INTOSAI Working Group on Public Debt

Accounting Chamber of Ukraine

30 November 2015

Summary of Joint Conclusions and Recommendations of the International Coordinated Parallel Audit of Public Debt Management Information Systems

During 2013-2014 the Supreme Audit Institutions of Brazil, Bulgaria, Fiji, Georgia, Moldova, Romania, Ukraine, Yemen, and Zambia (hereinafter – the participating SAIs) carried out the International Coordinated Parallel Audit of Public Debt Management Information Systems under the current Strategic Plan of the INTOSAI Working Group on Public Debt (WGPD). The SAIs of China, Egypt, Mexico and Russian Federation took part in the project as observers.

The present audit has been conducted on the basis of the Common Parallel Audit Programme [1], elaborated in 2012 by the Accounting Chamber of Ukraine (as parallel audit coordinator), according to the International Standards for Supreme Audit Institutions (ISSAI) and best national practices. Summaries of national audit reports, developed by the participating SAIs within the framework of the parallel audit, complement the Joint Parallel Audit Report.

The parallel audit was focused on assessment of efficiency of Public Debt Management Information Systems (PDMIS) functioning in jurisdictions of the participating SAIs. The primary objective of the audit was to ascertain:

- whether the management and control processes of national Public Debt Management Information Systems were in place, and
- whether the reviewed information systems were equipped with adequate general and application controls and if they were properly implemented.

The parallel audit demonstrated that the government bodies established reliable and sustainable Public Debt Management Information Systems along with respective infrastructure those were developed and maintained at the state-of-the-art technological level. In general, the reviewed information systems ensured capturing, processing and reporting debt data and transactions in accordance with the national requirements and users expectations of working capacity of the system facilitating the management of public debt. However, the audit revealed some deficiencies and weaknesses in general management, general and application controls relating to the debt information systems.

General management of PDMIS was not sufficiently oriented in order to ensure continuous development of the systems meeting overall strategic goals of the entity. Most of the reviewed national Debt Management Offices (DMO) did not have a formal PDM information system strategy. Even if overall IT strategy existed, it was not updated in line with the auditee's business processes. Integration of debt management into an Integrated Financial Management Information System (IFMIS) was not achieved. Scarcely ever the PDMIS were fully

[1] Approved by the participating SAIs at the Kick-off meeting held on April 2013 in Kyiv, Ukraine.

integrated to the financial/budget systems of government. There was a lack of project management plan or other formal document for development of the system.

Certain DMOs used locally-developed systems, specifically for domestic public debt, those were not interconnected with the Debt Management and Financial Analysis System (DMFAS) and even incompatible. Lack of covering entire process and all proceedings in the meaning of full automatization of public debt management was encountered. In many DMOs the auditors noticed unclear division of roles and responsibilities among the debt management personnel at technical level. Also, they reported unexceptional cases where entry access rights and payment approval rights were not properly segregated.

Risk assessment as identification of possible weaknesses which may compromise PDMIS was not conducted. Scarcely ever DMOs used a specialized application for the risk assessment of the hardware, software and communication infrastructure. No internal audit has been carried out on the PDMIS enforcing IT controls on the system. The trainings of staff were provided during the PDMIS implementation when required, but without regular training programme.

Security management and environmental controls of PDMIS were in position that maintains general business processes of debt management. However, many entities had no PDMIS security policy statement. Access to files and IT equipment through physical means was mostly well controlled. With the exception of single cases the servers had sufficient facilities and protection. While in individual jurisdictions the access to files and databases involved several levels of protection, the access controls for both programmes and critical data in many DMOs were not properly set up. Some PDMIS operated without an up-to-date antivirus. The password protection schemes were badly designed. Even if user's passwords had expiry date, in some cases, the passwords were weak to protect unauthorized access.

The audit noticed a lack of the IT Services continuity planning in particular due to absence of Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) or its poor consistency. Certain DMOs elaborated the internal rules to assure the security of information resources through regulated physical access, information system protection against damages, disasters and/or human interference, and back-up of information. In some cases the security incident reports were weak or not existed. The back-up policy (frequency and mode of back-up, type of back-up, backup storage media and their location) was not specified in many entities.

Operational controls and documentation met the local requirements on debt data processing. The PDMIS applications generally had sufficient controls existed to protect the debt database from unauthorized access. But many home-grown PDMIS did not record audit trails of their transactions. In two cases the DMOs deactivated audit trail capability. Any compensatory mechanisms to assure accountability and traceability of the transactions were not established. Lack of help-desk to provide trouble shooting assistance was observed in many entities.

As a rule, the application controls were in place and defined in guidance for controls. The audit certified a number of established input controls for protection of IT infrastructure and computerized applications. Input controls were adequate reducing the risk of error or fraud. However, some PDMIS was not free of duplicate input debt data and a number of duplicate transactions remained undetected. Having performed tests of processing controls concerning one of the PDM information systems the auditors found that many error messages were not clear and sometimes they did not appear to the user. Besides, lack of function for interrupting the user's session after closing and then opening again the internet browser used was discovered. Through output control application tests the auditors also noticed some fails.

Taking into consideration the parallel audit observations and findings the participating SAIs expressed the following key recommendations to the respective national governments:

- To develop/update PDM information system(s) strategy based on risk assessment procedures and in line with entity's business processes providing its gradual integration with related financial and budget management information systems.
- To ensure strengthening of PDMIS security policy and access control procedures, including proper business continuity planning and segregation of duties among the debt management personnel and system administration staff.
- To reinforce PDMIS capacities by maintaining reliable operational and application controls along with establishing reasonable internal audit and help-desk support.