ANDHRA PRADESH MAHESH CO-OP. URBAN BANK LIMITED

(Multi-State Scheduled Bank)

H.O.: 8-2-680/1&2, Road No 12, Banjara Hills, Hyderabad – 500 034 (T.S.)

Ph.: 23437103, 23437105, 23437106.

Website: www.apmaheshbank.com E-mail: info@apmaheshbank.com

TENDER DOCUMENT FOR CONDUCT OF INFORMATION SECURITY (IS) AUDIT & VAPT (VULNERABILITY ASSESSMENT AND PENETRATION TEST) OF OUR BANK

Bank invites sealed Tenders from reputed companies Public / Private Ltd Companies for conduct of IS AUDIT & VAPT, as per the Scope of work given below. Bidders can also improvise on the scope of work with more contemporary solution, if felt**:**

I. SCOPE OF WORK - IS AUDIT:

SN.	Audit Objective – To review	Assessment Scope Description
1	IT & IS Governance	• Roles and Responsibilities and organizational framework • IT Organization structure and IT Team management • Alignment of IT objective with business objective • IT Policies and Procedures • IT Risk Assessment • Management commitment, Management review of monitoring, reporting and action taken.
2	Alignment of IT Strategy with Business Strategy	IT Governance related processes, Long term IT Strategy and Short term IT Plans, Information Security Governance, IT Security Policy and its implementation, IT Architecture.
3	Application Security – Physical & Logical Access Control	Assessment of physical & logical access control mechanism for all applications. IT Asset inventory management
4	Acquisition and implementation of packaged software	Requirement Identification and Analysis Processes, Vendor Selection Processes, Contracts, Implementation and Post Implementation issues.
5	Operating System Control	OS Version maintenance, adherence to licensing requirements, User account management, Logical access controls, System Administration, Maintenance of sensitive user accounts.

6	Application Systems and Controls	Logical access controls, Input controls, processing controls, Output controls, authorization controls, Data integrity / file continuity controls, Review Logs and audit trails.
7	Database Controls	Physical access protection, referential integrity and accuracy, administration of Databases Operational at Primary & DR Site, Indexing, Backup procedures etc..
8	Network Management	Network Infrastructure, Security architecture at Gateway Level, Maintenance & Monitoring of Network communication channels, Log management, Maintenance of the Infrastructure.
9	Change Management	Change management process, CRF Forms, Monitoring of the processes.
10	Web Facing Applications – Internet Banking	Web Server, ecommerce Authentication Application, SSL Certificate, Operational activity, PIN Mailer processes etc..
11	Privacy and Data Protection	Confidentiality of the Customer Data, Procedure of modification / deletion, media contents, authorized and un-authorized contents, Data Classification etc..
12	Business Continuity Management	BCP method, DR Infrastructure, Plan, RTO & RPO, User Management in case of Disaster, DR Drills, Application and Data Access Management
13	IT Infrastructure & Asset Management	Data Center Infrastructure, Records maintenance, Inventory of IT Asset, Policy implementations, Remote Management, Review of access controls, Power protection systems, Internal Hardware troubleshooting and Monitoring etc..
14	IT Operations Management	Capacity Management, Service continuity assurance to the business, Managed Services, Securing of Data, Backup Methods and its related maintenance, Vendor Management, Ticketing of user issues, System Maintenance, Release Management, Test and UAT, Development, Web facing applications – Internal & External, KRA and Segregation of duties. Data Centre Procedures, Change management Back-up and recovery procedures, Malware control procedures, IT Services outsourcing, Vendor/Service Provider management procedures, vendor service report monitoring, review and MIS. Asset/equipment maintenance, Network connectivity management, Patch management, Software license management, Purging of data, Help Desk

15	SLA / Agreements – Services and Applications Banking Application Software Security of CBS, Internet Banking, Mobile Banking, SMS, AML, ATM switch, RTGS, NEFT, CTS, Treasury, Trade Finance (BG/LC) and any other software – of each application	• Review of application security controls on input validation, processing control and output control. • Review of logical access controls of all applications • Review of controls on master, parameter settings, interest application • Review on changes or updations of applications through change management procedure • Review of SLA with vendor for application support • Review of various test reports confirming data integrity, data quality (Black box, White box testing) • Review of rectification/ action taken report of error logs, exception reports generated based on earlier audits and internal reviews. Fully fledged VAPT is to be done. • Review of user support, user feedback and user training on applications. • Work flow based data flow (for approvals, document submissions, etc.) – Design & suggest
16	IT Services Outsourcing	Contractual obligations of the IT outsourcing, Security and Privacy in External Contracts, Monitoring of the External Parties, Access Control for the External Parties, Risk based approach for external parties, Security controls w.r.t. external parties, Transitioning Risks
17	HR Controls	On Boarding and Termination Process, Background Checks, privacy and security statements, role based access controls
18	RBI Compliance	All the Security aspects as mandated by the Reserve Bank of India circulars: 1. RBI/2018-19/63 DCBS. CO. PCB. Cir. No. 1 / 18.01.000/2018-19 dated October 19, 2018 - Basic Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) 2. RBI/2019-20/129 DoS .CO / CSITE / BC .4083 / 31.01.052 / 2019-20 dated December 31, 2019 - Comprehensive Cyber Security Framework for Primary (Urban) Cooperative Banks (UCBs) – A Graded Approach 3. RBI/2019-20/130 DoS . CO / CSITE / BC. 4084 /31.01.015/2019-20 dated December 31, 2019 - Cyber Security controls for Third party ATM Switch Application Service Providers 4. RBI/2017-18/206 DBS (CO) . CSITE / BC .5 / 31.01.015 / 2017-18 dated June 21, 2018 -

		Control measures for ATMs – Timeline for compliance

II. SCOPE OF WORK: VAPT -VULNERABILITY ASSESSMENT AND PENETRATION TEST.

SN	Audit Objective – To review	Assessment Scope Description
1	White Box Testing – 25 IPs of the Application / Service related Servers	Performing the tests from within the Network with the knowledge of Network Architecture and the Systems. This is also referred as Internal VAPT Testing. Identify the Gaps and suggest the mitigation methods to the Bank.
2	Black Box Testing - 25 IPs of the Application / Service related servers	Performing Test from the external network without prior knowledge of the internal networks and systems. Auditor has to use various tools and technologies to enter into the Bank's network through public network and try to penetrate the network. Assessment of the Network devices and its related configurations, whether the security appliances are equipped with the relevant policies to protect the environment from un-authorized access & ongoing threats. Identify the gaps and suggest the mitigation methods to the Bank.
3	Review of Information Security Architecture of the Bank	Review of the Network, Application, Physical Security Infrastructure operational at the Bank. Connectivity configuration with third party networks i.e., NPCI, IDRBT(IFTAS), CTS, ASP etc.., Router Configurations, Fortigate Firewall, Web Firewall Configurations etc.. and suggest the gaps if any to the Bank.
4	For the Web application and online services, the OWASP Top Ten list served as a guide and the domains need to be tested	**Injection**. Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization. **Broken Authentication.** Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently. **Sensitive Data Exposure.** Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit

		card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser. **XML External Entities (XXE).** Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks. **Broken Access Control.** Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc. **Security Misconfiguration.** Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion. **Cross-Site Scripting XSS.** XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites. **Insecure Deserialization.** Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks. **Using Components with Known Vulnerabilities.** Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and

		APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts. **Insufficient Logging & Monitoring**. Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

The above scope of work is only the broad areas of Audit coverage. The scope may vary / include the existing parameters / guidelines of auditing as per the RBI / NPCI /other authorities from time to time. While IS Audit is to be done once, VAPT needs to be conducted twice with a gap of 6 months. Both needs to be validated after Bank attends to the observations made in the report.

Eligibility Criteria:

i. The bidder must have completed at least 5 years of experience/operation in the field of conducting IS Audit /VAPT for Banks / Financial Institutions. CERT.in accredited Auditor firms are prefered.

ii. The Bidder should be a Pvt Ltd or Public Ltd organization. In exceptions cases partnership firms are also accepted.

iii. The bidder must submit Certificates issued by Certified Authority / Regulatory authority.

Financial Capability of bidder :

Turn over should be minimum 3 crores for FY 2018-19, 2017-18, 2016-17. Documents evidencing the same are to be submitted with the bid.

Experience of bidder :

The bidder should have successfully executed at least three contracts of similar nature of IS Audit / VAPT preferably Banks, within the past three years as on 30-June-2020.

Schedule of The Tender:

Particulars	Tender Schedule Details
Tender Reference No	**APMB/IT/ IS AUDIT & VAPT/03/2020**
Date of release of the Tender	17.07.2020
Last date for submission of the Tender Document	**01.08.2020, 5.00pm**

Address for communication:
Deputy General Manager, IT Department
Andhra Pradesh Mahesh Cooperative Urban Bank Limited
Head Office - 8-2-680/1 & 2, Road No. 12,
Banjara Hills, Hyderabad-500 034, Telangana.
GSTIN- 36AABAT4652K1Z8
E-mail : info@apmaheshbank.com, website**: www.apmaheshbank.com**

Vendor has to submit the Commercial and Scope of Work Bids separately clearly specifying on the cover of the Tender Document.

Filled in Tender Documents should be submitted on or before 01.08.2020 by 5:00 P.M. at IT Department, Head Office at the above mentioned address. Bank reserves the right to accept or reject any/all the tender (s) without assigning any reason whatsoever.

DATE : **17*.07.2020*** **Sd/-**

PLACE : HYDERABAD **Deputy General Manager**