ISSAI 5450

The International Standards of Supreme Audit Institutions, or ISSAIs, are issued by INTOSAI, the International Organisation of Supreme Audit Institutions. For more information visit *www.issai.org*

INTOSAI

Guidance on Auditing Public Debt Management Information Systems

December 2016

PSC-SECRETARIAT
RIGSREVISIONEN • LANDGREVEN 4 • 1301 COPENHAGEN K • DENMARK
TEL.:+45 3392 8400 • E-MAIL: INFO@RIGSREVISIONEN.DK

I N T O S A I

INTOSAI General Secretariat - RECHNUNGSHOF
(Austrian Court of Audit)
DAMPFSCHIFFSTRASSE 2
A-1033 VIENNA
AUSTRIA
Tel.: ++43 (1) 711 71 • Fax: ++43 (1) 718 09 69

E-MAIL: intosai@rechnungshof.gv.at
WORLD WIDE WEB: http://www.intosai.org

INTOSAI

Working Group on Public Debt

GUIDANCE ON AUDITING PUBLIC DEBT MANAGEMENT INFORMATION SYSTEMS

December 2016

TABLE OF CONTENTS

PREFACE

Public debt is at the center of any discussion of public finance management. In seeking to expand their economies and improve social services in their respective countries, most governments face great financial needs. In theory, the public debt is an effective tool for economic growth and for equitably distributing the tax burden between current and future generations of taxpayers. But because of its importance to the economic balance, it is essential to measure and manage public debt very carefully.

Debt management's main objective is obtaining stable financing, at the lowest possible cost and at prudent levels of risk, to sustain government activities. The *Revised Guidelines for Public Debt Management* by the World Bank and International Monetary Fund (IMF) provides a set of sound practices related to internal controls of debt management. Among them is the determination that "debt management activities should be supported by an accurate and comprehensive management information system with proper safeguards." Countries concerned about ensuring effective public debt management must give high priority to developing reliable systems for recording and reporting debt information. This is necessary not only to develop debt data and ensure timely payment in servicing the debt, but also to improve the quality of budget reporting and transparency of public financial accounts, which allow policymakers and public debt managers to achieve public debt goals.

The audit of public debt management information systems seeks to ensure the efficiency, efficacy, and effectiveness of public debt management. For this reason, any such audit should be classified as a performance audit. Nevertheless, this work can also be of great relevance in the context of financial audits, which focus on determining whether the financial information the government submitted is in accordance with the regulatory framework applicable to the presentation of financial reports and whether the information is reliable and free from fraud or error. In this context, this work becomes of great importance as it can contribute to achieving an information system that gathers and produces accurate and reliable information about one of the most significant government financial elements: the public debt.

This guide provides auditors with a descriptive guidance on auditing public debt management information systems. Because the International Organization of Supreme Audit Institutions (INTOSAI) already has some documents related to information technology (IT) audits, developed by the Working Group on IT Audit (WGITA), this guide focuses on the application controls, which must be specific for the public debt management information system.

LIST OF ABBREVIATIONS

BCP – business continuity planning
CAAT – computer-assisted audit techniques
CS-DRMS – Commonwealth Secretariat's Debt Recording and Management System
DMFAS – Debt Management and Financial Analysis System
DMO – debt management office
DRP – disaster recovery plan
FMIS – Financial Management Information System
IMF – International Monetary Fund
INTOSAI – International Organization of Supreme Audit Institutions
IT – information technology
PDMIS – public debt management information system
SAI – supreme audit institution
SID – Integrated Debt System of the Federal Government of Brazil
UNCTAD – United Nations Conference on Trade and Development
WGITA – Working Group on IT Audit
WGPD – Working Group on Public Debt

INTRODUCTION

Under the terms of reference established by the Governing Board of INTOSAI, the Working Group on Public Debt (WGPD) was tasked with publishing guidelines and other information materials to be used by supreme audit institutions (SAI) to encourage the proper reporting of public debt and sound public debt management.

This guide seeks to increase WGPD capacity by providing a general framework that can be used in SAIs audits to evaluate general and application controls of public debt management information systems (PDMIS). It is important to consider that in the references, PDMIS comprehends one or more information systems used in public debt management.

As IT has advanced, government organizations have increasingly depended on the use of IT to carry out their business operations and deliver services and to process, maintain, and report essential information. According to an IMF Working Paper, "a FMIS (Financial Management Information System) usually refers to computerization of public expenditure management process including budget formulation, budget execution and accounting with the help of a fully integrated system for financial management of the line ministries and other spending agencies."

Institute of Electrical and Electronics Engineers standard 1471 defines systems as "a collection of components organized to accomplish a specific function or set of functions." In particular, the major activity of a system in a debt office is to maintain the loan database for public sector borrowings using software that is adequate for both recording and undertaking the analytical functions of the debt management office (DMO).

IT audit can be classified with respect to predominant approaches, as follows:

- IT governance,
- data auditing,
- information system auditing,
- IT contracting, and
- information security.

In general, an IT auditor works with more than one approach; however, the auditor can choose the predominant approach. In this guidance, the predominant approach is *information system auditing*.

This guide is structured in three sections: planning, assessment of general controls, and assessment of application controls.

1. PLANNING

A PDMIS can be considered as a set of interdependent parts (physical structures, staff, and technology tools) that interact in order to record, to control, to assess, and to manage transactions that are generated in raising, maintaining, and clearing public debt.

This phase helps the auditor gain an understanding of the system's related operations and controls and related risks in view of public debt's inherent operation flow risks. Based on this understanding, the auditor evaluates the overall control environment, identifies the systems used in public debt management, surveys all the documentation relative to these systems, and makes a preliminary risk assessment. The result of the assessment will guide the extent of procedures to be employed in the testing phase.

The SAI also examines all the structures related to the public debt office, such as the staff, process, type of debts, data security, technology tools, and others.

In this phase, the auditor should include a preliminary evaluation of the public debt office structure and the public debt operation flows, covering the following:

- How the PDMIS is organized: what are the systems used for recording, processing, reporting, controlling, and managing public debt and what are the main processes and functions that each system performs.

- The functioning of internal audit.

- The results of previous audits (internal or external) on the PDMIS.

- The physical storage of the documents of the operations.

- The use of computer hardware and software and the responsibility for its maintenance.

- Operations processed by information systems and their relative significance.

- The relationship between public debt information components.

- Methods and procedures for implementing new operations or revisions to existing operations.

- Previous evaluation of DMO internal controls. If the DMO's internal controls were not previously evaluated, the SAI should make this assessment. This procedure is very important to evaluating the degree of existing risks and thereby determining the needed audit tests.

The sophistication level of the system does not affect the assessment of general controls, which should always be performed. However, it determines the audit procedures to be carried out and indicates how many IT specialists are necessary to perform the audit work. It is suggested at least one IT specialist on the team perform all work involving systems. For the auditors on the team who are new to IT audit, it is important to acquire knowledge about generally used terms. In this case, a good IT technical dictionary is an important investment for an SAI. The *Information Systems Auditing – Glossary of Terms*,

by the WGITA, is useful for this purpose. Some web glossaries can be useful; see http://www.webopedia.com or http://whatis.techtarget.com.

Auditors who are already familiar with IT terminology must also know the terminology used in the DMO, especially acronyms and abbreviations (types of headings, sectors of the DMO, creditors, names of systems, software used by DMO, etc.). It is essential to have this knowledge before carrying out the interviews. A useful glossary developed by the United Nations Conference on Trade and Development (UNCTAD) can be found at the following links:

- http://unctad.org/en/Docs/pogiddmfasm3r3.en.pdf – Debt and DMFAS Glossary (English version)
- http://www.unctad.org/sp/docs//pogiddmfasm3r3.sp.pdf – Glosario de la deuda y del SIGADE (Spanish version)

To understand a PDMIS in detail means to know the inherent data and information flows. Thus, it is very important at the planning stage to map the public debt key processes (recording, processing, control, security, reporting, and analysis) and to understand how these processes are carried out through the information system. After that, it is necessary to perform a risk assessment to identify the higher risks associated with key operational and management processes of public debt, considering their impact and probability of occurrence. The risk assessment is instrumental in determining the scope of procedures necessary to manage the associated risk levels. ISSAI 5410, *Guidance for Planning and Conducting an Audit of Internal Controls of Public Debt*, provides guidelines to perform the risk assessment. In addition, the risk assessment could be set in the context of financial audits.

The flows of a PDMIS are almost always settled in the DMO. Other offices can also be responsible for data entry of debt, for example, in the case of contractual debt. Where the DMO is divided into back, middle, and front offices, each core function has its own data and information flows. The front office is typically responsible for executing transactions in financial markets, including the management of auctions and other forms of borrowing, and all other funding operations. The back office handles the settlement of transactions and the maintenance of the financial records. A separate middle, or risk management, office usually undertakes risk analysis and monitors and reports on portfolio-related risks and assesses the performance of debt managers against any strategic targets/benchmarks. The majority of data flows related to public debt, including external data, are in the back office, which is charged with data entry recording and control.

As many countries use an off-the-shelf system developed and updated by third-party international organizations (e.g., Debt Management and Financial Analysis System (DMFAS) or Commonwealth Secretariat's Debt Recording and Management System (CS-DRMS)) in public debt management, the use of reports related to performance—for example, requests for system maintenance and records of incidents—is very important.

The DMFAS Program, developed by UNCTAD, focuses on "downstream" activities. These include the maintenance of debt databases, debt data validation, debt operations, internal and external debt reporting, debt statistics and basic debt analysis, and building system links between debt management and other financial software. They complement more "upstream" activities, such as debt sustainability analysis carried out by other

providers, such as the World Bank. Additionally, the program is increasingly helping countries to establish links between the DMFAS for debt management and other governmental software (e.g., that used for budgeting, cash management, and aid management) or within complex, integrated financial management systems as part of countries' overall public financial management efforts. For more information, see http://unctad.org/dmfas.

The CS-DRMS application, which is provided by Commonwealth Secretariat, assists SAIs in recording, managing, and analyzing their debt from a holistic perspective. It provides a central repository for several categories of public and privately secured external and domestic debt, including short-term debt. The system also handles grants, government lending, and on-lending. For more information, see http://www.csdrms.org.

In the case of countries that use DMFAS or CS-DRMS in public debt management, audit reports of the PDMIS carried out by other countries (other SAIs) could be useful for identifying deficiencies that are most frequent, have the greatest impact, or both.

A table about required information, procedures, and questions the SAI should answer that the audit team may use during the planning phase of the audit work of the public debt systems can be found in appendix I.

2. GENERAL CONTROLS

General controls provide the framework of overall controls for IT functions.[1] Those controls are designed to address issues in development, operations, and maintenance of the environment. The objectives of general controls are safeguard data, protect application programs, and ensure continued computer operations in case of unexpected interruptions.

Although a public debt system audit requires the verification of IT general controls, this document will not discuss these controls at length, as INTOSAI has issued documents on IT audit that address IT general controls in detail.

It is suggested that when performing a system audit, the audit team should use ISSAI 5310, *Guidelines on Information Systems Security (ISec) Audits*, a guide for reviewing information system security in government organizations.

Another document that may be useful for the planning of general controls is the WGITA's *IDI Handbook on IT Audit For Supreme Institutions*, which provides essential information and key questions needed for effectively planning IT audits.

In appendix II, there is a testing matrix with some general controls and suggested testing procedures, which can help the auditor to perform the general controls testing.

A comprehensive set of the various categories of general controls includes the items described below.

Organizational Controls

Organizational controls are the policies, procedures, and organizational framework established to ensure sound human resource policies and management practices, segregation of duties, and information security policies, and to provide methods for assessing effectiveness and ensuring operational controls and efficiency.

Physical Access Controls

Physical access controls include rules and practices to prevent unauthorized access to and interference with IT services, including administrative procedures, such as requiring staff identity badges and control of visitors, and physical measures such as mechanical key locks and electronic door locks, cameras, and other means to limit physical access to servers and other critical infrastructure.

Logical Access Controls

Logical access controls use a computer system's built-in security to prevent unauthorized access to sensitive files and data and to ensure that all users have access rights that are limited to the requirements of their job descriptions. These controls include firewalls, antivirus software, and intrusion and malware detection.

[1] IDI-e-Learning Course on Auditing Public Debt Management, Session 6: Auditing Public Debt Management Information System.

In modern systems, these controls are obtained in many and varied ways. They are implemented through application software, the operating system, the database management system, access control software, online transaction processing monitors, servers, the network, the local area network, and possibly other software.[2]

Environmental Controls

Environmental controls are rules, practices, and built-in conditions to prevent damage caused by electrical instabilities, fire, dust, water, food, extreme temperatures, humidity, or static electricity.

Although the focus of theses controls is the data center (or area devoted to IT equipment, which requires specific surroundings or at the least protection from theft), they also apply to all office surroundings.

Program Change Controls

Program change controls include rules to ensure that all changes to the system configuration are handled accurately, completely, and in a timely manner.

Upgrades and changes should have a formal process to ensure logging of all changes and to provide the ability to back out in case there are problems with the new version.

Formal approval should be required before programs are transferred from test to production libraries, and all of the system, operations, and program documentation should be kept complete; up-to-date; and in compliance with standards, policies, and procedures.

Business Continuity Planning and Disaster Recovery Plan

Business continuity planning (BCP) and related disaster recovery plan (DRP) are designed to address the availability objective. Contingency and disaster recovery planning, plan viability, testing, monitoring, and the need for continuous updating of plans are critical factors.[3]

BCP is an overall approach to providing alternative paths in support of critical business processes in the event of an emergency, disaster, or other disruption. The focus is on total business survival and not just IT. However, the overall plan must include consideration of information systems and telecommunications network requirements. This part of BCP is also DRP.

BCP and related DRP can be developed at the same time so that all aspects are considered simultaneously. At a minimum, a plan must include procedures and criteria to determine when a situation is a disaster, the person in charge of making such a determination, and how to formally declare an event a disaster and put the plan in motion.

[2]Xenia Ley Parker, *Information Technology Audits, CCH Incorporated, USA 2006*.

[3]Parker, *Information Technology Audits*.

3. APPLICATION CONTROLS

Application controls are automated in information system applications to help to ensure authorization, integrity, accuracy, and validity of transactions. They are embedded in the programming of an application and are prevalent in the input, processing, and output operations of the application. Their objective is to guarantee the completeness, reliability, and accuracy of data processing.

Examples of application controls include checks made by the application on the format of data entered in order to prevent the entry of invalid data, processing controls that prevent users from posting transactions that are not authorized, and detailed reports and controls over total transactions to ensure that all the transactions are registered completely and accurately.

Application controls can be classified as follows:

- input,
- processing, and
- output.

3.1. DOCUMENTATION STANDARDS

Documentation standards ensure that adequate and up-to-date application documentation is maintained. Careful updating of documentation is also important.[4]

Proper documentation is important to determining what controls are, or should be, in place.

Good application documentation also reduces the risk of users not following control procedures as intended by management. A review of comprehensive, up-to-date documentation aids the auditor in gaining an understanding of how each application operates and may help identify particular audit risks.

- Application documentation: Helps maintenance programmers understand the application, correct problems, and make enhancements. Documentation builds at each phase of the development process and can be created in various formats, such as flowcharts, graphs, tables, or text. The documentation may include details on the source of the data, data attributes, input screens, data validations, security procedures, description of calculations, program design, interfaces to other applications, control procedures, error handling, operating instructions, archive, backup, and storage and recovery procedures. The application documentation should be updated as the application is modified.

- User documentation: Includes descriptions of both automated and manual work flows to aid in initial training on the application and for ongoing reference. In both cases, the user documentation should be updated as the application is modified.

[4] India Office of the Comptroller and Auditor General, *Information Technology Audit – General Principles*, IT Audit Monograph Series # 1.

Documentation should include

- an application overview,

- user requirements specification,

- program descriptions and listings,

- input/output descriptions,

- file contents descriptions,

- user manuals,

- desk instructions,

- application security control descriptions,

- recent summary of security assessments,

- recent security decision and recommended actions, and

- status of recommended actions.

3.2. INPUT CONTROLS

Input controls are extremely important to reducing the risk of error or fraud in computerized applications. Controls over input are vital to the integrity of the data.

Input controls help ensure the authorization, accuracy, completeness, and timeliness of data entered into an application. Authorization is ensured by requiring secondary approvals of transactions above a defined threshold. Accuracy is ensured by edit checks that validate data entered before accepting a transaction for processing. Completeness is ensured through error-handling procedures that provide logging, reporting, and correction of errors. Timeliness is ensured through monitoring transaction flow, logging, and reporting exceptions.

Input controls can be in

- data input screens,

- data preparation routines,

- data input authorization,

- input documents retention,

- data input validation,

- procedures for error in data entry, and

- support mechanisms to data entry.

The controls outlined above may be circumvented if it is possible to bypass them by entering or altering data from outside the application. There should be automatic

application integrity checks that detect and report on any external changes to data. For example, a check should be in place to detect and report on unauthorized changes made to the underlying transaction database.

Data Input Screens

Standardized data input screens can ensure consistent data entry.

The PDMIS may include the following functionalities:

- input screens structured in a standardized form and layout;

- data input fields that restrict what users are allowed to input;

- mandatory input for certain fields; and

- a help function (e.g., F1) to help users fill out input data fields.

Data Preparation Routines

The aim of data preparation routines is to avoid failures during data input procedures.

The PDMIS may include built-in environments for data-sharing procedures to transfer data to other applications.

Data Input Authorization

Data input authorization aims to ensure that all of data input has been recorded and authorized by the appropriate person.

The PDMIS may include the following functionalities:

- required access password;

- record of access log when there is manual data entry; and

- requirement for two approvals for some sensitive operations (e.g., activating contracts, modifying interest rates, and modifying contract values).

Input Documents Retention

This dimension of data input controls refers to maintenance and control of original documents that support debt data records. In the case of automatic file transfers between applications, the PDMIS must keep the original data received from the other application for a period preset by the DMO.

Data Input Validation

Data validation controls are designed to ensure that input data are valid and accurate.

The PDMIS may include the following functionalities:

- Automatic checklists verify absence of values (e.g., in downloading a historical series of indexes, the PDMIS verifies whether a daily, monthly, or annual value is missing).

- All data entry screens identify clearly the mandatory fields, and the application permits confirmation of the operation only if all the mandatory information has been entered.

- Each database table must contain a specific rule on the fields where duplication of data is not allowed.

- If the application considers that duplicate data are being entered, the application will not accept the entry until the duplication has been resolved.

- The application does not allow for the modification of some data after entry (e.g., exchange rate on the date of the operation). With regard to other data, the application could allow alteration if some conditions are met (e.g., whenever a contract is in “Locked” or “Concluded” status, no data can be modified).

- Some fields, when filled out, require that other fields be filled (e.g., if the user enters the contract commitment fee, the user must also enter the commitment tax).

- The “date” fields are essential for the general control of a debt contract. They are particularly useful in calculations of installments, to avoid delays of payments, charging of fines, and so forth. Thus, the application must have basic rules for inserting the date.

- With the exception of simulated operations, the system application does not allow registration of data for a future date, for example, disbursement, reversal of disbursement, contract cancellation, or contract addition.

Data Entry Errors

An audit trail or audit log is a security-relevant chronological record, set of records, or destination and source of records that provides documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event. Audit trail or log files should be restricted to appropriate personnel.

The PDMIS may include the following functionalities:

- the DMO should define responsibility for suspense files;

- programs for logging error activity, reporting open errors, and recording error correction should be built into the application;

- in a process of automatic downloading of data, when the application identifies gaps in the series, an automatic e-mail is sent to appropriate users for follow-up; and

- the application should send periodic reports of unresolved errors—including how long the errors have remained unresolved and their priority—to appropriate personnel.

Support Mechanisms to Data Entry

These controls are related to support procedures in the DMO that help users input data into the computer application, reinitialize applications, and monitor user activities to avoid possible deviations from established rules.

These mechanisms are often included in general controls.

3.3. PROCESSING CONTROLS

Processing controls ensure the accuracy, completeness, and timeliness of data during either batch or online processing. These controls help ensure that data are accurately processed through the application and that no data are added, lost, or altered during processing.[5]

Completeness

Completeness can be ensured in batch processing by balancing transactions received by a system with transactions sent by a subsidiary system.

Balancing should occur between applications that share common data, by creating a reconciliation report that lists data from both applications and reports on any differences for a user group.[6]

Balancing totals should include a transaction count and totals for all amount fields for each type of transaction, and cross-foot totals for detail fields to total fields.[7]

In files where there are no meaningful totals, hash totals can be created that add all of the figures in a column to verify that the same total is accepted by the next process. For example, totaling debt agreement numbers is not meaningful, but this total can be used to verify that all the correct debt agreement numbers were included in processing.[8]

The PDMIS may include the following functionalities:

- In the interface with other systems between applications, if there is an error in file processing, an error file is generated and recorded in the system application. Users should develop a more in-depth interoperability approach for technical profiles and training across the entity.

- The application contains scheduled batch jobs for many tasks, for example, stock update, financial planning, indexes, and future payments. Users should assess soft real-time systems outputs, focusing on batch-based logs, as well as hard real-time capabilities for measuring up-to-date information processing.

- In case of error in processing of the batch jobs, the application sends a message to the user with information about the error. The user can verify consolidation abilities within the system for meeting error correction policies and configure control procedures.

- After the conclusion of an operation, the application displays a message confirming that processing has been successful and presenting a summary of the data entered.

- After a modification of data previously registered, the application displays a message that the modification was successful and presents a summary of the modified data.

- After deletion of previously entered data, the application displays a message that the deletion was successful and presents a summary of the deleted data.

---

[5]Frederick Gallegos, Sandra Senft, Daniel P. Manson, and Carol Gonzales, *Information Technology Control and Audit – Second Edition,* Auerbach Publications, USA 2004

[6]Gallegos, *Information Technology Control and Audit*.

[7]Gallegos, *Information Technology Control and Audit*.

[8]Gallegos, *Information Technology Control and Audit*.

- If the deletion of a record affects the relational integrity of the database, the application does not allow the deletion and displays a message indicating that the record cannot be deleted. For example, the data of a creditor bank cannot be deleted from the table of creditors if this creditor has contracts in progress in the application.

- The application performs some checks between data of front and back offices. For example, it requires the back office to validate input data from auctions. Users can check on communications for data architecture interrelations among components and systems to verify data flows according to the interoperability diagram.

3.4. OUTPUT CONTROLS

Output controls ensure the integrity of output and the correct and timely distribution of output produced.[9] Weaknesses in processing may sometimes be compensated for by strong controls over output. A well-controlled application for input and processing is likely to be completely undermined if output is uncontrolled.[10]

The completeness and integrity of output reports depend on restricting the ability to amend outputs and incorporating completeness checks, such as page numbers and check sums.[11]

Output files should be protected to reduce the risk of unauthorized amendment. Possible motivations for amending computer output include covering up unauthorized processing or manipulating undesirable financial results.[12]

Output from an IT application may form the input to another application. Where this is the case, the auditor should look for controls to ensure that outputs are accurately transferred from one processing stage to the next.[13]

In the PDMIS, output controls also can be programmed to identify critical information that requires priority actions by public debt management. For example, for contracts set to expire in the current month, the application can show daily alerts in the first screen of the system about contracts whose payment dates will expire in the next 5 days.

The application can also allow certain user profiles to generate reports in priority mode thus enabling the application to prioritize the reports to be generated.

The PDMIS may include the following functionalities:

- the application provides an automatic comparison of sum of origin data with sum of data processed;

- the application should inform users on the status of report generation requests, for example, “not started”, “in progress,” and “concluded;” and

- at the end of a report generation process, the application sends a message to the user who made the request informing him/her that the task was concluded.

---

[9] Gallegos, *Information Technology Control Audit*.

[10] Asian Organization of Supreme Audit Institutions, *IT Audit Guidelines – 6th Edition*, September 2003.

[11] India Office of the Comptroller and Auditor General, *Information Technology Audit – General Principles*.

[12] India Office of the Comptroller and Auditor General, *Information Technology Audit – General Principles*.

[13] India Office of the Comptroller and Auditor General, *Information Technology Audit – General Principles*.

3.5. APPLICATION CONTROLS TESTING

Once controls have been identified, the next step in an audit is to verify their effectiveness.

This can be accomplished by

- submitting a set of test data that, if the application functions properly, will produce known results;

- developing independent programs to re-perform the logic of the application; and

- evaluating the results of the application.

The above procedures test the integrity of a program built into the PDMIS and not data integrity.

If the application has a test environment, this can be used to test controls as long as the test environment is a confirmed copy of the production environment.

In order to test calculation rules, such as those that relate to updating stock or debt service, the auditor may need to use computer-assisted audit techniques (CAAT), which include many types of tools and techniques, such as generalized audit software, utility software, test data, application software tracing and mapping, and audit expert applications. They may include tools that analyze spreadsheet logic and calculations for accuracy. Tools may also be used to analyze database applications and produce a logical flowchart. Generalized audit software can be used to analyze data produced from most applications.

The auditor should evaluate the necessity to use a CAAT. Their use should be based on the sophistication of the public debt management application.

This document includes a suggested testing matrix (see appendix III), which may be used by the audit team as a reference to perform the application controls testing. This matrix identifies some requirements and functionalities that the public debt systems should provide, queries they should be able to perform, and the minimum capability requirements for such systems.

It is important to note that as the debt of each country has a different composition and characteristics, the systems of debt management also present different features. Thus, it is responsibility of the audit team to identify, to adjust if necessary, and to utilize the items applicable to debt system of its country.

3.6. REPORTING AUDIT RESULTS

In addition to complying with the *Lima Declaration of Guidelines on Auditing Precepts*, when appropriate, PDMIS audit reporting must be in accordance with requirements in ISSAI 5440, *Guidance for Conducting a Public Debt Audit – The Use of Substantive Tests in Financial Audits,* section 2.6 Reporting Audit Results.

As previously stated, a PDMIS audit is a performance audit, so it is important that the report follow the standards of performance audit reporting, as indicated by ISSAI 3000, *Standards and Guidelines for Performance Auditing Based on INTOSAI's Auditing Standards and Practical Experience* (part 5), and ISSAI 300, *Fundamental Principles of Performance Auditing* (page 16).

Appendix I: Planning Table

Required Information, Documents, and Reports
- Inventory of information systems used by the DMO and related system documentation - Inventory of both computer and network operating systems used by the DMO - Updated mapping of processes flows of the DMO - Previous audit reports on the DMO - Previous audit reports related to public debt IT systems - Laws and regulations related to the DMO framework and public debt management - List of DMO managers and IT management, business continuity management, human resources management, risk management, internal audit, and others, and their roles, addresses, e-mail addresses, and telephone numbers - Documents intended to show DMO functioning, its systems, or both as written policies and procedures manuals of the DMO or ministry of finance, as follows: • Personnel management • Information security • Change management • Physical access • IT environmental/location requirements • Logical access • Business continuity planning (BCP) • Disaster recovery plan (DRP) • Backup plan • Third-party service (IT services) • Prior risk assessment reports • Recent summary of security assessments • Recent security decision and recommended actions • Status of recommended actions • Senior management's approval to deploy the system - Reports disseminated by outsourced entities in charge of providing system maintenance - Other documents related to the DMO, its system, or both (e.g., slides, texts, targets, and annual debt management reports) - Number of DMO employees who are system users and their access profiles - Number of IT employees and job specifications (role definition) for both DMO and IT personnel - List of employees who have access to server room - Description of PDMIS access profile

- Formal specification of manner and regularity of update of operating system, firewalls, and antivirus software
- Roles of physical obstacles and automatic tools used in preventing unauthorized access to mainframe, workstations, servers, and other DMO facilities
- Location of each room inside and outside the DMO
- List of personnel, workstations, and servers
- Budget allocation for the last 5 years
- List of prior training for both PDMIS use (DMO personnel) and IT updating (IT personnel)
- Stated rules, practices, and built-in descriptions to prevent damage caused by electrical instabilities, fire, dust, water, food, extreme temperatures, humidity, or static electricity
- Specifications on functioning of uninterruptible power supply (if there is any)
- Incidents logs on the DMO's demands about PDMIS errors or use instructions reports
- Security incidents log reports
- List of changes in the PDMIS in the last 12 months
- Logs and reporting of prior BCP and DRP tests and effective events
- Application and user documentation
- Terms of use for each application
- Procedures manual to address processing errors
- Data sample to re-perform operations to test application controls and calculations

Procedures

- Studying the system documentation (manuals and terms of use) to understand the main processes of debt carried out in information systems; if there is insufficient documentation about the DMO's processes, the audit team should survey and map the processes
- Verifying existence of legal rules related to use, maintenance, and business management of the PDMIS
- Identifying, from previous audits, findings related to weak points on public debt operation flows, on public debt management systems, or both
- Identifying main general controls based on system documentation
- Identifying main application controls based on system documentation: data input, processing, and output controls
- Carrying out a risk assessment on these main general and application controls to assess what risks affect these systems and the severity of their impact on public debt management

- Determining which of the systems affect critical functions and data, such as input, processing and output of data, creditors list, public debt calculations, reporting, and decision making
- Identifying the internal controls implemented to mitigate or reduce the found risks
- Ranking the systems and processes based on the risk assessment and determining the audit scope
- Estimating resources and schedule
- Arranging interviews with head of the IT unit, managers, and the technical body responsible for working on development/maintenance/operation of the system
- Developing the matrix for the audit of general and application controls and determining which tests to carry out (see the suggested matrix in appendix III)

SAI should answer to the following questions

- What are the public debt management information systems and what is the role of each system in public debt management?
- Was the PDMIS developed by the DMO exclusively, or was it acquired from a third party? In case of the latter, has any customization been made in order to cater to any specific need of the DMO?
- Who should be interviewed about issues of IT general controls in the DMO?
- Who should be interviewed to clarify application controls of the PDMIS?
- Who are the main users of the PDMIS?
- What are the general and application controls of the PDMIS?
- Are the internal controls able to reduce the information systems risks that can affect public debt management?
- What are the higher risks related to data input, processing, and output of the PDMIS?
- What tests related to general and application controls should be implemented?

Appendix II: Testing Matrix for General Controls

GENERAL CONTROLS		
The objectives of general controls are to safeguard data, protect application programs, and ensure continued computer operations in case of unexpected interruptions.		
REQUIREMENT/ FUNCTIONALITY	**GENERAL CONTROL**	**SUGGESTED TESTING PROCEDURES**
General questions	The IT sector's actions must adhere to the DMO's mission There should be monitoring of the performance of the PDMIS in view of the DMO's objectives An internal audit should be performed periodically on DMO/PDMIS operations	Reviewing sample management decision or memos, related to IT actions, to ensure that they are clear, well substantiated, and adhere to the DMO's mission Evaluating performance measures for PDMIS against expected indicators and ensuring that senior management acknowledges those measures Assessing previous internal audit reports on IT general controls to identify serious shortcomings Evaluating both the relative quantity and the capability of IT workstations and other IT devices, and ensuring that the personnel have the necessary skills Evaluating the relative amount of budget allocation, and comparing it with those of previous periods and IT sectors of other government entities
Organization controls	The DMO or ministry of finance management should be committed to developing and maintaining a good general IT environment The DMO and IT personnel should have periodic and adequate training that includes security awareness	Interviewing DMO senior management about their interest in IT in order to evaluate their commitment to developing and maintaining a good general IT environment Reviewing evidence indicating that training has occurred

	There should be a training program There should be written policies and standard procedures related to the following: • Information security • Human resources • IT third-party services • Change management • Physical and logical access • Business continuity planning and disaster recovery The policies and standard procedures should be updated periodically The policies should be disseminated adequately by DMO senior management The DMO employees should know these policies There should be documented procedures for all activities of debt management The organization should implement an appropriate segregation of duties to ensure that users have no more authority than what their jobs require	Interviewing DMO users and IT personnel about the following: • the frequency of training • need for knowledge/training • knowledge of policies Evaluating the adequacy of written policies and standard procedures on IT services Observing whether DMO staff work in accordance with standard procedures (established in a manual)
Physical controls	Physical access to the mainframe and servers should be limited (for example through the use of doors, locks, etc.) There should be video supervision The windows of the room where the mainframe and servers are located should be protected against forced access Everyone who accesses the server room should be authorized to do so	Verifying the effective existence and functioning of physical obstacles that prevent unauthorized access to the mainframe, servers, and workstations of the DMO Verifying whether personnel's administrative procedures to prevent unauthorized access to and interference with IT services work as formally established In order to identify any weakness in automatic controls, observing how electronic tools—such as

		electronic door locks, electronic key lock systems, cameras, and other means to limit physical access to servers—and other critical infrastructure operate In case of key lock systems, checking for sharing of passwords among employees
Logical controls	If public debt IT services are outsourced, the contract should determine adequate controls to ensure no access by a third party to the business secrets, important data, and public debt strategies There should not be any former employee, person not employed by the DMO, or "virtual" user with an active access profile The access rights should be reviewed periodically The updated antivirus, firewall, and intrusion and malware detection software should work There should be a systematic update of the operating system on workstation(s) and server(s) The organization should define its procedures to authorize, revoke, or modify access control when conditions change (new hires, terminations, change of duties, etc.) The organization should announce its policy or guidelines on security passwords and other security controls (key cards, etc.) to all users of the PDMIS	Assessing if access profiles are based on employee's role Checking if any former employee or person not employed by the DMO still has an active access profile Verifying whether there are firewalls and updated antivirus, malware, and intrusion detectors Verifying whether the operating system is systematically updated on workstation(s) and server(s) Assessing whether the password policy is being properly implemented Verifying whether the procedures are defined and documented
Environmental controls	There should be pipes (water, heating system, electricity, etc.) throughout the server room There should be water, heat, and humidity detectors	Inspecting and assessing environmental conditions in the database server room Checking for the existence and effective maintenance of the devices used to

	There should be an antiflood system in the server room There should be smoke/fire detection devices There should be a raised floor, or equipment should be situated 15 to 20 centimeters above the floor on racks There should be an uninterruptible power supply for sustaining the operation of the mainframe and servers	prevent fire, flood, and humidity Verifying the existence and effective functioning of alternative power supplies to avoid interruption of IT services
Program change controls	IT management should keep an audit log of operational problems, incidents, and errors The log should trace each incident from underlying cause to resolution There should not be important, unresolved PDMIS instruction questions at the help desk There should be escalation of problem for critical events and appropriate level of response based on priority of event There should be a security incident report, which is provided to DMO managers The prior changes should follow standard procedures If a nonstandard debt management system is used, the organization should have its procedures for change control documented and should describe who is authorized to perform changes to the system The organization should track and monitor all changes to the system debt (audit trail)	Evaluating time spent to resolve the DMO's demands related to use instructions or failures in PDMIS functioning Identifying more frequent PDMIS failures and probable causes Comparing prior changes with standard procedures
BCP and DRP	There should be BCP and DRP established by the DMO The personnel responsible for operational continuity should	Assessing consistency and completeness of BCP and DRP and whether they are updated

	know their roles and responsibilities The weakness in prior BCP and DRP tests or effective events and the actions taken by the DMO to address those weaknesses should be reported The loan documentation should be securely stored and protected from theft, fire, flood, or other incidents that may damage or destroy it	Assessing reports on prior testing of BCP, DRP, and the backup plan Verifying whether BCP and DRP are properly disseminated to all the staff Verifying whether the off-site backups are in good condition and can be used to restart the system in case of failure

Appendix III: Testing Matrix for Application Controls

DOCUMENTATION STANDARDS		
The objectives of proper documentation standards are to ensure that controls will operate on a continuous basis and to reduce the risk of error.		
REQUIREMENT/ FUNCTIONALITY	**APPLICATION CONTROL**	**SUGGESTED TESTING PROCEDURES**
Documentation controls	The application documentation should be sufficiently comprehensive (with all application functionalities and related functioning)	Checking the documentation
	The documentation should be updated to reflect amendments to the application	Checking the documentation
	The application controls included in documentation should be implemented and working effectively	Checking a sample of application controls to determine whether they are implemented according to the documentation and working effectively
Documentation backup	A backup copy of the documentation should be held	Checking the documentation backup
INPUT CONTROLS		
The objective of input controls is to ensure the authorization, accuracy, completeness, and timeliness of data entered into an application.		
REQUIREMENT/ FUNCTIONALITY	**APPLICATION CONTROL**	**SUGGESTED TESTING PROCEDURES**
Fields with mandatory input	The application does not allow operation confirmation if any mandatory input field is not filled in	Confirming the operation by omitting necessary data and verifying that the transaction was not processed Applying this test to the following processes: contract register, contract activation, security issuance register, and so forth

Correct and proper data input	The application does not accept incorrect or improper data input	Checking data format in the database Reviewing input specifications and checking some at the application Attempting to insert incorrect or improper data and checking that the data is not accepted and an error message is generated Applying these tests to the following processes: contract register, contract activation, security issuance register, index updating, security redemption, and so forth
	The application does not allow data duplication	Attempting to register a contract or a security with the name of an existing one and checking that the data is not accepted and a duplication message is generated
	For contract interest rates, there should not be overlapping or uncovered periods regarding the applicability of interest rates	Checking the database for periods with overlapped or uncovered interest rates
	In case of a donation contract, the application should allow entry of the disbursement as, in this case, there are no amortization and interest operations	Attempting to enter a disbursement of a donation contract and checking whether the application does not require amortization and interest operations
	In the disbursement input screen, when the user searches for contracts in order to record a disbursement, the application should only show contracts with “active” status in the disbursement or disbursement and amortization phase	Attempting to enter a disbursement and checking the contracts phase showed by the application

	If the interest rate is floating, the application should require the inclusion of the index	Checking whether the application requires an index when floating interest rate is selected
	The application should not allow the entry of decimal numbers for the issued securities quantity	Attempting to insert decimal numbers for the issued securities quantity and checking whether the application does not accept the entry
	The application should allow the creation of a security before its issuance	Simulating creation of a security without performing its issuance
Information completeness	All relevant information about debt should be entered into the application	Checking whether all important debt data are entered into the application, for example, credit operations, guarantees, loans, interest rates, and exchange rates
Compatibility between dates	The beginning date for calculation of the commitment rate should be earlier than the date of project conclusion	Attempting to insert a beginning date for calculation of the commitment rate later than the date of project conclusion and checking that the data is not accepted and an error message is generated
	The effectiveness date should be earlier than the date of project conclusion	Attempting to insert a date of effectiveness later than the date of project conclusion and checking that the data is not accepted and an error message is generated

	The effectiveness date should be earlier than the date of the deadline for disbursement	Attempting to insert a date of effectiveness later than the date of the deadline for disbursement and checking that the data is not accepted and an error message is generated
	The deadline for disbursement date should be earlier than the date of project conclusion	Attempting to insert a deadline for disbursement date later than the date of project conclusion and checking that the data is not accepted and an error message is generated
	To get the Maturation Report, the final date of security maturation should be later than its initial date	Attempting to insert an initial date later than final date of security maturation and checking that an error message is generated
	The application does not accept future dates for the operations	Attempting to perform some operations by inserting a future date and checking that the data is not accepted and an error message is generated Applying this test to the following processes: contract register, contract activation, security issuance register, index updating, security redemption, disbursement recording, contract addition, and so forth

	The date of security issuance should be earlier than its maturity date	Attempting to insert a date of issuance later than the maturity date and checking that the data is not accepted and an error message is generated
	When registering an amortization payment, in cases where the amount or date entered differs from that in the application, the application should display a message informing the user of such situation before confirmation of the operation can be completed	Registering a payment with a date or value different from that in the application and checking whether the application displays a message
	If the liquidation date is different from the maturity date, the application should require that the “justification” or “creditor endorsement” fields be filled out	Inserting different dates for maturity and liquidation and checking whether the application requires a justification or endorsement
	Scheduled disbursements should not have overlapped periods; for example, the initial date of the second disbursement cannot be earlier than the final date of the first disbursement	Attempting to insert the date of second disbursement earlier than the first date and checking that the data is not accepted and an error message is generated
Security of data input and operations	The application should not allow unauthorized people to enter some data and perform some operations	Checking that token and other requirements exist for specific user profiles Attempting to enter data and perform some operations without having proper profile and checking that is not allowed Applying this test to the following processes: contract register, contract activation, security issuance register, index changing,

		security redemption, payment recording, and so forth
	The application should record an access log for manual data entry	Checking for restricted access logs and ensuring that the logs cannot be viewed or modified by individuals who are not approved to do so
	The application should not allow a value change of an active contract	Attempting to change the value of an active contract and checking that it is not allowed
	The application should prevent data modification and deletion of contracts with “canceled” or “concluded” status	Attempting to modify and delete some data of a sample of contracts with “canceled” or “concluded” status, and checking that it is not allowed
	The application should not allow the deletion of an active contract, unless the contract is in negotiation	Attempting to delete an active contract that is not in negotiation and checking that it is not allowed
	The application should not allow the improper exclusion of an issued security, unless there is no operation linked to the security	Attempting to delete an issued security that is not linked to an operation and checking that it is not allowed
	The application should require dual authorization to perform critical operations	Checking whether the critical operations require dual authorization to be completed Applying this test to the following processes: contract activation, security issuance, payment of amortization, security redemption, contract value changes, payment of coupons, payment reversal,

		interest rates changes, and so forth
	The application should only accept data input from recognized sources; the loan entered should be in accordance with the agreement and accepted standards	Checking that key data are input twice and that an error message occurs when the entries differ
	The application should allow the reduction of a contractual value as long as it is not greater than the value of the “balance to be disbursed”	Attempting to reduce the contract value more than the value of the balance to be disbursed and checking that the data is not accepted and an error message is generated
	The application should record all transactions once only	Performing some identical transactions (for example, payment of an amortization) and checking that the transactions are not processed and are not duplicated in the database
	When registering a payment, if the user’s permission is revoked, the application should only report on the revocation when the user attempts to enter the payment, thus allowing logs of both the failed attempt and of the data that user intended to insert	Attempting to register a payment with a revoked permission and checking that the data is not accepted and the attempt is logged
	In the case of automatic file transfers between applications, the PDMIS should keep the original data received from other applications for a period preset by the DMO	Checking the maintained data transferred from other applications to ensure that the data are encrypted or safeguarded against damage, loss, or violation
	The application should not allow modification of interest rates of an installment that has already been paid, and any alteration of an interest rate needs a second approval in order to be completed	Attempting to modify an interest rate of a paid installment and checking that the data is not accepted; also checking whether the application requires a

		second approval to change an interest rate
Compatibility between values	The tranche value should be less than the contract value	Attempting to insert a tranche value greater than the contract value and checking that the data is not accepted and an error message is generated
	The redemption value should be less than the issued security value	Attempting to make a security redemption with a value greater than the issued security value and checking that the data is not accepted and an error message is generated
	The application displays an alert about underpayments or overpayments before processing	Simulating an underpayment or an overpayment and checking for the alert
Source documents	A trail of source documents for the inputs should exist for guaranteeing the authenticity of data input	Selecting some data input and checking whether it has a respective source document (e.g., loan contract, e-mail, etc.)
PROCESSING CONTROLS		
The objective of processing controls is to ensure that data are accurately processed through the application and that no data are added, lost, or altered during processing.		
REQUIREMENT/ FUNCTIONALITY	**APPLICATION CONTROL**	**SUGGESTED TESTING PROCEDURES**
Proper status indication	The application should change the status of the contract after total disbursement	Simulating a conclusion of disbursement and checking whether the contract status changes from “disbursing” to “totally disbursed”
	The application should change the status of the security when its issuance is confirmed	Simulating a security issuance confirmation and checking whether the security status

		changes from “inactive” to “active”
	The application should change the status of the contract or security after total payment	Simulating the last payment and checking whether the contract or security status changes
	The application must foresee at least the following phases: • Disbursing: disbursements are created in this phase • Completely disbursed: disbursements in this phase are not allowed • Concluded: in this phase, disbursements do not receive any financial operation and modifying of data is not allowed	Creating a contract, attempting to perform a disbursement in each phase, and checking that the data is not accepted and an error message is generated
	The application should contain rules to make the status of the contract (active or inactive) compatible with the phases (disbursing, completely disbursed, amortizing, disbursing and amortizing, and concluded) in order to prevent contradictions in the information; for example, a contract with an inactive status cannot be in the disbursing or amortizing phase	Simulating some changes of contract status and contract phases and checking whether they are compatible
	The application must contain a program to update the phases of the contract; for example, when the balance to be disbursed is equal to zero, the application should modify the phase from disbursing to totally disbursed	Simulating the necessary conditions to change the contract phase and checking whether it changes
Correct calculation	The application should perform the calculation correctly	Checking calculation through re-performance Applying this calculation test to the following information: debt stock (contractual and securitized), maturation, amortization schedule (dates and values),

		agents' commission value, security payment flow, financial value of redemption security, and so forth
	After some input changes, the application should update data	Making some input changes and checking the data updates; for example: • Simulating a payment and checking whether the outstanding balance and amortization flow were updated • Changing some indexes and checking whether debt stock value was updated
	The application should contain in its programming at least the following methods for calculating installments: uniform distribution, simple interest, installment, price application, constant amortization application, Pool Unit basket of currencies (IBRD), and UAC basket of currencies (IDB)	Checking the methods the system uses to calculate the installments; the correctness of the methods may be checked using sample data
	Whenever the Contracted Value field is changed, the application must automatically recalculate the Contract Balance to Be Disbursed field	Changing the Contracted Value field and checking whether the Contract Balance to Be Disbursed field has updated correctly
	The application should automatically generate the installment dates using one of the following possible methods: • Initial date and fixed number of installments • Initial date, final date, and descending number of installments • Initial date, final date, and fixed number of installments	Inserting the data required by each possible method and checking whether the installment dates are correct

	• Initial date and number of periods • Periods	
	When the date of the installment is on a nonworking day, the application must offer two options: advance the date to the next working day or bring it forward to the previous working day	Configuring an installment with the date on a nonworking day and checking whether the application offers to change the date to the previous working day or the next working day
	The system should automatically update the securities nominal value whenever there is a change to the respective indexer	Changing an indexer of a security and checking whether the respective nominal value is updated
	In case of payment of an amount lower than the one calculated by the application, a message should be displayed at the moment of the entry of the payment; the message should be repeated until the due date of the next installment	Simulating a payment lower than the amount calculated by the application and checking for a message and whether that message repeats until the date of the next installment
	In its database, the system should differentiate the securities with simulated issuance	Within the database, checking whether the simulated securities are differentiated and whether they are disregarded in the calculations of debt stock and maturation
	When a user deletes a security, the application should delete the respective values in the database	Deleting a security and checking whether its value is deleted from the database
	Securities with “canceled” status should not be considered in the calculation of debt securities (e.g., IRR, maturation, etc.), that is, after they are canceled, the respective values should be excluded permanently from the database	Changing the status of a security to “canceled” and checking whether its value is disregarded in the calculations (of stock, maturation, etc.)

	The application should treat installments with overdue payments differently	Checking whether the application is correctly calculating all charges on overdue installments
Proper processing error control	Processing errors from days/weeks ago should not be left unresolved	Checking whether there are any criteria regarding the number of days it takes to resolve errors in the system, checking for error messages, and discussing with the system/debt managers the measures taken to correct any failures
	If there is a processing error, the application should cancel processing and store in the database the date, time, and technical reason for the problem	Simulating a process error and checking whether the application stores in the database the date, time, and technical reason for the problem
Correct recording	The application should enable debt managers to record cash flow (associated with foreign currency and domestic currency borrowings, hedging and trading activities, guarantees, and on-lending) accurately for all transactions	Performing a transaction and checking whether its record is correct and accurate
	The application should maintain a history of transactions carried out during the life of the contract and should include details on the creditor, contracted value, and closing date of the project and limit dates to disbursement fields	Selecting some contracts and checking whether each has a history of all transactions performed during its life, with all necessary details
	The application should have a log for each debt instrument	Checking whether the historical transactions related to a security or contract match up to its debt log
Correct schedule tasks	The application should have automatic starts for tasks in schedules set by the DMO to update indexes, debt stock, and so forth	Checking for automatic starts and if this process works properly

	For a type of security whose amortization is made in the same frequency as interest (price, for example), the system should ensure that both interest and amortization have the same payment schedule	Creating a security with amortization and interest in the same frequency and checking whether they have the same payment schedule
Audit trail	A PDMIS audit trail should be maintained to enable tracing of debt contract or security, from signature/issue to repayment	Checking for an audit trail for a sample of contracts and securities, from signature/issue through repayment
OUTPUT CONTROLS		
The objective of output controls is to ensure the integrity of output and the correct and timely distribution of output produced.		
REQUIREMENT/ FUNCTIONALITY	**APPLICATION CONTROL**	**SUGGESTED TESTING PROCEDURES**
Control on the information users	The application should have a reporting log to record the names of users who have requested reports and the dates and times of the requests	Requesting some reports and checking whether the application records the requests
	The application should require special authorization to load certain reports (especially those that contain sensitive information)	Attempting to produce these reports
Timely and reliable reporting	The application should produce predefined reports (bond, loan, and tranche classification, e.g., maturity, status, financing sources, financing type, credit, type of instrument, terms, unpaid bills, etc.)	Attempting to produce some predefined reports
	The application should produce reports properly, ensuring completeness and integrity of the information	Checking whether the reports are produced according to the terms of use Checking whether the reports present page numbers and totals Applying this test to the following reports: Maturation Report (for contractual and securitized debt),

		Outstanding Balance Report, Receiving Report, and so forth
	The application should allow the reporting, both global (all security debt) and specific, such as the following: • By securities status (issued, canceled, redeemed, etc.) • For events in a certain date range (emissions, redemptions, etc.) • For stock of short and long term • By portfolio position • By security type • By maturity interval	Attempting to generate reports, global and specific, using as a criterion the data below: • Securities status (issued, canceled, redeemed, etc.) • Events in a certain date range (emissions, redemptions, etc.) • Stock of short and long term • Portfolio position • Security type • Maturity interval
	The reports should present complete and correct information	Generating reports and re-performing the calculations Applying this test to the following reports: Maturation Report (for contractual and securitized debt), Outstanding Balance Report, Receiving Report, and so forth
	The reports should present exactly the same information as presented on the application screens	Comparing reports for consistency with the information presented on the application screens Applying this test to the following reports: Maturation Report (for contractual and securitized debt), Outstanding Balance Report, Receiving Report, and so forth

	The values presented in the Maturation Report, Outstanding Balance Report, and Stock Report should agree	Comparing these reports for consistency
	The system should be able to produce reports on debt totals on an individual and aggregated basis with forecasting of debt service on existing and future borrowings and securities	Attempting to produce such reports Verifying whether the reports cover both existing and expected debt operations
	The application should automatically generate daily financial schedule reports on all active contracts; it should also allow manual generation of reports for specific contracts	Checking for automatic reports generation for all active contracts and attempting to generate manual reports for specific contracts
Correct data transfer	The transfer of data between applications, processing stages, or both should be accurate and complete	Simulating a data transfer between applications and checking for data accuracy and completeness
Useful output messages	When a user accesses the application, it should display a message with the following information: • Contracts maturing in the next 5 days • Contracts with overdue payments of installments • Contracts with partially paid installments • Contracts with overdue disbursement dates • Contracts with a disbursement deadline of 5 days (the application should send a daily message until the disbursement is made, the value to be disbursed is canceled, or the deadline is modified)	Accessing the application and checking whether it displays all these messages
	The application should indicate the calculation status as either “running	Requesting a calculation and

	calculation" or "calculation completed"	checking whether the application indicates the status of the operation
	At the end of report generation, the application should display a message that the report generation is complete or display the requested report	Requesting a report and checking whether the application displays a message that the operation is complete or displays the requested report
	The application should indicate the generated report's status as "in progress" or "completed"	Generating a report and checking whether the application indicates the status of the operation
	If interest rates change, the application should display an alert message	Changing the interest rates and checking for an alert message
	Before processing the deletion or redemption of a security, the application should display a screen with the information being deleted or redeemed so that the user can confirm the operation	Attempting to redeem or delete a security and checking whether the application displays a message for the user to confirm the operation

Figure 1: Public Debt Audits by SAIs: The Case of Brazil

Audit carried out by the Brazilian Court of Audit on the Integrated Debt System (SID) of the Federal Government of Brazil in 2014

Considering that the SID is being tested for domestic securitized debt, the audit team chose to focus only on testing processes related to managing external debt (securitized and contractual). The audit observations and findings were as follows:

IT System Strategy & General Management

According to its *Operational Manual*, once the SID is fully implemented, it will offer the following functions:

a) a diverse range of calculations, such as the updated nominal value, unit price, stock (of both contractual and security debts), financial planning of contracts, and contract and bond pricing and maturity;

b) a variety of searches and reports of both data registration and results of calculations;

c) financial operations, such as bond issuance, contract repayments, redemption, and transfer, among others; and

d) an information register used to its full extent in the various business modules.

Regarding IT system strategy and general management, the main observations and audit findings were as follows:

- There is no training program for the most-used public debt management systems, Seorfi and SID.
- There is no expected date for the full implementation of the SID, including the domestic securitized debt.
- Some important operations, such as activating the contract, repayments, reverse repayments, change interest rates, or change contract values, are carried out by only one person. There is no need for approval and dual authorization in the system. The safety of operations relies solely on the adequacy of the profile, which creates a segregation of duties problem.
- Another segregation of duties problem is the lack of staff to develop the SID; the DMO's staff is developing it, along with carrying out the office's usual functions.
- The operational risks vulnerability assessment for IT processes is ready, but the assessment for mitigation of these risks has not yet occurred.

Security & Environmental Controls

Regarding security and environmental controls, the main observations and audit findings were as follows:

- The DMO has not appointed the Information Security and Communications Manager, and the Information Security Committee, which is responsible for appointing the manager, did not begin to work effectively.
- There is no BCP formalized, and the work processes of public debt management are being reviewed in order to prepare BCP.

- The audit team's analyses noted the existence of three active generic users, which hinders good IT practices, based on item 11.2.1 of ISO / IEC 27002: 2005, which recommends the use of unique user identification to ensure the accountability of each user in the system.
- Although defining access to the SID should be done only through an A3 digital certificate, and access by national identification number and password should be an exception, analysis of the SID user's database indicates that there is no deadline for use of the exception.
- The SID user's database analysis indicates failures in the user's access review process.
- The audit team also detected failures in the daily automatic routine maintenance of the SID user's database.
- The SID does not record audit trails for most of its transactions, and as a result, the DMO does not perform periodic review of audit trails generated by the system and also does not monitor the transactions in the SID.
- The SID does not have an auditing function that routinely generates, stores, and analyzes the system log.
- The audit team noticed the lack of a test plan and its associated results in the systems most used by the DMO, Seorfi and SID.
- The audit team has not received confirmation that an incident response team has been created for the computer networks, responsible for receiving, reviewing, and responding to security incidents.
- The audit team noticed the lack of an IT services continuity plan, which is the properly formalized document that describes the continuity initiatives for all IT services managed by the agency or entity.

Operational Controls & Documentation

Regarding operational controls and documentation, the main observations and audit findings were as follows:

- The interface is not very friendly, so SID users require more prior knowledge about the system.
- There is no SID user's manual.
- The processing speed of calculations required is low. This prevents the generation of calculations and reports concurrently. As there are multiple concurrent users to the system, this issue could reduce the system's efficiency. The audit team suggested that the DMO evaluate improvements in order to increase the processing capacity of the system.

Application Controls

After the audit team performed the input, processing, and output control tests on the SID for external public debt, the audit findings and observations were as follows:

- Many error messages are not clear, and sometimes they do not appear to the user.
- Through input application control tests, the audit team found several error messages that did not explain the cause of the error.

- Through processing application control tests in external contractual debt, the audit team found a difference of values in the Cash Flow Financial Report, referring to a reversal that was not considered in that report.
- In output control application tests, the audit team found that if the data inputted are not correct, the application does not generate some contractual debt reports, as expected, but the application also does not identify the error to the user.
- Through output control application tests, the audit team identified errors in contractual debt reports owing to the use of outdated indexes by the system.
- Some contractual debt reports were issued with incomplete information.

Recommendations

Considering the audit findings and observations reported, the audit team recommended that in 90 days, the National Treasure Secretariat develop an action plan containing the schedule for the implementation of the following:

- Establishing an expected date for the full implementation of the SID, including the domestic securitized debt.
- Appointing the Information Security and Communications Manager and the Information Security Committee.
- Formalizing BCP.
- Formalizing the IT Services Continuity Plan.
- Creating an Incident Response Team for Computer Networks.
- Assessing and mitigating operational IT risks.
- Reviewing the daily automatic routine maintenance of the SID user's database.
- Reviewing the SID user's access review process.
- Reviewing the SID generic user's access-granting process.
- Establishing procedures for periodic review of audit trails generated by the SID.
- Providing application log recording by the SID.
- Reviewing the SID error messages.
- Developing the SID user's manual.
- Reviewing the SID reporting routine.

Figure 2: Public Debt Audits by SAIs: The Case of Moldova

Application control assessment carried out by the Court of Accounts of the Republic of Moldova

The DMFAS application has sufficient integrated controls that automatically check whether data entry was performed accurately. However, there are some aspects that raise concerns and should be addressed: operators can enter data in system's classifiers and in other system tables, which can affect the accuracy and integrity of data through duplication or deletion of registrations.

Recommendation No 15: To revise operators' rights to enter, change, or delete data in the DMFAS database classifier, or identify such operations that result in duplication of data or erroneous input.

Besides the standard reports in place in the DMFAS application, a large number of generic reports have been developed in Excel, including most of the required aspects. Not all types of reports are systematically used. Most of the required reports are produced in Excel. However, there are certain reports generated manually from data obtained from other reports. Of concern is the renewing of data in Excel reports. Report generation is a complicated procedure, which could be drastically affected by human errors. Moreover, generated reports could be modified without authorization, and these errors may occur in other important summary reports, which should have maximum security and represent the primary activity of the Public Debt General Division.

As a result, some minor deficiencies could critically affect reliability and accuracy of data in important reports on the Public Debt General Division's activity.

Recommendation No 16: To consider optimizing or automating the process for modifying reports to be generated. To identify of way to automatically generate summary reports, eliminating the possibility of human error. To consider migrating to version 6.0.

BIBLIOGRAPHY

Asian Organization of Supreme Audit Institutions. Research Project. *IT Audit Guidelines – 6th Edition*. September 2003

Gallegos, Frederick, Sandra Senft, Daniel P. Manson, and Carol Gonzales. *Information Technology Control and Audit*. Auerbach Publications. USA 2004

India Office of the Comptroller and Auditor General. *Information Technology Audit – General Principles* (IT Audit Monograph Series # 1).

International Monetary Fund and the World Bank. *Guidelines for Public Debt Management*. April 1, 2014

International Organization of Supreme Audit Institution. ISSAI 5440, *Guidance for Conducting a Public Debt Audit – The Use of Substantive Tests in Financial Audits*. November 2007.

International Organization of Supreme Audit Institution. ISSAI 3000, *Standards and Guidelines for Performance Auditing Based on INTOSAI's Auditing Standards and Practical Experience*. July 2004.

International Organization of Supreme Audit Institution. ISSAI 5310, *Information System Security Review Methodology*. October 1995

INTOSAI Development Initiative. WGITA, *IDI Handbook on IT Audit for Supreme Audit Institutions*. February 2014.

Parker, Xenia Ley. *Information Technology Audits*. CCH Incorporated. USA 2006.

United States Department of Homeland Security web site: http://www.dhs.gov.

United States Government Accountability Office. *Federal Information System Controls Audit Manual (FISCAM)*. GAO-09-232G. February 2009.