PRESENTED TO THE
ODISHA LEGISLATIVE ASSEMBLY
ON THE 3RD OCTOBER, 2020

सत्यमेव जयते

ODISHA LEGISLATIVE ASSEMBLY

PUBLIC ACCOUNTS COMMITTEE

2020-2021
SIXTEENTH ASSEMBLY

3RD REPORT

ON

C & A. G OF INDIA (GENERAL AND SOCIAL SECTOR)
REPORT NO. 4 OF THE YEAR 2016
OF
ELECTRONICS AND INFORMATION TECHNOLOGY DEPARTMENT-2014-15

SECRETARIAT
OF
THE ODISHA LEGISLATIVE ASSEMBLY,
BHUBANESWAR-751001

CONTENTS

COMPOSITION OF THE PUBLIC ACCOUNTS COMMITTEE, 2020-21

C H A I R M A N

Shri Pradipta Kumar Naik,
Leader of Opposition.

M E M B E R S

Smt. Pramila Mallik,
Hon'ble Government Chief Whip.

Shri Mohan Charan Majhi,
Hon'ble Chief Whip, Bharatiya Janta Party

Shri Narasingha Mishra, M. L. A.

Shri Debiprasad Mishra, M. L. A.

Shri Jaya Narayan Mishra, M. L. A.

Shri Sarada Prasad Nayak, M. L. A.

Shri Pranab Prakash Das, M. L. A.

Shri Rajendra Dholakia, M. L. A.

Shri Braja Kishore Pradhan, M. L. A.

Shri Priti Ranjan Gharai, M. L. A.

Shri Ananta Narayan Jena, M. L. A.

S E C R E T A R I A T

Shri Dasharathi Satapathy, I. A. S., Secretary.

Smt. Sushila Mallick, Deputy Secretary.

Smt. Baijayanti Pattanayak, Under Secretary.

Shri Partha Sarathi Das, Section Officer.

Smt. Manjushree Tripathy, Assistant Section Officer.

COMPOSITION OF THE PUBLIC ACCOUNTS COMMITTEE, 2019-20

C H A I R M A N

Shri Pradipta Kumar Naik,
Leader of Opposition.

M E M B E R S

Smt. Pramila Mallik,
Hon'ble Government Chief Whip.

Shri Mohan Charan Majhi,
Hon'ble Chief Whip, Bharatiya Janta Party

Shri Narasingha Mishra, M. L. A.

Shri Debiprasad Mishra, M. L. A.

Shri Jaya Narayan Mishra, M. L. A.

Shri Sarada Prasad Nayak, M. L. A.

Shri Pranab Prakash Das, M. L. A.

Shri Rajendra Dholakia, M. L. A.

Shri Braja Kishore Pradhan, M. L. A.

Shri Priti Ranjan Gharai, M. L. A.

Shri Ananta Narayan Jena, M. L. A.

S E C R E T A R I A T

Shri Dasharathi Satapathy, I. A. S., Secretary.

Smt. Sushila Mallick, Deputy Secretary.

Smt. Baijayanti Pattanayak, Under Secretary.

Shri Partha Sarathi Das, Section Officer.

Smt. Manjushree Tripathy, Assistant Section Officer.

COMPOSITION OF THE PUBLIC ACCOUNTS COMMITTEE, 2018-19

C H A I R M A N

Shri Narasingha Mishra
Leader of Opposition.

M E M B E R S

Shri Debiprasad Mishra, M. L. A.

Smt. Pramila Mallik, M. L. A.

* Shri Dilip Kumar Ray, M. L. A.

Shri Pravata Kumar Tripathy, M. L. A.

Shri Pravat Ranjan Biswal, M. L. A.

Shri Mahesh Sahoo, M. L. A.

Shri Saroj Kumar Samal, M. L. A.

** Shri Naba Kishore Das, M. L. A.

Shri Samir Ranjan Dash, M. L. A.

Shri Chiranjib Biswal, M. L. A.

Shri Debasish Samantaray, M. L. A.

S E C R E T A R I A T

Shri Amiya Kumar Sarangi, Secretary.

Shri S. K. Swain, Joint Secretary.

Shri M. Dungdung, Under Secretary.

Shri Prafulla Kumar Parida, Desk Officer.

Smt. Baijayanti Pattanayak, Desk Officer.

N. B.:-

* The Membership of Shri Dilip Kumar Ray, M. L. A. was ceased w.e.f. 30.11.2018 vide notification No. 10486/L. A., dated 5th December 2018.

** The Membership of Shri Naba Kishore Das, M. L. A. was ceased w.e.f. 28.01.2019 vide notification No. 742/L. A., dated 30th January 2019.

COMPOSITION OF THE SUB-COMMITTEE-V OF THE PUBLIC ACCOUNTS COMMITTEE, 2018-19

C H A I R M A N

Shri Saroj Kumar Samal, M. L. A.

M E M B E R S

Shri Pravat Kumar Tripathy, M. L. A.

Shri Mahesh Sahoo, M. L. A.,

S E C R E T A R I A T

Shri Amiya Kumar Sarangi, Secretary.

Shri Shishir Kanta Swain, Joint Secretary.

Shri M. Dungdung, Under Secretary.

Shri Prafulla Kumar Parida, Desk Officer.

Smt. Baijayanti Pattanayak, Desk Officer.

Smt. Manjushree Tripathy, Assistant Section Officer.

INTRODUCTION

I, the Chairman of the Public Accounts Committee having been authorised by the Committee on their behalf present this 3rd Report of the Public Accounts Committee on the Report of the C & A. G of India (General & Social Sector) for the year 2014-15 relating to Electronics and Information Technology Department.

The Sub-Committee-V of Public Accounts Committee had examined the above subject in its meetings held on 25.06.2018, 24.12.2018 and 28.02.2019. The findings and conclusion which are based on the result of the examination of the Committee are presented herewith.

The Public Accounts Committee, 2019-20, finalized the Report in their sitting held on 20.03.2020 and reapproved by the Public Accounts Committee 2020-21 on 01.10.2020.

The Committee place on record their appreciation of the assistance rendered by the officers of the Departments of Electronics & Information Technology, Finance and the Office of the Accountant General (G & SSA), Odisha during the course of examination.

The Committee further express their thanks to the Officers and Staff of the Odisha Legislative Assembly Secretariat for their Secretarial assistance.

Sd/-

Bhubaneswar
Date: 01.10.2020

(PRADIPTA KUMAR NAIK)
C H A I R M A N
PUBLIC ACCOUNTS COMMITTEE

REPORT

1. Para-2.2.6 of the Report of the C & A. G of India (G & SSA) for the year 2014-15 Release of payment deviating from Service Level Agreement

The implementation of OSWAS in Odisha for making the work flow process of Government automated is an initiative for transparent governance and is a joint effort of user departments and OCAC. It had been a major challenge to make it acceptable to the system.

As per Service Level Agreement (SLA) between OCAC and TCS, payments were to be made after successful completion of milestones and submission of deliverables. Ten core applications, 20 common applications and 99 department specific applications for 37 departments and Chief Minister's Office were to be developed by January 2010. The common and department specific applications were to be set up on the functionalities of the core applications as per milestones specified in SLA.

2. Para-2.2.6.1 Non-Development of applications under OSWAS.

Audit pointed out that:-

- One (e-mail) core application out of 10 was not developed as yet.
- Out of the 20 common applications, six were not developed and 10 though developed, were found incomplete. The rest were used by some departments.
- None of the 99 department specific applications were developed.

OCAC stated (May 2016) that all applications had been developed except 50 department specific applications. During Exit conference, Principal Secretary instructed OCAC to show the e-mail module and six common applications to Audit, if developed. Accordingly, Audit re-examined (May 2016) the OSWAS but OCAC could not produce any evidence of development of one core and six common applications. OCAC released (as of March 2016) ₹ 8.31 crore out of ₹ 9.74 crore to TCS for software development, despite non-development of all core and common applications and without ensuring inclusion of key features in OSWAS.

The Department was of the opinion that:-

- The email module of core application had been developed and POC had been done. It was not deployed as mail server was not configured. As eDespatch was successfully implemented in all departments, both applications were integrated to achieve the email functionality.
- All common applications had been developed and demonstrated. As the implementation was joint effort of both user departments and OCAC,

delay in approval and acceptability of the applications by them delayed the implementation and some of the modules could not be deployed.

New 11 common applications were used extensively by the various Departments. There was a technical Committee headed by Director, IIIT and some of the key officers of some Departments were there. They used to evaluate the performance of the system. Basing on the recommendation of the Committee the payment was released. For common applications full payment was not released to TCS. Partly payment was released to TCS. For Departmental specific applications not a single pie was released as it had not been implemented and not in use.

- 49 Departments specific applications had been developed by TCS for which approval could not be obtained. Regarding the rest 50 applications, the requirements could not be finalized after several reminders.

Out of the expenditure of around ₹ 26 crore made under OSWAS, actual expenditure for OSWAS Application would be ₹ 9 crore which was payable to TCS. The payment had been released to TCS for the modules which had been implemented as per SLA Besides, though the expenditure incurred for provision of infrastructure like Desktops, UPS, Scanner etc. to users departments (officers and staff of Secretariat) under OSWAS project had been made out of the budgetary sanction of Governments, the same was not being used exclusively for OSWAS. The hardware was also being used for other official works by the Secretariat staff.

After a detail deliberation the Committee dropped the para.

3. Para-2.2.6.2 Non-receipt of deliverables.

Request for proposal (RFP) and SLA required that OSWAS would support Secure Sockets Layer (SSL), biometric based access, e-mail and fax integration and bilingual interface. It also required that the source code of all applications of OSWAS along with necessary documentations would be shared with OCAC/GoO. Audit pointed out that:-

- In absence of SSL, the password, personal notes, personal information of users and other confidential files were transmitted through the SECLAN in plain text and the transmissions were not secure.
- OSWAS had weak access control due to absence of biometric access control.
- In absence of e-mail and fax integration, the users had to print, scan, sign and send communication separately leading to unnecessary duplication of work and wastage of paper.
- Absence of local language i.e. Odia interface led to reduced user friendliness of OSWAS. It also failed in implementation of official language.

- In absence of delivery of source code along with database and application design documents, Government could not engage other vendors for up-gradation or further modification of OSWAS effectively, resulting in vendor lock-in.

OCAC released (as of March 2016) ₹ 8.31 crore out of ₹ 9.74 crore to TCS for software development, despite non-development of all core and common applications and without ensuring inclusion of key features in OSWAS.

The Department while accepting the fact, assured (May 2016) that efforts would be made to receive the deliverables, documentations and source code from the vendor.

The Departmental compliance stated that as security audit had been completed, the hosting of application would be done after obtaining SSL Certificate for the desired secured link.

POC had already been completed for Biometric based access, eMail and FAX features available in OSWAS Application and these features could be enabled after obtaining the required hardware devices. At present, eMail and FAX support for outward communication were being done through integration with eDispatch as it was successfully implemented across all departments along with line/subordinate offices.

As per the "Exit Management" clause in SLA, the exit process was to be initiated for knowledge transfer and submission of deliverables including source code etc. OCAC should ensure receipt of all the deliverable before release of final payments to TCS. The payments that had been released to TCS, as on date, were on completion of milestones as per SLA.

- Odia interface had been incorporated in OSWAS. Users had been trained and were being encouraged to use the official language.
- The agreement (SLA) with TCS for implementation of OSWAS were in force at the time of audit. Transfer of knowledge and the source code of the Application was part of Exit process as per SLA. Hence there were no scope of vendor lock-in.
- Though the project was being executed through TCS, Government of Odisha is the owner of the OSWAS Application, which includes all documentations and source code. A Committee constituted as per orders of Government had evaluated the deliverables and efforts of TCS for release of payments to TCS.

After a detail deliberation the Committee dropped the para.

4. Para -2.2.7 Absence of Business Process Reengineering.

Audit pointed out that as per RFP, the solution provider was to suggest necessary re-engineering of processes to enable adoption of the OSWAS. Programme

Setup Team (PST) was also constituted (December 2008) consisting of officers of various departments to facilitate Business Process Re-engineering (BPR) before finalising the SRS. PST recommended (February 2009) suitable changes in the Odisha Secretariat Instructions as per the systems designed by TCS instead of customising OSWAS to suit prevalent manual system.

This recommendation was not carried out and Secretariat Level Implementation Committee (SLIC) decided (January 2013) to constitute a BPR committee comprising of officers from departments along with members from OCAC and TCS to finalise BPR based on the feedback from user departments. The said committee was to meet every fortnight for this. But, the BPR committee was not constituted during 2013-14 to take up the work.

Therefore, the Manual for Office Procedure, i.e. OSI was not updated to incorporate the changes in workflow processes suiting to new electronic environment. It was noticed that OSWAS was used without incorporating checks provided in OSI for ensuring accountability. Moreover, it also led to lack of uniformity in handling files across departments.

- OSI required insertion of signatures in file for accountability and authenticity. However, digital signature was not implemented for all file/document users in OSWAS which led to accountability issues.
- Data received from 26 out of 43 Departments/organisational units, revealed that only Rural Development Department maintained consistency in file keeping as all files were in electronic form. 25 other Departments/units created 1,66,735 manual files and 92,035 electronic files during 2012-15. Departments were also maintaining files partly in manual and partly in electronic form, which resulted in bypassing of OSWAS.
- In absence of changes in business rules, other applications provided in OSWAS like management of Confidential Character Reports/Annual Confidential Reports, process for constitution and monitoring of committees, processing of Public Accounts Committee queries, grievance management system, audit assessment and appeal details system and asset management system were never put to use.

The Department stated that initially a PST (Programme setup team) was constituted to facilitate BPR for finalizing the SRS which could not perform due to non-availability of members.

The BPR Committee could not meet as committee members from the designated departments were nominated. Later GA Department, being the nodal department for Odisha Secretariat Instructions, was assigned to take up the BPR

activity for smooth implementation of OSWAS as per decision taken in the High Level Meetings.

OSWAS Application is now DSC enabled. The use of DSC would be made mandatory after acquiring of the same by all users of different Government Departments.

As stated earlier, the implementation of OSWAS had been a challenge for the Government. The user's acceptance could be achieved after several persuasion and dedicated handholding support.

- GA Department, being the nodal department for Odisha Secretariat Instructions, had initiated steps for necessary changes in the OSI.
- OSWAS Application had been developed based on the existing OSI and checks as per requirement are incorporated to ensure accountability. Common interface of OSWAS Application was used across departments to ensure uniformity in handling files.

Now the Chief Secretary office did not receive any manual file, they only allowed the file in OSWAS system. Due to the checking of Chief Secretary Office all the Departments were working through OSWAS system.

The Committee instructed to conduct a special meeting with G. A Department for BPR, so that OSI would be modified and minutes of the meeting should be supplied to Public Accounts Committee. In view of the Departmental compliance the para was dropped.

5. Para -2.2.8 Inadequate control over Database Administrator.

Database Administrator (DBA) is responsible for the performance, integrity and security of a database. DBA has the tools to establish controls over the database and the ability to override these controls. Therefore, Government must exercise close control over database administration through segregation of duties, supervisory review of access logs and activities and detective controls over the use of database tools.

Audit pointed out that (a) Segregation of duties is essential to ensure that a single person is not responsible for diverse and critical functions in such a way that errors or misappropriations could occur and not be detected in a timely manner and in the normal course of business processes. Therefore, DBA should not be given other responsibilities like system administrator, help desk and data entry. But it was noticed that even after six years of implementation of OSWAS, the software developer TCS continued both as system administrator and DBA. It was also entrusted with user management, help desk and master data entry roles. Government did not even plan to build capacity to take over the database administration and user management of OSWAS in spite of requests from user departments like Revenue and

Disaster Management Department. As a result, OCAC allowed TCS to unauthorisedly access all types of files of Government of Odisha and even manipulate/change notes in critical files.

(b) Inadequate compensating controls for DBA activities: Supervisor review of access logs and activities was essential to detect any suspicious activities of DBA or users. However, logs to track activity of Database Administrator of OSWAS were not enabled and any database vault system for OSWAS Oracle database in place to prevent unauthorised activity of data manipulation by DBA could not be activated. Further, OCAC did not conduct any supervisory review of OSWAS. Even third party audit as decided (January 2013) in SLIC meeting, was not conducted. As a result, unauthorised DBA activities remained undetected.

Besides, no compensating controls were provided such as DBA access and transaction logs, reconciliation with user department and exception reporting. Audit could not recreate the actual transaction flow from point of origination to its existence on an updated file in absence of audit trail of DBA activities.

Further, the logs to capture the activity of the users in OSWAS database were kept in the same server within the control of TCS since a separate remote log server outside the control of the database administrator was not set up. As a result, even user transaction logs were modified.

The Department stated that DBA was transitional based and that complete data base administration had not been taken over as there were lot of transitional issues and their PMU was not taken over the control. But to very precisely at the moment they had not taken up all the activities. Because they were continuously holding with the hand holding support provided by the TCS till that project period was there. But as far as DBA was concerned and since transitional issues were there the entire control had not been taken over at the movement. Further the Department stated that the Department had moved to OSWAS-2.0 in November and to had a segregation of duties and control as mentioned by A. G. in their observation. The Department had formed one PMU and they were the Departments staff engaged by OCAC and they were taking control of all the database administration and also control of users creation etc as regards other attributes are concerned the Department also engaged P.W.C. as third party Audit. In third party Audit, the Department did the SLA Audit, ONM Audit, Functional Audit, Infrastructure Audit and Security Audit/DABT, EMS configurations and review of project management etc.

The Committee after detailed discussion with the Departmental representatives and A. G officials concluded that in view of the steps taken by the Department for engagement of third party to ensure confidentiality, integrity and availability of information in OSWAS the para should be dropped.

6. Para -2.2.9.1 <u>Implementation of digital signature on file notes.</u>

Digital signature not made mandatory: Government of Odisha decided (2013) to incorporate digital signature facility in OSWAS from Under Secretary Level and above. Audit pointed out that however, only 242 digital signature certificates (DSCs) were procured against 686 officers of Under Secretary and above level officers. However, only 205 DSCs were issued.

As use of digital signature was not made mandatory in OSWAS, even officers who were issued digital signature did not append it on all notes. Since June 2014, out of 9, 22,275 notes created in OSWAS, only 38,387 were digitally signed.

Further, 64 digital signature keys issued were not used even once. Thus, non-enforcement of digital signature on note side in OSWAS rendered the electronic files generated open to risk of alterations. Paragraph V-34 of OSI stipulated that when an officer agrees with the preceding note or recommendation he shall append his signature. However, marginal notes or notes to emphasise special points might be made.

In such scenario, if changes were made in previous notes by DBA/insider/other elements, the basis of decision taken in succeeding note could not be ensured. Anomalies in notes i.e. deletion of notes, broken chronology, etc., were noticed in audit, confirming the failure of controls in authentication of the users. Thus, the purpose of including digital signature for signing of the approvals on the file noting was defeated. The Department stated that digital signature would be made mandatory to enforce accountability.

Repudiation of Digital Signature: Section 3 of IT Act, 2000 stipulated that the authentication of electronic record should be effected through the use of asymmetric crypto system and hash function which enveloped and transformed the initial electronic record into another record. Further, it also stipulated that any person by use of a public key of the subscriber could verify the electronic record.

For digital signature on note side, form signer with four licenses was procured from TCS at a cost of ₹ 12.98 lakh. However, TCS did not incorporate asymmetric crypto system as hashing algorithm was not applied to the note contents. Instead, OSWAS stored the original note details in one table and digitally signed encrypted content in another table, which it verified by decrypting and comparing with the original content.

Further, Audit revealed that 38,944 notes had been digitally signed by 141 officers of Secretariat. Test check of 643 OSWAS files revealed that 51 digitally signed notes pertaining to 40 files did not show verified signature on user screen. Further analysis revealed that these notes were modified after digital signature was applied. However, users could not be alerted of broken signature as nothing was

displayed on the screen. Besides, there was no other provision through which users could verify the breach of their digital signatures. Thus, the digital signature process followed in OSWAS did not comply with IT Act, 2000.

The table containing encrypted noting was tampered as it contained text 'null' in 35 occasions instead of encrypted value. It appeared that DBA had tested this type of manipulation in the back end in September and October 2014 when they changed four notings of Chief Secretary on 9th September 2014. Subsequently, 31 such notings were manipulated.

Database analysis also revealed 22 records containing encrypted value of noting without corresponding noting contents. This occurred because the note details were delinked from encrypted noting in the back end.

The integrity of digitally signed documents, thus, became doubtful as DBA log was also not maintained and other transaction logs were tampered with.

Admitting the inconsistencies, OCAC stated that TCS had been instructed to verify and rectify the inconsistencies and agreed to explore the possibility of making digital signature compliant with IT Act, 2000.

Audit pointed out that in case of providing files to external stakeholders such as judiciary, vigilance, audit, etc., PDF copies of files generated from OSWAS were required to contain digital signatures. But, OSWAS could not generate the PDF files with digital signatures even when the original digitally signed documents were available.

OCAC confirmed that PDF version of the file generated through OSWAS did not contain digital signature.

The Department stated that there was a provision in OSWAS Application to apply Digital signatures on the PDF documents (letters/correspondence) generated from OSWAS Application after approval. However, this had not been enforced by Government mandate.

Though the digital signature was enabled due to the practical difficulties it was not mandatory. Audit objected; as to why the DCS was not made mandatory in OSWAS. In the higher level meeting it was decided that file should go for first level of authentication based on user ID and password. And right now also the file having three more software authentication on was digital signature based in the new OSWAS, E-sign which was Aaddhar based and third was first level of authentication based on OTP. So user ID, password and OTP were used and DSC or E-sign was not mandatory.

The PDF copies were scanned copies of the letters signed by issuing authority which had been uploaded in OSWAS.

The Committee accepted the reply given by the Department and dropped the para.

7. Para -2.2.9.2 Unauthorised access of files and tampering of access logs.

The user accounts of Government employees (Users) are created in OSWAS to enable them to function in OSWAS. Login name and passwords are provided to users for securely accessing OSWAS. For monitoring unauthorised access, entry and exit time of each login session in OSWAS, a "transparency log" was displayed on the computer screen of the respective users for monitoring their login activities.

Audit found that the user accounts were accessed in 6,110 cases by DBA by passing login authentication without the knowledge of users. Audit analysis revealed that DBA unauthorisedly accessed OSWAS using the accounts of 1,308 users which included accounts of Chief Minister, Ministers, Chief Secretary and other Secretaries. In order to hide this unauthorised access from users, DBA also sanitised the transparency logs in the back end. Further, no system of supervision by Government was in place to detect the unauthorised activities of DBA. The tampering of logs by DBA was a violation under Section 43 of IT Act, 2000. The Department stated (May 2016) that action would be taken to avoid such breach of system in future.

The Department stated that TCS helpdesk supported associates access user accounts when any problem was encountered using Helpdesk machines. Also, before handling over the user account to respective owner, a basic testing was performed to validate the credentials and checking for errors (if any). Sometimes, users directly visit TCS helpdesk and login through their machines for troubleshooting.

TCS had no role to say as far as file process was concerned. If some reference were there, that might be test data created by, so that they simulate the situation.

The Committee directed the Department to provide detail information both to A. G and also to Assembly Secretariat regarding the action taken by the Department.

8. Para -2.2.9.3 Activity deletion from audit trail.

In OSWAS, file transactions like file approval, file sending, draft preparing and approving were captured in Audit trail table. Each activity on the file was identified by a consecutive serial number in order of operation carried out and as activity orders were numbered. Analysis of the database revealed gaps between two consecutive activity order numbers in three occasions. The missing activities were due to back end deletion of particular activities since the number of such occurrences were very small to indicate systemic error. Similarly, there were 12 gaps found in the note order indicating deletion of notes in the back end.

The Department stated that TCS was never allowed to access files. The user creation and deletion had been made on request of user departments.

The gap/discrepancy observed in the database was mostly due to the fact that there was a break in the usage of OSWAS Application after usage started in 2009. The Department stated that, the system was no more there and they had new platform.

As the system was obsolete the Committee dropped the para.

9. Para -2.2.10 Business Continuity and Disaster Management.

Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) are to be implemented to resume the business within defined timeframe in case of disaster. Audit noticed the following deficiencies:

- **Absence of BCP**: BCP was not framed and adopted for OSWAS even after lapse of more than six years of implementation. In its absence, the staff/ users were unaware of the procedure to be followed in the event of disruption/ disaster. They were also not trained in preventing, mitigating and responding to emergency situations. Thus, emergency response, user recovery, contingency plan and crisis management activities were missing from OSWAS implementation.
- **Absence of disaster recovery site:** DRP was not in place for the Data Centre hosting OSWAS. Disaster Recovery site or alternate processing facility was not established. Critical Government processes/functions were at a risk of disruption in the event of a disaster. The system, as a result, was prone to loss of data, applications, systems, documents, etc. Further, the environment controls in the Data Centre were poor as water/moisture detector, early fire alarm system, smoke detectors, raised floor, adequate fire suppression systems were not found installed making the data center vulnerable to damage.
- **Inadequate back-ups and restoration:** The system provided a schedule for daily and monthly backups for applications and database. However, it was not produced to Audit. Backups were never tested in scheduled manner for recovery and restoration.
- **Inadequate preventive and detective controls for viruses:** OCAC did not take adequate preventive and detective controls for computer viruses as servers (Windows) were not found protected by antivirus software. Desktop antivirus system was found to have expired as on January 2016.

The Department stated that steps were being taken to setup Disaster recovery facility for OSWAS project. The plan of establishing the BCP at OSDC was being explored.

- New SAN storage system had been installed for OSWAS and regular Backups of OSWAS Database were taken as per schedule. Backup and restore plan

using Tivoli Storage Manager would be resumed after installation of new Server hardware.

- As part of preventive control, centralized antivirus software had been installed on all systems. OSWAS had been configured for usage in Intranet environment in the Secretariat LAN and access to this environment was restricted through Firewall.

As per the instructions of the Committee Audit examined the sites and test checked the Business continuity plan. Disaster Recovery Plan, backups and restorations and observed as follows (i) the logs of one month generated during synchronization of data of data in May 2019 were checked and noticed that the file system data, database records and application were regularly replicated from DC site to BCP site. However, the BCP did not contain any provision for periodic testing of BCP Site. (ii) the OSWAS did not have DR Policy as such. The Department stated that as the data are replicated from the Primary data center to the BCP site at State Data Centre the disaster recovery plan of the Odisha State Data Centre (OSDC) was applicable. However, OCAC had not ensure testing of disaster recovery plan of OSWAS in OSDC. (iii) as regarding the backups and restoration logs the data of OSWAS were regularly backed up to Tape Library. The restoration check was carried out regularly. (iv) a Third Party Auditor (TPA) was appointed to monitor various aspects of OSWAS which included checking of backup and restore, BCP.

The Committee recommended that periodic testing of the BCP site should be made by the Department. Further, OCAC should ensure testing of disaster recovery plan of OSWAS in OSDC.

10. ***Para -2.2.11 Application Controls. Absence of administrative interface.***

The architectural design of OSWAS provided for master data management, back up operation and maintenance, etc., only through an administrative interface to ensure database security of the system. Accordingly, TCS had developed an Admin user manual defining two types of administrators i.e. Super Admin and Departmental Admin. Super Admin would do jobs like maintaining holiday data, resetting password of users, creation of department, units, designations, etc., whereas Departmental Admin would add/edit employees, maintain hierarchy for file movement and create subjects for indexing files, etc. Since Super Admin had many privileges, it was to be managed by Government.

Audit noticed that the Departmental Admin interface was not developed. Instead, Super Admin interface was used by TCS to provide for functions of Departmental Administrative interface. As a result, departments could not add/edit employees, manage hierarchy of file movement and create subjects for file indexing,

etc., by themselves. For these basic functions, Departments had to request TCS, leading to unnecessary delays.

It was further noticed that due to design flaws in the existing interface, functions like transfers, promotions, retirements, etc., could not be handled properly by OSWAS. TCS often resorted to back-end changes for such functions as DBA, leading to several inconsistencies in the database. Design deficiency in managing Transfer and Postings in OSWAS was as below:

- OSWAS users were mapped to units (posts) and access to files was attached to the same. As a result, on transfer of user to a new post (unit), the user was being mapped with the new unit and accordingly got access to all files attached to new post. If a unit remained unmapped, no one got access to files attached to that unit. Audit analysis revealed that there were 338 records lying with unmapped posts for four months to more than three years without any action in OSWAS. Files were marked to such units (posts) even when there was no user to take action on such files. Similarly, there were 525 employees active in the OSWAS who were not attached to any unit (post).
- In reality, there could be no post in a department without a user mapped to it. Even if someone holding the post retires or goes on leave, etc., someone was always given the additional/new charge. Such requirements were not inbuilt into OSWAS.

Thus, OSWAS did not ensure seamless transfer of responsibilities and authority when administrative routine events like superannuation, handing over charge, etc., took place.

The Department stated that all the data were handed over to the P.M.U and P.M.U would address all these problems.

The Committee settled the para.

11. (i) Para -2.2.12 Inefficient sequence management.

Para -2.2.12.1 Gaps in inward diary number.

In OSWAS, diarist in charge of receiving all dak of the department captured the relevant details into the system viz. letter number, reference number, subject, description, received from, category, priority enclosures, etc., of the dak. Subsequently, the scanned document of the dak is attached and the information is saved. The system automatically generates a unique dak number called diary number for further use in the system.

The audit pointed out that data analysis of the inward registry of year 2015 in OSWAS revealed 488 cases of gaps in the diary number related to 43 organisational units (Departments, directorates, etc.). Audit could not ascertain whether diary numbers of the dak were deleted from the database or the serial number skipped due

to technical error. Besides, mechanism to follow up the disposal of the dak after marking the same to the user was not in place.

The Department agreed with the observation and assured that such deficiencies would be corrected.

The Committee settled the para.

11. (ii) Para -2.2.12.2 Gaps in user activity log sequence.

OSWAS had system to capture user logins, logouts and duration of a session in a table for security and accountability. A serial number was assigned to identify unique login session. As per OSWAS database design, the serial number was sequential with an interval of one. Analysis of database in Audit revealed that 9,464 serial numbers were missing in the access logs indicating deletion of unauthorised access. This further indicated unauthorised access to files.

The Department accepted the observation and assured to rectify the defects.

The Committee dropped the para as it was a minor flaw.

12. *Para -2.2.13 Deficient timestamp management*.

As per Architectural Design of OSWAS, two database servers were provided to function in a cluster for efficient database operations. Timestamp of both the database servers were to be synchronised for generation of various logs and trails in OSWAS. Audit noticed that OSWAS maintained logs to capture login details, and updation of notes, changing or deleting the existing records, access of important files, etc., in order to ensure security and accountability of data transactions. Actions on logins, notes, movement of files, audit trail, etc., were supposed to happen in sequence and chronology as per the time of transactions.

Audit noticed inconsistent dates/times in important tables like login track, notes, audit trail and job movement.

Audit further noticed that:

- In 24,899 out of 16,81,588 cases in the login access logs, login time was greater than the logout time and
- There were 12,669 notes appeared to had been written before the files used by the concerned users.

The deficiencies observed by Audit had been complied with. The clocks of both physical servers had been tuned and synchronized. Network Time Protocol option for timestamp management would be considered in the upgraded version of OSWAS.

The Committee dropped the para.

13. ***Para -2.2.14 <u>Deficient session handling</u>***.

OSWAS was designed for multiple concurrent logins allowing the users to connect from multiple devices or browsers at the same time. For security, in case of multiple concurrent sessions, features such as notifying user of concurrent sessions, provision for sign out from all active sessions, alert to user for unusual login activity, provision for automatic session timeout were to be provided. However, OSWAS had no such features.

Para -2.2.14.1 <u>Inadequate login controls</u>.

Audit tested the application in simultaneous sessions and found that single document or draft could be changed even after it had been finalised and had moved to next hierarchy in other session. Similarly, the correspondence attached in file in one session could be deleted or changed in other concurrent sessions. This undermined the integrity of file security and also gave rise to problems of traceability of such unauthorised activities as logs of such activities were not maintained and hence non-repudiation could not be ensured.

Para -2.2.14.2 <u>Abnormal concurrent logins</u>.

Audit revealed that in 1,420 cases, the users were found operating 2 to 30 sessions simultaneously from same computer (IP). Similarly, users were also found to have concurrent logins from different computers in 86 occasions. Each such occasion had two to three simultaneous logins. As the transactions made in the database were not identified by session identity numbers, accountability could not be enforced on such transactions.

Para -2.2.14.3 <u>Incorrect recording of logout time</u>.

There were 465 file noting activities in respect of 45 users where the user was not even logged in as per logs. This occurred due to design flaw in the system. In case of user inactivity or abrupt session termination, the system should record log out time to ensure proper session control. But such controls were not properly designed in OSWAS.

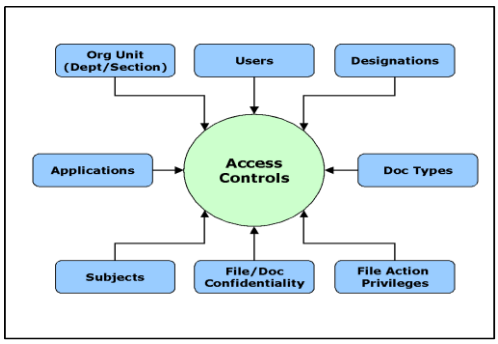
The Department stated that the suggestions submitted by A.G. had been noted and would be incorporated in the upgraded version of OSWAS to restrict changes triggered by multiple sessions.

As per the instruction of the Committee Audit checked the new version of OSWAS and observed that the failures in login controls as pointed out the IT Audit report were not been addressed in the new version of OSWAS.

<u>The Committee recommended that the login controls should be introduced in the system to strengthen accountability and security of data of OSWAS.</u>

14. ***Para -2.2.15*** ***<u>Application design – lack of access control provision</u>*****.**

Audit revealed that as per design documents, user could access and work in OSWAS only if eight parameters given in the following diagram, were fulfilled.



However, testing of the application revealed that such access controls were absent. OSWAS users had access to all files in OSWAS irrespective of his or her privilege by simply changing the website address in the browser. For example, dealing assistant of E&IT Department could access files of General Administration department. In addition to unauthorized viewing of files, one could also add or delete correspondence, modify drafts and even delete attached references in the notes in files lying at any level. This occurred due to weak access controls both in database and application level in addition to non-deployment of SSL. Further, no log of such activity was maintained.

The Department accepted the design flaw and stated (May 2016) that steps would be taken to correct the deficiencies in the upgrade version of OSWAS. The Department also agreed to add the security feature.

<u>As per the instruction of the Committee, Audit verified the application and observed that Secured Socket Layers (SSL) was implemented as suggested in It Audit Report.</u>

<u>The Committee dropped the para.</u>

15. ***Para -2.2.16*** ***<u>Lack of accountability on users</u>*****.**

(i) Para -2.2.16.1 <u>Different employees created note and record</u>.

OSWAS application was designed to send files from one user to another. In this process, the application created a blank record against a user to whom the file was sent for recording his Notings thereon.

Audit noticed that OSWAS failed to account for any new user while transacting in a note created by another user who was already transferred from the Department or unit, thereby weakening the accountability of users. Analysis of database revealed that there were 44,239 notes shown written against the employee who had actually not written those notes. All these instances happened during transfer of employees from one department to another or one post to another. The

increasing trend in such discrepancies ranged from 30 in 2009 to 16,750 in 2014. None of the users had noticed this problem because name of user was not displayed against the note. This, further created inconsistencies in reports as detailed below:

- The designation displayed against the employee who created the notes differed from that of the tabular pendency report.
- The name shown in the note side of a note differed from that of the name shown in the graphical pendency report.
- The department shown against names in the tabular report was null in many cases where as the same was available in the notes.

The Department accepted the comment and assured rectification of the defect in the upgraded version of OSWAS.

The Committee settled the para with the observation that ATN should be submitted for appraisal by the Public Accounts Committee.

(ii) Para -2.2.16.2 Notes against employees not available in employee data.

Audit revealed that 31,027 notes did not display the name of 256 officers who created the note(s) resulting in lack of accountability. This occurred because the employee details records were deleted/delinked in the back end from employee master table in the process of reconfiguration of those departments.

The Department stated that steps would be taken to correct such deficiencies.

The Committee dropped the para.

16. *Para -2.2.17 Input and validation controls*.

(i) Para -2.2.17.1 Inconsistent note created time.

Audit revealed that there were 934 files where the timestamp of notes in files at more than one level were exactly the same. The number of such notes with same time ranged from 2 to 18. Similar exceptions were noticed in margin notes of 8,663 documents. Further, it was noticed that in 679 files and 6,764 documents, one user was found to have created multiple notes at the same time. This occurred due to defective design and lack of control in OSWAS which allowed such inconsistent data in the database.

The Department stated that the observation was based on data analysis by Audit on the complete Database backup. The discrepancy observed is due to presence of some test data as data once created, was not deleted from OSWAS server and assured that the short comings would be corrected. Further the Department stated that there was a cluster of server.

The Committee accepted the reply of the Department and dropped the para.

(ii) Para -2.2.17.2 Deletion of document metadata.

All documents in OSWAS had metadata which is stored in a document master table. The document itself was stored in document container table. Consequently,

metadata of all documents in the document container table should be available in the document master table.

Audit noticed that there were 563 documents in the document container table without any corresponding record in the document master table. This indicated that the metadata of these documents were deleted from the database which resulted in disintegrated data set. The Department accepted the observation and assured that the system would be strengthened to avoid such inconsistency in future.

The Committee dropped the para.

(iii) Para -2.2.17.3 Inefficient user management.

A separate server named Lightweight Directory Access Protocol (LDAP) server was used in OSWAS for authentication of user's login. The server stored username, password, employee ID, etc. Employee master table in OSWAS database had all employee details except password. Whenever a user tried to access OSWAS, the user name was checked in the employee master of OSWAS database for availability and status. If found in service, the user name and password were sent to LDAP for authentication and when login was successful in LDAP server, the user was allowed to access OSWAS and his access control was managed through defined roles. Same users were to be available in OSWAS and LDAP servers since both databases complement the authentication process for the user accessing OSWAS. Audit, however, noticed discrepancies of user data between these two data sets as follows:

- **Discrepancy of user data in LDAP and OSWAS database:** Audit noticed that OSWAS database contained 7,205 users out of which 5,501 were active and LDAP server contained 5,101 users. Audit compared both the datasets and found that only 4,176 users were common in both. Thus, 2,104 users in OSWAS database were not linked to the LDAP server due to absence of input control. It was found that 925 users created in LDAP were deleted from the OSWAS database and reasons for such deletions were not found on record.
- **Same Login issued to two different employees:** For accountability of transactions, each user should have a single distinct login name. But analysis revealed that 15 login names were allotted to 30 different users. The Department assured that the deficiencies in the system would be rectified.

Ability to login to OSWAS application depends both on availability of LDAP ID and login flag in employee master table (database). A user having its login flag disabled could not access application, even if LDAP ID exists in the system. Similarly, a user cannot access application if its login flag was enable but did not have a LDAP ID. Sometimes, OSWAS database records were created in the database attributable to incorrect data received from department. In those cases, LDAP ID was

not created. Similarly, users had been removed, but not the LDAP ID. In those cases, there was variance in figures in both database and LDAP and inconsistency reports are generated. Hence no record had been deleted from OSWAS database in upgraded version of OSWAS.

The Committee dropped the para.

(iv) Para -2.2.17.4 Incomplete user profile – exposed OSWAS to unauthorised use.

As per industry's best practice, there should be robust password policy i.e. password expiry, automatic account termination on termination of service, rules for frequent changing of password, complexity of passwords, etc., in order to secure the application usage.

Audit revealed that there were 1,723 user accounts where the password expiry date was not available. Thus, password expiry policy was not enforced. Further, the date of birth field was blank in case of 4,041 out of 5,501 active users. Using Date of Birth column, automatic disabling of accounts of the user on retirement was not enforced. It was also noticed that 635 transactions in various tables against 38 users were present in the database after the accounts of these users were deactivated and the passwords expired.

The Department accepted the observations and assured that steps would be taken to make good such deficiencies.

The Committee dropped the para.

17. ***Para -2.2.18 Database Redundancy.***

Audit observed that as per the best practice, the databases of IT systems needed to be properly designed to ensure reliability and optimum performance by controlling data redundancy and ensuring consistency. Ideally, there should be one repository of document files/images/PDF files, etc., for easy access by multiple users, using document key identification link namely primary key. But, in OSWAS, this aspect was found absent. This resulted in unnecessary increase of database size providing scope for data inconsistency.

The Department assured that the OSWAS Application would be improved accordingly.

(i) Para -2.2.18.1 Inefficient document management.

Audit revealed that a single document (Dak) marked to more than one seat or department had been stored in multiple records in the database. For instance, letter No. 'U.O.I. No 630/ACS Rev. & D.M.' dated 21 June 2014 was found marked to various departments/units, stored in 484 locations. This increased the requirement of storage space by 483 times.

In respect of 27,376 documents (size of 22.7 GB) (which include 25,670 dak receipts from e-despatch system), data redundancy was noticed 99,197 times resulting in unnecessary increase of storage space by 60 GB. Such inefficient maintenance of storage would adversely impact the performance of database of OSWAS.

The Department accepted the observation and assured that alternative solution for better document management should be incorporated in the upgraded OSWAS Application.

The Committee dropped the para.

(ii) Para -2.2.18.2 Integration of e-Despatch and OSWAS.

The OSWAS was developed by OCAC without dak despatch system. However, e-Despatch system, developed on different platforms, was later implemented for dak despatch to field offices in the State. On technical advice of OCAC, E&IT Department decided to integrate e-Despatch with OSWAS.

For the said integration, a separate (Intermediary) server was set up to connect both systems with provision to store letters for sharing. Diarists were required to use OSWAS interface to receive and despatch letters through e-Despatch server. Thus, three sets of same data in three different locations i.e. e-Despatch system, intermediary server and OSWAS were generated. Analysis of OSWAS for receipt and despatch of letters through the server revealed the following.

- **Receiving of letters:** Out of 1,63,106 letters pertaining to 28 departments, only 88,670 letters were received into OSWAS and remaining 74,436 letters were still lying in the intermediary server.
- **Despatch of letters:** Despatch of letters of OSWAS through e-Despatch was not functional in any of the departments due to lack of support for digital signature in e-Despatch and absence of common system for centralised generation of outward letter numbers as per Odisha Secretariat Instruction Manual.

The user departments stated that unprocessed letters lying in intermediary server were already received by post or downloaded from e-Despatch website and processed into OSWAS using manual scanning process. However, for despatch of letters, users had to generate ink signed hardcopy of the letters and send to despatch section where the letters were scanned again into e-Despatch system. Due to lack of manpower, facility of integration of receiving letters remained unused. Thus, integration of systems failed to meet the objective of avoiding duplication of work and redundancy of hardware/software. Further no assurance can be given that all letters had been disposed in a desired manner.

The Department stated that in the present integration mechanism of OSWAS and e-Despatch, an intermediate FTP server was being used for sharing of data between both applications.

The letter lying in the intermediary server which had not been downloaded after 3 months of the date of letter were being cleansed. The outgoing part of integration modules had not been enforced as the DSC was not available with all the designated officers digitally sign the letters being dispatched.

The Departmental representative assured the Committee that the observations were noted and necessary improvements would be made in the integration module to eliminate the issues. Electronic mode of receipt as well as despatch of letters would be enforced to avoid duplication of work and redundancy of hardware/software.

The Committee suggested that e-despatch system be developed more effectively and reviewed regularly.

18. ***Para -2.2.19 Incomplete Leave Processing System*.**

Audit observed that TCS developed an incomplete application without required integration with core applications which gave rise to several deficiencies as discussed below.

- ***Non-linking of Departmental hierarchy with LPS:*** Database analysis revealed that 128 employees were not correctly linked to their approving officer, but linked to officers outside their department. Due to that, 13 employees had applied for leave on 43 occasions but their leave application could not be approved in OSWAS. Non-linking of LPS with proper departmental hierarchy resulted in ineffective handling of leave applications.
- ***Incorrect leave balance:*** Database analysis revealed inaccuracies in the leave accounts of 813 cases. Therefore, the departments had to depend upon the manual system for approving the leave as usual and had to duplicate their work in feeding the leave data online, thereby defeating the objective to have an efficient and effective common application.
- **Incorrect balance closing system:** Leaves like casual leave, optional leave, etc., are closed annually, whereas leaves like earned leave, half pay leave, etc., were to be closed every half year with credit of 15 or 10 days respectively, added to closing balances. Database analysis, however, revealed that there was no such provision of preserving half-yearly balance in the database through which leave ledger account of EL and HPL could be generated.
- **Lack of Business Process Re-engineering:** Like other applications, there was no Business Process Re-engineering done for the Leave Processing System. The Leave Rules of Government of Odisha were not mapped to the Leave Processing System under OSWAS as the leave types defined in LPS did not

include leaves like leave not due, special casual leave, child care leave, study leave, special disability leave, quarantine leave, etc. Similarly, rules for proportionate credit of leave in earned leave account in case of employees availing half pay leave/ extra ordinary leave, advance credit of half pay leave/earned leave were not found mapped in the design of LPS.

Due to deficiency of LPS, even though deployed and implemented under OSWAS, the departments had to maintain the manual system of leave account, thereby maintaining another set of leave data in electronic form without use.

The Department stated that deficient leave processing system was due to inadequate need assessment study and due to absence of BPR. It assured that steps would be taken to design the system as per relevant rules of Government.

LPS was not in the main scope of 20 common applications in SLA to be developed by TCS. As implementation of Common applications was delayed due to non-availability of feedback, in a review meeting held under the chairmanship of Secretary, IT on the progress of implementation of OSWAS, it was decided to develop and implement employee specific common applications which would be more easily adoptable.

The leave approver for the departmental users is set by the leave admin of the departmental users was set by the leave admin of the department only. Whenever an employee was transferred from one department to another, the approver of that employee was changed accordingly by the leave admin of the department.

LPS was developed as a standalone application rather than a workflow based application based on the feedback from users and instructions from authority.

The implementation of LPS was introduced in the mid cycle of a year and it was required to manually update current leave balances. An interface was also developed for updating leave balances whose access controls were provided to a department defined leave admin. Finance Department (being custodian of leave rules) was assigned the role of a super admin.

The users were being motivated at the Department to use the online system. The deficiencies could be brought into notice with more and more use of the system and those could be rectified to make the system robust.

Report on balance leaves could be obtained from OSWAS at any time.

The departmental admin could update the leave balance of any employee whenever needed. Even if the leave was not applied in the OSWAS applications and applied manually, the leave admin had the privilege to update the leave balance of the departmental employees.

Finance Department being the Nodal Department defining Leave Rules would be moved for necessary BPR for smooth implementation of LPS.

The observations had been noted. The users were being motivated at the Department level to use the online system. With more and more use of the system, the application would be rectified based on feedbacks from users.

In view of the assurance by the Department, the Committee dropped the para.

19. ***Para -2.2.20 Monitoring and evaluation.***

(i) Para -2.2.20.1 Security audit recommendation.

Based on a decision in meeting (January 2012) of Secretariat level Implementation Committee on OSWAS for hosting OSWAS in State Data Centre, OCAC conducted (March-June 2015) Security Audit of OSWAS through certain empanelled security auditor. The Security Auditor pointed out that four vulnerabilities viz. (i) User credentials were sent in clear text, (ii) Default credentials for admin accounts, (iii) Insecure Hypertext Transfer Protocol (HTTP) methods enabled and (iv) Information disclosure through HTTP header. The security auditor issued (June 2015) security clearance certificate after re-assessment (June 2015) of OSWAS for the vulnerabilities pointed out earlier and declared the site safe for hosting. The vulnerabilities were fixed only temporarily by TCS and when audit tested OSWAS, all four vulnerabilities still existed.

The Department accepted the non-implementation of security audit recommendations and assured that the same would be implemented.

The Committee dropped para.

(ii) Para -2.2.20.2 Technical obsolescence and poor interface functionality in OSWAS.

Applications updated with latest versions of the environments provide security by protection from common vulnerabilities and exposures already detected, besides performance enhancements assurances.

- ***Older Java version:*** OSWAS was only compatible with the older version of Java platform as TCS implemented OSWAS by customising the software developed for Government of Gujarat during 2005-07. It did not allow upgradation to latest versions of Java platforms. Older Java had several common vulnerabilities and exposures (CVEs) which made the system prone to attacks as it allowed remote and local attackers to affect confidentiality, integrity and availability. Besides, security benefits associated with subsequent releases could also not be ensured leading OSWAS to technical obsolescence and prone to risks.
- ***Cross browser compatibility:*** As per RFP, OSWAS should be based on web based multi-tiered architecture and the end user interface must be browser independent. Request was also made from Departmental heads to make

OSWAS browser independent to enable them to use OSWAS on tablets/ipads, etc. But it was noticed that OSWAS was dependent on one browser (Internet explorer) for its full functionality. Assessment of OSWAS in different popular browsers revealed that due to absence of compatibility features of OSWAS, various features remained non-functional in different browsers.

- ***Poor navigation features:*** Audit noticed that there were unnecessary non-functional menu and navigation links in OSWAS. Besides navigations in the OSWAS application which deteriorated user experience as stated below:
  - In home page, the link "Common Application" directed the screen to another index page (showing horizontal tabbed links to personal, common applications, budget and departmental applications) and not directly to Common Applications. The Index page hosting tabbed links were also not functional.
  - Excessive use of pop-ups in the application was unnecessary.
  - Dashboard screen displayed with iconic view contains links like UC monitoring, budget, Court cases and leave which were non-functional.
  - Link for EDN and Department specific applications were defunct.
  - Site map was not available for providing the navigation structure guide due to the fact that a consistent pattern was not used in the navigation system of OSWAS.
- ***Non-functional editing features in note side text editor:*** OSWAS provided Rich Text editor on the note side for word processing of the note content of the files/Daks/incoming correspondences with various text editing features including font size, font color, background color, hyper linking, indentations, cut-copy-paste, bulleting/numbering, bold/ italic/ underline, spell check, etc. On assessment of the said feature in OSWAS, it was found that the text editor embedded was functioning improperly and was not user friendly as detailed below.
  - The font size feature was not working dynamically as per value of the font size and the desired font style was not affected while typing in the editor.
  - The spell check facility was poorly designed as the word in the pop up was not highlighted in the editor for easy checking and assessment of sentence and there was no provision to add new frequently used words in the dictionary.
  - Linking facility was not working properly as the same replaced the text selected with the file name and website name in the editor instead of creating a link on them, i.e. a link created on text "ABCD" for www.google.com, deleted the ABCD text and inserted www.google.com.

In absence of proper functioning of the features in the said editor, they were not used in OSWAS. Similarly, the Work list rules provided in the menu were found non-functional. OCAC should have ensured the working functionality of these features, before releasing the payments.

The Department admitted the technical obsolescence and poor functionality of OSWAS and assured that platforms would be upgraded.

The observation on older Java version, cross browser compatibility had already been pointed out by users and steps were being taken for improvement of the Application.

OSWAS Application was based on the IDWMS frame work of TCS, implemented in other states and it had been customized for the State of Odisha. The features, as observed, were available as built in features of the product.

The Departmental Secretary stated that the observations were noted and TCS would be instructed to inactivate/hide the non-functional menus and options.

The recommendations of the Security audit would be implemented with the upgradation of OSWAS. OSWAS Application would be upgraded soon with an improved editor and made browser independent.

The Committee dropped the para.

(iii) Para -2.2.20.3 Inadequate usage of OSWAS.

The key objectives of OSWAS were office Automation, enhancing productivity, using Information Technology as an enabler to help in daily work, an efficient workplace, access controls at all levels and efficient and transparent administration. Audit assessed the usage of OSWAS by 26 out of 43 user departments which furnished data (2012-15). 15 Departments and two offices including E&IT Department had not furnished the information even after repeated persuasion. The audit findings are as follows:

- ***Creation and movement of manual files:*** Audit noticed that movement of manual files in 8 out of 26 departments had reduced during 2014-15, but the same was found to have increased during the period in other 11 departments.

  Audit noticed that creation of manual files in 13 out of 26 departments continued on an increasing trend during 2012-15, despite providing OSWAS login credentials to all users of these departments. During 2015, 81 per cent (21 out of 26) departments created more than 50 per cent of manual files outside OSWAS. Decrease in trend of manual files was noticed only in case of nine departments. Only Rural Development Department and Chief Secretary's Office did not create any manual file.

  Some departments stated that handling of confidential files, files processed for referral departments, legal files, etc., would be easy manually.

OCAC never assessed the reasons for lack of confidence among the user departments while handling such files. OCAC, the nodal agency itself had bypassed the application as it created 258 (73 per cent) manual files out of total 352 files, created during 2015.

- ***Poor usage of core and common applications:*** Out of 28 common applications, only two to six were being used in 26 departments. The most commonly used application was LPS which was also found deficient.

  Out of 10 core applications, seven to eight are being used in 26 test checked department whereas SMS, time-analysis and appointment scheduler was not being used in any of the departments.

- ***Inadequate training:*** As per SLA of OSWAS, OCAC was responsible for identifying the core team and the trainers to be trained and provide the necessary inputs to TCS for preparing the training plan. TCS was entrusted with responsibility of conducting training and also to conduct project specific training for users in the customised software. Audit found that in 26 user departments, 104 out of 260 trainings for core applications and 482 out of 520 trainings for common applications were not provided. Training on customised software was also not conducted.

The Department accepted the inadequate usage pattern and assured that steps would be taken for time bound phasing out of physical files.

It was agreed that both manual and online system of file processing were being followed by Department users. But, steps were on to move to complete online mode of file processing through OSWAS.

It had been planned to focus on those common applications which were in use in the new version of OSWAS.

Department further stated that two rounds of comprehensive training to all departmental users had been conducted with 25 participants per batch on computer fundamentals, use of scanner, printer, Internet Basics along with OSWAS. Application including hands on at the training centre of IT centre, Secretariat. Besides refresher trainings were being conducted from time to time as requested by departments at the Department premises.

The Committee accepted the Departmental explanation and dropped the para.

*****

MINUTES OF THE TENTH MEETING OF PUBLIC ACCOUNTS COMMITTEE, 2019-20 HELD AT 04:00 P. M. ON 20.03.2020 IN ROOM NO. 54 OF THE ODISHA LEGISLATIVE ASSEMBLY BUILDINGS, BHUBANESWAR.

****

P R E S E N T

Shri Pradipta Kumar Naik.	**CHAIRMAN**
Leader of Opposition.	
Shri Mohan Charan Majhi, Hon'ble Chief Whip, Bharatiya Janta Party	**MEMBERS**
Shri Debiprasad Mishra, M. L. A.	
Shri Jaya Narayan Mishra, M. L. A.	
Shri Rajendra Dholakia, M. L. A.	
Shri Ananta Narayan Jena, M. L. A.	

S E C R E T A R I A T

Shri Dasharathi Satapathy, I. A. S., Secretary.
Smt. Sushila Mallick, Deputy Secretary.
Smt. Baijayanti Pattanayak, Under Secretary.
Shri Partha Sarathi Das, Section Officer.

The Committee met as scheduled and approved the following Reports:-

1. 1st Report of PAC, 2019-20 on the Report of the C & A. G of India (Revenue Receipt) for the year 2007-08 relating to Finance Department.
2. 2nd Report of PAC, 2019-20 on the Report of the C & A. G of India (Revenue Receipt) for the year 2015-16 relating to Finance Department.
3. 3rd Report of PAC, 2019-20 on the Report of the C & A. G of India (G & SSA - Report No. 4 of the year 2016) relating to Electronics & Information Technology Department for the year, 2014-15.
4. 4th Report of PAC, 2019-20 on the Report of the C & A. G of India (G & SSA) for the year 2016-17 relating to Higher Education Department.
5. 5th Report of PAC, 2019-20 on the Report of the C & A. G of India (G & SSA) for the year 2014-15 relating to Home and Women & Child Development Department.
6. 6th Report of PAC, 2019-20 on the Report of the C & A. G of India (G & SSA) for the year 2013-14 relating to Rural Development Department.
7. 7th Report of PAC, 2019-20 on the Report of the C & A. G of India (G & SSA) for the year 2013-14 relating to Rural Development Department.
8. 8th Report of PAC, 2019-20 on the Report of the C & A. G of India (G & SSA) for the year 2014-15 relating to School & Mass Education Department.

The Committee also authorized the Chairman to present the same to the Assembly.

The meeting of the Committee adjourned *sine-die*.

Sd/-
PRADIPTA KUMAR NAIK
CHAIRMAN
PUBLIC ACCOUNTS COMMITTEE

MINUTES OF THE TENTH MEETING OF PUBLIC ACCOUNTS COMMITTEE, 2020-21 HELD ON 01.10.2020 AT 03:00 P. M. IN ROOM NO. 54 OF THE ODISHA LEGISLATIVE ASSEMBLY BUILDINGS, BHUBANESWAR.

****

P R E S E N T

Shri Pradipta Kumar Naik.	**CHAIRMAN**
Leader of Opposition.	
Shri Mohan Charan Majhi, Hon'ble Chief Whip, Bharatiya Janta Party	**MEMBERS**
Shri Debiprasad Mishra	
Shri Jaya Narayan Mishra, M. L. A.	
Shri Pranab Prakash Das, M. L. A.	
Shri Braja Kishore Pradhan, M. L. A.	

S E C R E T A R I A T

Shri Dasharathi Satapathy, I. A. S., Secretary.
Smt. Sushila Mallick, Deputy Secretary.
Smt. Baijayanti Pattanayak, Under Secretary.
Shri Partha Sarathi Das, Section Officer.

The Committee met as scheduled and approved the following Reports finalized previously by the Public Accounts Committee, 2019-20 on 20.03.2020 for presentation in the House during the 4th Session of the 16th Assembly.

1. 1st Report of PAC, 2020-21 on the Report of the C & A. G of India (Revenue Receipt) for the year 2007-08 relating to Finance Department.
2. 2nd Report of PAC, 2020-21 on the Report of the C & A. G of India (Revenue Receipt) for the year 2015-16 relating to Finance Department.
3. 3rd Report of PAC, 2020-21 on the Report of the C & A. G of India (G & SSA - Report No. 4 of the year 2016) relating to Electronics & Information Technology Department for the year, 2014-15.
4. 4th Report of PAC, 2020-21 on the Report of the C & A. G of India (G & SSA) for the year 2016-17 relating to Higher Education Department.
5. 5th Report of PAC, 2020-21 on the Report of the C & A. G of India (G & SSA) for the year 2014-15 relating to Home and Women & Child Development Department.
6. 6th Report of PAC, 2020-21 on the Report of the C & A. G of India (G & SSA) for the year 2013-14 relating to Rural Development Department.
7. 7th Report of PAC, 2020-21 on the Report of the C & A. G of India (G & SSA) for the year 2013-14 relating to Rural Development Department.
8. 8th Report of PAC, 2020-21 on the Report of the C & A. G of India (G & SSA) for the year 2014-15 relating to School & Mass Education Department.

The Committee also authorized the Chairman to present the same to the Assembly.

The meeting of the Committee adjourned *sine-die*.

Sd/-
PRADIPTA KUMAR NAIK
CHAIRMAN
PUBLIC ACCOUNTS COMMITTEE