

For Kind attention of ITSM Solution Providers

The Indian Audit and Accounts Department (IAAD) under the Comptroller and Auditor General of India envisions implementation of ITSM solution across its Field Audit Offices.

The functional requirements (tentative) for expected ITSM solution is attached as Annexure-I. All ITSM solution providers are requested to participate in half day work shop being organized in this office to share their views on the functional requirement and share industry trends relating to ITSM.

The venue and the timings of the work-shop is as under: -

Date:	26 December 2019
Timings	10.00 AM to 1.00 PM
Venue	INTERNATIONAL CENTRE FOR INFORMATION SYSTEMS & AU. A-52, SEC-62, INSTITUTIONAL AREA, PHASE-II NOIDA (U.P) - 201 307

The interested ITSM solution providers are requested to confirm their participation to sao4is@cag.gov.in by 24 December 2019.

Sd/
(Sreeraj Ashok)
Dy. Director (IS)

Annexure- I

Functional requirement of the prospective ITSM solution

1. IAAD is looking for authorised partners of commercial off the shelf IT Service Management applications or platforms for
 - a. IT Asset Management
 - b. IT Operations Management
 - c. Incident Management
 - d. Change Management
 - e. BI for administrator
2. The data should reside in India.
3. User management should be through Single Sign On using (LDAP of NIC-e PARICHAY) should be possible. Active Directory based solutions will not be accepted.
4. The solution should be able to handle Multiple OSs (Windows, Linux, Mac OS, Android, Chrome OS etc)
5. The partner shall also be responsible for training the end users based on blended learning approach (classroom training for trainers and videos). Training will be for around 300 users in New Delhi.
6. Under the **IT Asset Management** IAAD requires a solution for
 - a. Complete life cycle management of IT assets. The **request for a new IT Asset** should be raised by a Field office in the system. We should be able to **approve or deny the request through a configurable workflow** (configurability restricted to number of stages to grant approval).

- b. The allotment of Fund to field offices will occur outside this ITSM solution. Purchase of asset will occur through GeM or through local arrangement.
 - c. The purchase details, cost, contracts, warranty details etc should be capturable in the ITSM
 - d. At the first instance the new IT asset should be **hardened** using the IT policies defined by the department before allotment to an end user.
 - e. It should be possible to categorise the assets. In addition to the default categories provided by the solution, flexibility should be there for IAAD to add/edit/modify/delete categories.
 - f. End user should be mapped with the asset.
 - g. The configuration or parameters of the device should be automatically captured by the ITSM.
 - h. The Asset should be periodically (time period set by IAAD) tracked.
 - i. Once the predefined life cycle of an Asset is over, user should be able to request for **disposal** through ITSM and approval process should be possible through the ITSM
7. In the **IT Operations Management** IAAD requires a solution that can
- a. IT Hardware Management, Software License Management and Network Monitoring should be possible.
 - b. In **IT Hardware Management**, there should be features for:
 - i. Harden the IT asset before allotment to an end user
 - ii. End user mapping should be possible.
 - iii. IAAD should be able to enforce password policy and automatic password reset after a defined period should be possible.

- iv. Asset Discovery through agentless and agent-based approaches should be possible. End point devices while in NIC net should be scanned and updated through agentless approach. Those end points which are not connected to NIC net for a defined period, should be enforced to update information through an agent-based strategy.
- c. In the **IT Software Licence Management** there should be features for
 - i. The ITSM should scan and identify type of licenses we own, when they will expire, and if they are linked to any contracts.
 - ii. It should provide information on the type of licensing like volume, individual, OEM, CAL, concurrent, and perpetual etc.
 - iii. It should have feature to reconcile the existing licenses as per current inventory of IAAD with the scanned results of ITSM.
 - iv. The catalogue of software provided by Department should be available for an end user. They should be able to request for licenses stating the purpose in the ITSM.
 - v. Administrator should be able to disable licenses for some users through ITSM and re-allot the license to a new user.
 - vi. It should enable pushing of certain software for installation on selected end point devices
 - vii. Its should identify the devices on which certain software (like antivirus) are not installed and allow administrator to enforce installation.
- d. Using **Network Monitoring**, administrator should be able to
 - i. See the devices connected part of the network

- ii. Track the network speed available at different points in the network.
- iii. Enable user and site access policies on top of the NIC network policies.

8. In the **IT incident Management**

- a. The end users should be able to register their complaints or request for services.
- b. The service desk in each Field office should get notification on request.
- c. Those cases which cannot be handled by local field offices should be possible to be escalated to Headquarters office.
- d. The incident management details like, each device by incident registered over a period, status of incidents registered, disposal time for incidents etc. should be available.
- e. The diagnosis of problems and solving will occur the ITSM and is beyond the scope of expected role of MSP. Every field office will have their own service personnel, who will however use this ITSM solution for receiving complaints and will update status of the requests received.
- f. ITSM should have feature to record the root cause against the incident.

9. In the **IT Change Management**

- a. It should be possible to push updates for software to all end user devices from a central server.
- b. Keep track of configuration drifts and deploy secure configuration.
- c. Download, test and deploy patch updates to software.

10.BI for administrator

- a. The designated administrators Headquarters level should be able to get information such as
 - i. IT asset- field office wise, category wise, age wise etc
 - ii. Usage of hardware and licenses and assist in reducing unwanted spending by optimising usage.

Information for partners:

1. IAAD have around 241 field offices, spread across the country. CAG office in New Delhi acts as the Headquarters office
2. 141 offices are on NIC network, while others are availing service of other ISPs.
3. Total number of users of end point devices will be around 30000.
4. Each field office may have 2 service desk users/administrators in initial stage.
5. CAG office will have around 10 service desk users.

Limitation:

During the transition period of 2 years, there will be systems outside any internet connectivity. Feature to capture information manually, regarding these system into the central ITSM database will be helpful.