

Chapter II Performance Audit

This chapter contains the findings of Performance Audit on Implementation of Rashtriya Madhyamik Shiksha Abhiyan in the State and Information Technology Audit on Implementation of Odisha Secretariat Workflow Automation System.

School and Mass Education Department

2.1 Implementation of Rashtriya Madhyamik Shiksha Abhiyan in the State

EXECUTIVE SUMMARY

The objective of Rashtriya Madhyamik Shiksha Abhiyan (RMSA) was to provide access, quality and equity in secondary and higher secondary education to the eligible population in the country. Though the RMSA framework provides for one secondary school within a reasonable distance of five km from the residence, 3,167 eligible habitations did not have any secondary school. There was absence of preparatory work like formation of Core Group for micro planning at district level by conducting survey for assessing the requirement of infrastructure and prioritising them to implement the scheme. No planning was done to implement Vocationalisation of Secondary Education. The State could establish only 773 out of 1,535 new schools proposed in the Perspective Plan. There was shortfall in construction of new schools and strengthening of infrastructure in existing schools, resulting in classroom-student ratio exceeding the norm of 1:40. In addition, students were deprived of facilities like libraries, laboratories, etc. The quality of education suffered due to non-recruitment of 4,790 teachers and inadequate training to them. Implementation of ICT@Schools suffered due to deficient e-content, inferior quality furniture, non-supply of tablets with pre-installed e-content and ineffective ICT training to teachers. Monitoring of implementation of the scheme was deficient both at district and State level. Consequently, the physical milestones approved by the Government of India could not be achieved even after six years of implementation.

2.1.1 Introduction

Government of India (GoI) launched Rashtriya Madhyamik Shiksha Abhiyan (RMSA) in 2009 with the objective of providing access, quality and equity in secondary and higher secondary education in the country. In order to provide access to educational institutions, the scheme envisaged establishment of new secondary schools, upgradation of existing upper primary schools and strengthening of existing secondary schools. The scheme aimed at providing required infrastructure, engagement of adequate number of teachers and training for them for bringing quality. To maintain equity, the scheme provided for establishment of hostels, free lodging/ boarding for weaker sections of society and girl students besides facilities such as providing

assistive devices, teaching/ learning material, transport/ escort allowance, etc., to disabled students.

The earlier schemes launched by GoI namely Girls' Hostel (2009-10), ICT@Schools (2010-11), Inclusive Education for Disabled at Secondary Stage (IEDSS) (2013-14) and Vocational Education (VE) (2013-14) were subsumed under RMSA. While RMSA and ICT@Schools schemes were funded jointly by GoI and Government of Odisha (GoO) in the ratio of 75:25, Vocational Education and Girls' Hostel schemes were funded in the ratio of 90:10 and in case of IEDSS scheme, it was fully funded by the GoI. The scenario of secondary education in the State before launching of RMSA and at the end of academic year 2014-15 is indicated at **Table 2.1.1**.

Table 2.1.1: Statement showing category-wise schools, enrolment of students and teachers deployed during 2009-10 and 2014-15

Category	No. of schools		Enrolment ¹ in secondary schools		No. of teachers	
	2009-10	2014-15	2009-10	2014-15	2009-10	2014-15
Government	4,594	5,071	5,27,438	7,17,629	27,878	30,742
Aided	2,052	2,892	2,92,461	3,54,016	17,192	20,336
Others ²	1,272	1,528	1,27,656	1,53,914	NA	NA
Total	7,918	9,491	9,47,555	12,25,559	45,070	51,078

(Source: Information furnished by the Department and OMSM)

The number of Government schools to total schools in the State decreased from 58 per cent in 2009-10 to 53 per cent in 2014-15. However, the percentage of enrolment therein to the total enrolment increased from 56 to 59 during the same period. Despite increase in enrolment, the Government schools were not equipped with required teaching staff and infrastructure as discussed at **Paragraphs 2.1.6.4** and **2.1.8.1**.

2.1.2 Organisational set up

The State Government implemented RMSA and other four schemes through Odisha Madhyamik Shiksha Mission (OMSM), a registered society, established (2010) under the administrative control of School and Mass Education (S&ME) Department. While the Director of Secondary Education is responsible for overall administration of Secondary Education in the State, the State Project Director (SPD) of OMSM is overall in-charge of implementation of the scheme in the State. In each district, one District Education Officer (DEO) cum District Project Co-ordinator (DPC) is responsible for implementation and monitoring of the scheme. OMSM forwards consolidated proposals to the National Mission for release of funds and the same are examined and approved by the Project Appraisal and Approval Committee of the National Mission known as Project Appraisal Board (PAB).

¹ Enrolment does not include Class XI and XII as they are coming under Higher Education in this State

² Includes students in private, ICSE and CBSE schools

2.1.3 Audit objectives

The Performance Audit on implementation of RMSA aimed to assess whether:

- Required planning and institutional arrangements were made to bring all the eligible children under the RMSA fold;
- Programmes were implemented in accordance with the scheme guidelines and manuals;
- Required number of qualified teachers were recruited, trained and posted for providing quality education as per norms of the scheme;
- Funds were utilised economically, efficiently and effectively; and
- Adequate internal control and grievance redressal systems were in place and were effective.

2.1.4 Audit criteria

Performance Audit was evaluated with reference to the following criteria:

- Framework on Implementation of RMSA and Manual on Financial Management and Procurement on RMSA framed by GoI;
- Annual Work Plans & Budget and Annual Action Plans of OMSM;
- Orissa Budget Manual, Orissa Treasury Code and Orissa General Financial Rules;
- Odisha Public Works Department Code; and
- Instructions and orders issued by the GoI and State Government.

2.1.5 Scope and Methodology of Audit

Audit was conducted during September 2015 to January 2016 covering the period 2010-15. Audit test checked records of School and Mass Education Department, Directorate of Secondary Education, Odisha Madhyamik Shiksha Mission (OMSM), District Education Officers and Block Education Officers/ District Inspector of Schools of eight³ sample districts. The sample districts were selected based on the Random Sampling Without Replacement (RSWOR) method. In each district, one urban block and two rural blocks were selected and in each block three secondary schools were selected on RSWOR method. In the presence of and at the request of Audit, departmental officers conducted physical inspection of assets. Photographs were taken, wherever considered necessary. Interview of 10 students and five teachers in each sampled school were conducted through an administered questionnaire to ascertain the satisfactory level of teaching environment, availability of physical infrastructure and quality of teaching. The Audit objectives, criteria, scope and methodology of the Performance Audit were shared with the Commissioner *cum* Secretary, S&ME Department in an Entry Conference held on 7 August 2015. Exit Conference with Commissioner *cum* Secretary, S&ME was held on 12 May 2016, where the audit observations were discussed. The views of the Department were considered and suitably incorporated in the Report.

³ Balasore, Sundargarh, Sonepur, Kendrapara, Koraput, Jajpur, Rayagada and Dhenkanal

The audit findings are discussed in the succeeding paragraphs.

Audit Findings

2.1.6 Planning

2.1.6.1 Habitation without access to secondary school

The framework for implementation of RMSA, *inter alia*, provides for a secondary school within a reasonable distance of five kilometres from each habitation. As per the Perspective Plan prepared by the Department, 1,535 secondary schools (new and upgraded) were to be established during 2009-12⁴ to cover all eligible habitations. The coverage of habitations by secondary schools in 2009-10 and 2014-15 is indicated at **Table 2.1.2**.

Table 2.1.2: Status of coverage of habitations

Particulars	2009-10	2014-15
Total no. of eligible habitations for coverage under secondary schools	87,095	89,341
No. of eligible habitations not covered by secondary schools	1,235	3,167

(Source: Status Report of secondary education and AWP&B of the State)

Though the coverage of secondary schools increased by 2.58 *per cent* in 2014-15 as compared to 2009-10, the uncovered eligible habitations to total habitations increased from 1.42 *per cent* in 2009-10 to 3.54 *per cent* in 2014-15.

Audit observed that only 773 schools⁵ were established as of March 2015 due to delay /non-commencement of construction of new buildings in upgraded schools. However, no Perspective Plan was prepared beyond 2012. As of March 2015, out of 89,341 habitations in the State, 3,167 habitations (3.54 *per cent*) did not have a secondary school within the prescribed distance which included 1,195 eligible habitations in eight sample districts. During survey conducted by departmental officials in presence of Audit, 120 out of 649 students stated that they had to cover more than five km to reach the school.

The Department assured (May 2016) that the matter would be looked into.

2.1.6.2 Non-formation of Core Group and non-preparation of Perspective Plan at school level

As per RMSA framework, a Core Group was to be formed at district level comprising of governmental and non-governmental persons who would undertake an extensive visit of the district, by interacting with each household to ascertain the educational status and the educational need. Further, a School Management Committee (SMC) was to be formed at each school level who would prepare a school level Perspective Plan and Annual Plan. Annual Work Plans were prepared by the DPC based on the data available in Unified District Information System for Education (UDISE) as well as Census data and not on the basis of actual household and school surveys.

Audit noticed that:

- OMSM did not maintain any data on the availability of classrooms for secondary level to assess additional requirement for maintaining classroom-pupil ratio at 1:40 as per RMSA guidelines. Similarly,

⁴ 2009-10: 300, 2010-11: 800 and 2011-12: 435

⁵ 2009-10: 300, 2010-11: 400, 2011-12: 9, 2013-14: 45 and 2014-15: 19

critical infrastructure like laboratories, libraries, drinking water facilities, etc., were not assessed.

- Though SMCs were formed in all 50 sample schools, no Perspective or Annual Plan was prepared at school level. Committees like Building Committee and Academic Committee were not constituted to oversee construction of infrastructure and conduct of proper academic activities.

Thus, the planning process was not conducted as envisaged in the framework. The Department while admitting (May 2016) the fact, stated that the district functionaries of RMSA were being strengthened.

2.1.6.3 Absence of plan for Vocational Education and IEDSS

The Vocationalisation of Secondary Education scheme was subsumed in RMSA during 2013-14. GoI sanctioned ₹ 9.41 crore and released (March 2014) ₹ 4.70 crore. In addition, the State Government also released (March 2014) ₹ 43.80 lakh.

Audit noticed that the Department decided only in May 2015 to open two trades *i.e.* Information Technology/ Information Technology Enabled Services and Automobile from the academic year 2015-16 in 30 schools for 1,500 students. However, the trades were not opened in any of the schools as of December 2015 due to absence of plan.

Further, GoI launched IEDSS scheme with the objective of ensuring retention of all disabled children passing out of Class VIII by creating easily accessible appropriate environment in secondary schools. The scheme was implemented in the State through NGOs. Due to non-preparation of plan and proposal for the period 2012-15 by the Department, the scheme could not be implemented in the State. As a result, disabled students were deprived of the benefits of the scheme.

The Department stated (May 2016) that steps would be taken to implement the scheme in the State from 2016-17.

2.1.6.4 Non-posting of teaching and non-teaching staff

The PAB, while approving the upgradation of new schools and strengthening of existing schools, also approved new teaching and non-teaching posts to these schools from 2009-10 onwards. The details of teaching and non-teaching staff approved and actually recruited in these schools under the Scheme are detailed in the *Table 2.1.3*.

Table 2.1.3: Details of staff approved and in position

Year	PAB approval		Actual recruitment	
	Teacher	Non-teaching ⁶	Teacher	Non-teaching
2009-10	2,400	0	691	0
2010-11	3,200	1,400	687	0
2011-12	72	1,400	6	0
2012-13	0	807	0	0
2013-14	360	1,418	10	0
2014-15	152	0	0	0
Total	6,184	5,025	1,394	0

(Source: Information furnished by OMSM)

⁶ Laboratory Assistants, Library Assistant *cum* Office Assistant and Daftery

As against approval of 6,184 teachers, only 1,394 teachers (22.54 per cent) were appointed. In 2012-13 and 2014-15, no teachers were appointed though 5,654 and 1,499 teachers respectively were approved by PAB. In respect of non-teaching staff, no recruitments were made though PAB approved 1,394 posts. In this context, Audit noticed the following:

- In all 50 sampled Government schools, teachers were not available for five⁷ subjects as of March 2015 and in 13 schools, Teacher-Pupil ratio registered was 1:31 to 1:56 as of March 2015 against norm of 1:30.
- In 240 schools, as against requirement of 1,821 teachers, there were 2,359 teachers, resulting in excess of 538 teachers. At the same time, in 974 schools, there were 4,256 teachers against requirement of 7,202, resulting in shortage of 2,946 teachers.
- In Rayagada district, in three high schools, there were two Physical Education Teachers (PET) in each school, whereas 52 schools in the district did not have a single PET.

2.1.7 Financial Management

To achieve the intended objectives of the programme, the GoI and GoO released their share of funds to OMSM for further release to the DPCs for implementation of the programme. During 2009-15, OMSM received ₹ 1,321.31 crore⁸ and utilised only ₹ 560.76 crore (42.44 per cent). The year wise sanction and receipt of funds is detailed in *Appendix 2.1.1*. Except, 2014-15, the percentage of shortfall in utilisation of funds in the State during 2009-14 ranged from 51.27 (2009-10) to 94.13 (2010-11). The non-utilisation of funds was due to non-completion of construction of 414 schools, non-conducting of training programmes, non-implementation of VE scheme, etc., as discussed in *Paragraphs 2.1.6.3, 2.1.8.1 and 2.1.9.1*. Due to slow progress in implementation of the schemes, the State Government could avail of only ₹ 977.76 crore as against ₹ 1,752.44 crore approved by the GoI.

Audit also noticed the following irregularities:

- Advances amounting to ₹ 516.98 crore, sanctioned in favour of 30 DPCs, 30 DEOs of the Department and three Inspectors of Schools of SC&ST Department, were lying unadjusted, which included ₹ 58.24 crore in eight sampled districts as of March 2015.

The Department assured (May 2016) to initiate a drive to adjust the outstanding advances.

- OMSM advanced ₹ 1.10 crore to 12 institutions (₹ 96.67 lakh) and eight employees (₹ 13.22 lakh) during December 2011 to March 2015 for office contingency, training, renovation work, procurement of teaching kits, etc., which remained unadjusted as of December 2015. Out of them, six employees who took advance of ₹ 13.17 lakh had already been transferred out of the administrative control of OMSM as

⁷ TGT Arts: 16 schools, TGT Science: 10 schools, Hindi: 19 schools, Sanskrit: 13 schools and PET: 10 schools

⁸ GoI: ₹ 977.75 crore, GoO: ₹ 297.47 crore and interest: ₹ 46.09 crore

of December 2015 and no action was taken to recover the outstanding advances.

The Department stated (May 2016) that major amount of advances related to National Council for Educational Research and Training towards purchase of books.

- In three, out of eight sample districts, ₹ 88.43 lakh was diverted for other purposes under the orders of SPD, OMSM and ₹ 5.13 lakh was diverted for 'distribution of bicycle' to students by the DEO Kendrapara, which is a State sponsored scheme.
- Out of ₹ 21.87 crore released by GoI during 2009-12 under IEDSS scheme, the Department deducted ₹ 21.87 lakh towards Audit Fee, despite absence of any such provision in the scheme. However, no audit was conducted and no expenditure was incurred in this regard, as of August 2015. Despite this, the Department furnished full utilisation certificate to GoI.

The Department assured (May 2016) that the matter would be looked into.

2.1.8 Programme implementation

RMSA has a provision for infrastructure support to enhance access and to provide enabling conditions for quality education, including construction of new class rooms, laboratories, art and craft room, library, office room, girls' hostel, etc. The deficiencies in implementation of various components of RMSA are discussed below:

2.1.8.1 Shortfall in construction of new schools

As per the school mapping exercise conducted by OMSM, out of 87,095 habitations, 7,761 (8.91 per cent) had no secondary school within a radius of five km. This required establishment of 1,535 new secondary schools. The year-wise target and achievement in construction of new schools for the period 2009-15 are as under:

Table 2.1.4: Target vis-a-vis achievement in establishment of new secondary schools

Year	Perspective Plan (PP)	Proposal made in AWPB	PAB approved	As of March 2015			
				Completion	Shortfall	In progress	Not taken up
2009-10	300	300	300	195	105	58	47
2010-11	800	800	400	164	236	141	95
2011-12	435	42	9	0	9	0	9
2012-13	--	0	0	0	0	0	0
2013-14	--	70	45	0	45	25	20
2014-15	--	200	19	0	19	0	19
Total	1,535	1,412	773	359	414	224	190

(Source: Compiled from AWP&B)

Due to non construction of schools, the targets for completion of 1,535 schools

by the end of 2011-12 as per the Perspective Plan could not be achieved, leading to extension of construction plan beyond 2011-12.

Audit noticed that:

- Though the Department constructed/ upgraded 773 existing upper primary schools to secondary schools, it failed to create necessary infrastructure for 414 schools (53.56 per cent) as of March 2015.
- The executing agencies did not take up the works in 190 schools even after lapse of one to six years due to non-handing over of land (25), unsuitable locations (18), non-completion of tendering process by the executing agencies (88) and reasons for delay not found on record (59).
- Out of 50 test checked schools, construction of additional class rooms was not done in 10 schools upgraded during 2009-11 and in case of three schools, students of class IX and X were sitting together due to dearth of classrooms.

The Department stated (May 2016) that steps would be taken to complete construction of infrastructure.

2.1.8.2 Shortfall in strengthening of existing schools

In order to address the infrastructural constraints of existing 4,594 secondary schools, RMSA scheme envisaged construction of additional classrooms to maintain classroom-pupil ratio at 1:40. Further, the scheme also envisaged to convert the existing school buildings to all weather resilient buildings, construction of headmaster's rooms, library, laboratory, toilets, etc. Accordingly, the Department prepared Annual Work Plan & Budget (AWP&B) for each year for the period 2009-15, indicating number of units (*i.e.* class room, laboratory, etc.) to be strengthened. **Appendix 2.1.2** indicates creation of various infrastructures as of March 2015. Audit noticed following deficiencies:

- OMSM had neither maintained year-wise achievement against targets nor put in place a monitoring mechanism to watch execution of works.
- In the State, 685 schools did not have all weather buildings; 2,468 schools did not have headmaster's room, six secondary schools were housed in tents, 59 schools did not have blackboard, 1,452 and 802 schools did not have boys' and girls' toilets respectively. Further, 1,114 schools did not have electricity connections.
- Out of 50 sample Government schools, 27 schools did not have sufficient classrooms, resulting in classroom-pupil ratio as high as 1:52 to 1:135. Further, 38 schools had no laboratory and in 21 schools, required equipment were not available in laboratories.



As per RMSA, the School Management and Development Committees (SMDC) were empowered to execute works up to the value of ₹ 30 lakh. But in 50 sampled schools, it was noticed that these SMDCs were not involved in

any of the construction works and these works were executed through Rural Development and Public Works Departments.

The Department stated (May 2016) that steps would be taken to complete construction of infrastructure.

2.1.8.3 Implementation of ICT@Schools

The objective of ICT@Schools was to provide computer aided education in all secondary and higher secondary schools. The GoI approved implementation of the scheme in 6,000 schools⁹ in the State. The State Technical Committee recommended (December 2012) engagement of a technical consultant for implementation of the scheme through open selection process. However, the Department engaged (February 2013) Odisha Knowledge Corporation Limited (OKCL), a Special Purpose Vehicle formed (July 2011) by the State Government in collaboration with Maharashtra Knowledge Corporation Limited to provide IT enabled education and IT enabled services in the State, as the technical consultant on nomination basis to implement the scheme of ICT@Schools in 4,000 schools for a total cost of ₹ 790.12¹⁰ crore. The scope of work included procurement of hardware and physical infrastructure on behalf of the Department, inspection and monitoring of implementation of the scheme, conducting initial teachers' training for ICT, procurement and or development of software application, e-content, etc. Apart from this, OKCL had to supply tablets with pre-installed e-content, give web-based training and provide e-books based on NCERT syllabus to all the teachers. As of 31 March 2016, OMSM paid a sum of ₹ 204.30 crore towards non-recurring expenditure to OKCL. In addition, accrued interest of ₹ 3.97 crore was also advanced to OKCL. Audit noticed the following:

- **Deficient e-Content:** As per the agreement, OKCL would develop e-contents for Class IX and X of 4,000 schools at unit cost of ₹ 45,000 per school aggregating to ₹ 18 crore. Further, the e-contents would be approved by the Department before installation in the master computers of the schools. However, OKCL installed the e-contents in all the schools without the approval of the Department. The Executive Committee (March 2015) of OMSM observed that the e-contents were deficient and decided to explore the possibility of procurement of e-contents from other reputed organisations. However, no further action was taken by the Department.
- **Supply of inferior quality computer tables:** The computer tables (44,317) valuing ₹ 8.34 crore provided by OKCL did not conform¹¹ to the prescribed specifications, as reported (June 2015) by the Technical Committee of OMSM. The Committee opined either to reject all the tables and replace them or to impose penalty on OKCL. Despite this, the tables were being utilised in the schools without any replacement.

⁹ 2010-11: 4,000 schools and 2012-13: 2,000 schools

¹⁰ Non-recurring expenditure towards supply of hardware and software (₹ 295.50 crore), development of e-content (₹ 18 crore), teachers training (₹ 21.60 crore), recurring expenditure towards consumables, electricity, internet, petrol/diesel, telephone charges, school co-ordinator salary (₹ 440.02 crore) and monitoring (₹ 15 crore)

¹¹ Leg frame was 1-inch square pipe against specification of 1.5 square inch

- **Ineffective ICT training:** As per the training module prescribed by the GoI, web based induction training in ICT was to be given once to the teachers for a period of 80 hours¹² followed by refresher course of 40 hours¹³ each in succeeding years *i.e.* 240 hours in total. However, agreement with OKCL, provided only for induction training of 132 hours without provision for any refresher course. OKCL trained only 4,935 out of 24,555 teachers as of March 2016.
- **Non-supply of tablets to the teachers:** The agreement envisaged that OKCL would supply tablets to 40,000 teachers of 4,000 schools with pre-installed e-content and train them on its use. Since no timeframe was fixed for supply, OKCL was yet to supply the tablets as of March 2016 on the plea that the training was not fully completed. Audit also observed that OMSM had ordered 40,000 tablets when the number of teachers on roll were only 24,555. Thus the Department failed to project the actual requirement.

The Department while admitting (May 2016) the facts, stated that the matter would be looked into.

- **Deficiencies in the agreement:** Audit noticed the following deficiencies in the agreement entered by OMSM with OKCL.
 - There was no specific timeframe specified in the agreement for deliverables like completion of teachers training, supply of hardware and software, supply of tablets to the teachers, *etc.* As a result, all teachers were not trained in ICT programme and were not provided any tablets with built-in contents.
 - There were no penal clauses in the agreement for delay in supply and installation of hardware, software, maintenance of quality in e-content, failure to achieve the target of training of teachers, *etc.*, by OKCL. Due to this, no penal action could be taken by OMSM.
 - As per the agreement, OKCL had to develop a monitoring and inspection system for efficient functioning of the scheme like provision of first level supervision at schools, monitoring the schools through helpdesk to the users, learners, *etc.* But there was no role for OMSM or the Department to monitor the implementation of the scheme by OKCL.

Due to these deficiencies in the agreement, the interest of the State was not protected.

2.1.8.4 Extra expenditure in construction of Girls' Hostel

GoI introduced (2009-10) Girls' Hostel Scheme for setting up of hostels with lodging and boarding facilities in the Educationally Backward Blocks (EBBs) and areas near to the habitation of the target groups so that the girl students are not denied the opportunity of continuing their study due to societal factors. The GoI granted in-principle approval for construction of 130 girls' hostels

¹² Eight hours per day for 10 days

¹³ Eight hours per day for five days for every subsequent year

during the period 2009-11 at unit cost of ₹ 1.71 crore. The approval was subject to condition that Central share shall be released on submission of drawing/ design and estimate of the hostels in conformity with scheme guidelines.

Audit noticed that the drawing/ design and estimates furnished¹⁴ by the State Government were not as per the scheme guidelines. GoI while approving (April 2014) the drawing/ design and estimates stipulated that the Central share shall be limited to the cost of construction as per Schedule of Rates (SOR) 2010-11 and any extra cost shall be borne by the State Government. GoI released ₹ 87.94 crore in July 2014 as first instalment. The State Government also released ₹ 9.77 crore. The Department executed the works through Rural Development (RD) Department at unit cost of ₹ 2.28 crore based on SOR 2013-14. Thus, due to preparation of improper drawing/ design and estimates, the State Government will have to bear an extra financial burden of ₹ 74.10 crore in construction of 130 hostels.

The Department stated (May 2016) that steps would be taken for early completion of hostels.

2.1.9 Quality aspects

2.1.9.1 Training to teachers and management personnel

RMSA emphasised the necessity of continuously upgrading the quality of teachers through in-service education programmes. Accordingly, GoO prepared a subject-wise training module called 'SAMARTHYA' for teachers. Besides, RMSA also envisaged to sponsor other training programmes like induction training to newly recruited teachers, training to Headmasters, etc. The PAB approved 2,68,495¹⁵ training slots for teaching staff and 1,68,936¹⁶ training slots for management personnel during 2010-15. Audit noticed the following:

- Test check at sample schools revealed that training of 'SAMARTHYA' was imparted to only 299 teachers in 531 slots against allotted 1,389 slots.
- In 2010-11 and 2013-14, training slots for 60,689 and 4,612 respectively, for teachers were not utilised.
- Similarly, 1,68,936 training slots for management personnel were not utilised.

OMSM stated (February 2016) that inadequate training of teachers was due to shortage of manpower, lack of monitoring, inadequate expertise in assistances and improper dissemination in districts.

2.1.10 Slow pace in achievement of targets

Visions of RMSA included universal access of secondary education by 2017 (Gross Enrolment Ratio (GER) of 100 *per cent*) and universal retention by 2020. The broad indicators of secondary education in the State before launching of RMSA and at the end of academic year 2014-15 are as follows:

¹⁴ 16 August 2010, 2 March 2012 and 22 September 2012

¹⁵ 2010-11: 60,689, 2011-12: 55,070, 2012-13: 54,051, 2013-14: 70,175 and 2014-15: 28,510

¹⁶ 2011-12: 82,692, 2012-13: 86,184, 2013-14: 30 and 2014-15: 30

Table 2.1.5: Broad indicators of status of Secondary Education in the State

Year	GER	NER	Retention Rate
			(In per cent)
2009-10	59.89	40.39	79.03
2010-11	69.27	52.72	78.08
2011-12	77.43	64.18	83.56
2012-13	78.60	66.13	84.53
2013-14	78.70	65.00	83.51
2014-15	75.43	64.86	85.64

(Source: AWP&B 2015-16)

- GER, at the beginning of the implementation of RMSA (2009-10) was 59.89 which increased to 75.43 in 2014-15. However, three sample districts¹⁷ registered GER ranging from 53.23 to 74, which were below the State average.
- Though NER increased from 40.39 in 2009-10 to 64.86 in 2014-15, there was a decreasing trend in last three years and four sample districts¹⁸ were found below the State average in 2014-15.
- Similarly, the retention rate increased by 15.46 per cent during 2009-15 i.e. from 79.03 per cent in 2009-10 to 85.64 per cent in 2014-15 and the same was also inconsistent. Retention rates in five sample districts¹⁹ ranged from 74.63 to 84.60 per cent which were below the State average.

2.1.11 Monitoring and supervision

Audit noticed following deficiencies in monitoring and supervision of implementation of RMSA and other subsumed schemes in the State:

- **Inadequate review by Governing Council and Executive Council:** As per the charter of OMSM, the Governing Council (GC) and the Executive Council (EC) are required to conduct minimum one and four meetings per annum respectively. During 2011-15, GC and EC conducted only two and four meetings respectively. In absence of regular meetings of GC, monitoring of various activities was not adequate.
- **Non-constitution of District Level Committees:** In seven out of eight sample districts, District Level Committees were not constituted though required under the provisions of Financial Management and Procurement Manual of RMSA. In absence of committees, the intended objective of monitoring progress in implementation of various measures under RMSA, efficient utilisation of funds, etc., could not be ensured.
- **Inadequate inspection by district/ block level officials:** Clause 9.2.3 of RMSA framework emphasised regular field visits/ inspections to ensure comprehensive and continuous assessment of the scheme. The S&ME Department spelt out (July 2013) job specifications of DEOs and BEOs as per which, a DEO was to inspect at least 10 schools per month, while BEO was to inspect all high schools within his

¹⁷ Koraput (53.23), Rayagada (54.53) and Sundargarh (74)

¹⁸ Koraput (46.68), Rayagada (45.45) Jajpur (60.14) and Sundargarh (63.72)

¹⁹ Dhenkanal (83.33), Jajpur (77.82), Kendrapara (80.45), Sonapur (74.63) and Sundargarh (84.60)

jurisdiction. However, DEOs of eight sample districts conducted 979 inspections against requirement of 1,600 during 2013-15. Further, DEOs had no information about number of inspections conducted by BEOs.

- ***Inadequate functioning of School Management Development Committee (SMDC):*** As per provisions of RMSA guidelines, meeting of SMDC should be held frequently but not less than once in a fortnight. In 70 sample schools, 939 meetings (11 *per cent*) were conducted by SMDC as against requirement of 8,400 during 2010-15. Besides, sub-committees like, School Building Committee to monitor infrastructure and accounts matters and School Academic Committee to monitor academic activities were not constituted in any of the sampled schools.
- ***Inadequate Parent Teacher Association (PTA) meeting:*** Out of 1,400 secondary schools in eight sample districts, PTA was not constituted in 317 schools as of August 2015. In 70 test checked schools, PTA was constituted in 39 schools who met only 334 times during 2010-15 against requirement of 4,200 meetings. Thus, effectiveness of deliveries of the scheme was not assessed.
- ***Non-constitution of Grievance redressal cell:*** As per RMSA guidelines, the State Government was required to set up Grievance Redressal mechanism at State, district and school levels. However, no such cell was set up at any level as of March 2015. No records relating to receipt/ disposal of grievances were maintained.

The Department assured (May 2016) that steps would be taken to resolve the issues.

2.1.12 Conclusion

Preparatory work like formation of Core Group and conducting survey for assessing requirement of infrastructure was not done. No plan was made for implementation of Vocationalisation of Secondary Education and Inclusive Education for Disabled at Secondary Stage, leading to non-implementation of these schemes. The physical milestones approved by the Government of India could not be achieved even after six years of implementation, resulting in non-coverage of 3,167 habitations by secondary schools as of March 2015. Due to delay in creation of infrastructure, the class room-student ratio was higher than the norm of 1:40. In addition to that, students were deprived of facilities like laboratories, libraries, *etc.* Quality of education suffered due to non-recruitment of teachers. Deficient e-contents did not assure quality teaching to students. There was inadequate monitoring of implementation of the scheme at both district and State levels.

2.1.13 Recommendation

Government may consider the following recommendations.

- Prepare plan for implementation of Vocationalisation of Secondary Education and IEDSS for effective implementation of schemes.
- Take steps to cover the uncovered habitations.
- Improve infrastructure in the existing schools through timely completion of works.
- Recruitment of teaching and non-teaching staff should be made to improve quality of education.

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.

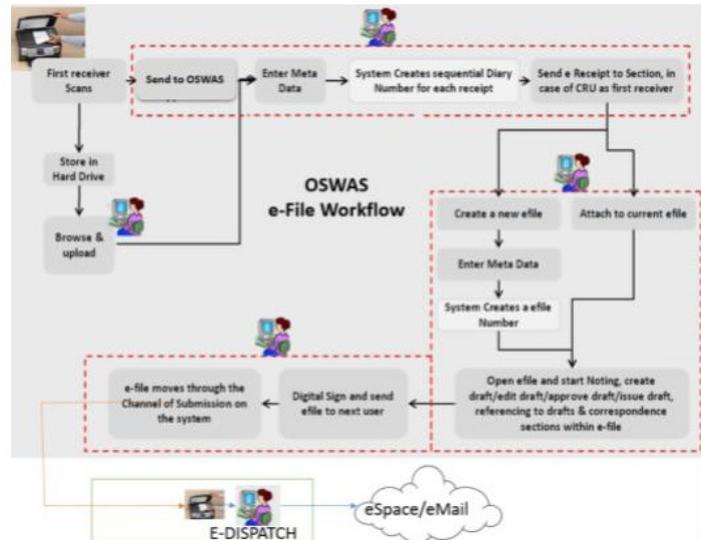
Access controls were found inadequate in OSWAS as the files were accessible to any user irrespective of department, post and confidentiality. User management was given to the vendor without any control of OCAC. OSWAS used outdated platforms making Government business vulnerable. Several features in user 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.* SECLAN²⁰, 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 office 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 analysis²¹ 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, six²² were not developed and 10²³ 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/ organisational²⁵ 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 officers²⁶ 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 2014²⁷, 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 notes²⁸ 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 43²⁹ 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 interface³⁰ 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 changed³¹ 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.

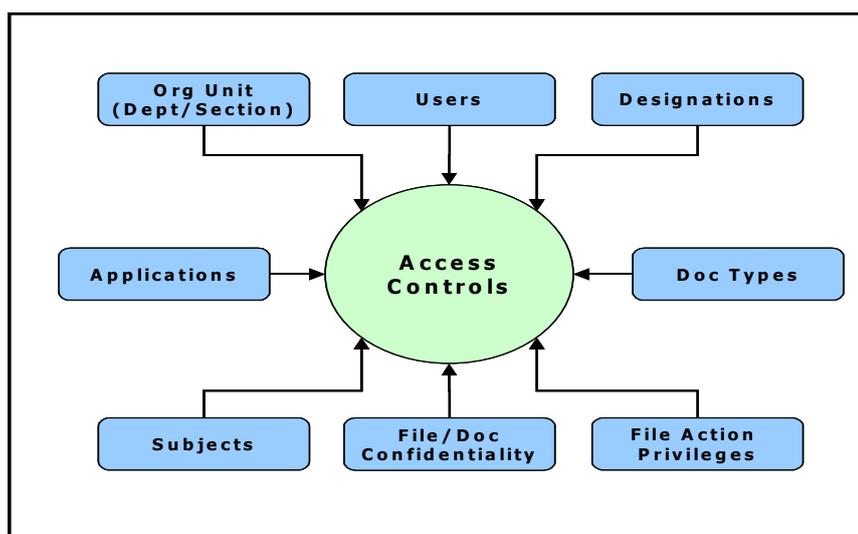
2.2.14.3 Incorrect recording of logout time

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 control provision

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 exactly³² 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.

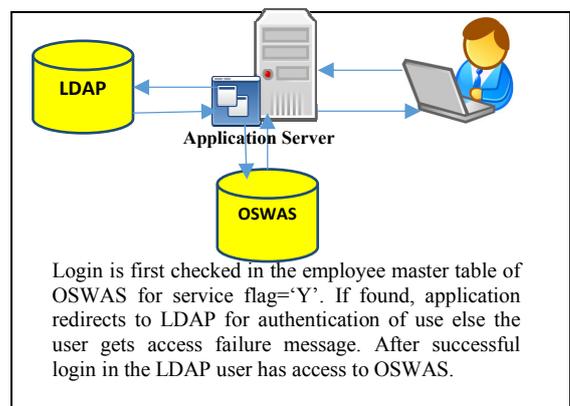
2.2.17.2 *Deletion of document metadata*

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 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 (May 2016) that the system would be strengthened to avoid such inconsistency in future.

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

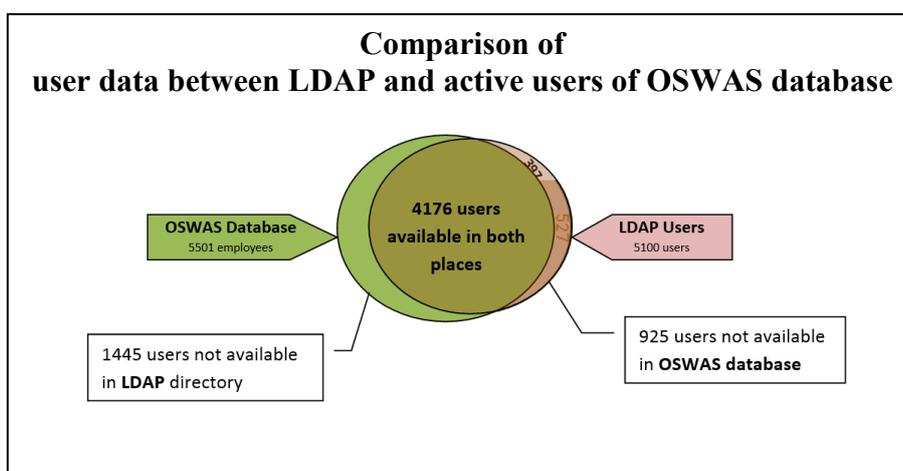


to access OSWAS, the user name was checked in the employee master of OSWAS database for availability and status. If found in service, the username and password were sent to LDAP for authentication and when login was

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 platforms³³, 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 letters³⁴ 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-in³⁵ 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 Java³⁶ platform as TCS implemented OSWAS by customising the software developed for Government of Gujarat during 2005-07. It does not allow upgradation to latest versions³⁷ 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*

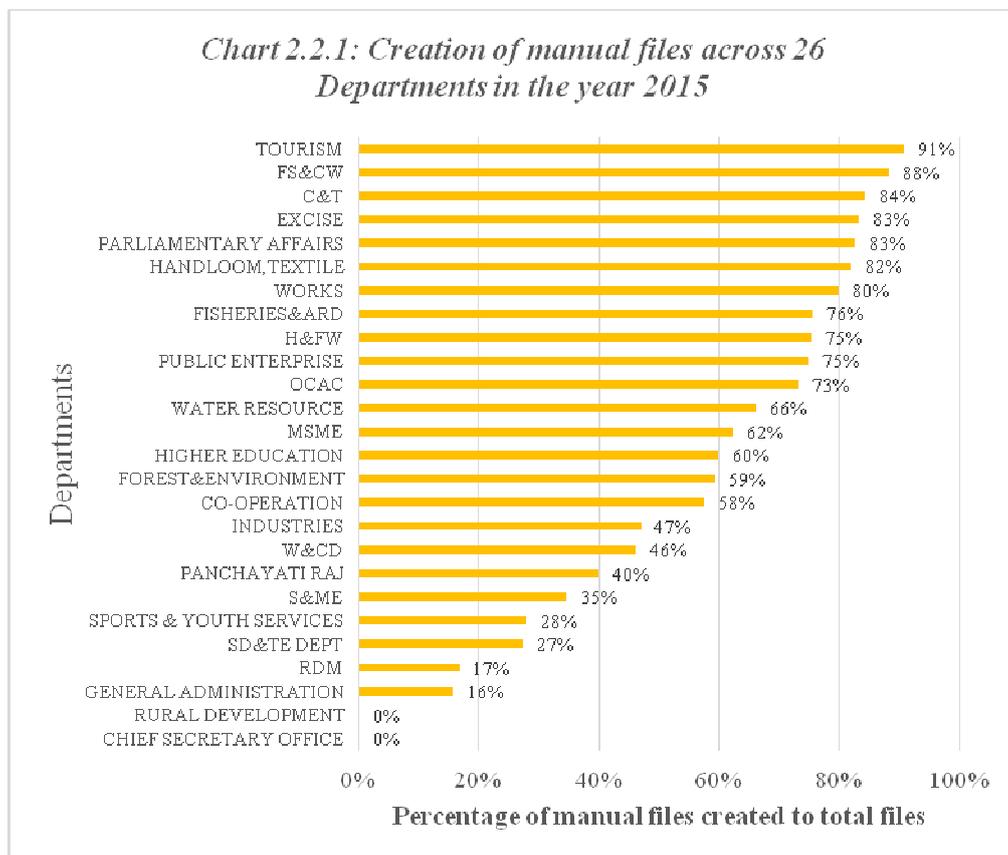
The key objectives of OSWAS were office Automation, enhancing productivity, using Information Technology as an enabler to help in daily work, an efficient workplace, access controls at all levels and efficient and transparent administration. Audit assessed the usage of OSWAS by 26 out of 43³⁸ (May 2016) 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*.



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 applications³⁹, 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.