:** The Recipient/ Receiving Party shall, upon request of the Disclosing Party , in writing ,return to the Disclosing party all drawings, documents and other tangible manifestations of Proprietary Information received by the Recipient/ Receiving Party pursuant to this Agreement (and all copies and reproductions thereof) within a reasonable period. Each party agrees that in the event, it is not inclined to proceed further with the engagement, business discussions and negotiations or in the event of termination of this Agreement, the Recipient/ Receiving Party will promptly return to the other part or with the consent of the other party, destroy the Proprietary Information of the other party. Provided however

the Receiving Party shall retain copies to be in compliance with its statutory, regulatory, internal policy or professional obligations.

6. **Communications: Written** communications requesting transferring Proprietary Information under this Agreement shall be addressed only to the respective designees as follows (or to such designees as the parties hereto may from time to time designate in writing)

_____ **NATIONAL HOUSING BANK**

(IS Auditor)

7. Term: The obligation pursuant to clause 2 and 3 (Confidentiality & Non-Disclosure of Proprietary Information) will survive for a period of _____ years from the termination of the SLA.

8. The provisions of this Agreement are necessary for the protection of the business goodwill of the parties and are considered by the parties to be reasonable for such purposes. Both the parties agree that any breach of this Agreement will cause substantial and irreparable damages to the other party and, therefore, in the event of such breach by one party, the other party shall be entitled to appropriate remedy, which may be available under law.

9. Notwithstanding anything stated in this Agreement, any report/finding/document delivered/submitted by the IS Auditor to NHB as a part of the outcome or deliverables under the SLA and which, in the opinion of NHB, requires any further study/analysis by any third party agency/institution depending on the requirement of the case, the same can be shared by NHB with such third party agency/institution for conducting such study/analysis and no prior consent of the IS Auditor is required for the same. Such report/finding/document delivered/ submitted by the IS Auditor to NHB shall become exclusive property of NHB and as such NHB shall not be bound by any restriction from disclosure of such report/ finding/ document or content thereof, being the Receiving Party.

10. This Agreement shall be governed and construed in accordance with the laws of India and shall be subjected to the Jurisdiction of courts at Delhi**.** It is agreed that any dispute or differences arising out of or touching this Agreement if not resolved amicably shall be referred to the arbitration as per clause _____ of the SLA executed between the parties hereto.

11. **Miscellaneous**

a) This Agreement may not be modified, changed or discharged, in whole or in part, except by a further Agreement/amendment in writing signed by both the parties.

b) This Agreement will be binding upon & enure to the benefit of the parties hereto and it includes their respective successors & assigns

c) The Agreement shall be construed & and interpreted in accordance with the laws prevailing in India.

d) In witness whereof, the parties hereto have agreed, accepted and acknowledged and signed these presents, on the day, month and year mentioned herein above.

FOR ____(Name of IS auditor_____)___	**FOR NATIONAL HOUSING BANK**
Authorized Signatory	Authorized Signatory
Name:	Name:
Designation:	Designation:
Place:	Place:
Date:	Date:

WITNESSES:

1.

2.

Annexure VI

CERTIFICATE

I have read the Clause 12.2 of this RP regarding restriction on procurement from a bidder of a country which shares a land border with India; I certify that **<< name of the Bidder >>** is not from such a country or, if from such a country, has been registered with the Competent Authority. I hereby certify that this bidder fulfills all requirements in this regard and is eligible to be considered. [Evidence of valid registration by the Competent Authority shall be attached.]

Authorized Signatories

(Name & Designation, seal of the company)
Date:

Annexure VII

Pre-Contract Integrity Pact

(To be executed on a non- judicial stamp paper)

This pre-bid/pre-contract Agreement (hereinafter called "**this Integrity Pact**") between, the National Housing Bank, a bank established under the provisions of the National Housing Bank Act, 1987 having its Head Office at Core 5A, India Habitat Centre, Lodhi Road, New Delhi-110003 represented through Shri/Ms _____ , (Designation) (hereinafter called "NHB", which expression shall mean and include, unless the context otherwise requires, its successors in office and assigns) of the First Part

AND

M/s _____ represented by Shri_____, Chief Executive Officer (hereinafter called the "Bidder" which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

*(The party of the First Part and the party of the Second Part are hereinafter collectively referred to as the **"Parties"** and individually as the **"Party"**)*

WHEREAS NHB proposes to procure _____ (name of the items/services) as mentioned in the RFP No._____ ("RFP") and the Bidder is willing to offer/has offered _____ (name of the items/services) as desired by NHB in terms of the RFP;

WHEREAS the Bidder is a private company/public company/Government undertaking/ partnership/registered export agency, constituted in accordance with the relevant law in the matter and NHB is a statutory body established under the Act of Parliament;

WHEREAS to avoid all forms of corruption by following a system that is fair, transparent and free from any influence/prejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to:-

(i) enabling NHB to obtain the desired said stores/equipment/services at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement and

(ii) enabling Bidders to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt

practices and NHB will commit to prevent corruption, in any form, by its officials by following transparent procedures.

AND WHEREAS the Parties hereto hereby agree to enter into this Integrity Pact on the terms and conditions mentioned hereinafter.

NOW IT IS THEREFORE AGREED BY AND BETWEEN THE PARTIES HERETO AS FOLLOWS:

1. Commitments of NHB

1.1 NHB undertakes that no official of NHB, connected directly or indirectly with the contract, will demand, take a promise for or accept, directly or through intermediaries , any bribe, consideration, gift, reward, favour or any material or immaterial benefit or any other advantage from the Bidder, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, Bid evaluation, contracting or implementation process related to the contract.

1.2 NHB will, during the pre-contract stage, treat all Bidders alike and will provide to all Bidders the same information and will not provide any such information to any particular Bidder which could afford an advantage to that particular Bidder in comparison to other Bidders.

1.3 All the officials of NHB will report to the appropriate Government office any attempted or completed breaches of the above commitments as well as any substantial suspicion of such a breach.

2. In case any such preceding misconduct on the part of such official(s) is reported by the Bidder to NHB with full and verifiable facts and the same is prima facie found to be correct by NHB, necessary disciplinary proceedings, or any other action as deemed fit, including criminal proceedings may be initiated by NHB and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by NHB the proceeding under the contract would not be stalled.

3. Commitments of Bidders

3.1 Compliance of the Instructions of GOI/Guidelines of CVC/Others: The Bidder undertakes that in case of its selection as the successful Bidder, it shall perform its duties under the Contract in strict compliance of the relevant and extant instructions of Government of India, GFR issued by Ministry of Finance, Guidelines of CVC and provisions of the Procurement Manual/relevant instructions of NHB, as applicable to the subject matter.

3.2 The Bidder represents that it has the expertise to undertake the assignment/contract and also has the capability to deliver efficient and effective advice/services to NHB under the contract in terms of the RFP.

3.3 The Bidder commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its Bid or during any pre-contract or post-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following:-

(a) The Bidder will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of NHB, connected directly or indirectly with the Bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the Bidding, evaluation, contracting and implementation of the contract.

(b) The Bidder has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees , brokerage or inducement to any official of NHB or otherwise in procuring the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Government for showing or forbearing to show favour or disfavor to any person in relation to the contract or any other contract with the Government.

(c)* The Bidder shall disclose the name and address of its agents and representatives including its foreign principals or associates.

(d)* The Bidder shall disclose the payments to be made by it to agents/brokers or any other intermediary, in connection with this Bid/contract.

(e)* The Bidder has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in any way to recommend to NHB or any of its functionaries, whether officially or unofficially to the award of the contract to the Bidder, nor has any amount been paid, promised or intended to be paid to any such individual, firm or company in respect or any such intercession, facilitation or recommendation.

(f) The Bidder, either while presenting the Bid or during pre-contract negotiations or before signing the contract, shall disclose any payments he has made, is committed to or intends to make to officials of NHB or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.

(g) The Bidder will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, Bid evaluation, contracting and implementation of the contract.

(h) The Bidder will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

(i) The Bidder shall not use improperly, for purposes of competition or personal gain or pass on to others, any information provided by NHB as part of the business relationship, regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The Bidder also undertakes to exercise due and adequate care lest any such information is divulged.

(j) The Bidder commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

(k) The Bidder shall not instigate or cause to instigate any third person to commit any of the actions mentioned above.

(l) If the Bidder or any employee of the Bidder or any person acting on behalf of the Bidder, either directly or indirectly is a relative of any of the officers of NHB or alternatively, if any relative of an officer of NHB has financial interest/stake in the Bidders firm, the same shall be disclosed by the Bidder at the time of filing of tender.

The term 'relative' for this purpose would be as defined in Section 6 of the Companies Act 1956.

(m) The Bidder shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employee of NHB.

(n) The Bidders shall disclose any transgressions with any other company that may impinge on the anti-corruption principle.

(o) The Bidder has not entered into any undisclosed agreement or understanding with other Bidders with respect of prices, specifications, certifications, subsidiary contracts, etc.

3.4 The Bidder undertakes and affirms that it shall take all measures necessary to prevent any possible conflict of interest and in particular commit itself to the following:

(a) The Bidder shall avoid any conflict of interest while discharging contractual obligations and bring, beforehand, any possible instance of conflict of interest to the knowledge of NHB, while rendering any advice or service.

(b) The Bidder shall act/perform, at all times, in the interest of NHB and render any advice/service with highest standard of professional integrity.

(c) The Bidder undertakes that in case of its selection as the successful Bidder, it shall provide professional, objective, and impartial advice and at all times and shall hold NHB's interests paramount, without

any consideration for future work, and that in providing advice it shall avoid conflicts with other assignments and its own interests.

(d) The Bidder declares/affirms that it has not been hired by NHB for any assignment that would be in conflict with its prior or current obligations to other employers/buyers, or that may place it in a position of being unable to carry out the assignment/contract in the best interest of NHB. Without limitation on the generality of the foregoing, the Bidder further declares/affirms as set forth below:

(i) **Conflict between consulting activities and procurement of goods, works or non-consulting services (i.e. services other than consulting services)** - The Bidder has not been engaged by NHB to provide goods, works, or non-consulting services for a project, or any affiliate that directly or indirectly controls, is controlled by, or is under common control with the Bidder. The Bidder is fully aware that it shall be disqualified from providing consulting services resulting from or directly related to those goods, works, or non-consulting services. Further, the Bidder is also aware of the fact that in case it has been hired to provide consulting services for the preparation or implementation of a project, or any affiliate that directly or indirectly controls, is controlled by, or is under common control with the firm, shall be disqualified from subsequently providing goods, works, or services (other than consulting services) resulting from or directly related to the consulting services for such preparation or implementation.

This provision does not apply to the various firms (IS Auditors, contractors, or suppliers) which together are performing the Bidder's obligations under a turnkey or design and build contract.

(ii) **Conflict among consulting assignments** – The Bidder understands that neither Bidder (including their personnel and sub-IS Auditors), nor any affiliate that directly or indirectly controls, is controlled by, or is under common control with the firm, shall be hired for the assignment that, by its nature, may be in conflict with another assignment of the Bidder. *As an example, Bidders assisting NHB in the privatization of public assets shall neither purchase, nor advise purchasers of, such assets. Similarly, Bidders hired to prepare Terms of Reference (TOR) for an assignment shall not be hired for the assignment in question.*

(iii) **Relationship with NHB's staff** – The Bidder is aware that the contract may not be awarded to the Bidder in case it is observed that it, including its experts and other personnel, and sub-IS Auditors, has/have a close business or family relationship with a professional staff of NHB (or of the project implementing agency) who are directly or indirectly involved in any part of: (i) the preparation of the TOR for the assignment, (ii) the selection

process for the contract; or (iii) the supervision of such contract, unless the conflict stemming from this relationship has been resolved in a manner acceptable to NHB throughout the selection process and the execution of the contract.

(iv) **A Bidder shall submit only one proposal either individually or as a joint venture partner in another proposal:** If the Bidder, including a joint venture partner, submits or participates in more than one proposal, all such proposals shall be disqualified. This does not, however, preclude a consulting firm to participate as a sub-IS Auditor, or an individual to participate as a team member, in more than one proposal when circumstances justify and if permitted by the RFP.

4. Previous Transgression

4.1 The Bidder declares that no previous transgression occurred in the last three years immediately before signing of this Integrity Pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any Public Sector Enterprise in India or any Government Department in India that could justify Bidder's exclusion from the tender process.

4.2 The Bidder agrees that if it makes incorrect statement on this subject, Bidder can be disqualified from the tender process or the contract, if already awarded can be terminated for such reason.

5. Accountability

5.1 The Bidder undertakes that in case of its selection as the successful Bidder and assignment of the contract to the Bidder, it shall be accountable for the advice/supply made/to be made and/or for any service rendered/to be rendered by it to NHB, keeping in view norms of ethical business, professionalism and the fact that such advice / services to be rendered by it for a consideration.

5.2 The Bidder shall be accountable in case of improper discharge of contractual obligations and/or any deviant conduct by the Bidder.

6. Personal Liability

The Bidder understands that in case of its selection as the successful Bidder, the Bidder is expected to carry out its assignment with due diligence and in accordance with prevailing standards of the profession. The Bidder shall be liable to NHB for any violation of this Integrity Pact as per the applicable law, besides being liable to NHB as may be provided under the service level agreement/contract to be executed.

7. Transparency and Competitiveness

The Bidder undertakes that in case of its selection as the successful Bidder, it shall keep in view transparency, competitiveness, economy, efficiency and equal opportunity to all prospective tenderers/Bidders, while

rendering any advice/service to NHB, in regard with matters related to selection of technology and determination of design and specifications of the subject matter, Bid eligibility criteria and Bid evaluation criteria, mode of tendering, tender notification, etc.

8. Co-operation in the Processes:

The Bidder shall cooperate fully with any legitimately provided/constituted investigative body, conducting inquiry into processing or execution of the consultancy contract/any other matter related with discharge of contractual obligations by the Bidder.

9. Sanctions for Violations

9.1 Any breach of the aforesaid provisions by the Bidder or any one employed by it or acting on its behalf (whether with or without the knowledge of the Bidder) shall entitle NHB to take all or any one of the following actions, whenever required:

(i) To immediately call off the pre contract negotiations without assigning any reason or giving any compensation to the Bidder. However the proceedings with the other Bidder(S) would continue.

(ii) The Earnest Money Deposit (in per-contract stage) and / or Security Deposit /Performance Bond/PBG (after the contract is signed) shall stand forfeited either fully or partially, as decided by NHB and NHB shall not be required to assign any reason therefor.

(iii) To immediately cancel the contract, if already signed, without giving any compensation to the Bidder.

(iv) To recover all sums already paid by NHB, and in case of an Indian Bidder with interest thereon at 2% higher than the prevailing Prime Lending Rate of State Bank of India, while in case of a Bidder from a country other than India with interest thereon at 2% higher than the LIBOR. If any outstanding payment is due to the Bidder from NHB in connection with any other contract, such outstanding payment could also be utilized and appropriated by NHB to recover the aforesaid sum and interest.

(v) To encash the advance bank guarantee and performance bond/warranty bond, if furnished by the Bidder, in order to recover the payments already made by NHB, along with interest.

(vi) To cancel all or any other contracts with the Bidder. The Bidder shall be liable to pay compensation for any loss or damage to NHB resulting from such cancellation /rescission and NHB shall be entitled to deduct the amount so payable from the money(s) due to the Bidder.

(vii) To debar the Bidder from participating in future Bidding process of NHB for a minimum period of five year which may be further extended at the discretion of NHB.

(viii) To recover all sums paid in violation of this Integrity Pact by Bidder(S) to any middleman or agent or broker with a view to securing the contract.

(ix) In cases where irrevocable Letters of Credit have been received in respect of any contract signed by NHB with the Bidder, the same shall not be opened.

(x) Forfeiture of Performance Bond/PBG in case of a decision by NHB to forfeit the same without assigning any reason for imposing sanction for violation of this Integrity Pact.

9.2 NHB will be entitled to take all or any the actions mentioned at para 10.1(i) to (x) of this Integrity Pact also on the Commission by the Bidder or any one employed by it or acting on its behalf (whether with or without the knowledge of the Bidder), of an offence as defined in Chapter IX of the Indian Penal Code, 1860 or Prevention or Corruption Act, 1988 or any other statute enacted for prevention of corruption.

9.3 The decision of NHB to the effect that a breach of the provisions of this Integrity Pact has been committed by the Bidder shall be final and conclusive on the Bidder. However the Bidder can approach the Independent Monitor(s) appointed for the purposes of this Integrity Pact.

10. Fall Clause:

The Bidder undertakes that it has not supplied/is not supplying similar product/systems or subsystems at a price lower than that offered in the present Bid in respect of any other Ministry/Department of the Government of India or PSU/Public Sector Bank and if it is found at any stage that similar product/systems was supplied by the Bidder to any other Ministry/Department of the Government of India or a PSU at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the Bidder to NHB, if the contract has already been concluded.

11. Disqualification & Forfeiture of EMD/PBG etc

The Bidder(s) agree(s) that:

(a) Prior to award of contract or during execution of the contract, if the Bidder (s) has/have committed any transgression/breach of this Integrity Pact, NHB is entitled to disqualify the Bidder(s) from the tendering process/terminate the contract.

(b) If NHB disqualifies the Bidders(s) from the tendering process prior to award of contract under clause (a) above, NHB is entitled to demand and recover the damages equivalent to the EMD and in such event, the EMD shall be forfeited.

(c) After selection of the successful Bidder and/or during execution of the contract, any breach/violation by the successful Bidder of this Integrity Pact under clause (a) above shall entail forfeiture of performance bond/Performance Bank Guarantee (PBG).

(a) It is agreed that the decision of NHB regarding forfeiture of EMD/performance bonds/ PBG shall be final and binding.

12. Independent External Monitors:

12.1 NHB has appointed Shri Lov Verma, IAS (Retd.)- lov_56@yahoo.com and Shri Hare Krushna Das, IAS (Retd.) - E-mail: hkdash184@hotmail.com as independent external monitors for the Integrity Pact in consultation with the Central Vigilance Commission

12.2 The task of the Monitors shall be to review independently and objectively whether and to what extent the Parties comply with the obligations under this Integrity Pact.

12.3 The Monitors shall not be subject to instructions by the representatives of the Parties and perform their functions neutrally and independently.

12.4 Both the Parties accept that the Monitors have the right to access all the documents relating to the project procurement including minutes of meeting.

12.5 As soon as the Monitor notices, or has reason to believe a violation of this Integrity Pact, he will so inform the Authority designated by NHB.

12.6 The Bidder accepts that the Monitor has the right to access without restriction to all project documentation of NHB including that provided by the Bidder. The Bidder will also grant the Monitor upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to sub-contractors. The Monitor shall be under contractual obligation to treat the information and documents (s) of the Bidder/sub-contractor with confidentiality.

12.7 NHB will provide to the Monitor sufficient information about all meetings among the Parties related to the project provided such meeting could have an impact on the contractual relations between the Parties. The Parties will offer to the Monitor the option to participate in such meeting.

12.8 The Monitor will submit a written report to the designated Authority of NHB within 8 to 10 weeks from the date of reference or intimation to him by NHB/Bidder and, should the occasion arise, submit proposals for correcting problematic situations.

13. Facilitation of Investigation:

In case of any allegation of violation of any provision to this Integrity Pact or payment of commission, NHB or its agencies shall be entitled to examine all the documents including the Books of Accounting of the Bidder and the Bidder shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

14. Law and Place of Jurisdiction:

This Integrity Pact is subject to Indian Law. Any dispute arising out of this shall be subject the jurisdictions of the Courts at New Delhi.

15. Other Legal Action:

The actions stipulated in this Integrity Pact are without prejudice to any other legal action that may follow in accordance with the provision of the extant law in force relating to any civil or criminal proceedings. However, the Parties shall not approach the Courts of Law while representing the matters to the Monitor/s and shall await the decision of the Monitor/s in the matter.

16. Validity:

16.1 The validity of this Integrity Pact shall be from date of its signing and extend up to 5 years or the complete execution of the contract to the satisfaction of both NHB and the Bidder, including warranty period, whichever is later. In case Bidder is unsuccessful, this Integrity Pact shall expire after six month from the date of the signing of this Integrity Pact.

16.2 Should one or several provisions of this Integrity Pact turn out or be invalid, the remainder of this Integrity Pact shall remain valid. In this case the Parties will strive to come to an agreement to their original intentions.

The Parties hereto sign this Integrity Pact on the day, month and year and at the place mentioned herein below.

For National Housing Bank	**For IS Auditor**
(Authorised Signatory)	**(Authorised Signatory)**
Place: **Date:**	**Place:** **Date:**
Witness **1.**_____ _____ **(Name & Address)** **2.**_____ _____ **(Name & Address)**	**Witness** **1.**_____ _____ **(Name & Address)** **2.**_____ _____ **(Name & Address)**

(* provisions of these clauses would need to be amended/deleted in line with the policy of NHB in regard to involvement of Indian agents of foreign suppliers.)