Exhibit-E

Audit Report : IT Audit Report on 'Effectiveness of controls in Public Expenditure Management System
Schedule of Audit : April 4, 2016 to May 15, 2016
Date of Issue : August 31, 2016
Name of Agency : Department of Public Accounts, Ministry of Finance

No.	Recommendation	Action taken (as per the detailed action plan/report submitted).	Status/Progress of corrective actions taken by the audited agency	Reasons for non-completion of action on any recommendations
1	**Comprehensive ICT security policy should be developed** *The Department lacks a comprehensive ICT security policy, which may impede effective management of security measures to safeguard confidentiality, integrity, and availability of critical information. The Department should, therefore, develop a comprehensive ICT security policy specific to their department and the policy should be communicated to every employee of the Department for their awareness, understanding and greater compliance.*	**Action Plan**: *DPA will develop a separate ICT security policy at DPA specifically for PEMS.* **Timeline:** September 2017	**Agreed to Implement by September 2017.**	*Information on the progress of implementation, if any were not available.*
2	**Department should perform periodic reconciliation of account balances of non-revenue and refundable deposits** *The RAA noted a huge difference of accounts balances of Non-revenue and refundable deposits between the budgetary agencies and at the DPA level. Besides, inconsistent and inaccuracies in information and account balances, there may be risks of such misuse of these balances if appropriate measures are not put in place. Thus, the Department should establish a system of performing periodic reconciliation of these account balances by obtaining and comparing monthly bank balances with control totals of deposits by budgetary agencies. Possibility of incorporating such feature in PEMS should also be explored by the Department.*	**Action Plan**: *DPA will try to implement possible controls/ validations in PEMS. In addition, DPA will also create awareness by sending out specific notification to the budgetary agencies related to NRD and RD.* **Timeline:** *June 2017*	**Agreed to Implement by June 2017**	*Information on the progress of implementation, if any were not available.*

Exhibit-E

3	**Department should institute mechanism to ensure completeness and correctness of financial statements** *Many account heads included in the annual financial statements contain errors and inconsistencies, which would undermine the very purpose of financial reporting. Considering the adverse effect of erroneous financial statements, the Department should institute mechanism to ensure that financial statements, particularly RP statements, generated by PEMS are complete and accurate. Input validation, output controls, exception listings and verification and reconciliation of control totals and other balances are some of the measures to ensure accuracy, integrity and reliability of the system, information and reports.*	*Since FY 2015-2016, with necessary checks and controls implemented in the system, there has been no problem in the financial statement (Receipts and Payments statement).* *The differences worked out by the RAA in the RP statement for the FY 2013-2014 is due to the inclusion of the reversed transactions. This has been re-verified by DPA and the net effect is same.*	***Partially implemented:*** *After receiving the responses from DPA on 8/08/2016, the RAA team reviewed the capital expenditure working for FY 2013-2014 submitted by DPA and found the same difference as reported by the team. Moreover, the RAA excluded all reversal transactions while performing the calculations.* *However, during the audit of AFS 2015-16 conducted in February and March 2017, no such differences were noted.*	
4	**Control over the monthly bank reconciliation should be strengthened** *The RAA found vulnerability in the current bank reconciliation process due to manual intervention from users. Thus, as an important mitigating control, where-possible the Department should, amongst other controls:* *a) Segregate this process from those preparing the accounts – implementing maker and checker concept in larger organizations;* *b) Minimize manual intervention by automating some features such as directly importing bank statements into PEMS; and*	**Action Plan:** *DPA proposed to work on possible solutions to fetch total withdrawal data from Bank of Bhutan Ltd. in order to semi-automate the BRS in PEMS.* **Timeline**: June 2017	***Agreed to Implement by June 2017*** .	*Information on the progress of implementation, if any were not available*

Exhibit-E

	c) *Bank Reconciliations should be independently verified by supervisors.* d) *Independent monitoring and review at DPA level on regular basis to identify unreconciled BRS and requiring the agencies to reconcile the differences.* e) *The budgetary agencies should be required to reconcile the unreconciled BRS as indicated in the report, possibility by working backward from 2015-2016.*			
5	**Strong validation controls should be implemented in PEMS** *Most lapses noted by the RAA were mainly caused due to weak input validation controls in the system. Thus, the Department should ensure that strong input validation controls are incorporated and implemented so that the system does not accept garbage, duplicates, invalid data, and process data incorrectly or illogically. Additionally, strong validation controls over masterfiles should be applied since masterfiles are important files used as references and input for processing transactions.* *Similarly, strong validations should also be implemented in budgetary releases so that releases are made within approved budget, releases are not made without budget, releases are properly accounted for, and duplicate releases are not recorded.* *Further, the Department should review issues discussed under 3.2.1.4- Weak validation controls in budgetary releases in the Report and initiate appropriate corrective/preventive measures.*	**Action Plan:** *With regard to budgetary releases more than approved budget, DPA mentioned that control already exist in PEMS to ascertain that the release can be made only up to the budget balance. One of the main causes was due to budget getting re-appropriated after release has been made. This has already discussed with DNB and DNB has developed necessary controls since June 2016. DPA will further monitor, review, and validate.* *Difference in releases approved by the department and in RP: Regarding this DPA said that this is not happening since FY 2015-2016.* *Controls/validations have already been developed and implemented but monitoring has to be done.* *Refund of earnest Money/security deposits*	**Agreed to Implement by June 2017**	*RAA yet to validate the controls during the Follow-up audit, which will be conducted next year.*

Exhibit-E

		(EMD/SD) without obtaining RD release: Controls /validations have been implemented in PEMS but DPA proposed to further review and monitor. **Timeline:** June 2017		
6	**Adequate processing controls should be implemented** *There were inadequate processing controls particularly in payrolls which resulted in inaccuracies in HC, PF contributions, TDS etc. The Department should implement adequate processing controls in PEMS to prevent erroneous, incorrect calculations and variations in payroll. As evident from the past trends, payroll is one of the vulnerable areas where irregularities occur, thus, implementing robust processing controls would result in correct processing and calculations of pay and remittances in PEMS.*	**Action Plan:** *DPA mentioned having controls and validation in PEMS- Payroll for EMPID, CID, TPN, GIS and PF as well as duplicate checks.* *However, format/datatype and other possible validations need to be analyzed and developed.*	**Agreed to Implement by December 2017**	*Information on the progress of implementation, if any were not available.*
7	**Effective access control management should be established** *a. The RAA observed weaknesses in user access controls which might lead to unauthorised access to PEMS with possible risk of unauthorised activities. The Department should ensure strong access control mechanism in order to avoid duplicate user IDs, multiple user accounts, and generic user accounts in PEMS. Some of the access control procedures include:* *b. The lapses in access control occurred due to decentralization of user account management to agencies. Hence, the Department should study the implications of decentralization of user access management and monitoring mechanism that can be put in place to ensure that user access is properly managed at all levels.* *c. Proper naming convention should be followed for creating users and further user accounts must be created for individual person*	**Action Plan:** *DPA will clean and centralize Creation of users in DPA.* **Timeline:** December 2017	**Agreed to Implement by December 2017**	*Information on the progress of implementation, if any were not available.*

Exhibit-E

	not for agencies or designations. In addition, user accounts must be tagged with proper user names and employee IDs/CIDs for easy identification. d. *In conjunction to this, attempts to logon to the system with invalid passwords or usernames should also be limited in order to reduce the risks of gaining access by unauthorized users.* e. *There is also a need to match the user accounts in PEMS with National Account Service's list for identifying authorized users from unauthorized users. Also for easy fixing of accountability in the event of wrong doings in the system.* f. *Proper procedures must be put in place to assign access rights and privileges and this should be based on 'need to know' and 'lease privilege' principles*			
8	**Effective password management should be instituted** a. *Ineffective password management was observed during the audit. Thus, in order to minimize the risk of gaining unauthorized access to PEMS, the Department should implement an effective password policy. These may include the following:* b. *Passwords or for that matter anything related to the confidentiality of the password must be encrypted while storing in the database in order to avoid disclosure;* c. *The requirement of minimum password length should be set;* d. *Appropriate composition of passwords (containing numbers and alphabets) should be enforced and on the other hand, use of simple words such as person's name, places' name, and dictionary words should be restricted;* e. *Password sharing should be prohibited by educating the users on the consequences of sharing passwords.*	**Action Plan:** *DPA will implement Password policy such as unique password, alpha- numeric, minimum length and etc.* ***Timeline***: *December 2017*	**Agreed to Implement by December 2017**	*Information on the progress of implementation, if any were not available.*
9	**Proper segregation of duties should be instituted** *Although organizations are facing challenges in implementing segregation of duties because of additional overhead cost and*	**Action Plan:**	**Not Implemented**	*DPA justified that it is the responsibility of the budgetary*

Exhibit-E

	complicated IT systems, it is very essential to separate financial functions amongst individuals so as to minimize the risk of fraud and also to introduce good management practices. *Therefore, the Department should ensure that maker and checker concept, embedded in PEMS, is enforced as far as possible in order to implement segregation of duties according to the roles and responsibilities of financial personnel in the larger budgetary agencies.* *The Department should identify agencies where segregation of duties are to be made mandatory depending on size of agencies and volume of transactions so as to ensure that cost of implementation of maker-checker concept does not outweigh the benefits.* *Further, the system should also ensure that users can generate disbursement vouchers only upon approval of authorised official(s) to minimise the risk of fraudulent transactions.*	*DPA mentioned that it is duty of the budgetary agencies to follow the internal control mechanisms. The Department also mentioned that enough awareness has already been created to the agencies during the PEMS Training.*		*agencies to institute proper segregation of duties.* *RAA asserts that DPA, being the nodal agency for institution of Internal Control Mechanisms in implementation of PEMS, should take responsibility.*
10	**Department should establish mechanism to validate remittances with NPPF, RICBL and Heath Trust Fund** *The RAA observed discrepancies in amounts of remittances processed in PEMS and actually received by the NPPF. This led the RAA to believe that the same must be occurring in remittances to other agencies such as RICBL and Health Trust Fund. Therefore, as a mitigating control, the Department should establish mechanism to validate the remittances of PF with NPPF. Besides, the Department should also establish procedures to reconcile the remittances made to other agencies such as RICBL and Health Trust Fund periodically in order to ensure that these remittances are correctly made.*	**Action Plan:** *DPA will develop possible validations and controls in PEMS but budgetary agencies and individual stakeholders should be responsible for validating the remittances.*	**Agreed to implement:** *DPA agreed to develop possible validations and controls in PEMS.* *DPA justified that it is the responsibilities of individual budgetary agencies to reconcile the remittances made to other agencies.*	
11	**Adequate audit logs and trails should be maintained** *Audit logs and trails are important tools for tracking unanticipated or unauthorized activities of users in the system. These tools are useful when there is a need to trace unauthorized activities of users or to detect inadvertent incidents/errors in the system.*	**Action Plan:** *DPA mentioned that once the user creation is centralized in the Department, mapping of*	**Agreed to implement**	*DPA agreed to Map user IDs with user details once user creation is centralized. However no*

Exhibit-E

	Thus, with the plan to integrate e-payment gateway in PEMS, the Department should make sure that the system has adequate audit logs and trails to capture every activity of users so as to prevent unauthorized activities remaining undetected by the system.	*user ID with user details will also be streamlined.*		*definite timeframe is given.*
12	**Adequate documentation of the system development should be maintained** *Currently, with limited documentation of the system and ICT personnel being the source of knowledge about the system, there is a risk of losing the know-how of the system, which might hinder the operations and future enhancements of PEMS. Hence, it is essential for the Department to develop documentation of PEMS and ensure regular updates in case of changes to the system in line with existing best practices.* *Additionally, in the process developing any information system in the future, the Department should, henceforth maintain proper documents including project documents, costing of the system, system requirement specifications, any other appropriate documents related to the system/project. It will assist in assessing the achievement of the intended objectives and maintenance of the system.* *The Department should reconstruct the system documents of PEMS for future reference and improvements.*	**Action Plan:** *DPA will document any changes made to PEMS.*	**Agreed to implement**	*DPA agreed to document the changes made to PEMS in future.*
13	**Department should establish a disaster recovery site for PEMS** *Disaster can strike at any time without warning, impairing the daily operation of the organization. Such disruption might cause a huge financial loss and destruction of data that are critical for the continuity of business operation. Considering the criticality of PEMS in the overall financial operation and functioning of budgetary agencies, the Disaster Recovery Site is imperative for the PEMS. However, presently there is no such site established for*	**Action Plan:** *DPA stated that even now the test and operational environment is segregated. All testing is done in the local server and approved by the PEMS technical working group before implementing in the live environment.*	**Partially Implemented:** *PEMS is relocated to Government Data Centre.* *However, DPA is yet to set up remote database*	

Exhibit-E

	PEMS. Thus, it is important for DPA to establish a DR site for PEMS so as to build resilience to disasters and to minimize impact on the budgetary agencies' operations in the event of interruption to PEMS. *As DITT is pioneering the establishment of DC/DR sites for all government agencies, the DPA is advised to establish a temporary site. The Department should work closely with DITT to establish DR site for PEMS. However, in view of the criticality of operations of PEMS for budgetary agencies, it may be advisable to obtain reasonable assurance on the reliability and resilience of DR site.*	*DPA also proposed to create a proper test server once PEMS is successfully relocated to Government Data Centre. A remote database backup will also be set up in DPA with existing severs until DITT comes with remote database back up and archiving server in DITT.* **Timeline:** June 2017	*back up and archiving server in DITT.*	
14	**Department should perform data cleaning of PEMS database** *As it may be seen from the findings in Chapter 3, PEMS contains numerous junk data which might lead to inaccurate and wrong information. These pertain to employees' details, PF account numbers, GIS numbers, CID numbers etc. More importantly since PEMS is used as an essential source of information by the stakeholders, it is utmost important that the Department takes initiative to clean the data. Data cleaning may be carried out in consultation and coordination with relevant agencies viz. RCSC, NPPF, RICBL, DRC, and Department of Civil Registration.*	**Action Plan:** *DPA will clean existing data in PEMS.* **Timeline:** December 2017	**Agreed to implement** *The agency has submitted the action plan and time line for which the timeframe of implementation is still valid.*	
15	**Department should validate data migration and proper testing should be conducted before implementing a new system** *The RAA noted several instances of outstanding account balances not brought forward into PEMS from BAS during the data migration period. As such, the Department should institute appropriate measures to make sure that such cases do not happen in the future while performing data migration into a new system. In the process of migration, the Department should validate all data to be migrated into the new system even by excluding redundant data.* *As assured, the DPA should verify from CBA system where consolidated data were stored and require all the agencies to*	**Action Plan:** *DPA will institute proper measures to make sure that such cases do not happen in the future while performing data migration into a new system.*	**Not Implemented:**	*Although DPA states that the issue shall be taken care in future, there is no justifications on the current lapses.*

Exhibit-E

	update their outstanding advance balances if not captured in the PEMS. Considering the possible financial implications of the omission in data migration, it is necessary that the Department accords due priority to identify and address the issues. *Furthermore, the Department should avoid cut-over implementation of any IT system and extensive testing of system should be carried out before any system is put into operation.*			
16	**Department should establish proper change management process** *Change management is an important aspect of an ICT system. The Department, however, did not have properly documented change management process. Absence of such a system would inhibit effective monitoring over and accountability on the change management. The Department should, therefore, establish effective change management process to ensure that any changes made to PEMS are properly authorized, tested and approved. Such process may also include a log of changes made to PEMS, change request form, approval for changes, report on impact of changes, etc.*	**Action Plan:** *DPA will further expand the change management process already exist for making any changes in PEMS based on the requirements after due deliberations.* Timeline: December 2017	**<u>Agreed to implement by December 2017</u>** *The agency has submitted the action plan and time line for which the timeframe of implementation is still valid.*	
17	**Department should use PEMS database for business analytics to support decision making** *The Department should take advantage of data existing in PEMS to mine and discover patterns or insights that will help the decision makers in making informed decisions. They could collect or extract data from PEMS database and perform analysis including trend and predictive analysis in regard to budgets and expenditures or in other relevant areas. The system may also be used to extract and analyse budget utilization information at regular intervals particularly capital budgets to identify instances of allocated funds remaining idle for considerable period of time or even beyond the fiscal year, which could otherwise be allotted to priority areas. Such measures may also avoid necessity of short-term borrowings by the Government.*	**Action Plan:** *DPA has been using PEMS for business analytics to support decision making. Eg. Budget Utilisation Plan data is used for ascertaining the internal borrowings and also DPA provides data from PEMS to other government agencies as and when requested.*	**<u>Implemented</u>**	