NHB (ND)/ Audit Department/Web-Publish & email/2021
August 31, 2021

राष्ट्रीय आवास बैंक
NATIONAL HOUSING BANK

<<Vendor Name >>
<<Address >>

Madam/Dear Sir,

Quotation for undertaking Information Security & Cyber Security Audit for the Year 2020-21(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 2020-21 (July-June). Necessary '**Requirement Proposal'** 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**' document 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.

- 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 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 2020-21(July-June)"** and must reach at the following address-

रा.आ.बैंक (नदि)/लेखा परीक्षा विभाग/ वेब-प्रकाशित और ईमेल / 2021
अगस्त 31, 2021

<< विक्रेता का नाम >>
<< पता >>

महोदया/महोदय,

वर्ष 2020-21 (जुलाई-जून) के लिए सूचना सुरक्षा एवं साइबर सुरक्षा लेखा परीक्षा करने हेतु कोटेशन

कृपया दिनांक 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 2020-21 (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 II** 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 छ: 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 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-विंडो मुहरबंद लिफाफे में संलग्न कर, उस पर **"वर्ष 2020-21 (जुलाई-जून) के लिए सूचना सुरक्षा तथा साइबर सुरक्षा लेखा परीक्षा करने हेतु वाणिज्यिक कोटेशन"** लिख कर निम्नलिखित पते पर भेंजे–

The Deputy 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 September 14th, 2021 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 the Bid document on or before **September 07, 2021 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.

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)
Deputy General Manager

Encl: As Above

उप 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 **14 सितंबर, 2021 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 **07 सितंबर, 2021 को शाम 6:00** बजे 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)
उप महाप्रबंधक

संलग्न: यथोपरि

For Undertaking Information Security & Cyber Security Audit for the Year 2020-2021(July-June)

"Requirement Proposal"

1. PROJECT

Most of the functions of 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.

NHB proposes to undertake Information Security Audit (ISA), 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 Information Security Audit (ISA) & Cyber Security Audit (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 (& amendments thereafter) and other standard international guidelines for the same.

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 20-June 21
2.	VAPT	Quarterly	July 21 -June 22

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 / Representative 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 representative 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, RO Mumbai & Regional Representative Offices (RROs) 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 & RROs	2 Mbps

Presently Bank has 10 no. of ROs & RROs at Ahmedabad, Bengaluru, Bhopal*, Chennai*, Guwahati*, Hyderabad, Lucknow*, Kolkata, Mumbai and Delhi.

**MPLS connectivity is yet to be provided*

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, DR Site and Internet broadband is available at Mumbai. 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 2008/ 2012/2016 platform - including SQL Server/ Outlook/SAP Servers and others	92

PCs	PLATFORM	NUMBERS
1. Client Machines on LAN	Windows Vista/7/Windows 8/10	176
2. Laptops/Mobile Computers	Windows 7/8/10	154

DR Site, Navi Mumbai

SERVERS	NUMBERS
Servers- on Windows 2008/ 2012/2016 platform- including SQL Server	14

PCs	PLATFORM	NUMBERS
1. Client Machines on LAN	Windows Vista/7/Windows 8/10	20
2. Laptops/Mobile Computers	Windows 7/8/10	7

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

3. PROJECT SCOPE OF WORK

This Information Security & Cyber Security Audit 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 Representative Offices at Ahmedabad, Bengaluru, Kolkata and Hyderabad and other places as mentioned above, which are connected to the centralized Data Centre located at Head Office. The Information Security & Cyber Security Audit will cover the access control mechanism implemented for these representative offices also.

The Information Security & Cyber Security Audit is to be conducted in following three phases:

PHASE – I EVALUATION

PHASE – II COMMUNICATION

PHASE – III REVIEW & CERTIFICATION/FINAL COMPLAINCE 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.

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.

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, ORMIS, 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 Code Audit of applications and portals developed in-house.

- 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. The details of Bank's web-facing applications/portals are as under:
    - ✓ SAP Employee Portal
    - ✓ GRIDS
    - ✓ ORMIS
    - ✓ PMAY-CLSS Portal

- ✓ RESIDEX
- ✓ Meeting Management Portal
- ✓ Virtual Office
- ✓ Automated Data Flow (ADF)

e. Evaluation of Cyber Security Framework, Policy, CSOC in lines with the guidelines as indicated in the RFP;
f. 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 guideline as indicted in the RFP.

PHASE – II: COMMUNICATION

1. **User Training**

   Creating awareness among NHB employees on issues related to IT & Cyber Security and impart training in security aspects. The training shall be carried out at Delhi in 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. Information and Cyber Security Audit 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 for the ISA & CSA

These are described in the following sub sections below: -

4.1. Information Security Audit & Cyber Security Audit

(Type - Services)

Under this project the vendor/ 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.

4.2. Vulnerability Assessment, Analysis and Resolution

(Type – Documentation & Service)

- Under this project the vendor/ 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).

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 IS Audit report and Cyber Audit 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 vendor/ selected empanelled auditor, the response received from the employees of the Bank and the vendor's / 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 vendor/ 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 vendor/ selected empanelled auditor is to provide NHB a certification/compliance report each for ISA and for CSA (separately)

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 IS Audit and Cyber Security audit 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. Procurement Policy
4. Hardware Disposal Policy
5. Cyber Security Framework

5. PROJECT SCHEDULE

After empanelment of IS & Cyber Security Auditors, from the list of empanelled IS & Cyber Security Auditors, commercial bids would be called and the L1 (lowest) bidder shall be selected for carrying out IS & Cyber Security Audit. The selected vendor/ selected empanelled auditor has to depute their officials at NHB Delhi and Mumbai for conducting IS and Cyber Security Audit 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 and that for Phase - II would be 2-3 weeks. An exercise to review the compliance with the findings and recommendations of IS & Cyber Security Auditor had to be undertaken by the vendor/ selected empanelled auditor (Phase - III). The exercise would be undertaken after 1-2 months of completion of the ISA and Cyber Security Audit 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 IS & Cyber Security Audit shall not exceed 6 months. 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.

6. PENALTY

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

7. INSTRUCTION TO BIDDERS:

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, along with Service Level Agreement (SLA) and Confidentiality cum Non-Disclosure Agreement (NDA) will be applicable, unless specified otherwise by NHB.

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 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.

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 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 2020-21(July-June)"** and must reach at the following address-

The Deputy 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 September 14th, 2021, 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 **September 07, 2021 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.

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

Ashish Jain, Regional Manager, Audit Department National Housing Bank, Head Office Core 5-A, 4th Floor, India Habitat Centre, Lodhi Road, New Delhi – 110003 Phone No : 011-39187107 Email: ashish.jain@nhb.org.in	Rounak Agrawal Assistant Manager Audit Department National Housing Bank Head Office Core 5 A, 4th Floor, India Habitat Centre, Lodhi road, New Delhi, 110003 Phone No: 011-39187259 Email: rounak.agrawal@nhb.org.in

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

8. SIGNING OF CONTRACT

The successful Bidder(s) will sign a Service Level Agreement (SLA), and the Confidentiality cum Non-Disclosure Agreement (NDA) with NHB within 30 days of award of the service order or within such extended period as may be decided by NHB. All expenses, stamp duty and other charges/ expenses in connection with the execution of the Agreement/s as a result of this RFP /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.

9. BID OPENING AND EVALUATION

The Bank will open the Commercial Bids, in the presence of Bidders 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 vendor/bidder based on marks scored during technical evaluation.

10. PAYMENT TERMS

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

- 50% 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 (2020-2021) and VAPT report for Quarter 1 (July 2021- Sept 2021).
- 10% on Submission of VAPT report for Quarter 2 (Oct 2021- Dec 2021)
- 10% on Submission of VAPT report for Quarter 3 (Jan 2022- March 2022)
- 20% on providing all deliverables as mentioned in RFP/Bid Document and/or Work Order {including Final Compliance reports of IS and Cyber Audit (2020-2021) and VAPT Reports (2021-2022)}.

Note: *If the selected vendor/empanelled auditor does not submit Bank Guarantee 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.*

वर्ष 2020-2021 (जुलाई-जून) हेतु सूचना सुरक्षा और साइबर सुरक्षा ऑडिट करने के सम्बन्ध में

"आवश्यकता प्रस्ताव"

1. परियोजना

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।

राष्ट्रीय आवास बैंक ने मौजूदा बुनियादी ढांचे की लोचता, सुरक्षा उपायों को बढ़ाने और उचित समय में सर्वोत्तम अंतरराष्ट्रीय प्रथाओं और मानकों को अपनाने के साथ आईटी इंफ्रास्ट्रक्चर सिस्टम, एप्लिकेशन और वेब फेसिंग एप्लिकेशन/पोर्टल्स की सूचना सुरक्षा ऑडिट (आईएसए), वीएपीटी और साइबर सुरक्षा ऑडिट (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।

ऑडिट निम्नलिखित आवृत्ति के अनुसार किए जाने हैं:-

क्र. सं.	ऑडिट का प्रकार	ऑडिट की आवृत्ति	सम्बंधित अवधि
1.	सूचना सुरक्षा ऑडिट एवं साइबर सुरक्षा ऑडिट	वार्षिक	जुलाई 20 - जून 21
2.	वीएपीटी	तिमाही	जुलाई 21 - जून 22

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।

एनएचबी 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 प्रतिनिधि कार्यालयों (आरआरओ) 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*, चेन्नई*, गुवाहाटी*, हैदराबाद, लखनऊ*, कोलकाता, मुंबई और दिल्ली में कुल 10 आरओ और आरआरओ हैं।

**एमपीएलएस कनेक्टिविटी प्रदान की जानी बाकी है*

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- विंडोज 2008/2012/2016 प्लेटफॉर्म पर - SQL सर्वर/आउटलुक/एसएपी सर्वर और अन्य सहित	92

कंप्यूटर	प्लेटफार्म	संख्या
1. लैन पर क्लाइंट मशीनें	विंडोज़ विस्टा/7/ विंडोज़ 8/10	176
2. लैपटॉप/मोबाइल कंप्यूटर	विंडोज़ 7/8/10	154

डीआर साइट, नवी मुंबई

सर्वर	संख्या
सर्वर- विंडोज 2008/2012/2016 प्लेटफॉर्म पर - SQL सर्वरसहित	14

कंप्यूटर	प्लेटफार्म	संख्या
1. लैन पर क्लाइंट मशीनें	विंडोज़ विस्टा/7/ विंडोज़ 8/10	20
2. लैपटॉप/मोबाइल कंप्यूटर	विंडोज़ 7/8/10	7

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

3. परियोजना हेतु कार्य का दायरा

अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

5. परियोजना डिलिवरबल्स

अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

6. परियोजना समयावधि

अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

7. दंड

अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

8. 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।

नोट: *यदि चयनित विक्रेता/सूचीबद्ध लेखापरीक्षक कार्य आदेश देने के एक महीने के भीतर बैंक गारंटी जमा नहीं करता है, तो कोई अग्रिम राशि जारी नहीं की जाएगी और पूरा भुगतान पूरी परियोजना के पूरा होने के बाद ही किया जाएगा।*

अनुलग्नक हेतु अंग्रेजी प्रस्ताव का सन्दर्भ लेने का कष्ट करें।

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.
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.

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
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.
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

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
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.
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 IP or 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.

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
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.
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 .

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
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.
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

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
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
68	SOC	% of higher priority incidents (P1 and P2) closed within 2 hrs	Percentage of higher priority (P1 and P2) incidents closed 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 to within 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

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
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.
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.

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
81	Cyber Security (SOC) Incident Closure Rate	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 month)*100	>=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 reduce the high percentage of such incidents.
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 cycle for 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.
101	Third Party Risk Assessments - RFI/RFP/Contracts Reviewed	All RFI/RFP/Vendor Contracts to be reviewed	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.

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
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 to be 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.
112	Other External/Regulatory Cyber Security Audits	Total Number of Issues reported in other audits / reviews 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 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 audit during the month	Number of audit observations that were reported during 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.

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
114	Audit Observations closed	Total number of audit observations to be closed 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.
124	Password Policy	All user accounts on AD/systems/network devices/applications/databases following password 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 per Bank's Password policy.

Sr No	Metrics Name	Opportunities	Defects	Metric Calculation	Compliance/Threshold			Periodicity	Responsibility	Action Required
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 administrator rights 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)

S. No.	Particulars	Amount / Rate (in ₹)
1.	For Undertaking Information Security Audit & Cyber Security Audit for Year 2020-21 (July -June) and Quarterly VAPT for Year 2021-22 (July -June)	
Total		

Bidders are requested to note the following-

a) The bidder must submit the commercial bid in the above format.
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 / Rate (in ₹) will 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.

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: