

Chapter IV

Evaluation of Controls in Aasara IT Application

Chapter IV - Evaluation of Controls in Aasara IT Application

- Password policy management through Aasara IT Application is inadequate.
- Login/logout/IP Address/session details (including time stamps) of officials/staff operating through Aasara IT Application are not maintained.
- Contrary to the guidelines of National Critical Information Infrastructure Protection Centre (NCIIPC) on Proper Backup plan and policy, critical/important information was stored at same location.
- Details of Verification Officer (viz., name, designation) are not captured.
- Inbuilt business rule did not exist for 'Household income' and the system accepted higher incomes than stipulated in the criteria.
- Payments were made to ineligible beneficiaries due to inadequacies in capture of reliable and accurate data and there were gaps in Processing controls and Output controls in Aasara IT Application.

4.1 Evaluation of IT Controls implemented in Aasara Application

For implementing Aasara Pensions scheme, the CEO, SERP issued (December 2014) a work order to the service provider for designing, developing and hosting a dedicated IT application (Web based) and its maintenance for a specified period. The service provider completed the software development and implemented the Aasara IT Application with effect from January 2015. The database is being maintained at the State Data Centre (SDC), Hyderabad. Audit evaluated the controls implemented in the IT application.

4.1.1 General controls

General controls are crucial to ensure effective implementation of IT application and security/integrity of IT and IT systems.

The processes involved in a System Development Lifecycle are (a) Feasibility Study, (b) Requirement Projection & Analysis, (c) Designing & Development, (d) Testing/User Acceptance & Quality Assurance (e) Deployment and (f) Continued Maintenance and Improvements to the product, etc. Audit assessed IT controls associated with development and implementation of Aasara software and observed following gaps:

4.1.1.1 Non-adherence to bidding procedures

The Telangana State Financial Code⁴⁸ stipulates that all State Government Departments/ Agencies shall follow 'open tender system' for procuring goods/services where the estimated value of the order is ₹5 lakh or more. Audit observed that open tendering method/competitive bidding process was not followed for identifying the service provider. A direct work order⁴⁹ was issued (value: ₹38.20 lakh) to the pre-determined vendor (TCS)

⁴⁸ Rule 3 article 125 of Vol-I

⁴⁹ 05/SERP.APS/2014 dated 23 December 2014

on a techno-commercial proposal, prepared by the vendor in October 2014 i.e., three weeks before the Scheme guidelines were issued in November 2014. This indicated that competitive bidding process was not explored.

Government accepted the observation and stated (June 2022) that proposal for ratification is under consideration.

4.1.1.2 Lack of documentation and policies

A) Audit requested SERP to provide records relating to project initiation such as User Requirement Specification (URS), Software Requirements Specification (SRS), Change Management, etc. Documentation on High Level Design, Database Design, SRS, Deployment Manual and Server details only were furnished. URS, Change Requests, Knowledge Transfer terms were not furnished despite repeated written requests. In this background, the gaps between URS and SRS could not be ascertained by Audit.

B) IT Policies and procedures instrumental for assuring protection of information system assets like data, software, hardware, etc. Evaluation of relevant policies and procedures implemented revealed the following:

- Password policy management through Aasara IT Application is inadequate, since enforcement of periodical password change was not made mandatory. Government accepted that password change is mandatory only on first time login.
- Login/logout/IP Address/session details (including time stamps) of officials/staff operating through Aasara IT Application are not maintained and Audit could not evaluate unauthorised access/changes, if any, to the critical/sensitive data. Government replied (June 2022) that IP address and session details were captured but the reply was silent on access or changes to sensitive/critical data.
- Effective User awareness & liability ensure risk free changes to Master data like Bank Account Number, Disability percentage, etc. Audit noticed from analysis of 'ALL_DELETIONS_TILL_NOW' table that payment in respect of 255 beneficiaries was withheld (July 2019) in Charminar Mandal due to change of bank account numbers abnormally, as noticed from Management Information System (MIS) reports. This indicates gaps in access /privilege management, lack of audit logs/trails and review mechanism. Government reply (June 2022) was silent on audit observation. However, CEO, SERP replied (June 2022) that the said case is under investigation by Cyber Crime team of Police.
- Audit sought details of documentation/test cases/acceptance certificates pertaining to the changes implemented. Though access to the periodical work done report on changes was provided to Audit, documentation relevant to major/minor changes proposed/approved with budgets/review by technical committee for implementation of changes along with testing and review reports were not available. This indicates lapses in change management procedures adopted.
- Business Continuity Plan (BCP) and Disaster Recovery management policy (DRP) were not drafted. Audit sought vulnerability assessment reports done by SERP. No specific reply was furnished by the Government for this observation.

- National Critical Information Infrastructure Protection Centre (NCIIPC⁵⁰), guidelines (January 2015) on protection of Critical Information Infrastructure stipulate ‘Proper Backup plan and policy should be in place for the protection of all types of data on the regular basis’ as a best practice. However, Audit observed from the operational log that copies of backup media are being stored at same location (i.e. SDC, Hyderabad) and storing of critical/important information is not being done at any other alternate location, where they may be recovered from, in case of disaster. No specific reply was furnished by the Government for this observation.
- Audit sought documentation on emergency response strategy/testing/alarm procedures and expected response scenarios for attending various levels of emergencies to safeguard the IT assets at SDC or SERP. Excepting Fire Safety Adherence compliance as per SDC norms, no specific reply was furnished for other types of emergencies/disasters.
- Audit observed that adequate training was not provided to staff working at all the implementation levels.
Government reply (June 2022) is not specific to the trainings imparted to field level staff subordinate to MPDOs/Municipal Commissioners/DRDOs.
- Except for Web application security audit (last done in June 2020 for the audit period to end of March 2021), Aasara IT infrastructure lacks defined IT Security Policy and periodical audits, either at SDC or SERP, to ensure security of Database/Network.

4.1.2 Inadequate Input controls

Input controls ensure entry of correct and complete information being fed into the database, thereby, assuring data integrity and reliability. Audit evaluated input controls of Aasara IT Application and the following gaps are noticed:

- Details of Verification Officer (like name, designation) are not captured;
Government replied (June 2022) that details of Verification Officer were captured. However, data analysis by Audit revealed that in 60 *per cent* records (29,20,671 out of 48,51,310 records), Verification Officer details were not available.
- ‘SKS ID’ captured in Aasara IT Application was not standardised;
Government replied (June 2022) that SKS data was not integrated with Aasara IT Application. The reply is not acceptable as it is not in compliance with the Scheme Guidelines.
- Inbuilt business rule was non-existent for ‘Household income’ and the system accepted higher incomes than stipulated in the criteria.
Government accepted the lapse and replied (June 2022) that suitable validation has been incorporated in the system.
- Data entry screens were not designed, as per requirements (SRS), to implement mandatory capture of inputs (like SKS ID, Date of Birth, Age, Account Number, etc).

⁵⁰ Nodal Agency notified (January 2014) by GoI for Critical Information Infrastructure Protection under Section 70A of Information Technology Act 2000

Government replied (June 2022) that capture of information against these columns is mandatory. However, scrutiny of data for the audit period revealed that out of 50,30,158 beneficiaries, important data like Date of Birth against 45,87,465 beneficiaries and Bank Account Number in respect of 7,80,019 beneficiaries was not available. Further, issues referred in paragraphs 3.1.3, 3.2.2.2, 3.2.2.4 and 3.2.3 also indicate inadequate input controls. This has resulted in incomplete/incorrect/duplicate data capture as well as financial loss, as indicated, previously.

4.1.3 Gaps in Processing controls

Data analysis showed that there were ineligible payments to disabled beneficiaries after expiry of the validity of SADAREM certificates. Similarly, cases of payments to beneficiaries with duplicate/improper SADAREM IDs and lesser degree of disability than the prescribed limits⁵¹ were detected. Details of payments made to ineligible beneficiaries due to inadequacies in capture of reliable and accurate data are described below:

- In 7,675 cases, pension payments of ₹14.01 crore were made even after expiry of SADAREM certificate during the Audit period. This indicates that validity/renewal of disability certificate (SADAREM) was not checked/carried out periodically. Government replied (June 2022) that ratification proposals are under consideration.
- In respect of 7,336 cases improper/duplicate SADAREM IDs were detected and 1,302 beneficiaries were paid pensions of ₹5.56 crore during the audit period. This indicates that department had sanctioned pensions without verifying the uniqueness of the SADAREM ID. Government replied (June 2022) that validation to prevent duplicate SADAREM IDs was put in place since February 2019. However, Audit detected six cases of duplication even after February 2019.
- The degree of disability in respect of 73 hearing impaired and 304 other than hearing impaired (Total: 377 cases) was less than the percentage stipulated. Amounts of ₹10 lakh and ₹28 lakh respectively were disbursed to these ineligible beneficiaries during audit period.

Government replied (June 2022) that validation for percentage of disability was put in place since February 2019 and upon reassessment, pension was stopped if the percentage is less than the stipulation. However, scrutiny of data revealed three instances of sanctions with lesser disability percentage after February 2019 also.

- Cross-checking of Aasara data with National Voters' Service Portal, Aadhaar particulars and details submitted in the physical applications revealed that 14 applicants⁵² having age less than 65 years were sanctioned Aasara Pension under OAP category in violation of the inclusion criteria. Payments made to these ineligible persons during the audit period worked out to ₹5 lakh. Beneficiaries age should be updated/ calculated automatically after initial data entry. However, the department stated (December 2021) that the age captured during data entry was not being updated periodically.

Government confirmed (June 2022) the ineligibility of the beneficiaries in 11 cases and stated that enquiry is pending against three cases.

⁵¹ Hearing Impaired: 51 per cent and other categories: 40 per cent

⁵² Hyderabad district: one case-₹0.55 lakh; Medak district: seven cases-₹2.35 lakh; Siddipet district: five cases: ₹1.53 lakh; Yadadri-Bhuvanagiri district: one case-₹ 0.57 lakh

- Further, during the scrutiny of sampled applications, Audit detected that 13 beneficiaries under widow (6 cases), OAP (4 cases) and disabled (3 cases) categories though not eligible under the respective categories (as per inclusion and exclusion criteria) were sanctioned pension.

Government confirmed (June 2022) the ineligibility in these cases.

Above observations indicate inadequate processing controls.

4.1.4 Gaps in Output controls

Output controls provide reasonable assurance for matching the results of authorised and approved input processes with the output generated. Control totals produced in outputs during processing need to be compared and reconciled with input control totals.

- Audit observed that the MIS Report R5.1(b) generated through Aasara Portal for the month of March 2020 was erratic since there was a mismatch between number of beneficiaries and corresponding amount for undisbursed totals. This indicates lapses in reporting/output generation.
- There was mismatch between the sanction orders relating to new pensioners added in Siddipet district and total sanctioned pensioners' report (R 2.2 of Aasara Portal) for the period from November 2016 to September 2020. Aasara IT Application is not facilitated to carry out reconciliation of funds (control unit wise) for flagging of undisbursed/unutilised amounts for recovery purpose. Government concurred (June 2022) that reconciliation of undisbursed funds is taking place under DoP mode only, leaving out undisbursed funds in bank and manual modes.
- Under the jurisdiction of Greater Warangal Municipal Corporation, 10 beneficiaries were being credited with Aasara Pension amount even though these beneficiaries were reported as deceased/expired (May 2020). Aasara IT Application reflected the current status of these beneficiaries as 'live'. This indicated that the current status of a beneficiary and the IT Application reports are not being updated in a timely manner. Non-updating of beneficiary data in these cases resulted in erratic output as well as ineligible payment of ₹0.73 lakh during April 2018 to March 2021 for nine beneficiaries. Status of these beneficiaries was updated after intimation of audit observation. Similar lapses pertaining to live status of beneficiaries have been brought in *paragraph 3.3.4 supra*. Government concurred (June 2022) that pensions were credited to deceased beneficiary accounts due to delay in reporting of death/updation.

These cases indicate that Aasara IT Application has certain gaps in implementing effective/adequate output controls. Further, issues relating to age criterion and disability percentage level as referred to in *paragraph 3.5 supra* also indicate inadequate output controls.

4.1.5 Lacunae in data management system controls

Standard data management controls assure accurate and consistent data maintenance. Ineffective data management controls do not mitigate the risks relating to data integrity and security.

- Scrutiny of data revealed that important information like age, bank account number, SKS ID and surname are not accurately captured. Further, mechanisms to maintain/update accurate data do not exist, due to which implementation of criteria in categorisation/disbursement processes were affected as brought out in *paragraph 3.2 supra*. Government replied (June 2022) that capture of Bank Account details was made mandatory for beneficiaries drawing pensions under DoP mode since January 2017. However, scrutiny of data revealed that bank account numbers are not available against beneficiaries who were sanctioned pension prior to January 2017. This indicates lack of data updating for such persons.
- Audit observed that the software maintenance service provider was directed (January 2018) to make changes to Aasara data unilaterally by updating age of Old Age pensioners having age as null in the database to 66 years. Similarly, the age of widow pensioners was directed to be updated between 35-40 years and for other categories to the age prescribed in eligibility criteria. As a result, the age of 3,88,005 (out of 17,76,109) OAP pensioners and that of 2,08,555 (out of 16,88,180) widows was updated without any basis. This indicates that Aasara data is not supported with documentary proof of age stipulated in the Aasara Pensions scheme guidelines. Government did not furnish specific reply to this observation. Responsibility on the concerned officials needs to be fixed and disciplinary action should be taken.
- Aasara IT Application lacks provisions for uploading of manual application/verification report and also does not facilitate the capture of all required details to ascertain eligibility. This indicates that Aasara IT Application is ineffective in providing assurance for transparency/verifiability in sanction process as brought out in *paragraph 3.2 supra*. Government stated (June 2022) that a facility has since been created in the Portal enabling uploading of scanned copy of beneficiary application, duly certified by PS/BC and MPDO/Municipal Commissioner.
- Due to lack of standard data maintenance practices and cleansing activities, inadequacies/inconsistencies were noticed as brought out in *paragraph 3.2 supra*. Department stated (June 2022) that data cleansing activities would be taken up.

During the exit meeting, the Government accepted the audit observations and stated that the audit process had aided in identifying the gaps in the Aasara IT application and necessary rectifications shall be carried out.

4.1.6 Grievance Redressal Mechanism

An effective Grievance Redressal System enables users and stakeholders to escalate and resolve issues and prevents delay in services provided through IT solution.

Scrutiny of grievances data revealed that 53,097 issues were reported through Aasara IT Application. Of this, 51,653 (97 *per cent*) issues relate to rolling back the status of beneficiary (from ineligible to eligible), 1362 relate to change of address, 72 relate to issues with Point of Transaction Devices (POTD Module), 6 relate to Name Correction of Pensioner and 4 relate to wrong tagging of SADAREM (SADAREM ID Wrong Tagging Module).

Ninety-seven *per cent* of issues in Rollback module indicate that beneficiaries were excluded in erratic manner or on misrepresented facts. This indicates that in these cases,

verification status of beneficiaries (like death, permanent migration/temporary migration/marital status and other inclusive criteria) was not obtained and authenticated in proper manner, necessitating generation of many change requests. In 3,838 cases, “death” of beneficiary was reported by PS but subsequently, requests were received from Heads of Jurisdictional unit offices to change the beneficiary status to “live”. This indicates that due diligence was missing while escalating the facts and acting on such false cases disturbed timely disbursal of benefit to the beneficiaries.

Audit sought for the evidence regarding objective and verifiable methods implemented to ensure accuracy/authenticity of the reports given by the verifying staff/officers. The same was not furnished. This indicates gaps in controls to prevent the risk of incorrect verification reports.

4.2 Conclusion

There were deficiencies in input, processing and output controls which led to payment of benefits to ineligible persons. There were certain inadequacies and errors in data capture which should be rectified to ensure accuracy, adequacy and consistency.

4.3 Recommendations


Aasara IT Application should be upgraded and strengthened to render an end-to-end solution for effective service delivery and to counter manual intervention and the possibility of preferential sanctions.

Hyderabad
The


(SUDHA RAJAN)
Accountant General (Audit)
Telangana

Countersigned

New Delhi
The


(GIRISH CHANDRA MURMU)
Comptroller and Auditor General of India