Stock Holding Corporation of India Limited

(StockHolding)

RFP Reference Number: IT-06/2024-25

Date: 09-Jul-2024

GEM Reference No. - GEM/2024/B/5144124

**Request for Proposal (RFP) for Supply, Implementation, Monitoring, Maintenance and Management of On-Premise Information Technology Service Management (ITSM)
And
Information Technology Asset Management (ITAM) Solutions for 05 (five) years**

DISCLAIMER

The information contained in this Request for Proposal (RFP) document or information provided subsequently to bidder(s) or applicants whether verbally or in documentary form by or on behalf of Stock Holding Corporation of India Limited (StockHolding), is provided to the bidder(s) on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided.

This RFP document is not an agreement and is not an offer or invitation by StockHolding to any parties other than the applicants who are qualified to submit the bids ("bidders"). The purpose of this RFP is to provide the bidder(s) within formation to assist the formulation of their proposals. This RFP does not claim to contain all the information each bidder may require. Each bidder should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice. StockHolding makes no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. StockHolding may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP.

RFP Document Details

Sr. No.	Description	Remarks
1	Name of Organization	Stock Holding Corporation of India Limited
2	RFP Reference Number	IT-06/2024-25
3	Requirement	RFP for Supply, Implementation, Monitoring, Maintenance and Management of On-premise Information Technology Service Management (ITSM) and Information Technology Asset Management (ITAM) Solution for 05 (five) years
4	Interest free Earnest Money Deposit (EMD) [*]	Rs.2,00,000/- (Indian Rupees Two Lakhs only) by way of RTGS/NEFT to be paid to Stock Holding Corporation of India Limited as Earnest Money Deposit should be submitted separately before submission of online bids by way of RTGS/NEFT on StockHolding's Bank Account No.: 004103000033442 Bank: IDBI Bank (Nariman Point Branch) IFSC: IBKL0000004. Please share the UTR details to us on below mentioned email address.
5	Email Id for queries up to Pre-Bid Meet	PRIT@stockholding.com
6	Date of Issue of RFP Document	09-Jul-2024
7	Date, Time and place for online Pre-bid meeting	16-Jul-2024 11:00 AM For participation in pre-bid meeting, please send mail for online meeting link to PRIT@stockholding.com before 15-Jul-2024 04:00 PM
8	Last Date for Submission of Online Bid	30-Jul-2024 05:00 PM
9	Date of opening bid	30-Jul-2024 05:30 PM

[*] - Bidders registered under Micro, Small and Medium Enterprises (MSME) for specific trade are exempted from EMD. Bidders shall upload the scanned copy of necessary documents as part of eligibility criteria documents.

This bid document is not transferable.

StockHolding reserves the right to modify/update activities/ dates as per requirements of the process.

Table of Contents

SUBMISSION OF PROPOSAL

StockHolding invites e-tender through GeM Portal, in two bid system (Technical and Commercial bid), from firm/company for Supply, Implementation, Monitoring, Maintenance and Management of On-premise Information Technology Service Management (ITSM) and Information Technology Asset Management (ITAM) Solutions for StockHolding.

Submission of Bids:

The online bids will have to be submitted within the time specified on website https://gem.gov.in/ the following manner:-

1. Technical Bid (.pdf files)
2. Commercial Bid (.pdf files)

Invitation for bids:

This "Invitation for bid" is meant for the exclusive purpose of "Supply, Implementation, Monitoring, Maintenance and Management of On-premise Information Technology Service Management (ITSM) and Information Technology Asset Management (ITAM) Solutions for StockHolding" as per the terms, conditions, and specifications indicated in this RFP and shall not be transferred, reproduced or otherwise used for purposes other than for which it is specifically issued.

Due Diligence:

The bidder is expected to examine all instructions, Forms, Terms, Conditions and Specifications in this RFP. Bids shall be deemed to have been made after careful study and examination of this RFP with full understanding of its Implications. The Bid should be precise, complete with all details required as per this RFP document. Failure to furnish all information required by this RFP or submission of Bid not as per RFP requirements will be at the bidder's risk and may result in rejection of the bid and the decision of StockHolding in this regard will be final and conclusive and binding.

Cost of Bidding:

The bidder shall bear all costs associated with the preparation & submission of its bid and StockHolding will in no case be held responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

Contents of this RFP Document:

The requirements, bidding procedure, general terms & conditions are prescribed in this RFP document with various sections

a Bidder Details – Annexure 1
b Requirement with Scope of Service and Terms and Conditions
c Format for Eligibility Criteria - Annexure 2
d Technical Compliance – Annexure 3
e Format for Price Bid (Commercial) Bids - Annexure 4
f Integrity Pact (Text) - Annexure 5
g Covering Letter of Integrity Pact - Annexure 6
h Compliance Statement – Annexure 7
i Format of Bank Guarantee – Annexure 9

Clarifications regarding RFP Document:

a Before bidding, the bidders are requested to carefully examine the RFP Document and the Terms and Conditions specified therein, and if there appears to be any ambiguity, contradictions, gap(s) and/or discrepancy in the RFP Document, they should forthwith refer the matter to StockHolding for necessary clarifications.

b A bidder requiring any clarification for their queries on this RFP may be obtained via email to PRIT@StockHolding.com

c StockHolding shall not be responsible for any external agency delays.

d StockHolding reserves the sole right for carrying out any amendments / modifications / changes in the bidding process including any addendum to this entire RFP

e At any time before the deadline for submission of bids / offers, StockHolding may, for any reason whatsoever, whether at its own initiative or in response to a clarification requested by bidders, modify this RFP Document.

f StockHolding reserves the rights to extend the deadline for the submission of bids, if required. However, no request from the bidders for extending the deadline for submission of bids, shall be binding on StockHolding.

g StockHolding reserves the right to amend / cancel / postpone / pre-pone the RFP without assigning any reasons.

h It may be noted that notice regarding corrigendum/addendums/amendments/response to bidder's queries etc., will be published on StockHolding's website only. Prospective bidders shall regularly visit StockHolding's same website for any changes/development in relation to this RFP.

i It may be noted that bidder mentioned in the document may be either OEM/Distributor/System Integrator (SI).

Validity of offer:

The offer should remain valid for a period of at least **90 days** from the date of submission.

ELIGIBILITY CRITERIA (Documents to be Submitted Online)

Guidelines to be followed prior to submitting an application-

Bidder should upload all supporting documents at the time of submission duly signed and stamped on their company's letter head.

SI. No	Criteria	Documents to be submitted by Bidder
1	The Bidder should be a registered Company in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013 and should be operating in India for the past 05 (five) years with experience of Implementation or Maintenance ITSM and ITAM Solutions in India for at least 03 (three) years.	Copy of Certificate of Incorporation issued by the Registrar of Companies and Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory
2	Should have an average annual turnover of at least Rs. 05 (five) Crores per annum for last three financial years (2020-21, 2021-22 and 2022-23). It should be of individual company and not of Group of Companies	Certificate from CA mentioning annual turnover for last three financial years.
3	Bidder should have Positive Net worth in the last 03 (three) audited financial years	Certificate from CA mentioning profit/loss for the past three financial years.
4	Bidder should not be blacklisted by any Government, Government Body, PSU, Bank, Autonomous body and any other entity for any reasons within last 2 years from the RFP date.	Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory
5	Bidder should be either OEM or OEM the Authorized Partner / Reseller of the Proposed Solution on the date of RFP, with an authority to sell, upgrade, supply, service and maintain the proposed Solution. Note: Either OEM or their authorized partner should participate in the RFP. In case, both OEM & his authorized partner participate, only bid of the OEM will be considered.	Bidder needs to provide Manufacturer Authorization Form (MAF) from OEM stating that bidder is authorized partner of OEM and authorized to participate in this tender and in case the bidder is not able to perform obligations as per contract during the contract period, contracted services will be provided by OEM within the stipulated time.
6	Bidder should have experience of supply & implementation of ITSM and ITAM solution of minimum 02 (two) projects during the past 03 (three) years in India.	Copy of Purchase Orders / Completion Certificate
7	Bidder should have Support office at MMRDA Region.	Bidder to provide office address along with GST details.

BIDS PREPARATION AND SUBMISSION DETAILS

The online bids will have to be submitted within the time specified on website https://gem.gov.in/. Bidders must familiarize (if not already) with the Portal and check/ fulfil the pre-requisites to access and submit the bid there.

Submission of Bids

a The required documents for Eligibility Criteria, Commercial Bid must be submitted (uploaded) online on GeM portal. Eligibility Criteria and Commercial Bid should be complete in all respects and contain all information asked for in this RFP document

b The offer should be valid for a period of at least **90 days** from the date of submission of bid.

c The Bidder shall fulfil all statutory requirements as described by the law and Government notices. The Bidder shall be solely responsible for any failure to fulfil the statutory obligations and shall indemnify StockHolding against all such liabilities, which are likely to arise out of the agency's failure to fulfil such statutory obligations.

d The bidders are expected to examine all instructions, forms, terms, project requirements and other information in the RFP document(s). Failure to furnish all information required as mentioned in the RFP document(s) or submission of a proposal not substantially responsive to the RFP document(s) in every respect will be at the bidder's risk and may result in rejection of the proposal.

e Delayed and/or incomplete bid shall not be considered.

f There may not be any extension(s) to the last date of online submission of Eligibility Criteria details and commercial Price bids. This will be at the sole discretion of StockHolding.

Evaluation of Bids

StockHolding will evaluate the bid submitted by the bidders under this RFP. The Bidder needs to comply with all the Eligibility criteria and Technical Compliance criteria mentioned in the RFP to be evaluated for evaluation. Noncompliance to any of the mentioned criteria would result in outright rejection of the bidder's proposal. The decision of *StockHolding* would be final and binding on all the bidders to this document. Bidders who qualify in Eligibility and Technical evaluation will eligible for Commercial bid evaluation. L1 bidder will be selected based on the lowest quote submitted. Further, StockHolding reserves the right to negotiate with L1 bidder and based on the negotiation price submitted, order will be placed to the selected bidder.

StockHolding may accept or reject an offer without assigning any reason what so ever. The bidder is required to comply with the requirement mentioned in the RFP. Non-compliance to this may lead to disqualification of a bidder, which would be at the discretion of *StockHolding*.

REQUIREMENT

Stockholding inviting bids from firm/company for Supply, Implementation, Monitoring, Maintenance and Management of On-premise Information Technology Service Management (ITSM) and Information Technology Asset Management (ITAM) Solutions for StockHolding for the period of 05 (five) years.

Description	Requirement
Required License Type	Perpetual
Number of Years for Annual Maintenance & Support (AMS), if Perpetual	Required
How many number of AD Domains to be managed?	1
How many number of helpdesk technicians needs access?	6 users
Endpoint MFA(Multi Factor Authentication) add on	For 3000 machines
No. of Domain users need access to the Self Service Console	3000 users
IT Technician for ITSM tool	50 users
Nodes	4000

Scope of Work

StockHolding intends to procure the IT Service Management (ITSM) and IT Asset Management (ITAM) solutions along with commissioning, installation, implementation, maintenance, monitoring & management etc. The modules of required solutions/product are mentioned below:

A. Service Management

1. Ticketing
2. Service Desk
3. Change & Request Management
4. Incident & Problem Management
5. Knowledge Management
6. SLA Management
7. Configuration management
8. Request Management Modules, Service Catalog
9. Workflow & Orchestration
10. Built-in MIS reports

B. Asset Management with Discovery

1. Hardware Asset Management
2. Software Asset Management.

Type of Licenses: Perpetual Mode

Scope involves the provisioning and management of mentioned ITSM & ITAM Solutions, based on the StockHolding's requirement as stated below:

- The Bidder should provide all required software licenses and detailed Scope of Work (SoW) for ITSM and ITAM Solutions of the RFP. The bidder should provide perpetual licenses /subscriptions for all software components proposed in the solution in the name of StockHolding Corporation of India. The Software licenses proposed for all the components should be independent of hardware.
- Bidder should provide details of recommended hardware specifications (itemized) required to host the entire solution.
- All the Solutions should be deployed in the StockHolding's DC/DR on-premises setup. The public cloud based solutions should not be proposed under this RFP and if proposed, will not be considered.

- The Successful bidder must submit a letter from the OEM confirming the "Back- to-Back" agreement / arrangement for next 5 years to StockHolding Corporation of India.
- The implementation shall be done by OEM, the bidder shall do back to back tie- ups with OEM for the same. The bidder shall have Implementation Plan with OEM Implementation methodology duly signed by OEM and Bidder.
- Technical and functional documentation of the entire project and relevant SOPs should be submitted to StockHolding in Printed / Digital Book Format before signoff.
- Solutions should effectively and efficiently manage operations and security posture of the StockHolding by preparing for and responding to cyber risks/threats, facilitate business continuity and recovery from cyber-attacks / incidents.
- The bidder shall ensure Support & Subscription services from the OEM with unlimited number of support requests remote support, access to product updates/upgrades and 24x7 supports for Severity Level-1 issues.
- The proposed solutions shall be tightly integrated with all existing setup and new infrastructure /Assets of the StockHolding. The selected bidder shall supply, implement and maintain these IT Tools/ Solutions for StockHolding's IT Infrastructure for a period of 5 years.

General Scope:

- The bidder shall provide complete services for the solutions under the scope including installation, implementation, integration, management, maintenance, support, audit compliance and knowledge transfer.
- The solution shall include all components and subcomponents like software licenses, accessories and the bidder should supply other components at no extra cost to the StockHolding. (Required for commissioning of the solution as a part of RFP).
- The bidder shall ensure that during various phases of implementation, the performance, security, network availability, etc. of the existing network setup must not be compromised.
- The bidder should ensure compliance with various standards such as The bidder should ensure compliance with various standards such as ISO 27001:2013, ISO 27001:2022, Soc2 Type2, ISO 22301 or higher standards etc..
- The bidder shall follow all respective technical/statutory guidelines, validations, System Context Design (SCD) should be implemented, checked & verified, and related reports including SOP, SCD, Software Integrity Certificate and VAPT Clearance must be submitted, duly certified by OEM to the StockHolding for sign off the successful installation.
- The solutions should be scalable, designed and deployed throughout the IT infrastructure of the StockHolding.
- The solution deployment should be compliant with StockHolding's CISP (The Cyber Security Information Sharing Partnership), IT and Cyber policies, internal guidelines, regulatory standards and countrywide regulations and laws from time to time.
- The proposed solution should be able to integrate with SIEM, Active Directory/ LDAP (Lightweight Directory Access Protocol) / PIM (Privileged Identity Management) for user authentication or with any other solution/ tool as stated by the StockHolding in order to have control and visibility.
- The URLs of the management server/software of proposed solution should be accessible on HTTPS/TLS 1.3 or latest Protocol with valid certificate.
- The Proposed solution should be free from any kind of vulnerabilities and as and when vulnerabilities are notified by the StockHolding, regulators, Govt. of India or any other Govt agencies, it should be patched within prescribed time.
- The bidder shall install the solution On-site at StockHolding DC (Mumbai) and StockHolding DR (Bangalore) and implement the same at all branches/offices of StockHolding.

- The solution should standardize ITIL (Information Technology infrastructure library) processes for StockHolding requirements related to change, incident, problem, configuration management, SLA and asset management etc.
- The Proposed solution should be able to work with or without an agent in the StockHolding's environment.
- The bidder shall be responsible for on-premise installation and commissioning of the proposed solution along with database, storage and any other components required for solution for fulfilment of scope.
- The bidder should engage OEM for onsite implementation of the respective solutions. The bidder/OEM shall ensure necessary engagement and deputation of skilled professionals for the smooth implementation up to sign off of the Project. OEM support should include advising and helping StockHolding in implementing controls for the risk advised by various regulators from BFSI sectors/Govt. of India.
- The bidder should follow a standard process to ensure that proposed solution meets functional, security performance and regulatory requirements of StockHolding.
- The selected bidder must generate and provide a complete holistic signoff report before handover to ensure 100% serviceability of delivered solution.
- The bidder must provide detailed architecture of the provided solution/ every module along with installation and administration guide, which must include high-level design (HLD), and Low Level Design (LLD) along with Technical bid.
- The configuration as per the technical and other specifications offered of all equipment and other items must be operational / functional and installed from day one.
- The bidder shall confirm the integrity of the software supplied i.e. the software is free from bugs, malware, covert channels in code etc. and Integrity certificate should be submitted to the StockHolding as per the related format.
- The proposed solution shall have the ability to freely change forms, fields, workflows, escalations and authorization structures and reports according to StockHolding requirements/processes without affecting the future tool updates and integration with other /third party Solutions.
- Solution shall have centralized architecture with web or Graphical User Interface (GUI) based dashboard console to monitor, reporting, notification, maintaining and policy push for the registered users centrally. This should be a single console for service management, infra management and configuration management.
- Remote access capabilities on its management interface should be supported by the software via HTTPS or SSH access.
- Role based administration like Administrator, Database Reader and Read-only access users shall be mandatorily supported in the solution.
- Solutions should be capable of adding exceptions.
- Solution should have built in reports and can generate custom reports such as Executive Report, Detection Life Cycle Report, and End Point Compliance Report, Top 10 reports for different categories and Health Reports etc.
- Solution should provide reports in HTML / CSV / Excel and other required formats. All reports should be configured to generate auto or scheduled responses and send via SMTP on daily/monthly/yearly as per the StockHolding requirement.
- The solution should provide scheduling and customization of the reports along with flexibility.
- The bidder must have an arrangement with the OEM such that the bidder/ StockHolding's SI/ StockHolding should be able to log a call with the OEM directly.
- The bidder should have a 24x7x365 days support contact center in order to log the calls. The contact center numbers should be provided to StockHolding along with the escalation matrix mentioning the contact person's name, number and designation in the company.
- All the industry standard protocols for functioning, detection of risks, mitigation should be supported and complied by the respective solution.

- The scope of the services and maintenance is to be provided for a period of Five (5) years from the date of acceptance by StockHolding (i.e. 1-year warranty and 4 years ATS post warranty).
- The bidder shall provide perpetual licenses and the StockHolding is free to procure ATS for all or part of the licenses provided in this contract.
- The bidder shall arrange for OEM Certification/ training within three months of sign off/ deployment for every solution thereafter once in every year to the StockHolding team and resources involved.
- The selected bidder shall install and configure the software provided as per the timelines and uptime/ SLA levels prescribed in the RFP.
- The services/ solutions offered should be modular, scalable both horizontally & vertically, and should be able to address StockHolding's requirements during the period of contract and even beyond future license figures given.
- The bidder shall provide all the software/accessories/related tools supplied that shall be compatible with IPv6 and comply with all latest security protocols/industry standards. The proposed solution shall be TLS 1.3 or higher ready.
- Deployment of solution requires coordination with different service provider has/ project application vendors. The bidder shall coordinate with the all solution providers/ vendors while installing and ensure installation and commissioning for running the application. The bidder shall coordinate with all other vendors for seamless integration, implementation and operations. The selected bidder must generate and provide a complete holistic signoff report before handover to ensure 100% serviceability of delivered solution.
- StockHolding has a complex infrastructure with multiple resources maintained and managed through multiple vendors. The bidder shall coordinate with all other vendors for seamless integration, implementation and operations.
- The bidder shall implement all the functionalities proposed in the technical specifications & demonstrate the same to the StockHolding team for complete sign off the solution.
- The bidder shall prepare the SOPs (Standard Operating Procedures) with periodical review as per industry practices and regulatory guidelines. The drafted SOPs shall be submitted to the StockHolding for its review and Approval.
- The bidders shall also provide the following documents as part of the deliverables of the project.
  - Original manuals of all proposed software/applications
  - Standard Operating Procedures
  - Installation & Technical Configuration Documents
  - Network & Security Design Documents (Will be approved by the StockHolding)
  - Troubleshooting Manual
  - Executive summary report for the project to the management
  - Functional and operational requirements
  - Project design/plan
  - Product description
  - Guidance for best practices, implementation guidelines
  - User acceptance test plan, if any
  - Training materials
  - Once a year health check-up report by OEM.

- The bidder shall configure the SLA Levels for all applications (including tools & software) in IT Service Management tool with the functionality of auto- escalation of incident/ticket to appropriate StockHolding authorities in case of breach of defined timelines for resolution of incident/ticket.
- The solution should be fully standards compliant, scalable, and ideal for businesses of all sizes.
- System shall be scalable enough to support clustered deployment for high availability.
- The bidder shall supply all modules, Software Applications with required licenses and do the installation, integration configuration & deployment of the solution at the StockHolding's DC and DR Site.

- Post implementation of the solution, the scope of bidder contains support for the following activities, but not limited to, from time to time, in relation to maintenance and upgrades/updates/patches:
  - IOS Upgrades / up to date patching,
  - Troubleshooting & Performance Tuning,
  - Upgrades of supplied software,
  - Advisories on software upgrades & vulnerabilities,
  - DR Drills,
  - VA/ PT Compliance/Audit /Review as per StockHolding's requirement /Statuary guidelines
  - Any support required to make system & solution up and running as per SLA.
- The list mentioned above is an indicative list; however, the successful bidder should provide end-to-end support and repair for any activities and resolution of any issues related to new deployment without any extra cost to the StockHolding.
- The bidder shall replace and upgrade the out-of-support, out-of-service, end- of-life (EOL), and end of support (EOS) as soon as the respective OEM announced the same at no additional cost to the StockHolding throughout the 5 years of contract period. The bidder shall carry out such replacement & up gradation of components (Tools & Software) before due date. Failure to replace within three months of intimation by StockHolding will be treated as violation of SLA, StockHolding will procure the new solution as same, and cost will be deducted from payables/ payments as penalty or by invoking performance guarantee.
- During the period of the contract, all upgrades/updates or requirements in software, licensing, implementation of upgrades/patches/version changes etc., due to whatsoever reason including but not limited to EOL or EOS, shall be done by the bidder within stipulated time but not later than one month without any additional cost to the StockHolding. EOS/EOL solution will not be accepted and if any solution is declared EOS/EOL during the period of contract, the bidder shall do the necessary upgrade as stated above.
- The bidder shall inform to StockHolding if any new version/update/service pack/upgrade of the proposed solution is released by OEM, within seven (7) days of such release and provide the upgraded solution within one month of such release without any cost to the StockHolding covering all parts, labour and accessories at the respective locations (DC and DR) of the StockHolding during the period of the contract.
- The patches (critical / non-critical) as and when released by OEM, for the proposed solution to be tested first in test environment, and thereafter deployed, installed and configured by bidder's team at StockHolding's site, as per StockHolding's requirement during the contract period without any additional cost to StockHolding.
- Post installation of Solution with its components including VA & PT (Vulnerability Assessment & Penetration Testing) shall be conducted and StockHolding Info Sec Team will provide a report to the vendor. All findings/issues pointed out in the report to be complied/fixed before production of the software (All components i.e. Database, application). The InfoSec Team and Other statutory authorities conduct review/ audit of the solutions time to time. All such Audit reports including VAPT Reports to be compiled/attended by bidder/OEM within the timelines, during the entire period of contract also conduct periodic review audit of the database and application.
- The bidder shall adhere to the Service Level Agreements (SLA) and regular monitoring and reporting it to the StockHolding.
- The bidder shall conduct preventive maintenance as may be necessary from time to time (Minimum Once in a year) to ensure that equipment is in efficient running condition to ensure trouble free functioning.
- The bidder shall make DR to be made identical to DC and able to run with full load at any point in time. The bidder shall do quarterly DC and DR cutover for the solution running from DR and DC respectively and submit a report to the StockHolding.
- The proposed solutions shall be tightly integrated with all existing setup and new infrastructure/Assets of the organisation. The selected bidder shall supply, implement and maintain these IT Tools/ Solutions

for StockHolding's IT Infrastructure for a period of 5 years including all the upgrades/patches/enhancement of the solution from time to time and also as per the StockHolding's future enhancements/regulatories requirements. The scope of the services and maintenance is to be provided for a period of Five (5) years must be from the date of acceptance by StockHolding (i.e. 1-year warranty and 4 years ATS post warranty). The bidder shall provide perpetual licenses and StockHolding is free to procure ATS for all or part of the licenses provided in this contract.

- The bidder should keep the StockHolding explicitly informed about the end of support dates of the related products and should ensure support during the warranty and ATS period.
- The bidder shall do regular backup of the solutions as per the defined StockHolding's backup policy.
- The Bidder shall be responsible for delivering the solution and its support post implementation. The proposed solutions should be integrated with StockHolding's existing and new Security Solutions. In case, if any OEM can't integrate with a third party monitoring tool for an OEM product, then the bidder needs to bundle OEM tools in his response to the bid. (Performance, Availability, Patching, Monitoring, Dashboard with Graphical representation).
- A solution shall not be a "point of failure" in the flow of network traffic; failure of one or more of the solution components should not affect the functionality of the organizational network. The solution should be capable of being bypassed in the event of any failure of the solution.
- The overall Technical support with comprehensive maintenance shall be of 5 years. (From the starting of the project till end of 5th year).
- If during the contract period, the solution is not performing as per specifications in this RFP, the bidder shall upgrade/ enhance the solution or put additional services and reconfigure the system without any extra cost to the StockHolding till the required performance is achieved.
- The proposed solutions must be integrated with existing StockHolding infrastructure and Network.
- The bidder should provide the complete documentation including technical, operations, user manual, design documents, process documents, technical manuals, functional specification, system configuration documents, system/database administrative documents, debugging/ diagnostics documents, test procedures etc. The bidder shall share all kinds of procedures/ documents upon any level or version changes, clarification, corrections and modifications in the above-mentioned documents in a timely manner.
- The vendor must provide an alert service for any problems with the service being unavailable. This can be in the form of e-Mails and should be sent to all concerned in the escalation matrix. The bidder should integrate with the StockHolding's Email Service for sharing the alerts /email with the respective Team as per escalation matrix on a proactive basis.
- The proposed solutions should be scalable tools and architecture to suffice future growth.
- Service Desk Management (Change Management, Incident Management, Problem Management, Request Fulfil management and knowledge management) and Ticketing with CMDB.
- The proposed solution should do complete end-to-end Asset Management of all hardware and software assets.
- Event Correlation and fault-finding - from user to network layer to server layer to application code.
- Single console view for Troubleshooting, Remediation and Root Cause Analysis (RCA) for service impacts.
- Availability of different dashboards for different business services.
- On Demand Dashboard for daily & historic network health, reports with web and mobile supported.
- The bidder shall ensure end to end completion of all activities initiated as part of the project. The bidder shall coordinate with other stakeholders also for completion of activity.
- The bidder shall integrate all StockHolding assets (Servers, Storage and Network Devices) in the monitoring tools and provide the unified dashboard for monitoring and management.
- To install and configure comprehensive monitoring of end to end IT Services (Network, Server, Storage, Appliance, Database and Applications across locations.

<u>Scalability for ITSM & ITAM Solutions</u>

- The services/ solutions offered should not require any major Network Architecture change in existing Network Architecture or existing device replacement on the part of the StockHolding Except Following-
  - There are some solutions, which will be in line, and need architecture and data flow to reroute changes without which the solutions cannot be deployed.
  - Port mirroring for solutions that work on Mirror traffic.
- The Solution should be able to keep one-year data online while backup of older data more than one year till five years shall be backed up using StockHolding's proposed backup solution with solution's application, and restorable whenever required by solution's application.
- The solution cost offered shall be inclusive of all predicted/ unpredicted expenses to meet the scope as mentioned in the RFP.
- The Proposed Solution should support all heterogeneous OS, Database, Hypervisor, Container Platforms etc.
- High Availability in DC and DR in the StockHolding environment wherever proposed by the StockHolding.
- The proposed solution must support onboard retention of logs for a period of minimum 6 months.
- The critical data / database should be stored in encrypted form as per Information Security Guidelines.
- Proposed solutions should have very high-scale architecture on a platform that scales efficiently. The solution should also support 64-bit architecture environments for high scalability. Solution should support installation on Windows and various flavors of the Linux environment. Solutions should have extensible architecture for easy integration and automation. Solution installation should support Dockers Containers & Virtual cloud for easy, deployment and building on premises **(VMware virtualisation Platform)**. Should support multiple-deployment options - centralized, distributed and hybrid deployments with option for a centralized operations console view. The architecture should support High Availability inbuilt into the product.
- The bidder shall be responsible for on-prim installation and commissioning of the proposed solution along with database, storage and any other components required for solution for fulfillment of scope.
- The proposed solutions should comply with **StockHolding's ISMS policies, Internal Guidelines, Regulatory Standards and external regulatory compliances from SEBI, RBI, NSDL, CDSL, IRDAI, DPDP Act 2023** and any other financial services related regulatory requirements with updates from time to time.
- The successful bidder has to complete End-to-End Implementation (Supply, Installation, Implementation, Integration, Customisation, management, support, Training & Knowledge Transfer, Sign-off etc.,) within 12 weeks with a detailed plan.
- As per StockHolding's ISMS policies approximately there will be 50-60 templates. The exact count will be given to the successful bidder during the implementation phase. The total time period to customise required templates will be 45 days.
- For customization of templates additional 45 days will be given apart from the 3 months of End-to-End Implementation period. Payment for the customization will be depending on the number of templates which will be freezed by the successful bidder and StockHolding.

Scope of Services

All features mentioned below are part of Mandatory Requirements and these have to be made available in the solution. The following are mandatory technical and functional requirements that must be met to remain eligible for consideration. Bidder must clearly show that your product meets all of these mandatory technical and functional requirements. Those that do not clearly demonstrate they meet all of the mandatory technical and functional requirements shall be rejected by StockHolding without further consideration.

A. Information Technology Service Management (ITSM)

Capabilities	Compliant (Y/N)
Incident management	
The tool should be able to create tickets from multiple sources including emails, web forms, chat messages or phone calls	
The tool should be able to convert incidents into service requests and vice versa	
The tool should allow the service desk team to collect all relevant information from requesters with custom incident and request templates	
The tool should allow technicians to create shared or separate catalogs for incidents and service requests	
The tool should allow service desk admins to provide role-based access to technicians and end users	
The tool should allow service desk admins to restrict end user access to request templates based on site, category, and user groups.	
The tool should allow technicians to link, merge or clone incidents	
The tool should allow service desk admins to create custom categories, subcategories and items	
The tool should automatically assign categories to tickets based on the ticket parameters	
The tool should automatically assign tickets to technicians based on algorithms like round-robin and load balancing or based on ticket parameters like category, priority, impact and more	
The tool should allow service desk admins to view the list of all available technicians	
The tool should allow service desk admins to monitor technician availability, and setup backup technicians for unavailable technicians	
The tool should allow service desk admins and technicians to send a broadcast message to all logged-in technicians	
The tool should be able to automatically determine the priority of a request based on the impact and urgency	
The team should allow service desk admins to preconfigure incident lifecycles to handle various incidents	
The tool should automatically assign SLAs based on ticket parameters	
The tool should allow technicians to handle requests from VIP users with high priority	
The tool should help technicians search the knowledge base for a solution from within a request and copy the resolution into it	
The tool should allow technicians to create problems and changes from the within an incident	
The tool should allow technicians to collaborate with other technicians and groups by sharing the incident	
The tool should allow technicians to get real-time updates from other technicians working on the same ticket	
The tool should enable service desk admins to mandate fields and mark tasks that to be completed for incident closure	
The tool should allow technicians to create worklogs and record the cost, effort and time taken to resolve the incident	
The tool must be able to send out user surveys when the incident is closed	
Problem management	

The tool should allow technicians to create problems from an incident	
The tool should allow technicians to associate incidents and changes to problems	
The tool should allow technicians to mark a problem as known error	
The tool should facilitate technicians to analyse the impact of a problem and document it	
The tool should facilitate technicians to identify and documents symptoms and root cause of a problem	
The tool should allow technicians to provide a temporary solution for a problem with a workaround	
The tool should allow technicians to provide a permanent solution for the problem	
The tool should enable technicians to break up a problem resolution into multiple tasks and assign them to different technicians	
The tool should allow technicians to create a change record to further resolve the underlying issues if needed	
The tool should allow technicians to copy problem solution and workaround to all associated incidents	
The tool should allow technicians to automatically close all associate incidents on closure of the problem	
The tool should allow technicians to create worklogs and record the cost, effort and time taken to resolve the problem	
Change management	
The tool should allow technicians to create changes from incidents and problem with information carried over	
The tool should allow technicians to collect all the necessary information with custom change templates	
The tool should allow service desk admins to create different type of changes, and create unique workflows for each of these	
The tool should help service desk teams involve the right stakeholders by defining change roles	
The team should allow technicians to create elaborate change plans with impact analysis, roll out, back out and downtime plans	
The tool should allow service desk teams to maintain a checklist of essential steps to be completed	
The tool should allow service desk admins to form multiple change advisory boards	
The tool should allow service desk teams to configure multiple levels of approvals	
The tool should allow technicians to breakdown changes into tasks	
The tool should allow technicians to handle change implementation as projects	
The tool should allow technicians to track all associated incidents and problems causing and caused by the change	
The tool should allow service desk teams to schedule downtime and announce them to key stakeholders	
The tool should allow service desk teams to conduct and document post implementation review	
The tool should allow service desk admins and change managers to create distinct change workflows	

The tool should allow service desk admins and change managers to configure various actions like conditions, notifications, field updates and approvals within the change workflow	
Asset management	
The tool should allow service desk managers to build a detailed asset inventory	
The tool should allow service desk teams to discover and inventory all their windows machines	
The tool should allow service desk teams to discover and inventory all other devices including Macs, Linus machines, printers, and other network devices	
The tool should allow service desk teams to discover and inventory assets from multiple sites	
The tool should allow service desk teams to scan and discover assets using barcodes	
The tool should allow service desk teams to discover and inventory all their software	
The tool should allow service desk teams to inventory all available licenses with suite licensing, ability to upgrade and downgrade licenses	
The tool should allow service desk teams to create multiple license types for each manufacturer	
The tool should allow service desks teams to track and manage the compliance of multiple software licenses	
The tool should allow service desk teams to keep track of all assets in a central location	
The tool should allow service desk admins to configure multiple asset states	
The tool should allow service desk teams automatically scan all assets at set intervals	
The tool should allow service desk admins to configure depreciation for assets	
The tool should allow service desk teams to loan, and track loaned assets	
The tool should allow service desk teams to create standard and custom asset reports	
CMDB (Configuration Management Database)	
The tool should allow service desk admins to define CIs with custom CI types	
The tools should allow service desk teams to configure graphical views of CIs and their relationship maps	
The tool should allow service desk teams to create unique relationship maps specific to all key services	
The tool should allow service desk teams to import CIs through a CSV file	
The tool should allow service desk teams to import CI relationships through an XLS file	
The tool should allow technicians to export the relationship maps as PNG or PDF	
Purchase management	
The tool should allow service desk admins to manage asset and service purchases in a central location	
The tool should allow service desk admins to track purchases in multiple currencies	
The tool should allow service desk teams to associate multiple service request to a purchase order	

The tool should allow service desk admins to configure 5 levels of approvals for Purchase Orders	
The tool should allow technicians to add invoice and payment information	
The tool should allow service desk teams to integrate purchase management with asset management processes	
Contract management	
The tool should allow service desk teams to manage all contracts from one place	
The tool should allow service desk teams to associate multiple assets to a contract	
The tool should allow service desk teams to create child contracts within the contracts	
The tool should allow service desk teams to associate costs for each contract	
The tool should allow service desk admins to configure automatic notifications for a contract expiry	
Project management	
The tool should allow service desk admins to create custom project templates and types	
The tool should allow technicians to track the progress of projects using Gantt chart	
The tool should allow service desk admins to define level of access for various users to each project	
The tool should allow service desk teams to break down the project into smaller manageable chunks	
The tool should allow technicians to export the Gantt map and project overview map as PDFs	
Service catalog	
The tool should allow service desk admins to create multiple service templates under appropriate service categories	
The tool should allow service desk admins to configure custom service request templates	
The tools should allow service desk admins to automate templates through condition-based activities like mandating fields, populating fields, enabling and disabling fields based on ticket criteria during creating or after editing the ticket	
The tool should allow service desk admins to make the template dynamic with condition-based actions like hiding or showing fields in real time based on the information given by the requester	
The tool should enable service desk admins to associate costs to assets, and account them during the request creation	
The tool should allow easy integration of the service catalog and CMDB	
The team should allow service desk admins to provide role-based access to each service request template	
The tool should allow service desk admins to configure roles like department in-charge, and managers to approve service requests	
The tool should allow service desk admins to configure a multi-stage approval process	
The tool should automatically associate SLAs and business rules to service request templates	
The tool should allow service desk admins to associate multiple tasks to each service request template	

The tool should allow service desk admins to configure a visual mapping of the task execution sequence for each service request template	
Self-service	
The tool should allow service desk admins to configure unique service desk portal for technicians and end users	
The self-service portal should allow easy access to incident and service catalog	
The self-service portal should allow users to view announcements and access the knowledge base	
The tool should automatically suggest related solutions based on the subject of the request during request creation	
The tool should automatically mention related announcements based on the subject of the request during request creation	
Knowledge management	
The tool should allow service desk admins and technicians to publish solutions to the knowledge base with an approval process	
The tool should allow service desk admins to organize solution under relevant topics	
The tool should allow service desk admins to configure role-based access and site-based access to each solution	
The tool should allow service desk admins to configure resolution templates for repeat requests with the same solution	
The tool should allow service desk admins to set expiry dates for solutions	
Reports	
The tool should allow technicians to generate reports easily with pre-built standard reports	
The tool should allow technicians to create custom reports, and custom query reports	
The tool should allow technicians to create custom dashboards with role-based access	
The tool should allow technicians to organize reports under custom report folders	
The tool should allow technicians to create reports of multiple types including tabular, matrix, summary, audit or CI history reports	
The tool should allow technicians to depict reports visually as pie charts, bar charts, line charts, time series charts, area charts or ring charts	
The tool should allow technicians to export reports into CSV, HTML, XLS and PDF formats	
The tool should allow technicians to schedule reports at a specific frequency	
The tool should allow technicians to generate reports and automatically share with it users	
User surveys	
The tool should allow technicians to create separate surveys for incidents and service requests	
The tool should allow technicians to create surveys with multiple question types including rating, opinion scale, binary and radio	
The tool should allow technicians to configure user surveys in multiple language	
The tool should allow technicians to configure when and under what conditions a survey has to be triggered	

The tool should allow service desk admins to collate data from survey reports for analysis	
IT and business integrations	
The tool should integrate with end point management tools to perform desktop and mobile device management activities from within the service desk console	
The tool should integrate with network monitoring devices to automatically convert network alerts into service desk tickets and automatically assign them to technicians and notify them	
The tool should integrate with business analytics tools for in-depth analysis	
The tool should integrate with application monitoring tools out-of-the-box	
The tool should integrate with enterprise password management applications out-of-the-box, to establish a strict authentication process for launching secure remote session from the service desk	
The tool should integrate with AD management applications to allow users and technicians to perform AD Management activities from the service desk	
The tool should have an out-of-the-box integration with SCCM	
The tool should allow event-driven API calls for easy third-party integrations	

B. Active Directory(AD) Manager

Active Directory Manager	Compliant (Y/N)
Create new users individually or in bulk via user creation templates or CSV files.	
Locate and modify the attributes of multiple users at once using user modification templates or CSV files.	
The tool serves as a centralized password manager for bulk password management, automated password reset, and actionable password reports.	
Enable or disable multiple user accounts and also specify the account expiry date, in a single action.	
Bulk move AD users across OUs.	
Delete or disable users in bulk to cleanup your AD.	
Add/remove users from groups, set primary groups of users, and more.	
Create multiple AD security and distribution groups, and assign various group attributes at once.	
Bulk move groups to a different OU/container.	
Delete multiple AD groups, in bulk, at once.	
Bulk create and modify AD contacts and the respective attributes.	
Delete AD contacts individually or in bulk by importing a CSV containing the list of contacts to be deleted.	
Create and modify shared, room, equipment, and linked mailbox in groups, at once, using templates.	
Bulk create, delete, and move OUs with just mouse clicks.	
Grant, modify, revoke NTFS and Share permissions of multiple users and groups. Configure and manage Netapp and Isilon servers as well.	
Create and manage GPOs and GPO links.	
Obtain general password reports and password status reports on different users.	
Generate general group reports, member-based reports, and reports based on the group type.	
Fetch general computer reports and account status reports of all computers in your AD.	

Obtain general Exchange reports, reports based on the delivery recipient settings, and feature- based reports.	
Stay on top of all the information about contacts such as the list of all contacts, mail enabled contacts, recently created/modified contacts, and more.	
View which users have access to terminal services and their properties.	
Utilize general GPO-related reports and reports involving GPO scope, status, and settings.	
Obtain OU-related information such as users/computers-only OUs, recently created/modified OUs, and more.	
View, analyze, and modify NTFS and share permissions or ACLs assigned to Windows or NetApp servers, folders, and files.	
View information about users' password and account lockout policies and the printers available in specific domains.	
Demonstrate product compliance with various regulatory compliance mandates such as SOX, HIPAA, PCI, FISMA, GLBA, and GDPR.	
Gain in-depth information on all, active, and suspended Google Workspace users.	
Generate reports based on LDAP queries and custom attributes of AD objects.	
Export all reports to multiple formats such as PDF, XLS, CSV, and HTML.	
Automate report generation and emailing of reports to user-specified email addresses.	
Create and manage Azure AD users, groups, contacts, and licenses.	
Manage Exchange mailboxes, shared mailboxes, and calendars.	
Generate reports on Azure AD users (including passwords, user logon, and account status), groups, contacts, and licenses.	
Obtain reports on Exchange mailboxes (including content, shared mailbox, and account status reports) and OWA.	
Create and assign custom roles with the selected tasks to delegate to help desk technicians, to empower them to perform those tasks, only in the specified domains/OUs.	
List all the operations performed by help desk technicians in your environment.	
View the list of all actions (creation, deletion, and modification) performed on help desk technicians and roles.	
Configure a second authentication method (Single sign on, two factor authentication, or smart card authentication) to login to the product.	
List all available help desk technicians, along with details such as delegated roles and administrative limits.	
View the logon details of help desk technicians, along with details such as their logon status, and authentication methods for all their logons.	
Define an order of execution for management operations, with different checkpoints like request, review, approve, and execute.	
Create workflow requests for AD objects creation (users) and modification (users, computers, contacts, groups.)	
View the list of all requests created by a technician and the requests that are assigned to that technician.	
Configure multiple workflow agents (requesters, reviewers, approvers, and executors) and define the roles of each of them.	
Create rules to assign requests to appropriate technicians automatically.	
Employ full automation or controlled automation to carry out any management/administrative task such as AD cleanup, group membership management,	
Automate a sequence/series of tasks and also specify the intervals at which each task in the sequence should be executed.	
Create personalized naming formats as per your organization's policies with this custom naming format builder.	

Add/remove titles, departments, offices, and companies based on your organization's needs.	
Configure a custom format that has to be adhered to, for generating random passwords.	
Set up domain-specific delete and disable policies that will be executed whenever user accounts are disabled or deleted.	
Configure custom notification profiles, high availability, and integrations with various third- party applications.	
While exporting reports, password protect the files for added security.	
Allow users to reset their Active Directory domain passwords without admin intervention.	
Allow users to unlock their Active Directory domain accounts without admin intervention.	
Notify users about impending password expiration.	
Notify users about impending account expiration.	
Update cached credentials when users reset their passwords even if they are not connected to the corporate network.	
Integrate password self-service with your review and approval-based help desk software.	
Limit the number of times that users can reset passwords and unlock accounts in a specific duration.	
Notify users when their password is reset or changed or their account is unlocked successfully.	
Schedule automatic password reset and account unlock for users with expired passwords and locked-out accounts respectively.	
A maximum of three authentication factors can be configured for MFA in addition to passwords.	
Secure self-service password resets and account unlock attempts using MFA.	
Protect Windows, macOS, and Linux logins with MFA.	
Verify the user’s identity during VPN logins using MFA.	
Secure endpoints supporting RADIUS authentication, like Citrix Gateway, VMware Horizon, and Microsoft Remote Desktop Gateway.	
Force users to enrol with the product when they log in to their machines.	
Remind users of product enrolment through email or SMS.	
Enrol users without their intervention by importing enrolment data through CSV files or external databases.	
Use Active Directory attribute values to enrol users automatically for SMS and email OTP.	
Automatically synchronize users’ Active Directory passwords with cloud applications and other on-premises systems.	
Allow users to access all their cloud apps after logging in only once.	
Allow users to update their Active Directory information without admin intervention.	
Let users subscribe or unsubscribe from mail groups of their choice.	
Provide admins and users with an option to search and view information about themselves and other domain users.	
Let users find their position in the organization hierarchy.	
Analyzes and displays the strength of the password being created.	
Enforce Active Directory password history settings during password reset.	
View a graphical representation of password statuses, user actions, and enrolment data.	
The product includes built-in reports to audit user actions and user statuses.	
Get reports on locked-out users and users with expired or soon-to-expire passwords.	
Available reports:	

Locked-out users	
Users with soon-to-expire passwords Users with expired passwords	
Get reports on reset passwords, unlocked accounts, identity verification, and user login attempts. Available audit reports:	
Reset passwords Unlocked accounts Self-update Changed password Notification delivery	
Identity verification failure User attempts	
Get reports on enrolled users, non-enrolled users, and licensed users. Available reports:	
Enrolled users	
Configure custom password policies for domains, organizational units, and groups using these password policy rules: Number of special characters to include: X. Number of numeric characters to include: X. Number of unicode characters: X Must contain at least X uppercase characters. Must contain at least X lowercase characters. Password must begin with an uppercase alphabet, a lowercase alphabet, a special character, or a number. Restrict numerals as the last character. Restrict the use of a character more than X times consecutively. Restrict the use of X consecutive characters from the username. Restrict the use of X consecutive character(s) from the old password. Number of old passwords to be restricted during password reset: X. Restrict palindrome passwords. Restrict the use of dictionary words. Restrict the use of specific patterns. Minimum password length: X. Maximum password length: X. **Or** A specific number of special, numeric, and unicode characters must be included. A minimum number of uppercase and lowercase letters must be used. An uppercase letter, a lowercase letter, a special character, or a number must be the first character. A number is restricted from being the last character. A character cannot be used consecutively more than a specific number of times. Consecutive characters from the username or an old password cannot be used. A specific number of old passwords can be restricted from use during password reset. Palindromes, dictionary words, and patterns can be restricted. A minimum and maximum password length can be fixed.	
The authentication methods supported out of the box for MFA are:	
Fingerprint/Face ID authentication YubiKey authentication	
Microsoft Authenticator Google Authenticator	
Zoho OneAuth TOTP authentication Custom TOTP authenticator	
Duo Security	
Push notification authentication QR code-based authentication TOTP authentication	
Email verification SMS verification RSA SecurID	
RADIUS authentication SAML authentication AD security questions	
Security questions and answers Smart card authentication	

- At least 3 out of the available options should be implementable as per StockHolding's existing Infrastructure.

Active Directory Self-Service Management

Active Directory Self-Service Management	Compliant (Y/N)
Allow users to reset their Active Directory domain passwords without admin intervention.	
Allow users to unlock their Active Directory domain accounts without admin intervention.	
Notify users about impending password expiration.	
Notify users about impending account expiration.	
Update cached credentials when users reset their passwords even if they are not connected to the corporate network.	
Integrate password self-service with your review and approval-based help desk software.	
Limit the number of times that users can reset passwords and unlock accounts in a specific duration.	
Notify users when their password is reset or changed or their account is unlocked successfully.	
Schedule automatic password reset and account unlock for users with expired passwords and locked-out accounts respectively.	
A maximum of three authentication factors can be configured for MFA in addition to passwords.	
Secure self-service password resets and account unlock attempts using MFA.	
Protect Windows, macOS, and Linux logins with MFA.	
Verify the user's identity during VPN logins using MFA.	
Secure endpoints supporting RADIUS authentication, like Citrix Gateway, VMware Horizon, and Microsoft Remote Desktop Gateway.	
Force users to enrol with the product when they log in to their machines.	
Remind users of product enrolment through email or SMS.	
Enrol users without their intervention by importing enrolment data through CSV files or external databases.	
Use Active Directory attribute values to enrol users automatically for SMS and email OTP.	
Automatically synchronize users' Active Directory passwords with cloud applications and other on-premises systems.	
Allow users to access all their cloud apps after logging in only once.	
Allow users to update their Active Directory information without admin intervention.	
Let users subscribe or unsubscribe from mail groups of their choice.	
Provide admins and users with an option to search and view information about themselves and other domain users.	
Let users find their position in the organization hierarchy.	
Analyzes and displays the strength of the password being created.	
Enforce Active Directory password history settings during password reset.	
View a graphical representation of password statuses, user actions, and enrolment data.	
The product includes built-in reports to audit user actions and user statuses.	
Get reports on locked-out users and users with expired or soon-to-expire passwords.	
Available reports:	
Locked-out users	
Users with soon-to-expire passwords Users with expired passwords	
Get reports on reset passwords, unlocked accounts, identity verification, and user login attempts. Available audit reports:	

Reset passwords Unlocked accounts Self-update Changed password Notification delivery	
Identity verification failure User attempts	
Get reports on enrolled users, non-enrolled users, and licensed users. Available reports:	
Enrolled users	
Configure custom password policies for domains, organizational units, and groups using these password policy rules: Number of special characters to include: X. Number of numeric characters to include: X. Number of unicode characters: Must contain at least X uppercase characters. Must contain at least X lowercase characters. Password must begin with an uppercase alphabet, a lowercase alphabet, a special character, or a number. Restrict numerals as the last character. Restrict the use of a character more than X times consecutively. Restrict the use of X consecutive characters from the username. Restrict the use of X consecutive character(s) from the old password. Number of old passwords to be restricted during password reset: X. Restrict palindrome passwords. Restrict the use of dictionary words. Restrict the use of specific patterns. Minimum password length: X. Maximum password length: X. Or A specific number of special, numeric, and unicode characters must be included. A minimum number of uppercase and lowercase letters must be used. An uppercase letter, a lowercase letter, a special character, or a number must be the first character. A number is restricted from being the last character. A character cannot be used consecutively more than a specific number of times. Consecutive characters from the username or an old password cannot be used. A specific number of old passwords can be restricted from use during password reset. Palindromes, dictionary words, and patterns can be restricted. A minimum and maximum password length can be fixed.	
The authentication methods supported out of the box for MFA are:	
Fingerprint/Face ID authentication YubiKey authentication	
Microsoft Authenticator Google Authenticator	
Zoho OneAuth TOTP authentication Custom TOTP authenticator	
Duo Security	
Push notification authentication QR code-based authentication TOTP authentication	
Email verification SMS verification RSA SecurID	
RADIUS authentication SAML authentication AD security questions	
Security questions and answers Smart card authentication	

- At least 3 out of the available options should be implementable as per StockHolding's existing Infrastructure.

C. Active Directory Audit

Active Directory Audit	Compliant (Y/N)
Get information on all logon activity, from logon failures to logon history, across domain controllers, Windows Servers, and workstations.	

Get notified of a lockout and receive information on the source of the authentication failure from an extensive list of Windows components such as Windows services, scheduled tasks, network drive mappings, and more.	
Get information on changes to AD objects such as users, computers, groups, organizational units (OUs), DNS, schema, sites, PSO objects, and more.	
Get information on changes to	
Group Policy Objects (GPOs) and their settings, such as password policy, account lockout policy, and more.	
Get information on changes in AD permissions across OUs, groups, users, computers, schema, configuration, DNS, and more.	
Get information on all activities performed by privileged users in the domain.	
Get information on the old and new values of changed attributes in the domain.	
Get information on all successful and failed logons.	
Get information on all user and device management actions.	
Get information on membership changes to groups and dynamic groups, and the assignment and removal of roles to users.	
Get information on applications that have been added, updated, and deleted, and consent given to APIs.	
Get information on changes to users' and groups' licenses.	
Get contextual information like a user's on-premises Distinguished Name, SID, and GUID.	
Get information on file read, create, modify, delete, rename, move, and other actions.	
Get information on failed attempts to read, write, and delete files.	
Get information on file DACL and SACL changes.	
Get information on remote desktop connections and remote logons occurring via Remote Desktop Gateway (RDG) servers and RADIUS Network Policy Servers (NPS).	
Get information on both successful and failed AD FS logons.	
Get information on the first in, last out, active, and idle time spent by employees at their workstations.	
Get information on local user and group management actions.	
Get information on changes to local security policy.	
Get information on changes to system, program, and other critical local files.	
Get information on usage and file activity across printers and removable storage devices such as USBs, external hard drives, and more.	
Get information on scheduled tasks that have been created, deleted, or modified, and processes that have been started or stopped.	
Get information on who is viewing or modifying local admin credentials.	
Get information on PowerShell processes that run on Windows Servers, along with the commands executed in them.	
Leverage Active Directory Audit’s machine learning capabilities to establish activity patterns and spot subtle anomalies such as an unusual volume of logon failures.	
Get notified via email and SMS about critical activities such as when a user is added to privileged or sensitive groups.	
Define thresholds based on volume, time, and other criteria to spot suspicious activities like mass file access.	
Execute scripts to automate response actions, like shutting down a device or disabling an account once an alert gets triggered.	
Get a complete audit trail of who did what, when, and from where, with	

Create reports to meet specific business needs.	
Tracking down specific information contained in reports quickly.	
Get a visual representation of audit data.	
Export reports to multiple formats such as PDF, XLS, CSV, and HTML.	
Automate generation of reports at user defined time intervals.	
Automate emailing of reports to user specified email addresses	
Retain audit data safely for as long as you want.	
Forward audit data to Syslog servers and other SIEM solutions.	
Exclude data that's irrelevant to audits based on user, file type, and other criteria.	
Access the product over the web.	
Grant different users varying levels of access to the product.	
Leverage both agentless and agent- based audit data collection.	

Service Level Agreement (SLA) and Penalty

The bidder needs to execute a Service Level Agreement with the StockHolding covering all terms and conditions of this tender. Bidder need to strictly adhere to Service Level Agreements (SLA). This solution has to be available 24x7 and hence any technical problem should be resolved as per below SLA from the time of lodge of complaint. The bidder needs to strictly adhere to Service Level Agreements (SLA).

Sl. No	Severity	Severity Description	Response Time	Resolution Time	Penalty Amount (Rs.)
1	Moderate - Severity 1	The issue is severe in nature, but database/ Application server services are available with restricted operations and some manageable workarounds. However, it cannot be functioned for a long with available workarounds.	Within 4 hours of call reported/ informed.	24 Hours	Rs.2000/- for every hour beyond resolution time
2	Normal- Severity 2	Minor loss of service and the impact of the issue could be minor in nature which may require some workaround to bring the normal functioning.	Within 8 hours of call reported/ informed.	48 Hours	Rs.1000/- for every hour beyond resolution time

Contract Duration

Successful bidder shall enter into contract for the period of 05 (five) years. The bidder will provide support and maintenance of the software during the support period of 01 year and ATS for 04 years with back to back arrangements with the respective OEMs.

Terms and Conditions

A. Payment:

Milestone	Payment Term
One Time Implementation Cost On Successful completion of Implementation and Project Signoff	100%
Software / License Cost of the Product on Delivery and Acceptance of delivery	100%
Software Support /ATS for 5 years	Annual payment on submission of Invoice
Customization of templates (50 nos.)	On pro-rate basis for each template

Taxes & levies:

a. Applicable TDS will be deducted (recovered) from the payment(s).
b. Applicable Penalty/Penalties may be recovered from payment.
c. Payments will be released only after submission and verification of the required Bank Guarantee (BG). No payment will be made to successful bidder, until the BG is submitted.

B. Location Details:

The Proposed solution being procured will be delivered & installed on PR (Primary Data Centre) site in Mumbai and Disaster Recovery (DR) Site- Bangalore for all StockHolding Branches/Offices.

Refund of Earnest Money Deposit (EMD):

a. EMD will be refunded through NEFT to the successful bidder on providing (a) an acceptance confirmation against the PO issued by *StockHolding* and (b) submission of Performance Bank Guarantee wherever applicable and should be valid for 30 days beyond the contract period.
b. In case of unsuccessful bidders, the EMD will be refunded to them through NEFT within 15 days after selection of successful bidder subject to internal approval of *StockHolding*.

Performance Bank Guarantee (PBG):

Successful Bidder shall, at own expense, deposit with the *StockHolding*, within seven (7) days on issuance of PO, a Bank Guarantee (BG) for the value of 5% of the Contract Value from scheduled commercial banks as per Annexure - 8. This Bank Guarantee shall be valid up to 60 days beyond the completion of the contract period. No payment will be due to the successful bidder based on performance, until the BG is submitted.

Bank Guarantee may be discharged / returned by *StockHolding* upon being satisfied that there has been due performance of the obligations of the Bidder under the contract. However, no interest shall be payable on the Bank Guarantee.

StockHolding reserves the right to invoke the BG in the event of non-performance by the successful bidder.

Force Majeure

Neither the StockHolding nor the Bidder shall be responsible for any failure to fulfil any term or condition of the CONTRACT if and to the extent that fulfilment has been delayed or temporarily prevented by a Force Majeure occurrence, defined as "Force Majeure". For purposes of this clause, “Force Majeure” mean an event beyond the control of the Parties and which prevents a Party from complying with any of its obligations under this Contract, including but not limited to: acts of God not confined to the premises of the Party claiming the Force Majeure, flood, drought, lightning or fire, earthquakes, strike, lock-outs beyond its control, labour disturbance not caused at the instance of the Party claiming Force Majeure, acts of government or other competent authority, war, terrorist activities, military operations, riots, epidemics, civil commotions etc.

The Party seeking to rely on Force Majeure shall promptly, within 5 days, notify the other Party of the occurrence of a Force Majeure event as a condition precedent to the availability of this defence with particulars detailed in writing to the other Party and shall demonstrate that it has taken and is taking all reasonable measures to mitigate the events of Force Majeure. And, all Parties will endeavor to agree on an alternate mode of performance in order to ensure the continuity of service and implementation of the obligations of a party under the Contract and to minimize any adverse consequences of Force Majeure. Each PARTY shall bear its own cost in relation to the force majeure occurrence.

However, any failure or lapse on the part of the Bidder to mitigate the damage that may be caused due to the above-mentioned events or the failure to provide adequate disaster management/recovery or any failure in setting up a contingency mechanism would not constitute force Majeure, as set out above.

If the duration of delay exceeds ninety (90) consecutive or one hundred eighty (180) cumulative days, StockHolding and the Bidder shall hold consultations with each other in an endeavor to find a solution to the problem. Notwithstanding above, the decision of the StockHolding, shall be final and binding on the bidder.

Dispute Resolution

In the event of any dispute arising out of or in connection with this Order, the parties shall use their best endeavour to resolve the same amicably AND if the dispute could not be settled amicably, the matter shall be settled in the court under Mumbai jurisdiction only. The final payment will be released only after the Bidder complies with above-mentioned clause

Right to alter RFP

a. StockHolding reserves the right to alter the RFP terms and conditions at any time before submission of the bids.
b. StockHolding reserves the right to modify, amend, alter and/or cancel the entire RFP at any stage without assigning any reason whatsoever. We further understand and accept that StockHolding's decision in this regard will be final and binding on all bidders.

Integrity Pact

The Bidder will have to enter in to an Integrity Pact with StockHolding. The format (text) for the Integrity Pact is provided as Annexure-5. The successful Bidder will have to submit a signed and stamped copy of the Integrity Pact by the authorized signatory of the successful Bidder.

Non-Disclosure Agreement (NDA)

The successful Bidder will sign a Non-Disclosure Agreement (NDA) with StockHolding for the contract period. The draft text of the NDA will have to be approved by legal department of StockHolding.

Indemnity

The Bidder should hereby indemnify, protect and save StockHolding against all claims, losses, costs, damages, expenses, action suits and other proceedings, resulting from infringement of any patent, trademarks, copyrights etc. or such other statutory infringements in respect of all the equipment offered by the Bidder. Any publicity by Bidder in which name of StockHolding is used should be done only with the explicit permission of StockHolding.

Subcontracting

As per scope of this RFP, sub-contracting is not permitted. The bidder shall not assign or sub-contract the assignment or any part thereof to any other person/firm.

Termination Clause

StockHolding reserves right to terminate the contract by giving 90 days prior written notice in advance –

a) If there is a delay of more than 4 weeks in completion of the Implementation Stage by the SI, StockHolding may terminate the Contract after affording a reasonable opportunity to the SI to explain the circumstances leading to such a delay.;
b) If penalty amount is equal to or more than 10% of PO value of a particular year;
c) If at any point of time, StockHolding finds out deviation to sub-contracting clause;
d) In the event of a reasonable apprehension of bankruptcy of the System Integrator;

Note: Upon termination of this MSA, the Parties will comply with the Exit Management.

Exit Management

a. Plan: An Exit Management plan shall be furnished by System Integrator in writing to StockHolding within 60 days from the acceptance of PO/Contract, which shall deal with at least the following aspects of exit management in relation to the contract as a whole and in relation to the Project Implementation, and the SLA.

b. Purpose: In the case of termination of the Contract, the Exit Management procedure should start 90 days before the expiry or termination of contact.

c. Transfer of assets: StockHolding shall be entitled to place notice in writing on the SI at any time during the Exit management period as detailed hereinabove requiring the SI to provide StockHolding with a complete and up to date list of the Project assets within 30 days of such notice. StockHolding shall be entitled to place a written notice to the SI requiring the SI to transfer all the Project assets to StockHolding. SI shall hand over possession, in a peaceful and unconditional manner, of all Project assets to the StockHolding prior 30 days of the date of expiry or termination of the contact.

   Additionally, the outgoing vendor would be required to support StockHolding or the new vendor for smooth handover of the entire system by assisting in any manner whatsoever which shall include amongst others handing over of all technical documents such as SDLC, Design Documents etc.

d. Confidential Information, Security and Data: The SI will promptly on the commencement of the exit management period supply to StockHolding the following:

   - Information relating to the current services rendered.
   - Documentation relating to Project's Intellectual Property Rights.
   - Project Data and Confidential Information.
   - All current and updated project data as is reasonably required for purposes of transitioning the services to its Replacement SI in a readily available format specified by StockHolding.

ANNEXURE - 1 - Details of Bidder's Profile

(To be submitted along with technical bid on Company letter head)

Details filled in this form must be accompanied by sufficient documentary evidence, in order to verify the correctness of the information.

Sl. No	**Parameters**	**Response**	
1	Name of the Company		
2	Year of Incorporation in India		
3	Names of the Partners/Directors		
4	Company PAN no		
5	Company GSTN no. (please attach annexures for all states)		
6	Addresses of Company		
	a) Head Office		
	b) Local Office in Mumbai(if any)		
7	Authorized Contact person		
	a) Name and Designation		
	b) Telephone number		
	c) E-mail ID		
8	Years of experience of on ITSM & ITAM Solution		
9	**Financial parameters**		
	Business Results (last three years)	Annual Turnover	Operating Profit
		(Rs. in Crores)	(Rs. in Crores)
	2020-21		
	2021-22		
	2022-23		
	(Only Company figures need to be mentioned not to include group/subsidiary Company figures)	(Mention the above Amount in INR only)	

N.B. Enclose copies of Audited Balance Sheet along with enclosures

Dated this........ Day of 2024

(Signature)

(In the capacity of)

ANNEXURE - 2 – Eligibility Criteria

To be submitted as part of Technical Bid

SI. No	Criteria	Documents to be submitted by Bidder
1	The Bidder should be a registered Company in India as per Indian Companies Act, 1956 or Indian Companies Act, 2013 and should be operating in India for the past 05 (five) years with experience of Implementation or Maintenance ITSM and ITAM Solutions in India for at least 03 (three) years.	Copy of Certificate of Incorporation issued by the Registrar of Companies and Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory
2	Should have an average annual turnover of at least Rs. 05 (five) Crores per annum for last three financial years (2020-21, 2021-22 and 2022-23). It should be of individual company and not of Group of Companies	Certificate from CA mentioning annual turnover for last three financial years.
3	Bidder should have Positive Net worth in the last 03 (three) audited financial years	Certificate from CA mentioning profit/loss for the past three financial years.
4	Bidder should not be blacklisted by any Government, Government Body, PSU, Bank, Autonomous body and any other entity for any reasons within last 2 years from the RFP date.	Self-declaration by the bidder on it Letter Head duly signed by the Authorized Signatory
5	Bidder should be either OEM or OEM the Authorized Partner / Reseller of the Proposed Solution on the date of RFP, with an authority to sell, upgrade, supply, service and maintain the proposed Solution. Note: Either OEM or their authorized partner should participate in the RFP. In case, both OEM & his authorized partner participate, only bid of the OEM will be considered.	Bidder needs to provide Manufacturer Authorization Form (MAF) from OEM stating that bidder is authorized partner of OEM and authorized to participate in this tender and in case the bidder is not able to perform obligations as per contract during the contract period, contracted services will be provided by OEM within the stipulated time.
6	Bidder should have experience of supply & implementation of ITSM and ITAM solution of minimum 02 (two) projects during the past 03 (three) years in India.	Copy of Purchase Orders / Completion Certificate
7	Bidder should have Support office at MMRDA Region.	Bidder to provide office address along with GST details.

Note:

a. All self-certificates shall be duly signed and Stamped by Authorized signatory of the Bidder Firm unless specified otherwise.

b. Bidder response should be complete, Yes/No answer is not acceptable.

c. Details of clients and relevant contact details are mandatory. Bidders may take necessary approval of the clients in advance before submission of related information. StockHolding will not make any separate request for submission of such information.

Dated this........ Day of 2024
(Signature)

(In the capacity of)
Duly authorized to sign bid with seal for & on behalf of (Name & Address of the Bidder)

ANNEXURE – 3 – Technical Compliance

The bidder is required to submit a response along with solution document by responding to the above requirements with "Yes" or "No" against them (bidder to add additional column "Compliance (YES/NO)" to each requirement). The same should be submitted along with the bid documents.

A. Information Technology Service Management (ITSM)

Capabilities	Compliant (Y/N)
Incident management	
The tool should be able to create tickets from multiple sources including emails, web forms, chat messages or phone calls	
The tool should be able to convert incidents into service requests and vice versa	
The tool should allow the service desk team to collect all relevant information from requesters with custom incident and request templates	
The tool should allow technicians to create shared or separate catalogs for incidents and service requests	
The tool should allow service desk admins to provide role-based access to technicians and end users	
The tool should allow service desk admins to restrict end user access to request templates based on site, category, and user groups.	
The tool should allow technicians to link, merge or clone incidents	
The tool should allow service desk admins to create custom categories, subcategories and items	
The tool should automatically assign categories to tickets based on the ticket parameters	
The tool should automatically assign tickets to technicians based on algorithms like round-robin and load balancing or based on ticket parameters like category, priority, impact and more	
The tool should allow service desk admins to view the list of all available technicians	
The tool should allow service desk admins to monitor technician availability, and setup backup technicians for unavailable technicians	
The tool should allow service desk admins and technicians to send a broadcast message to all logged-in technicians	
The tool should be able to automatically determine the priority of a request based on the impact and urgency	
The team should allow service desk admins to preconfigure incident lifecycles to handle various incidents	
The tool should automatically assign SLAs based on ticket parameters	
The tool should allow technicians to handle requests from VIP users with high priority	
The tool should help technicians search the knowledge base for a solution from within a request and copy the resolution into it	
The tool should allow technicians to create problems and changes from the within an incident	
The tool should allow technicians to collaborate with other technicians and groups by sharing the incident	
The tool should allow technicians to get real-time updates from other technicians working on the same ticket	

The tool should enable service desk admins to mandate fields and mark tasks that to be completed for incident closure	
The tool should allow technicians to create worklogs and record the cost, effort and time taken to resolve the incident	
The tool must be able to send out user surveys when the incident is closed	
Problem management	
The tool should allow technicians to create problems from an incident	
The tool should allow technicians to associate incidents and changes to problems	
The tool should allow technicians to mark a problem as known error	
The tool should facilitate technicians to analyse the impact of a problem and document it	
The tool should facilitate technicians to identify and documents symptoms and root cause of a problem	
The tool should allow technicians to provide a temporary solution for a problem with a workaround	
The tool should allow technicians to provide a permanent solution for the problem	
The tool should enable technicians to break up a problem resolution into multiple tasks and assign them to different technicians	
The tool should allow technicians to create a change record to further resolve the underlying issues if needed	
The tool should allow technicians to copy problem solution and workaround to all associated incidents	
The tool should allow technicians to automatically close all associate incidents on closure of the problem	
The tool should allow technicians to create worklogs and record the cost, effort and time taken to resolve the problem	
Change management	
The tool should allow technicians to create changes from incidents and problem with information carried over	
The tool should allow technicians to collect all the necessary information with custom change templates	
The tool should allow service desk admins to create different type of changes, and create unique workflows for each of these	
The tool should help service desk teams involve the right stakeholders by defining change roles	
The team should allow technicians to create elaborate change plans with impact analysis, roll out, back out and downtime plans	
The tool should allow service desk teams to maintain a checklist of essential steps to be completed	
The tool should allow service desk admins to form multiple change advisory boards	
The tool should allow service desk teams to configure multiple levels of approvals	
The tool should allow technicians to breakdown changes into tasks	
The tool should allow technicians to handle change implementation as projects	

The tool should allow technicians to track all associated incidents and problems causing and caused by the change	
The tool should allow service desk teams to schedule downtime and announce them to key stakeholders	
The tool should allow service desk teams to conduct and document post implementation review	
The tool should allow service desk admins and change managers to create distinct change workflows	
The tool should allow service desk admins and change managers to configure various actions like conditions, notifications, field updates and approvals within the change workflow	
Asset management	
The tool should allow service desk managers to build a detailed asset inventory	
The tool should allow service desk teams to discover and inventory all their windows machines	
The tool should allow service desk teams to discover and inventory all other devices including Macs, Linus machines, printers, and other network devices	
The tool should allow service desk teams to discover and inventory assets from multiple sites	
The tool should allow service desk teams to scan and discover assets using barcodes	
The tool should allow service desk teams to discover and inventory all their software	
The tool should allow service desk teams to inventory all available licenses with suite licensing, ability to upgrade and downgrade licenses	
The tool should allow service desk teams to create multiple license types for each manufacturer	
The tool should allow service desks teams to track and manage the compliance of multiple software licenses	
The tool should allow service desk teams to keep track of all assets in a central location	
The tool should allow service desk admins to configure multiple asset states	
The tool should allow service desk teams automatically scan all assets at set intervals	
The tool should allow service desk admins to configure depreciation for assets	
The tool should allow service desk teams to loan, and track loaned assets	
The tool should allow service desk teams to create standard and custom asset reports	
CMDB (Configuration Management Database)	
The tool should allow service desk admins to define CIs with custom CI types	
The tools should allow service desk teams to configure graphical views of CIs and their relationship maps	
The tool should allow service desk teams to create unique relationship maps specific to all key services	
The tool should allow service desk teams to import CIs through a CSV file	
The tool should allow service desk teams to import CI relationships through an XLS file	
The tool should allow technicians to export the relationship maps as PNG or PDF	

Purchase management	
The tool should allow service desk admins to manage asset and service purchases in a central location	
The tool should allow service desk admins to track purchases in multiple currencies	
The tool should allow service desk teams to associate multiple service request to a purchase order	
The tool should allow service desk admins to configure 5 levels of approvals for Purchase Orders	
The tool should allow technicians to add invoice and payment information	
The tool should allow service desk teams to integrate purchase management with asset management processes	
Contract management	
The tool should allow service desk teams to manage all contracts from one place	
The tool should allow service desk teams to associate multiple assets to a contract	
The tool should allow service desk teams to create child contracts within the contracts	
The tool should allow service desk teams to associate costs for each contract	
The tool should allow service desk admins to configure automatic notifications for a contract expiry	
Project management	
The tool should allow service desk admins to create custom project templates and types	
The tool should allow technicians to track the progress of projects using Gantt chart	
The tool should allow service desk admins to define level of access for various users to each project	
The tool should allow service desk teams to break down the project into smaller manageable chunks	
The tool should allow technicians to export the Gantt map and project overview map as PDFs	
Service catalog	
The tool should allow service desk admins to create multiple service templates under appropriate service categories	
The tool should allow service desk admins to configure custom service request templates	
The tools should allow service desk admins to automate templates through condition-based activities like mandating fields, populating fields, enabling and disabling fields based on ticket criteria during creating or after editing the ticket	
The tool should allow service desk admins to make the template dynamic with condition-based actions like hiding or showing fields in real time based on the information given by the requester	
The tool should enable service desk admins to associate costs to assets, and account them during the request creation	
The tool should allow easy integration of the service catalog and CMDB	
The team should allow service desk admins to provide role-based access to each service request template	

The tool should allow service desk admins to configure roles like department in-charge, and managers to approve service requests	
The tool should allow service desk admins to configure a multi-stage approval process	
The tool should automatically associate SLAs and business rules to service request templates	
The tool should allow service desk admins to associate multiple tasks to each service request template	
The tool should allow service desk admins to configure a visual mapping of the task execution sequence for each service request template	
Self-service	
The tool should allow service desk admins to configure unique service desk portal for technicians and end users	
The self-service portal should allow easy access to incident and service catalog	
The self-service portal should allow users to view announcements and access the knowledge base	
The tool should automatically suggest related solutions based on the subject of the request during request creation	
The tool should automatically mention related announcements based on the subject of the request during request creation	
Knowledge management	
The tool should allow service desk admins and technicians to publish solutions to the knowledge base with an approval process	
The tool should allow service desk admins to organize solution under relevant topics	
The tool should allow service desk admins to configure role-based access and site-based access to each solution	
The tool should allow service desk admins to configure resolution templates for repeat requests with the same solution	
The tool should allow service desk admins to set expiry dates for solutions	
Reports	
The tool should allow technicians to generate reports easily with pre-built standard reports	
The tool should allow technicians to create custom reports, and custom query reports	
The tool should allow technicians to create custom dashboards with role-based access	
The tool should allow technicians to organize reports under custom report folders	
The tool should allow technicians to create reports of multiple types including tabular, matrix, summary, audit or CI history reports	
The tool should allow technicians to depict reports visually as pie charts, bar charts, line charts, time series charts, area charts or ring charts	
The tool should allow technicians to export reports into CSV, HTML, XLS and PDF formats	
The tool should allow technicians to schedule reports at a specific frequency	
The tool should allow technicians to generate reports and automatically share with it users	
User surveys	

The tool should allow technicians to create separate surveys for incidents and service requests	
The tool should allow technicians to create surveys with multiple question types including rating, opinion scale, binary and radio	
The tool should allow technicians to configure user surveys in multiple language	
The tool should allow technicians to configure when and under what conditions a survey has to be triggered	
The tool should allow service desk admins to collate data from survey reports for analysis	
IT and business integrations	
The tool should integrate with end point management tools to perform desktop and mobile device management activities from within the service desk console	
The tool should integrate with network monitoring devices to automatically convert network alerts into service desk tickets and automatically assign them to technicians and notify them	
The tool should integrate with business analytics tools for in-depth analysis	
The tool should integrate with application monitoring tools out-of-the-box	
The tool should integrate with enterprise password management applications out-of-the-box, to establish a strict authentication process for launching secure remote session from the service desk	
The tool should integrate with AD management applications to allow users and technicians to perform AD Management activities from the service desk	
The tool should have an out-of-the-box integration with SCCM	
The tool should allow event-driven API calls for easy third-party integrations	

B. Active Directory(AD) Manager

Active Directory Manager	Compliant (Y/N)
Create new users individually or in bulk via user creation templates or CSV files.	
Locate and modify the attributes of multiple users at once using user modification templates or CSV files.	
The tool serves as a centralized password manager for bulk password management, automated password reset, and actionable password reports.	
Enable or disable multiple user accounts and also specify the account expiry date, in a single action.	
Bulk move AD users across OUs.	
Delete or disable users in bulk to cleanup your AD.	
Add/remove users from groups, set primary groups of users, and more.	
Create multiple AD security and distribution groups, and assign various group attributes at once.	
Bulk move groups to a different OU/container.	
Delete multiple AD groups, in bulk, at once.	
Bulk create and modify AD contacts and the respective attributes.	
Delete AD contacts individually or in bulk by importing a CSV containing the list of contacts to be deleted.	
Create and modify shared, room, equipment, and linked mailbox in groups, at once, using templates.	
Bulk create, delete, and move OUs with just mouse clicks.	

Grant, modify, revoke NTFS and Share permissions of multiple users and groups. Configure and manage Netapp and Isilon servers as well.	
Create and manage GPOs and GPO links.	
Obtain general password reports and password status reports on different users.	
Generate general group reports, member-based reports, and reports based on the group type.	
Fetch general computer reports and account status reports of all computers in your AD.	
Obtain general Exchange reports, reports based on the delivery recipient settings, and feature- based reports.	
Stay on top of all the information about contacts such as the list of all contacts, mail enabled contacts, recently created/modified contacts, and more.	
View which users have access to terminal services and their properties.	
Utilize general GPO-related reports and reports involving GPO scope, status, and settings.	
Obtain OU-related information such as users/computers-only OUs, recently created/modified OUs, and more.	
View, analyze, and modify NTFS and share permissions or ACLs assigned to Windows or NetApp servers, folders, and files.	
View information about users' password and account lockout policies and the printers available in specific domains.	
Demonstrate product compliance with various regulatory compliance mandates such as SOX, HIPAA, PCI, FISMA, GLBA, and GDPR.	
Gain in-depth information on all, active, and suspended Google Workspace users.	
Generate reports based on LDAP queries and custom attributes of AD objects.	
Export all reports to multiple formats such as PDF, XLS, CSV, and HTML.	
Automate report generation and emailing of reports to user-specified email addresses.	
Create and manage Azure AD users, groups, contacts, and licenses.	
Manage Exchange mailboxes, shared mailboxes, and calendars.	
Generate reports on Azure AD users (including passwords, user logon, and account status), groups, contacts, and licenses.	
Obtain reports on Exchange mailboxes (including content, shared mailbox, and account status reports) and OWA.	
Create and assign custom roles with the selected tasks to delegate to help desk technicians, to empower them to perform those tasks, only in the specified domains/OUs.	
List all the operations performed by help desk technicians in your environment.	
View the list of all actions (creation, deletion, and modification) performed on help desk technicians and roles.	
Configure a second authentication method (Single sign on, two factor authentication, or smart card authentication) to login to the product.	
List all available help desk technicians, along with details such as delegated roles and administrative limits.	
View the logon details of help desk technicians, along with details such as their logon status, and authentication methods for all their logons.	
Define an order of execution for management operations, with different checkpoints like request, review, approve, and execute.	
Create workflow requests for AD objects creation (users) and modification (users, computers, contacts, groups.)	
View the list of all requests created by a technician and the requests that are assigned to that technician.	
Configure multiple workflow agents (requesters, reviewers, approvers, and executors) and define the roles of each of them.	

Create rules to assign requests to appropriate technicians automatically.	
Employ full automation or controlled automation to carry out any management/administrative task such as AD cleanup, group membership management,	
Automate a sequence/series of tasks and also specify the intervals at which each task in the sequence should be executed.	
Create personalized naming formats as per your organization's policies with this custom naming format builder.	
Add/remove titles, departments, offices, and companies based on your organization's needs.	
Configure a custom format that has to be adhered to, for generating random passwords.	
Set up domain-specific delete and disable policies that will be executed whenever user accounts are disabled or deleted.	
Configure custom notification profiles, high availability, and integrations with various third- party applications.	
While exporting reports, password protect the files for added security.	
Allow users to reset their Active Directory domain passwords without admin intervention.	
Allow users to unlock their Active Directory domain accounts without admin intervention.	
Notify users about impending password expiration.	
Notify users about impending account expiration.	
Update cached credentials when users reset their passwords even if they are not connected to the corporate network.	
Integrate password self-service with your review and approval-based help desk software.	
Limit the number of times that users can reset passwords and unlock accounts in a specific duration.	
Notify users when their password is reset or changed or their account is unlocked successfully.	
Schedule automatic password reset and account unlock for users with expired passwords and locked-out accounts respectively.	
A maximum of three authentication factors can be configured for MFA in addition to passwords.	
Secure self-service password resets and account unlock attempts using MFA.	
Protect Windows, macOS, and Linux logins with MFA.	
Verify the user’s identity during VPN logins using MFA.	
Secure endpoints supporting RADIUS authentication, like Citrix Gateway, VMware Horizon, and Microsoft Remote Desktop Gateway.	
Force users to enrol with the product when they log in to their machines.	
Remind users of product enrolment through email or SMS.	
Enrol users without their intervention by importing enrolment data through CSV files or external databases.	
Use Active Directory attribute values to enrol users automatically for SMS and email OTP.	
Automatically synchronize users’ Active Directory passwords with cloud applications and other on-premises systems.	
Allow users to access all their cloud apps after logging in only once.	
Allow users to update their Active Directory information without admin intervention.	
Let users subscribe or unsubscribe from mail groups of their choice.	
Provide admins and users with an option to search and view information about themselves and other domain users.	
Let users find their position in the organization hierarchy.	
Analyzes and displays the strength of the password being created.	

Enforce Active Directory password history settings during password reset.	
View a graphical representation of password statuses, user actions, and enrolment data.	
The product includes built-in reports to audit user actions and user statuses.	
Get reports on locked-out users and users with expired or soon-to-expire passwords.	
Available reports:	
Locked-out users	
Users with soon-to-expire passwords Users with expired passwords	
Get reports on reset passwords, unlocked accounts, identity verification, and user login attempts. Available audit reports:	
Reset passwords Unlocked accounts Self-update Changed password Notification delivery	
Identity verification failure User attempts	
Get reports on enrolled users, non-enrolled users, and licensed users. Available reports:	
Enrolled users	
Configure custom password policies for domains, organizational units, and groups using these password policy rules: Number of special characters to include: X. Number of numeric characters to include: X. Number of unicode characters: X Must contain at least X uppercase characters. Must contain at least X lowercase characters. Password must begin with an uppercase alphabet, a lowercase alphabet, a special character, or a number. Restrict numerals as the last character. Restrict the use of a character more than X times consecutively. Restrict the use of X consecutive characters from the username. Restrict the use of X consecutive character(s) from the old password. Number of old passwords to be restricted during password reset: X. Restrict palindrome passwords. Restrict the use of dictionary words. Restrict the use of specific patterns. Minimum password length: X. Maximum password length: X. **Or** A specific number of special, numeric, and unicode characters must be included. A minimum number of uppercase and lowercase letters must be used. An uppercase letter, a lowercase letter, a special character, or a number must be the first character. A number is restricted from being the last character. A character cannot be used consecutively more than a specific number of times. Consecutive characters from the username or an old password cannot be used. A specific number of old passwords can be restricted from use during password reset. Palindromes, dictionary words, and patterns can be restricted. A minimum and maximum password length can be fixed.	
The authentication methods supported out of the box for MFA are:	
Fingerprint/Face ID authentication YubiKey authentication	
Microsoft Authenticator Google Authenticator	
Zoho OneAuth TOTP authentication Custom TOTP authenticator	
Duo Security	
Push notification authentication QR code-based authentication TOTP authentication	
Email verification SMS verification RSA SecurID	
RADIUS authentication SAML authentication AD security questions	
Security questions and answers Smart card authentication	

- At least 3 out of the available options should be implementable as per StockHolding's existing Infrastructure.

Active Directory Self-Service Management

Active Directory Self-Service Management	Compliant (Y/N)
Allow users to reset their Active Directory domain passwords without admin intervention.	
Allow users to unlock their Active Directory domain accounts without admin intervention.	
Notify users about impending password expiration.	
Notify users about impending account expiration.	
Update cached credentials when users reset their passwords even if they are not connected to the corporate network.	
Integrate password self-service with your review and approval-based help desk software.	
Limit the number of times that users can reset passwords and unlock accounts in a specific duration.	
Notify users when their password is reset or changed or their account is unlocked successfully.	
Schedule automatic password reset and account unlock for users with expired passwords and locked-out accounts respectively.	
A maximum of three authentication factors can be configured for MFA in addition to passwords.	
Secure self-service password resets and account unlock attempts using MFA.	
Protect Windows, macOS, and Linux logins with MFA.	
Verify the user's identity during VPN logins using MFA.	
Secure endpoints supporting RADIUS authentication, like Citrix Gateway, VMware Horizon, and Microsoft Remote Desktop Gateway.	
Force users to enrol with the product when they log in to their machines.	
Remind users of product enrolment through email or SMS.	
Enrol users without their intervention by importing enrolment data through CSV files or external databases.	
Use Active Directory attribute values to enrol users automatically for SMS and email OTP.	
Automatically synchronize users' Active Directory passwords with cloud applications and other on-premises systems.	
Allow users to access all their cloud apps after logging in only once.	
Allow users to update their Active Directory information without admin intervention.	
Let users subscribe or unsubscribe from mail groups of their choice.	
Provide admins and users with an option to search and view information about themselves and other domain users.	
Let users find their position in the organization hierarchy.	
Analyzes and displays the strength of the password being created.	
Enforce Active Directory password history settings during password reset.	
View a graphical representation of password statuses, user actions, and enrolment data.	
The product includes built-in reports to audit user actions and user statuses.	
Get reports on locked-out users and users with expired or soon-to-expire passwords.	
Available reports:	
Locked-out users	

Users with soon-to-expire passwords Users with expired passwords	
Get reports on reset passwords, unlocked accounts, identity verification, and user login attempts. Available audit reports:	
Reset passwords Unlocked accounts Self-update Changed password Notification delivery	
Identity verification failure User attempts	
Get reports on enrolled users, non-enrolled users, and licensed users. Available reports:	
Enrolled users	
Configure custom password policies for domains, organizational units, and groups using these password policy rules: Number of special characters to include: X. Number of numeric characters to include: X. Number of unicode characters: X. Must contain at least X uppercase characters. Must contain at least X lowercase characters. Password must begin with an uppercase alphabet, a lowercase alphabet, a special character, or a number. Restrict numerals as the last character. Restrict the use of a character more than X times consecutively. Restrict the use of X consecutive characters from the username. Restrict the use of X consecutive character(s) from the old password. Number of old passwords to be restricted during password reset: X. Restrict palindrome passwords. Restrict the use of dictionary words. Restrict the use of specific patterns. Minimum password length: X. Maximum password length: X. Or A specific number of special, numeric, and unicode characters must be included. A minimum number of uppercase and lowercase letters must be used. An uppercase letter, a lowercase letter, a special character, or a number must be the first character. A number is restricted from being the last character. A character cannot be used consecutively more than a specific number of times. Consecutive characters from the username or an old password cannot be used. A specific number of old passwords can be restricted from use during password reset. Palindromes, dictionary words, and patterns can be restricted. A minimum and maximum password length can be fixed.	
The authentication methods supported out of the box for MFA are:	
Fingerprint/Face ID authentication YubiKey authentication	
Microsoft Authenticator Google Authenticator	
Zoho OneAuth TOTP authentication Custom TOTP authenticator	
Duo Security	
Push notification authentication QR code-based authentication TOTP authentication	
Email verification SMS verification RSA SecurID	
RADIUS authentication SAML authentication AD security questions	
Security questions and answers Smart card authentication	

- At least 3 out of the available options should be implementable as per StockHolding's existing Infrastructure.

C. Active Directory Audit

Active Directory Audit	Compliant (Y/N)

Get information on all logon activity, from logon failures to logon history, across domain controllers, Windows Servers, and workstations.	
Get notified of a lockout and receive information on the source of the authentication failure from an extensive list of Windows components such as Windows services, scheduled tasks, network drive mappings, and more.	
Get information on changes to AD objects such as users, computers, groups, organizational units (OUs), DNS, schema, sites, PSO objects, and more.	
Get information on changes to	
Group Policy Objects (GPOs) and their settings, such as password policy, account lockout policy, and more.	
Get information on changes in AD permissions across OUs, groups, users, computers, schema, configuration, DNS, and more.	
Get information on all activities performed by privileged users in the domain.	
Get information on the old and new values of changed attributes in the domain.	
Get information on all successful and failed logons.	
Get information on all user and device management actions.	
Get information on membership changes to groups and dynamic groups, and the assignment and removal of roles to users.	
Get information on applications that have been added, updated, and deleted, and consent given to APIs.	
Get information on changes to users' and groups' licenses.	
Get contextual information like a user's on-premises Distinguished Name, SID, and GUID.	
Get information on file read, create, modify, delete, rename, move, and other actions.	
Get information on failed attempts to read, write, and delete files.	
Get information on file DACL and SACL changes.	
Get information on remote desktop connections and remote logons occurring via Remote Desktop Gateway (RDG) servers and RADIUS Network Policy Servers (NPS).	
Get information on both successful and failed AD FS logons.	
Get information on the first in, last out, active, and idle time spent by employees at their workstations.	
Get information on local user and group management actions.	
Get information on changes to local security policy.	
Get information on changes to system, program, and other critical local files.	
Get information on usage and file activity across printers and removable storage devices such as USBs, external hard drives, and more.	
Get information on scheduled tasks that have been created, deleted, or modified, and processes that have been started or stopped.	
Get information on who is viewing or modifying local admin credentials.	
Get information on PowerShell processes that run on Windows Servers, along with the commands executed in them.	
Leverage Active Directory Audit’s machine learning capabilities to establish activity patterns and spot subtle anomalies such as an unusual volume of logon failures.	
Get notified via email and SMS about critical activities such as when a user is added to privileged or sensitive groups.	
Define thresholds based on volume, time, and other criteria to spot suspicious activities like mass file access.	

Execute scripts to automate response actions, like shutting down a device or disabling an account once an alert gets triggered.	
Get a complete audit trail of who did what, when, and from where, with	
Create reports to meet specific business needs.	
Tracking down specific information contained in reports quickly.	
Get a visual representation of audit data.	
Export reports to multiple formats such as PDF, XLS, CSV, and HTML.	
Automate generation of reports at user defined time intervals.	
Automate emailing of reports to user specified email addresses	
Retain audit data safely for as long as you want.	
Forward audit data to Syslog servers and other SIEM solutions.	
Exclude data that's irrelevant to audits based on user, file type, and other criteria.	
Access the product over the web.	
Grant different users varying levels of access to the product.	
Leverage both agentless and agent- based audit data collection.	

Dated this........ Day of 2024
(Signature)

(In the capacity of)
Duly authorized to sign bid with seal for & on behalf of (Name & Address of the Bidder)

ANNEXURE - 4 - Commercial Price Bid Format

Commercial Price Bid Format

1. **Software Implementation Cost:**

Table I:

S/N.	Item Description	Total Cost (₹)	GST (₹)	Total Cost with GST (₹)
1.	Cost of Implementation of all software/Solutions/ Tools for operationalizing ITSM and ITAM solutions as per the requirement of this RFP			

2. **Software / Tools Cost with Perpetual Licenses:**

Table II:

S/N.	Name of Software/ Tool	License Cost Per Unit (₹)	No. of licenses required	Total Cost (₹)	GST (₹)	Total Cost with GST (₹)
1.	<<Bidder to propose>>					
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
	Total Cost (₹)					

3. **Software Support /ATS for 5 years:**

Table III:

S/N.	Item Description	1st Year Price (₹) [A]	2nd Year Price (₹) [B]	3rd Year Price (₹) [C]	4th Year Price (₹) [D]	5th Year Price (₹) [E]
1	Support Cost					
GST (₹)						
Cost with GST (₹)						
Total Cost for 5 Years(₹)						

4. **Customization Cost for Templates:**

Table IV:

S/N.	Item Description	Qty	Unit Cost (₹)	Total Cost (₹)	GST (₹)	Total Cost with GST (₹)
1.	Customization of templates	50				

Total Cost to Ownership (TCO):

S/N.	Item	Total Cost for the contract period of 5 years (₹)	GST (₹)	Total Cost for the contract period of 5 years with GST (₹)
1.	Software Implementation Cost [Table I]			
2.	Software / Tools Cost with Perpetual Licenses [Table II]			
3.	Software Support /ATS for 5 years [Table III]			
4.	Customization of templates (50 nos.) [Table IV]			
			Grand Total (₹)	

Notes:

a Price to be quoted is for contract period of 05 (five) years including GST while uploading financial bids on GeM portal.

b Bidder who quotes lowest bid for total price will be selected as L1 bidder.

c Payment will be made on pro-rate basis for each template based on customizations.

d StockHolding reserves the right to negotiate with L1 bidder.

e Bidder must take care in filling price information in the Commercial Offer, to ensure that there are no typographical or arithmetic errors. All fields must be filled in correctly. Please note that any Commercial Offer, which is conditional and / or qualified or subjected to suggestions, will also be summarily rejected. This offer shall not contain any deviation in terms & conditions or any specifications, if so such an offer will also be summarily rejected.

f All payments will be made in INR.

g The prices finalized shall remain valid for 06 (six) months from the date of initial Purchase Order. StockHolding may place Purchase Order (PO) for additional requirements at the discovered license price through this RFP process within 01 (one) year from the date of purchase order. However, ATS prices of Software etc. will remain valid for 04 (four) years for all software post warranty.

ANNEXURE - 5 – Integrity Pact

(To be executed on plain paper and submitted only by the successful bidder)

(__________________________________ Name of the Department / Office) RFP No.___________ for_______________________________

This pre-bid pre-contract Integrity Pact (Agreement) (hereinafter called the Integrity Pact) (IP) is made on ______ day of the _______________________, between, on one hand, StockHolding ., a company incorporated under Companies Act, 1956, with its Registered Office at 301, Centre Point Building, Dr. B R Ambedkar Road, Parel, Mumbai – 400012 , acting through its authorized officer, (hereinafter called **Principal**), which expression shall mean and include unless the context otherwise requires, his successors in office and assigns) of the First Part **And** M/s.____(with complete address and contact details)represented by Shri ____ (i.e. Bidders hereinafter called the **`Counter Party'**) which expression shall mean and include , unless the context otherwise requires, his successors and permitted assigns) of the Second Part.

AND WHEREAS the PRINCIPAL/Owner values full compliance with all relevant laws of the land, rules, regulations economic use of resources and of fairness/transparency in its relation with Bidder(s) /Contractor(s)/Counter Party(ies).

AND WHEREAS, in order to achieve these goals, the Principal/Owner has appointed Independent External Monitors (IEM) to monitor the Tender (RFP) process and the execution of the Contract for compliance with the principles as laid down in this Agreement.

WHEREAS THE Principal proposes to procure the Goods/services and Counter Party is willing to supply/has promised to supply the goods OR to offer/has offered the services and WHEREAS the Counter Party is a private Company/Public Company/Government Undertaking/ Partnership, constituted in accorded with the relevant law in the matter and the Principal is a Government Company performing its functions as a registered Public Limited Company regulated by Securities Exchange Board of India. **NOW THEREFORE**, To avoid all forms of corruption by following a system that is fair, transparent and free from any influence prejudiced dealings prior to, during and subsequent to the tenor of the contract to be entered into with a view to "- Enabling the PRINCIPAL to obtain the desired goods/services at competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and Enabling the Counter Party to abstain from bribing or indulging in any type of corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the PRINCIPAL will commit to prevent corruption, in any form, by its officials by following transparent procedures. The parties hereto hereby agree to enter into this Integrity Pact and agree as follows**:**

I. Commitment of the Principal / Buyer

1. The Principal Owner commits itself to take all measures necessary to prevent corruption and to observe the following principles:-

a) No employee of the Principal/Owner, personally or through any of his/her family members, will in connection with the Tender (RFP) or the execution of the contract, procurement or services/goods, demand, take a promise for or accept for self or third person, any material or immaterial benefit which the person not legally entitled to.

b) The Principal/Owner will, during the Tender (RFP) Process treat all Bidder(s)/Counter Party(ies) with equity and reason. The Principal / Owner will, in particular, before and during the Tender (RFP) Process, provide to all Bidder(s) / Counter Party (ies) the same information and will not provide to any Bidder(s)/Counter Party (ies) confidential / additional information through which the Bidder(s)/Counter Party (ies) could obtain an advantage in relation to the Tender (RFP) Process or the Contract execution.

c) The Principal / Owner shall endeavor to exclude from the Tender (RFP) process any person, whose conduct in the past been of biased nature.

2. If the Principal / Owner obtains information on the conduct of any of its employees which is a criminal offence under the Indian Penal Code (IPC) / Prevention of Corruption Act, 1988 (PC Act) or is in violation of the principles herein mentioned or if there is a substantive suspicion in this regard, the Principal / Owner / StockHolding will inform the Chief Vigilance Officer through the Vigilance Officer and in addition can also initiate disciplinary actions as per its internal laid down policies and procedures.

II. Commitments of Counter Parties/Bidders

1. The Counter Party commits itself to take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of bid or during any pre-contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following. Counter Party (ies) / Bidders commits himself to observe these principles during participation in the Tender (RFP) Process and during the Contract execution.
2. The Counter Party will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the PRINCIPAL, connected directly or indirectly with the bidding process, or to any person organization or third party related to the contract in exchange for any advantage in the bidding, evaluation, contracting and implementation of the contract.
3. The Counter Party further undertakes that it has not given, offered or promised to give directly or indirectly any bribe, gift, consideration, reward, favour, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the Principal / StockHolding or otherwise in procurement the Contract or forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Principal / StockHolding for forbearing to show favour or disfavor to any person in relation to the contract or any other contract with the Principal / StockHolding.
4. Bidder / Counter Party shall disclose the name and address of agents and representatives, if any, handling the procurement / service contract.
5. Bidder / Counter Party shall disclose the payments to be made by them to agents / brokers; or any other intermediary if any, in connection with the bid / contract.
6. The Bidder / Counter Party has to further confirm and declare to the Principal / StockHolding that the Bidder / Counter Party is the original integrator and has not engaged any other individual or firm or company, whether Indian or foreign to intercede, facilitate or in any way to recommend to Principal / StockHolding or any of its functionaries whether officially or unofficially to the award of the contract to the Bidder / Counter Party nor has any amount been paid, promised or intended to the be paid to any such individual, firm or company in respect of any such intercession, facilitation or recommendation.

7. The Bidder / Counter Party has to submit a Declaration along with Eligibility Criteria, as given at **Annexure**. If bids are invited through a Consultant a Declaration has to be submitted along with the Eligibility Criteria as given at **Annexure**.
8. The Bidder / Counter Party, either while presenting the bid or during pre- contract negotiation or before signing the contract shall disclose any payments made, is committed to or intends to make to officials of StockHolding /Principal, or their family members, agents, brokers or any other intermediaries in connection with the contract and the details of services agreed upon for such payments.
9. The Bidder / Counter Party will not collude with other parties interested in the contract to impair the transparency, fairness and progress of bidding process, bid evaluation, contracting and implementation of the Contract.
10. The Bidder / Counter Party shall not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.
11. The Bidder shall not use improperly, for purposes of competition or personal gain, or pass on to others, any information provided by the Principal / StockHolding as part of the business relationship, regarding plans, proposals and business details, including information contained in any electronic data carrier. The Bidder / Counter Party also Undertakes to exercise due and adequate care lest any such information is divulged.
12. The Bidder / Counter Party commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.
13. The Bidder / Counter Party shall not instigate or cause to instigate any third person including their competitor(s) of bidding to commit any of the actions mentioned above.
14. If the Bidder / Counter Party or any employee of the Bidder or any person acting on behalf of the Bidder / Counter Party, either directly or indirectly, is a relative of any of the official / employee of Principal / StockHolding, or alternatively, if any relative of an official / employee of Principal / StockHolding has financial interest / stake in the Bidder's / Counter Party firm, the same shall be disclosed by the Bidder / Counter Party at the time of filing of tender (RFP).

15. The term `relative‟ for this purpose would be as defined in Section 2 Sub Section 77 of the Companies Act, 2013.
16. The Bidder / Counter Party shall not lend to or borrow any money from or enter into any monetary dealings or transactions, directly or indirectly, with any employees / officials of the Principal / StockHolding
17. The Bidder / Counter Party declares that no previous transgression occurred in the last three years immediately before signing of this IP, with any other Company / Firm/ PSU/ Departments in respect of any corrupt practices envisaged hereunder that could justify Bidder / Counter Party exclusion from the Tender (RFP) Process.
18. The Bidder / Counter Party agrees that if it makes incorrect statement on this subject, Bidder / Counter Party can be disqualified from the tender (RFP) process or the contract, if already awarded, can be terminated for such reason.

III. Disqualification from Tender (RFP) Process and exclusion from Future Contracts

1. If the Bidder(s) / Contractor(s), either before award or during execution of Contract has committed a transgression through a violation of Article II above or in any other form, such as to put his reliability or credibility in question, the Principal / StockHolding is entitled to disqualify the Bidder / Counter Party / Contractor from the Tender (RFP) Process or terminate the Contract, if already executed or exclude the Bidder / Counter Party / Contractor from future contract award processes. The imposition and duration of the exclusion will be determined by the severity of transgression and determined by Principal / StockHolding. Such

exclusion may be for a period of 1 year to 3 years as per the procedure prescribed in guidelines of the Principal / StockHolding.

2. The Bidder / Contractor / Counter Party accepts and undertake to respect and uphold the Principal / StockHolding's absolute right to resort to and impose such exclusion.
3. Apart from the above, the Principal / StockHolding may take action for banning of business dealings / holiday listing of the Bidder / Counter Party / Contractor as deemed fit by the Principal / Owner / StockHolding.
4. The Bidder / Contractor / Counter Party can prove that it has resorted / recouped the damage caused and has installed a suitable corruption prevention system, the Principal / Owner/ StockHolding may at its own discretion, as per laid down organizational procedure, revoke the exclusion prematurely.

IV. Consequences of Breach Without prejudice to any rights that may be available to the Principal / StockHolding / Owner under Law or the Contract or its established policies and laid down procedure, the Principal / StockHolding / Owner shall have the following rights in case of breach of this Integrity Pact by the Bidder / Contractor(s) / Counter Party:-

1. Forfeiture of EMD / Security Deposit : If the Principal / StockHolding / Owner has disqualified the Bidder(s)/Counter Party(ies) from the Tender (RFP) Process prior to the award of the Contract or terminated the Contract or has accrued the right to terminate the Contract according the Article III, the Principal / StockHolding / Owner apart from exercising any legal rights that may have accrued to the Principal / StockHolding / Owner, may in its considered opinion forfeit the Earnest Money Deposit / Bid Security amount of the Bidder / Contractor / Counter Party.
2. Criminal Liability: If the Principal / Owner / StockHolding obtains knowledge of conduct of a Bidder / Counter Party / Contractor, or of an employee of a representative or an associate of a Bidder / Counter Party / Contractor which constitute corruption within the meaning of PC Act, or if the Principal / Owner / StockHolding has substantive suspicion in this regard, the Principal /
StockHolding / Owner will inform the same to the Chief Vigilance Officer through the Vigilance Officer.

IV. Equal Treatment of all Bidders/Contractors / Subcontractors / Counter Parties

1. The Bidder(s) / Contractor(s) / Counter Party (ies) undertake (s) to demand from all subcontractors a commitment in conformity with this Integrity Pact. The Bidder / Contractor / Counter-Party shall be responsible for any violation(s) of the principles laid down in this Agreement / Pact by any of its sub-contractors / sub-bidders.
2. The Principal / StockHolding / Owner will enter into Pacts on identical terms as this one with all Bidders / Counterparties and Contractors.
3. The Principal / StockHolding / Owner will disqualify Bidders / Counter Parties / Contractors who do not submit, the duly signed Pact, between the Principal / Owner / StockHolding and the Bidder/Counter Parties, along with the Tender (RFP) or violate its provisions at any stage of the Tender (RFP) process, from the Tender (RFP) process.

VI. Independent External Monitor (IEM)

1. The Principal / Owner / StockHolding has appointed competent and credible Independent External Monitor (s) (IEM) for this Pact. The task of the Monitor is to review independently and objectively, whether and to what extent the parties comply with the obligations under this Integrity Pact.
2. The IEM is not subject to instructions by the representatives of the parties and performs his functions neutrally and independently. He reports to the Chief Executive Officer and Managing Director, StockHolding Ltd.

3. The Bidder(s)/Contractor(s) / Counter Party(ies) accepts that the IEM has the right to access without restriction, to all Tender (RFP) documentation related papers / files of the Principal / StockHolding / Owner including that provided by the Contractor(s) / Bidder / Counter Party. The Counter Party / Bidder / Contractor will also grant the IEM, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his or any of his Sub-Contractor‟s Tender (RFP) Documentation / papers / files. The IEM is under contractual obligation to treat the information and documents of the Bidder(s) / Contractor(s) / Sub-Contractors / Counter Party (ies) with confidentiality.
4. In case of tender (RFP)s having value of 5 crore or more, the Principal / StockHolding / Owner will provide the IEM sufficient information about all the meetings among the parties related to the Contract/Tender (RFP) and shall keep the IEM apprised of all the developments in the Tender (RFP) Process.
5. As soon the IEM notices, or believes to notice, a violation of this Pact, he will so inform the Management of the Principal / Owner /StockHolding and request the Management to discontinue or take corrective action, or to take other relevant action. The IEM can in this regard submit nonbinding recommendations. Beyond this, the IEM has no right to demand from the parties that they act in a specific manner, refrain from action or tolerate action.
6. The IEM will submit a written report to the CEO&MD, StockHolding. Within 6 to 8 weeks from the date of reference or intimation to him by the Principal / Owner / StockHolding and should the occasion arise, submit proposals for correcting problematic situations.
7. If the IEM has reported to the CEO&MD, StockHolding Ltd. a substantiated suspicion of an offence under the relevant IPC/PC Act, and the CEO&MD, StockHolding has not within reasonable time taken visible action to proceed against such offence or reported it to the Chief Vigilance Officer, the IEM may also transmit the information directly to the Central Vigilance Officer.
8. The word `IEM‟ would include both singular and plural.

VII. Duration of the Integrity Pact (IP)

This IP begins when both the parties have legally signed it. It expires for the Counter Party / Contractor / Bidder, 12 months after the completion of work under the Contract, or till continuation of defect liability period, whichever is more and for all other Bidders, till the Contract has been awarded. If any claim is made / lodged during the time, the same shall be binding and continue to be valid despite the lapse of this Integrity Pact as specified above, unless it is discharged / determined by the CEO&MD StockHolding

VIII. Other Provisions

1. This IP is subject to Indian Law, place of performance and jurisdiction is the Head Office / Regional Offices of the StockHolding /Principal / Owner who has floated the Tender (RFP).
2. Changes and supplements in any Procurement / Services Contract / Tender (RFP) need to be made in writing. Change and supplement in IP need to be made in writing.
3. If the Contractor is a partnership or a consortium, this IP must be signed by all the partners and consortium members. In case of a Company, the IP must be signed by a representative duly authorized by Board resolution.
4. Should one or several provisions of this IP turn out to be invalid; the remainder of this Pact remains valid. In this case, the parties will strive to come to an agreement to their original intentions.
5. Any dispute or difference arising between the parties with regard to the terms of this Agreement / Pact, any action taken by the Principal / Owner / StockHolding in accordance with this Agreement / Pact or interpretation thereof shall not be subject to arbitration.

IX. Legal and Prior Rights

All rights and remedies of the parties hereto shall be in addition to all the other legal rights and remedies belonging to such parties under the Contract and / or law and the same shall be deemed to be cumulative and not alternative to such legal rights and remedies aforesaid. For the sake of brevity, both the Parties agrees that this Pact will have precedence over the Tender (RFP) / Contract documents with regard to any of the provisions covered under this Integrity Pact.

IN WITHNESS WHEREOF the parties have signed and executed this Integrity Pact (IP) at the place and date first above mentioned in the presence of the following witnesses:-

----
(For and on behalf of Principal / Owner / StockHolding

(For and on behalf of Bidder / Counter Party / Contractor)

WITNESSES:

1.____ (Signature, name and address)

2.____ (Signature, name and address)

Note: In case of Purchase Orders wherein formal agreements are not signed references to witnesses may be deleted from the past part of the Agreement.

ANNEXURE - 6 - Covering Letter on bidder’s Letterhead of Integrity Pact

To,

--- ---

Sub**:** RFP REF NO: IT-06/2024-25 dated 09-Jul-2024 for Supply, Implementation, Monitoring, Maintenance and Management of Information Technology Service Management (ITSM) and Information Technology Asset Management (ITAM) Solutions for 05 (five) years

Dear Sir,

DECLARATION

Stock Holding Corporation of India Limited (StockHolding) hereby declares that StockHolding has adopted Integrity Pact (IP) Program as advised by Central Vigilance Commission vide its Letter No. ------------------ Dated --------------- and stands committed to following the principles of transparency, equity and competitiveness in public procurement. The subject Notice Inviting Tender (RFP) (NIT) is an invitation to offer made on the condition that the Bidder will sign the Integrity Agreement, which is an integral part of tender (RFP) documents, failing which the tender (RFP)er / bidder will stand disqualified from the tender (RFP)ing process and the bid of the bidder would be summarily rejected. This Declaration shall form part and parcel of the Integrity Agreement and signing of the same shall be deemed as acceptance and signing of the Integrity Agreement on behalf of the StockHolding

Yours faithfully,

For and on behalf of StockHolding Corporation of India Limited
(Authorized Signatory)

ANNEXURE – 7 – Compliance Statement

(To be submitted on Company Letter Head)

RFP REF NO: IT-06/2024-25 dated 09-Jul-2024 for Supply, Implementation, Monitoring, Maintenance and Management of Information Technology Service Management (ITSM) and Information Technology Asset Management (ITAM) Solutions for 05 (five) years

Subject: Supply, Implementation, Monitoring, Maintenance and Management of ITSM and ITAM Solution for StockHolding

DECLARATION

We understand that any deviations mentioned elsewhere in the bid will not be considered and evaluated by the StockHolding. We also agree that the StockHolding reserves its right to reject the bid, if the bid is not submitted in proper format as per subject RFP.

Sr. No.	Item / Clause of the RFP	Compliance (Yes / No)	Remarks/Deviations (if any)
1	Objective of the RFP		
2	Scope of Work		
3	Eligibility Criteria		
4	Service Level Agreement (SLA) / Scope of Work		
5	Non-Disclosure Agreement		
6	Payment Terms		
7	Bid Validity		
8	Integrity Pact		
9	All General & Other Terms & Conditions in the RFP		
10	Requirement		

(If Remarks/Deviations column is left blank it will be construed that there is no deviation from the specifications given above)

Date:

Signature with seal

Name & Designation:

ANNEXURE – 9 – Format of Bank Guarantee

This Bank Guarantee is executed by the --------------------------- (Bank name) a Banking Company incorporated under the Companies Act, 1956 and a Scheduled Bank within the meaning of the Reserve Bank of India Act, 1934 and having its head office at -------------------------- and branch office at ________________(hereinafter referred to as the “Bank”, which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns) and Branch office at __________________ in favour of Stock Holding Corporation of India Limited, a Company incorporated under the Companies Act, 1956 and having its Registered Office at 301, Centre Point, Dr. Babasaheb Ambedkar Road, Parel, Mumbai 400 012 (hereinafter referred to as “StockHolding”, which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns) at the request of _________________, a Company incorporated under the Companies Act, 1956 and having its Registered Office at (hereinafter referred to as the “Service Provider”, which term shall mean and include, unless to repugnant to the context or meaning thereof, its successors and permitted assigns).

Whereas

A. StockHolding has, pursuant to the Tender No. ____________, issued the Purchase Order dated ___________ to the Service Provider for providing __________________
B. In terms of the said Tender, the Service Provider has agreed to furnish to StockHolding, a Bank guarantee for Rs. _____________ /- (Rupees ________________ only) till __________ (date).
C. The Bank has, at the request of the Service Provider**,** agreed to give this guarantee as under.

NOW IN CONSIDERATION OF THE FOREGOING:

1. We, the Bank, at the request the Service Provider, do hereby unconditionally provide this guarantee to StockHolding as security for due performance and fulfilment by the Service Provider of its engagements, commitments, operations, obligations or liabilities including but not limited to any sums / obligations / claims due by the Service Provider to StockHolding for meeting, satisfying, discharging or fulfilling all or any obligation or liability of the Service Provider, under the said Tender / Purchase Order.

2. We, the Bank, hereby guarantee and undertake to pay StockHolding up to a total amount of Rs. _________/- (Rupees ________________ only) under this guarantee, upon first written demand of StockHolding and without any demur, protest and without any reference to the Service Provider**.**
3. Any such demand made by StockHolding shall be conclusive and binding on the Bank as regards the amount due and payable notwithstanding any disputes pending before any court, Tribunal, or any other authority and/ or any other matter or thing whatsoever as the liability of the Bank under these presents being absolute and unequivocal.
4. We, the Bank, agree that StockHolding shall have the fullest liberty without consent of the Bank to vary the terms of the said Tender/ Purchase Order or to postpone for any time or time to time exercise of any powers vested in StockHolding against the Service Provider and to forbear or enforce any of the Terms & Conditions relating to the said Tender / Purchase Order and the Bank shall not be relieved from its liability by the reason of any such variation, or extension being granted to the Service Provider or for any forbearance, act or omission or any such matter or thing whatsoever.
5. We, the Bank, agree that the guarantee herein contained shall be irrevocable and shall continue to be enforceable until it is discharged.
6. This Guarantee shall not be affected by any change in the Constitution of the Bank or the Service Provider or StockHolding.

NOTWITHSTANDING ANYTHING CONTAINED HEREIN ABOVE:

1. The liability of the bank under this guarantee is restricted to a sum of Rs. _________/- (Rupees ________________ only).
2. This Bank Guarantee will be valid for a period up to _______________ (date).
3. A written claim or demand for payment under this Bank Guarantee on or before _______________ (date) is the only condition precedent for payment of part/full sum under this guarantee.

For Issuing Bank

Name of Issuing Authority:

Designation of Issuing Authority:

Employee Code:

Contact Number:

Email ID: