Electronics and Information Technology Department

2.2 Information Technology Audit on Implementation of Odisha Secretariat Workflow Automation System

Executive Summary

Government of Odisha implemented Odisha Secretariat Workflow Automation System (OSWAS), a workflow automation system at the State Secretariat, to bring in efficiency and effectiveness in its functioning. Even after six years of implementation, all envisaged core, common and department specific applications could not be developed.

OSWAS had weak management controls. Business Process Re-engineering was not conducted which created inefficiencies and inconsistencies in file management. Business Continuity and Disaster Recovery Plan was not framed. Odisha Computer Application Centre (OCAC) could not exercise adequate control over database administration activities.

The digital signature was partially implemented which failed to protect the integrity of notes created through OSWAS. OSWAS had design deficiencies like incomplete administrator interface, non-provision for transfer/ posting, ineffective session management, inconsistencies in reports and time-stamping, etc.

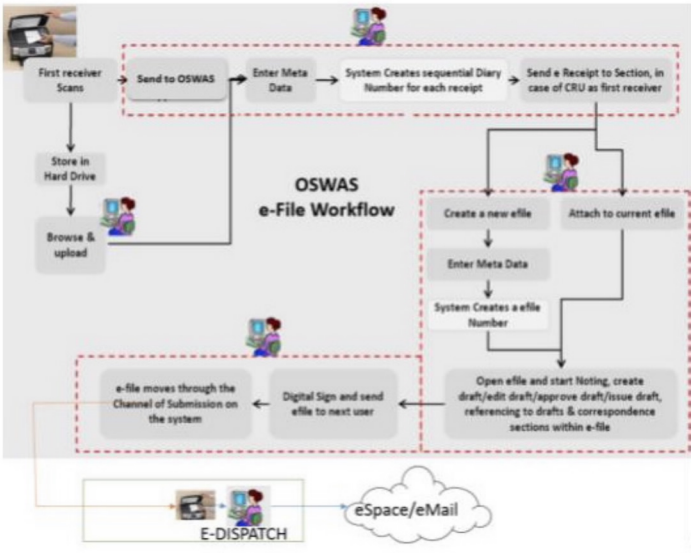
Access controls were found inadequate in OSWAS as the files were accessible to any user irrespective of department, post and confidentiality. User management was given to the vendor without any control of OCAC. OSWAS used outdated platforms making Government business vulnerable. Several features in user interface were non-functional.

Usage of OSWAS was low, as 81 per cent of departments had created more than 50 per cent of files in physical form outside OSWAS. Training to users on core and common applications was inadequate.

2.2.1 Introduction

Government decided (December 2007) to implement Odisha Secretariat Workflow Automation System (OSWAS) at the State Secretariat and engaged (September 2008) Tata Consultancy Services Limited (TCS) through open tender. The objective of the system is to tackle various issues like high proportion of establishment work, increasing number of files, prioritisation of files, multiple levels of processing, inter-departmental consultations, file tracing and tracking and maintaining large number of Acts and Regulations, orders, *etc*., at State Secretariat.

OSWAS was developed using Java in the front-end and Oracle database at the back-end. Oracle web-logic Server and Apache were used as application and web server respectively. It was deployed on the intranet of Secretariat *i.e*. SECLAN[20], which has connectivity to all 40 departments as well as offices of Hon' ble Governor, Chief Minister and Chief Secretary.



During the period 2008-16, ` 28.01 crore was spent on OSWAS, which included the cost of hardware, system software, training, project monitoring (` 19.70 crore) and software application (` 8.31 crore). The project was implemented in phased manner since September 2008 by TCS.

2.2.2 Organisational set up

The Electronics and Information Technology (E&IT) Department of the State Government, headed by the Secretary, is responsible for implementing, maintaining, modifying, *etc*., different computerised systems in the offices of the State Government. OCAC, headed by a Chairman, is the technical directorate of E&IT Department. OCAC is the nodal agency for implementation of OSWAS.

2.2.3 Audit objectives

The Information Technology Audit was conducted to assess whether:

- Planning, including system development process and procedures followed at various stages was robust;
- The system met the Government' s objectives of offi**c** automation;
- Controls in Information Technology system were adequate and effective;
- Information Technology system security and Business Continuity issues were adequately addressed; and
- Monitoring and supervision was adequate and effective.

[20] Secretariat Local Area Network

2.2.4 Audit criteria

IT Audit was conducted with reference to the following criteria:

- Technical documentation like user requirement specification (URS)/ software requirement specification (SRS)/ architecture/ manuals/ project plans/ system and database designs;
- Service Level Agreements (SLAs) and Request for Proposal (RFP) of OSWAS and other terms of agreement with the vendor;
- Information Technology (IT) Act, 2000 and subsequent amendments;
- e-Governance policies and standards; and
- Odisha Secretariat Instructions (OSI) and Odisha Government Rules of Business (OGRB).

2.2.5 Scope and methodology of Audit

The implementation of OSWAS was examined across all departments through data analysis[21] using computer assisted audit techniques like IDEA/ SQL, assessment of applications on test server, user department responses and study of relevant records during November 2015 to January 2016. An entry conference was held with Principal Secretary on 24 August 2015. Exit conference with Principal Secretary, E&IT was held on 13 May 2016, where the audit observations were discussed. The views of the Department were considered and suitably incorporated in the Report.

Audit Findings

General Controls

2.2.6 Release of payment deviating from Service Level Agreement

As per Service Level Agreement (SLA) (September 2008) 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 as listed in ***Appendix 2.2.1***. The common and department specific applications were to be set up on the functionalities of the core applications as per milestones (***Appendix 2.2.2***) specified in SLA. Audit noticed the following:

2.2.6.1 Non-Development of applications under OSWAS

Following applications were either not developed or not put to use till May 2016:

- One (e-mail) core application out of 10, was not developed as yet.

[21] Incomplete OSWAS database dumps were provided to Audit on four occasions (20 June 2015, 29 June 2015, September 2015 and December 2015) before a complete set was furnished in January 2016

- Out of the 20 common applications, six[22] were not developed and 10[23] though developed, were found incomplete. The rest were used by some departments.
- None of the 99 department specific applications was developed.

OCAC stated (May 2016) that all applications have 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.

The Department stated (May 2016) that vendor's claim of doing assigned work is being sorted out.

2.2.6.2 Non-receipt of deliverables

Request for proposal (RFP) and SLA required that OSWAS would support Secure Sockets Layer (SSL)[24], 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. However, these key features and deliverables were not ensured, which led to the following:

- 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 have 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 cannot engage other

[22] Expenditure management and tracking system; Process for introduction of Bills or Amendments in the Legislative Assembly; Application for Cabinet Memorandum; Tracking of Foreign travel; Request and processing for telephone facility; Knowledge based system for Government Rules/ Regulation/ Circulars/ Acts and advanced search facility

[23] RTI; Assembly questions; Application for management of CCRs/ ACR of different categories of officers; Monitoring of Government of India issues; Process for constitution and monitoring of committees; Application for vehicle management and fuel consumption; Processing of Public Accounts Committee queries; Application for training of employees; Audit assessment and appeal details; Asset management system

[24] Secure Sockets Layer is the standard security technology for establishing an encrypted link between a web server and a browser

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.

2.2.7 Absence of Business Process Re-engineering

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 2013-16 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 as discussed below:

- OSI requires 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 as discussed in ***Paragraphs 2.2.9.1*** and ***2.2.9.3***.
- Data received from 26 out of 43 Departments/ organisational[25] 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. The scope for bypassing OSWAS would have been restricted, if BPR had been undertaken and the rules modified in OSI suitably.
- In absence of changes in business rules, other applications provided in OSWAS like management of Confidential Character Reports/ Annual

[25] Other Departments including E&IT Department had not furnished the information

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 accepted the observations and stated (May 2016) that BPR could not be done before implementation of OSWAS, due to which the processes had become complex. However, in future, BPR would be done before implementation of upgraded version of OSWAS.

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. However, OSWAS had following deficiencies:

***Segregation of duties*:** 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 inspite 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 as indicated in ***Paragraphs 2.2.9.1*** and ***Paragraph 2.2.9.3***. Even users were created and deleted unauthorisedly as discussed in ***Paragraph 2.2.17.3***.

***Inadequate compensating controls for DBA activities*:** Supervisor review of access logs and activities is 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 as discussed in ***Paragraph 2.2.9.2***.

Accepting the observations, the Department stated (May 2016) that OCAC would be strengthened and Government would create a core team to take over the data administration job of OSWAS.

2.2.9 Security controls

2.2.9.1 Implementation of digital signature on file notes

Government of Odisha introduced digital signature on note side of the Government files in OSWAS since critical, sensitive and important decisions were taken through the system. Digital Signature was to be provided as per Information Technology (IT) Act, 2000 to bring legal validity and accountability to the notings created through OSWAS.

* ***Digital signature not made mandatory:*** Government of Odisha decided (2013) to incorporate digital signature facility in OSWAS from Under Secretary level and above. However, only 242 digital signature certificates (DSCs) were procured against 686 officers[26] 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[27], 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 may be made. Details containing number of notings made at each level, number of notings digitally signed at each level and number of cases where preceding note was not digitally signed are given in ***Table 2.2.1***.

[26] Number of Officers from Under Secretary level and above were 686 as per Human Resource Management System data furnished to Audit

[27] Cut-off date has been taken as 1 June 2014

Table 2.2.1: Post-wise status of digital signature in OSWAS file notings (since 1 June 2014)

Sl. No.	Designation against which DSCs were issued	Total notes in OSWAS files	Total notes with digital signature	With previous notes having digital signature	With preceding note without digital signature
1.	Chief Secretary	8,611	1,369	784	585
2.	Secretary level officers and above	74,613	17,270	3,057	14,213
3.	Additional/ Special/ Joint Secretary level officers	1,11,279	10,623	1,446	9,177
4.	Deputy Secretary level officers	95,595	4,691	533	4,158
5.	Under Secretary level officers	51,102	4,434	247	4,187
	Total	**3,41,200**	**38,387**	**6,067**	**32,320**

(Source: OSWAS database)

In such scenario, if changes are made in previous notes by DBA/ insider/ other elements, the basis of decision taken in succeeding note cannot 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 (May 2016) that digital signature would be made mandatory to enforce accountability.

* ***Repudiation of Digital Signature****:* Section 3 of IT Act, 2000 stipulates that the authentication of electronic record shall be effected through the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another record. Further, it also stipulates that any person by use of a public key of the subscriber can verify the electronic record.

  For digital signature on note side, form signer with four licenses was procured (March 2014) 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, analysis of database revealed that 38,944 notes[28] 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 is no other provision through which users can verify the breach of their digital signatures. Thus, the digital signature process followed in OSWAS does not comply with IT Act, 2000.

[28] From May 2009 to December 2015

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 backend in September and October 2014 when they changed four notings of Chief Secretary on 9 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 backend.

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 (May 2016) 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.

* ***Non-availability of digital signatures in the electronic PDF form:*** Section 5 of IT Act, 2000 stipulates that where any law provides that information or any other matter shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person and such information or matter is authenticated by means of digital signature affixed in such manner as may be prescribed by the Central Government.

  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 (April 2016) that PDF version of the file generated through OSWAS did not contain digital signature.

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" is 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[29] of IT Act, 2000. The Department stated (May 2016) that action would be taken to avoid such breach of system in future.

2.2.9.3 Activity deletion from audit trail

In OSWAS, file transactions like file approval, file sending, draft preparing and approving are 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 are numbered. Analysis of the database revealed gaps between two consecutive activity order numbers in three occasions. The missing activities were due to backend deletion of particular activities since the number of such occurrences was very small to indicate systemic error. Similarly, there were 12 gaps found in the note order indicating deletion of notes in the backend. The Department assured (May 2016) that action would be taken for preventing it in future.

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.

[29] Section 43(d) provided that if any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programmes residing in such computer, computer system or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected

- ***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 (May 2016) that steps would be taken for framing Disaster Recovery/ Business Continuity Plans for OSWAS and maintaining environmental controls.

Application Controls

2.2.11 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[30] 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 Department 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 is explained 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 remains unmapped, no one gets 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).

[30] Provision in the software to manage administrative functions *viz*. transfer postings of staff, addition of file subject, distribution of works among officers, addition of employees, *etc*., through a dedicated screen

- In reality, there can 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 is 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 (May 2016) that considering the importance of transfer and posting module and department specific administrative modules, steps would be taken to correct the deficiencies in OSWAS.

2.2.12 Inefficient sequence management

2.2.12.1 Gaps in inward diary number

Chapter-IV-1 of the Odisha Secretariat Instructions provided that a diary register, which is a chronological register of correspondence received in a department, is to be maintained by diarist. Entries in the said register are to be consecutively numbered.

In OSWAS, diarist in charge of receiving all dak of the department captures 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.

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 accepted (May 2016) the observation and assured that such deficiencies would be corrected.

2.2.12.2 Gaps in user activity log sequence

OSWAS has system to capture user logins, logouts and duration of a session in a table for security and accountability. A serial number is assigned to identify unique login session. As per OSWAS database design, the serial number is 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 and an attempt to omit the trail as already discussed in ***Paragraph 2.2.9.2***.

The Department accepted (May 2016) the observation and assured to rectify the defects.

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. It was 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*., are 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 as given in ***Table 2.2.2***.

Table 2.2.2: Statement showing details of discrepancy in timestamp in vital tables

Sl. No.	Description	Number of records where later transaction had earlier time			Total
		By less than 125 seconds	By more than 125 seconds	With maximum time gap	
1	Logs of Login Track	8,225	41,150	4 days	49,375
2	Notes	1,12,589	2,613	More than 3 months	1,15,202
3	File Movements	5,437	--	--	5,437
4	Audit Trail	68,880	--	--	68,880

(Source: OSWAS database)

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 have been written before the files used by the concerned users.

The Department accepted (May 2016) the flaw noticed in OSWAS and assured rectification of the defect through the vendor.

2.2.14 Deficient session handling

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 are to be provided. However, OSWAS had no such features.

2.2.14.1 Inadequate login controls

Audit tested the application in simultaneous sessions and found that single document or draft could be changed[31] 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.

2.2.14.2 Abnormal concurrent logins

Further analysis 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.

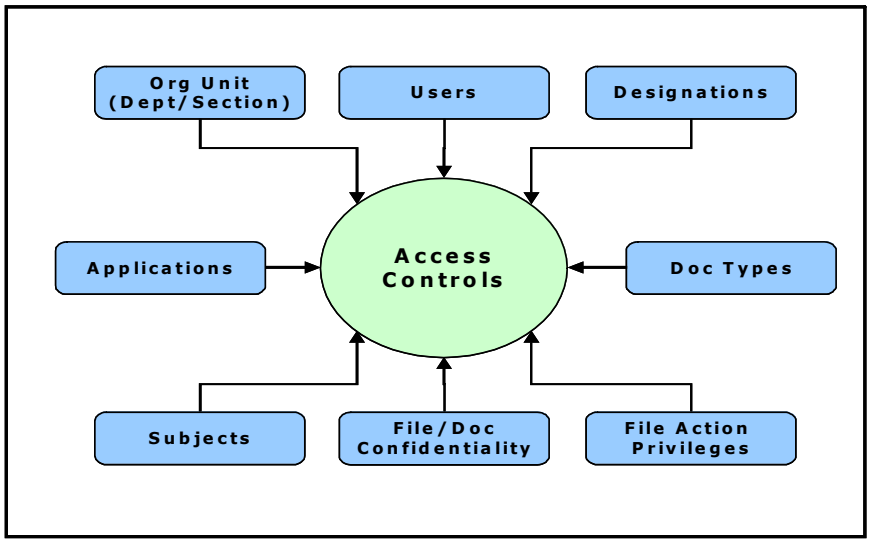
2.2.14.3 Incorrect recording of logout time

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 accepted the observations and assured (May 2016) that adequate application controls would be enforced.

2.2.15 Application design – lack of access controlprovision

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



[31] As an instance, the draft can be replaced/ changed by an Assistant Section Officer, even after it has moved to various levels like Desk Officer, Under Secretary, Deputy Secretary, Additional Secretary, *etc*., without anyone's knowledge. The draft link on the note side in MS Word format could be manipulated by any level even after approval of the draft

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 can access files of General Administration department. In addition to unauthorised viewing of files, one can 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 as discussed in ***Paragraph 2.2.6.2***. 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.

2.2.16 Lack of accountability on users

2.2.16.1 Different employees created note and record

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

It was 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 (May 2016) the comment and assured rectification of the defect.

2.2.16.2 Notes against employees not available in employee data

Database analysis 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 (May 2016) that steps would be taken to correct such deficiencies.

2.2.17 Input and validation controls

2.2.17.1 Inconsistent note created time

The process of preparing content of the file noting and saving in OSWAS involves sufficient user activity and time. Thus, the noting timestamp of a file created at different levels in hierarchy of workflow cannot be same in a file and also should strictly be in chronologically ascending order. Further, it is practically impossible to have multiple notes created by the same user at same time.

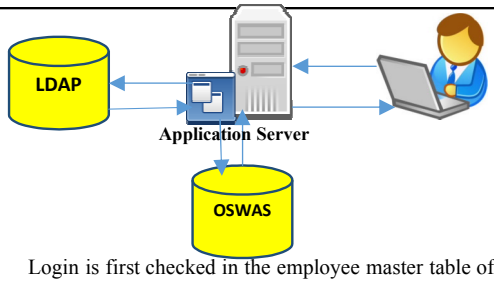
Data analysis revealed that there were 934 files where the timestamp of notes in files at more than one level were exactly[32] the same. The number of such notes with same time ranged from 2 to 18. Similar exceptions were noticed in margin notes of 8,663 documents. Further, it was noticed that in 679 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 (May 2016) that such exceptions were due to problems in OSWAS and assured that the shortcomings would be corrected.

2.2.17.2 Deletion of document metadata

All documents in OSWAS have metadata which is stored in a document master table. The document itself is 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 ma ster 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 (May 2016) that the system would be strengthened to avoid such inconsistency in future.

2.2.17.3 Inefficient user management



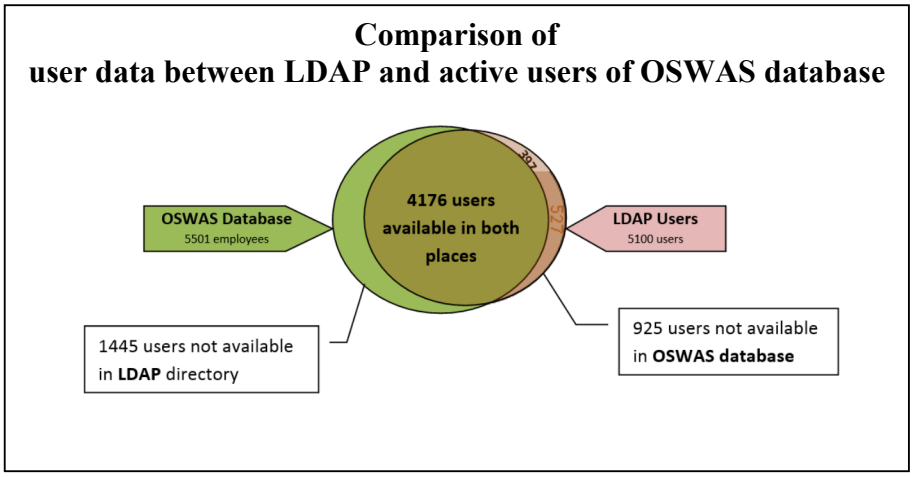
Login is first checked in the employee master table of OSWAS for service flag=‘ Y’ . If found, application redirects to LDAP for authentication of use else the user gets access failure message. After successful login in the LDAP user has access to OSWAS.

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 username and password were sent to LDAP for authentication and when login was

[32] Up to a second of creation

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.

  Further, analysis of database revealed that login names were re-allotted to different users after transfer of the persons. For instance, the login name allotted to Excise Minister was allotted to another Minister on his taking charge of the portfolio. Subsequently, on change of portfolio, the same login name was again allotted to another Minister currently holding the portfolio. The login name should be person specific to ensure responsibility. But in this case, same login name was used by three different users.

The Department assured (May 2016) that the deficiencies in the system would be rectified.

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.

Analysis of database 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 (May 2016) the observations and assured that steps would be taken to make good such deficiencies.

2.2.18 Database Redundancy

As per the best practice, the databases of IT systems need 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.

2.2.18.1 Inefficient document management

Database analysis 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 (May 2016) the observation and assured that corrective action would be taken.

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[33], 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

[33] e-Despatch was developed on dot net (.NET) framework with Asp.net as front-end and MS SQL Server being the database system with Internet Information System (IIS) being the web server

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[34] 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 (May 2016) that the integration between OSWAS and e-Despatch would be strengthened.

2.2.19 Incomplete Leave Processing System

Leave Processing System (LPS) was implemented in the Odisha Secretariat as a common application of OSWAS. LPS was implemented in all the departments but was found configured only for 2,017 out of 7,205 users. 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 this, 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

[34] 4,294 letters of 2013, 34,459 of 2014 and 35,683 of 2015 were pending for processing in OSWAS

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*., are 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 not 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 (May 2016) 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.

2.2.20 Monitoring and evaluation

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 cert-in[35] empaneled security auditor. The Security Auditor conducted the audit (March 2015) and pointed out four vulnerabilities *viz*. (i) User credentials are 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 in January 2016, all four vulnerabilities still existed.

[35] Indian Computer Emergency Response Team, Department of Technology, Government of India

The Department accepted (May 2016) the non-implementation of security audit recommendations and assured that the same would be implemented.

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 is only compatible with the older version of Java[36] platform as TCS implemented OSWAS by customising the software developed for Government of Gujarat during 2005-07. It does not allow upgradation to latest versions[37] of Java platforms. Older Java has several common vulnerabilities and exposures (CVEs) which makes the system prone to attacks as it allows 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 deteriorates user experience as stated below:

  - In home page, the link " Common Application" directs 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.

[36] JRE version 6 (1.6.0.25 /6u25)
[37] JRE with version 8

- 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 effected 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 (May 2016) the technical obsolescence and poor functionality of OSWAS and assured that platforms would be upgraded.

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[38] (May 2016) 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:

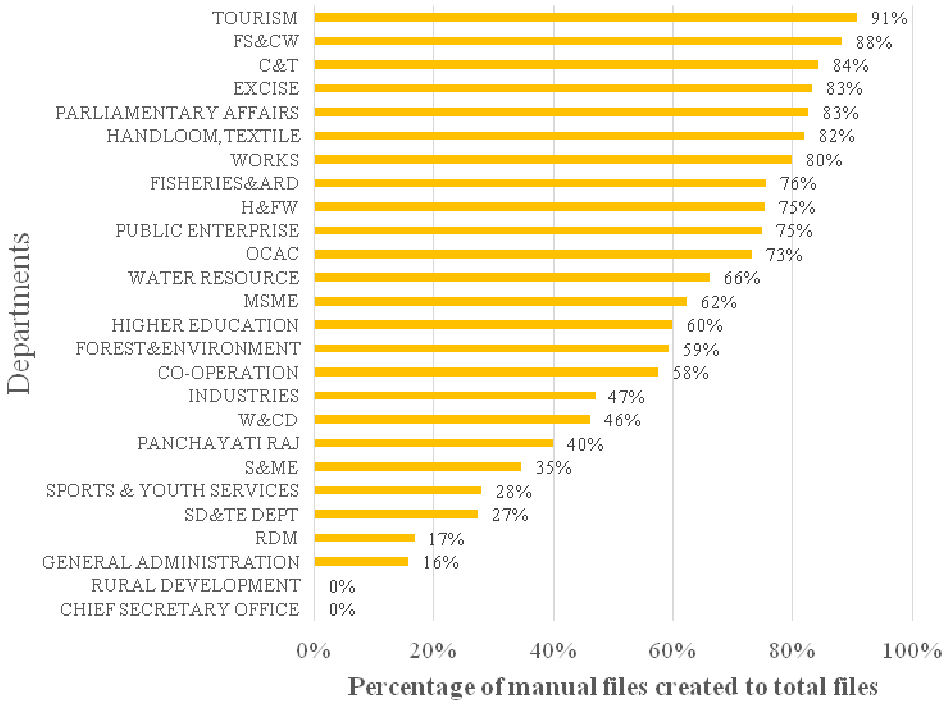
* ***Creation and movement of manual files:*** Audit noticed that movement of manual files in 8 out of 26 departments had reduced

[38] Departments in OSWAS include 39 departments and four offices *i.e.* Chief Secretary Office, Chief Minister's Office, OCAC and Hon'ble Governor's Office

during 2014-15, but the same was found to have increased during the period in other 11 departments as depicted in ***Appendix 2.2.3***.

Usage of OSWAS for file management varied hugely across departments. Percentage of creation of manual files to the total files created in the year 2015 in 26 departments is given in ***Chart 2.2.1***.

Chart 2.2.1: Creation of manual files across 26 Departments in the year 2015



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. The trend of creation of files in these departments is given in ***Appendix 2.2.3***. 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[39], only two to six were being used in 26 departments. The most commonly used application was LPS which was also found deficient as discussed in ***Paragraph 2.2.19***.

  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 (January 2016) as detailed in ***Appendix 2.2.4***. Training on customised software was also not conducted.

The Department accepted (May 2016) the inadequate usage pattern and assured that steps would be taken for time bound phasing out of physical files.

2.2.21 Conclusion

Odisha Secretariat Workflow Automation System (OSWAS) was implemented by Government of Odisha to bring in efficiency and effectiveness in the functioning of State Secretariat. However, OSWAS failed to achieve its objective even after six years of implementation. All the applications of OSWAS were not implemented so far. Only one department is using OSWAS fully and others are using it partially. OSWAS had weak management controls as payment was released without ensuring deliverables, conducting business process re-engineering and framing Business Continuity Plan. OCAC did not exercise adequate control over Database Administration activities. The applications of OSWAS had design deficiencies like incomplete administrator interface, non-provision of transfer/ posting, ineffective session management, time-stamp inconsistencies, *etc*. This resulted in inefficiency in the workflow of the Secretariat. Access control was found inadequate in OSWAS as the files were available to everybody irrespective of department, post and privilege. Due to improper design and non-implementation of secured sockets layer authentication system, security of the system was weak. Lack of normalisation resulted in unnecessary increase in size of database which affected the performance of OSWAS. The digital signature was partially implemented which failed to protect the integrity of notes. Leave Processing System was found to be incomplete. Usage of OSWAS was low as 81 *per cent* of departments had created more than 50 *per cent* of files, bypassing OSWAS.

[39] As per SLA, 20 Common applications for departmental use. Eight common applications identified in RFP as employee specific

2.2.22 Recommendations

- Business Processes should be reviewed to suit the legal requirement and Odisha Secretariat Instructions should be modified accordingly.
- All deliverables from the vendor as per Service Level Agreement may be ensured.
- Proper documentation like database design, application design and system design documents may be prepared along with transferring of source code to Government to avoid excessive dependence on vendor support in maintenance of OSWAS.
- OCAC may be strengthened to take up jobs of database administration, database maintenance, system administration, *etc*., with due segregation of duties to ensure security of IT systems.
- Business Continuity Plan and Disaster Recovery mechanism for OSWAS should be put in place.
- Periodic third party audits should be conducted to ensure confidentiality, integrity and availability of information in OSWAS.
- Appropriate input and validation controls along with adequate access control mechanism and enforcement of digital signature as per Information Technology Act should be provided.