Presentation

Dear Reader:

It is with great satisfaction that we present the results of the Coordinated Audit by the Federal Court of Accounts Brazil (TCU) on Information Technology (IT) Governance.

This theme refers to the area of corporate governance that seeks to assure that the use of IT adds value to business, with acceptable risk levels. For this reason, we sought to avoid or mitigate still common deficiencies in management of institutions, such as inadequate planning processes, recurrence of failed projects, and contracts that do not achieve their proposed ends, resulting in a loss in quality and efficiency.

Moreover, it is important to emphasize that adequate governance of information technology in the public sector promotes protection of critical information and contributes to public agencies achieving their institutional objectives.

This joint undertaking relied on the participation of eleven supreme audit institutions (SAIs) in the following member countries of the Latin American and Caribbean Organization of Supreme Audit Institutions (OLACEFS*):* Bolivia, Brazil, Chile, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Panama, Paraguay, and Peru. With support from the member audit entities and the efforts of the technical teams involved, this was an opportunity to audit the level of maturity of IT governance in the public agencies of the participating countries.

The findings provide a true picture of the subject in the public agencies of the participating SAIs and the main challenges to enhancing their degree of maturity.

In conclusion, we stress that the SAIs, in promoting joint evaluations, encourage compliance with international agreements and stimulate the refinement of IT governance, which will have repercussions in the services provided by public administration and will bring benefits to the countries and their citizens.

I hope you enjoy reading this report.

Minister Aroldo Cedraz de Oliveira

Executive Summary of the Coordinated Audit on IT Governance

1. Introduction

1.1. The theme of governance in the sector should be prioritized in an effort to increase awareness in public agencies and in society about the benefits of adopting the internationally recognized best practices that support achievement of the main objectives sought by public institutions.

1.2. The mechanisms of governance involved will make it possible to provide services more efficiently, once they are guided by mechanisms to justify decision making, observing the processes, functions, responsibilities and implicit limits, while giving accountability to society under the paradigm of public transparency.

1.3. In this context, governance of information technology (IT) has a special place due to its natural importance and to the growing dependence of public institutions on new technologies developed and put at everyone's disposal.

1.4. Although data processing equipment has been used since the beginning of the last century, the use of information technology experienced exponential acceleration beginning in the 1970s. With the development of microcomputers and their popularization, the IT market and users have witnessed a real revolution. The exclusive use of mainframe computers gave way to networks and client/server types of systems.

1.5. Beginning in the 1990s, with the expansion of the internet to all users, a second revolution was set off. IT use reached all sectors of society, which gave rise to a vast array of applications to make new activities and businesses possible. The systems became web oriented and oriented to service delivery for clients and citizens.

1.6. In this decade, one could allege there has been a third revolution with the intensive use of mobile equipment, broadband internet connections and cloud processing and storage. With all this, changes that result in new technologies have occurred more rapidly, bringing even deeper consequences and making IT competency a key factor in the success of all branches of activity.

1.7. Presently, there is a deep dependence on IT that is revolutionizing the way public administration conducts its business. Maximum use of IT is essential for the public sector to achieve its goals and fulfill its institutional mission.

1.8. Certainly, the results of the coordinated audit on IT governance will contribute to enhancing the degree of maturity in IT governance in the public administrations of the OLACEFS member countries.

2. Background on Coordinated Audits

2.1. Undertaking coordinated audits facilitates sharing knowledge and experience among the supreme audit institutions (SAIs) in the chosen themes. The

coordinated audit on IT governance is in line with strategic goal 3 (Knowledge Management) in the OLACEFS 2011-2015 Strategic Plan. The SAIs involved in the coordinated audits can share costs derived from recruiting consultants, developing preliminary studies, and realizing reference panels and seminars. The international norms and best practices can also be publicized more effectively to each auditor through the coordinated audit strategy. Moreover, the existence of internationally accepted norms for IT governance facilitates sharing and exchanging experiences among the audit teams from different countries.

2.2. Based on successful experience of the Development Initiative of INTOSAI (IDI), OLACEFS is consolidating its strategy centered on training by acquiring knowledge and competencies for each phase of the coordinated audits.

2.3. The coordinated audit on IT governance was preceded by another three projects that took advantage of the same strategy: coordinated audits on hydrocarbons, water resources and protected areas (Biodiversity).

3. Objective

3.1. The coordinated audit had the goal of assessing IT governance in the OLACEFS member countries, based on audits accomplished in the institutions representing diverse sectors of public administration in each of the participating countries.

3.2. This work seeks to obtain information that permits the elaboration of a strategy to raise the level and maturity of IT governance and the dissemination of knowledge and techniques used in the field work. During planning of the audit the following results were projected:

a) Inducing improvements to the IT governance structure and mechanisms in public institutions in the countries involved, whose progress will be obtained based on the recommendations directed to the institutions evaluated in the audit;

b) Identifying the areas with weaknesses and which can be the target for joint action under the aegis of OLACEFS with the goal of improvement by means of cooperation, interchange of experiences, identification of best practices, and training;

c) Disseminating knowledge and best practices for IT governance in public administration in the OLACEFS area of activity.

4. Methods Used

4.1. Several preparatory activities were undertaken to increase the possibility of success of the audit.

4.2. Between February and May 2014, 43 auditors and 15 SAI audit participants were trained via a distance course.

4.3. The International Seminar on IT Governance Auditing was held in Brasília, Brazil, from July 21-22, 2014. There were 10 presentations addressing three large topics: IT Governance and Management, IT Security and IT Planning. In addition to the Brazilian auditors, 21 auditors from the other 10 participating SAIs discussed subjects related to the audit and learned about successful cases in implementing IT governance processes in Brazilian public agencies.

4.4. A technical meeting was held during the next three days to define the planning matrix for carrying out the audit. Four large areas were selected to be defined as the focus of the field work: IT Governance Structure, IT Planning, IT contracting, and Information Security. The planning matrix proposed the following audit questions:

Q1. Have the IT governance structures and mechanisms been defined and implemented adequately in the institution?

Q2. Is there an IT planning process?

Q3. Is there a process for acquiring IT solutions?

Q4. Is there a process for information security management?

4.5. Eleven countries were selected to participate in the audit: Bolivia, Brazil, Chile, Costa Rica, Ecuador, El Salvador, Guatemala, Honduras, Panamá, Paraguay and Peru.

4.6. Forty one audits have been carried out since August 2014 in 11 different countries using the same planning matrix. Information was exchanged on the work in process during the execution of the audits by means of email and video conferencing.

4.7. A meeting was held in San Jose, Costa Rica, from March 24-26, 2015, to consider the findings of the audits carried out in the participating countries and to define the content of this coordinated audit report.

4.8. Defining the topics assessed and the audit criteria to be used was based on the legislation of each country, international technical norms, and internationally recognized best practices.

4.9. As an audit criterion, in addition to the applicable legislation from each country, the coordinated audit adopted the controls contained in norm ISO/IEC 27002:2013 (code of best practices for managing information security), those in norm ISO/IEC 27005:2008 (managing information security risks) and in norm ISO/IEC 38500:2008, COBIT 5 and ISACA, which provide models for best practices for governance of information technology.

5. IT Governance

5.1. IT governance is the part of corporate governance that seeks to assure that using IT adds value to business within acceptable risks. With this goal, IT governance seeks to avoid or mitigate deficiencies in institutional management, such as inadequate planning processes, IT projects without results, and contracting IT that does not meets its objectives, resulting in a loss of quality and efficiency.

5.2. In practice, IT governance translates into a set of policies, processes, roles and responsibilities associated to structures and persons in the organization, in order to clearly establish the decision-making process, the management guidelines and the use of IT.

5.3. Norm ISO/IEC 38500, item 1.6.3, defines IT governance as, "the system by which the present and future use of IT is directed and controlled".

5.4. To complement this concept, the IT Governance Institute (ITGI) specifies that "IT governance is a structure of relationships and processes to direct and control IT to achieve the goals of the institution for added value, while maintaining balance of risks versus return on this function and its processes."

5.5. The objective of IT governance is to assure that IT activities are aligned with the organization's business, adding value. Return from the IT area should be measured, resources should be properly assigned and inherent risks should be mitigated. Thus, it is possible to manage and control IT initiatives in the institutions to assure return on investment and the adoption of improvements to the organizational processes.

5.6. Adequate governance of the IT area in the public sector promotes the protection of critical information and contributes to public institutions achieving their objectives. Moreover, assuring the correct application of resources used in information technology is increasingly important, given the strong dependence of public administration on IT.

6. Key Findings

6.1. The main findings with respect to IT governance mechanisms and structures were deficiencies in IT governance mechanisms and the absence of IT committees.

Structures and Mechanisms of IT Governance

6.2. It was observed that, in almost half of the institutions audited (46%), IT governance structures and mechanisms were not adequately employed.

6.3. Many institutions lack officially approved processes or plans for managing IT risks and do not evaluate fulfillment of the IT goals planned, essential mechanisms, which are essential to directing and evaluating IT management and corporate use.

6.4. Many agencies lacked a process for continuous improvement on IT governance. No actions were identified that aimed at diagnosing the level of IT governance maturity or to define governmental objectives for the next years. Another very common deficiency observed was the lack of a formal personnel structure to allocate personnel to improve IT governance.

6.5. In other institutions, despite having approved IT Director Plans (ITDP), there is no formalized comprehensive system of objectives related to improving IT governance, performance indicators for each goal, objectives for each indicator and mechanisms to monitor routinely these indicators. IT governance goals were not defined or formalized in the ITDP based on governance parameters, business needs, and important risks, nor were there indicators to monitor and evaluate the fulfillment of these objectives.

6.6. Many institutions are not developing actions to improve their level of IT governance. This inertia can compromise the necessary evaluation of the maturity level of IT governance, as well as, in the last analysis, hinder the achievement of the IT objectives. In this way, it can be understood how an opportune recommendation for the institutions to develop and approve a process for continuous improvement of IT governance (according to good practices in chapter 3 of the reference guide for implementing COBIT 5), which contemplates, at a minimum, definition of the roles and responsibilities directed specifically to improving IT governance; carrying out diagnostics or self-evaluations of IT governance and management, and defining and observing the goals for IT governance and the actions needed to achieve it, based on the governance parameters, business needs and relevant risks.

6.7. Another essential aspect of IT governance is the existence of IT committees to determine investment priorities and assignment of resources for IT projects and activities and the business of the organization, as well as to optimize available resources. The fact that these committees are composed of representatives from the IT area and others in the organization makes it possible to make investment decisions based on a broader organizational vision that reduces the risks of unnecessary expenses or those that do not benefit the organization.

6.8. It was found that 44% of the institutions audited had not created IT committees with the functions advocated by COBIT 5. It is worth stressing that in Brazil where regulatory norms mandate committees, there were committees in all eight audited institutions.

6.9. The fact that around half of the audited institutions have no functioning IT committee indicates that the importance of participation of all sectors of the organization in IT strategic decisions has still not been consolidated. The existence of IT committees, along with strategic institutional and IT plans constitutes a valuable tool to guide IT investment, increase the success of IT projects and reduces the risk of wasting resources.

6.10. It can also be stressed that the existence of a norm requiring the creation of IT committees within institutions favors their adherence to international best practices in IT governance.

The IT planning process

6.11. Three findings stand out regarding the issue of IT planning processes: the absence of this process in many institutions, the lack of documentation of strategic planning, and the absence of an IT monitoring plan by upper management.

6.12. A significant percentage of the audited institutions (39%) do not have a functioning IT process in place. This means that these institutions, although they might have some IT plan, do not have the culture of strategically planning their actions and, in the majority of situations, can only react to demands and changes that occur in their area of activity, making it difficult to plan IT activities.

6.13. The incorporation of an IT planning process minimizes the possibility of inadequate allocation of resources. Further, this process avoids organizational dependence on specific persons. Moreover, even if a significant number of professionals leave, the IT area could continue to follow the planned direction, concluding on-going processes and continue to function adequately.

6.14. Only implementation of the IT planning process will allow public institutions the most efficient use of IT resources. The lack of this process in a significant number of public institutions requires the action of the SAI in the sense of raising the awareness of upper management and the IT managers about the importance of IT planning.

6.15. Additionally, most institutions that do have an IT planning process do not produce IT strategic planning documents.

6.16. Almost two-thirds (63%) of the audited institutions do not carry out IT strategic planning. The importance of strategic planning to IT governance must be stressed once again. For IT strategic planning to be effective and provide the expected results, it must be aligned with institutional strategic planning. For this reason, its absence can impede the desired alignment and makes it difficult to establish guidelines for the IT area.

6.17. Obviously, one should not confuse a lack of strategic planning with the absence of any kind of planning. The organizations and/or entities could have some type of planning, usually an annual action plan. Despite being necessary, annual action plans are not sufficient because they do no indicate paths and strategies, they only forecast how to assign available resources for that year. Moreover, these plans are not good instruments to follow and support medium and long range projects, common in the IT area. Another commonly observed problem occurs when, due to lack of strategic planning these projects are discontinued and result in an unnecessary use of resources.

6.18. IT strategic planning must indicate which projects and IT services will receive resources, beyond costs, from the resource sources and the goals to be achieved. This should be a regular activity and the resulting documents must be approved by upper management.

6.19. IT strategic planning must make it possible to define, together with the main interested parties, the way in which IT objectives contribute to achieving the organization's strategic goals, taking into account the associated costs and risks. The document resulting from this planning must cover IT services, IT assets and the ways in which each IT area will provide support to projects that depend on information technology. The IT area must define how it will achieve the objectives, the metrics to be used and the procedures to obtain the formal approval of the interested parties. The strategic IT plan must contain proposals for investment and maintenance of IT, the source of resources, the strategy for acquisitions and the legal and regulatory requirements. The strategic plan must be sufficiently detailed to be deployed into tactical IT plans.

6.20. It is fundamental to disseminate the strategic planning culture to public institutions; the SAIs must demand their results.

6.21. Another point that merits attention is the lack of IT monitoring by upper management.

6.22. In nearly a third of the audited institutions (29%) it was found that upper management did not monitor the execution of IT plans. In some cases, despite the existence of the plans, the organization had not formally defined control mechanisms to achieve management goals and the corporative use of IT. In other situations, despite the IT Strategic Plan (containing definitions of goals), there is no information on how to measure and control the objectives.

6.23. In other situations, management objectives and corporate use of IT were not formally established, and neither were the associated goals. Upper management did not follow the indicators for strategic results from the main information systems. Moreover, there are no control mechanisms for filling management goals and corporate use of IT, nor are there management mechanisms for risks related to these objectives. They also failed to approve internal audit plans to assess risks considered critical to the business and the effectiveness of the respective controls.

6.24. The SAIs must recommend to the audit institutions that they formally establish mechanisms for upper management to follow up the returns from IT and risk management mechanisms related to management objectives and corporate use of IT.

6.25. Moreover, an annual internal auditing plan must be written which includes among others, activities for the purposes of evaluating risks to the business and the effectiveness of the respective controls related to the management and corporate use of IT.

The Process for Acquiring IT Solutions

6.26. The formalization of the acquisition process for IT solutions was observed at the majority of the audited institutions. Nevertheless, it was found that this process and the subsequent process of managing IT contracts were not monitored.

6.27. In addition to implementing processes to contract IT, it is necessary to constantly monitor the results achieved to enhance the process in itself and also to minimize deviations and waste. This monitoring was not done in 39% of the institutions audited.

6.28. The allocation and optimization of resources must be controlled according to the established goals and priorities using the agreed upon goals and metrics. Following this, return on investment must be compared to the goals, the causes of any deviations must be analyzed and corrective measure to resolve the underlying causes must be initiated.

6.29. The purposes of constantly monitoring the contracting process are to improve the process, to reinforce the alignment between IT and the business areas, to allocate resources efficiently and to optimize the organization's IT resources.

6.30. In 29% of the audited institutions, the contract management process is not monitored. In the same way that it is important to have a formalized work process for IT contracts, it is essential that contracts for these acquisitions are well administered and that their management process is monitored.

6.31. In addition to enhancing the IT contract management process, this monitoring allows verification of the results achieved through each contract based on pre-established metrics.

6.32. The objectives of continuous monitoring of the contract management process are: to enhance the process; to assure the necessary IT resources for the various business areas; to allocate sufficient resources and to optimize the organizations IT results.

Managing Information Security

6.33. Traditionally, the information security area presents a lot of deficiencies. In this work, we highlight six findings: the lack of approved information security policies (ISP); the lack of formal designation of those responsible for managing information security; the absence of an access control policy (ACP); the lack of a process to manage information security risks; the absence of a management process of the continuity of IT services; and the lack of a business continuity plan (BCP).

6.34. It was found that in 46% of the audited institutions, there was no approved or published information security policy (ISP).

6.35. The ISP is the document that contains organizational guidelines for treating information security. According to norm ISO/IEC 27002:2013, the policy must make

upper management's commitment to information security explicit. Moreover, it must also define the terms within the organizational environment and assign control objectives, the controls themselves, the structure to implement these controls, responsibility and policies for the norms that regulate and complement this document, including references to legislation, regulatory and contractual requirements. In general, this is the document from which the specifics of each information security management activity will be derived.

6.36. It is essential that upper management establishes clear policies aligned with the business objectives and demonstrates support and commitment to information security by means of publication and maintaining the ISP for the entire organization.

6.37. To implement the ISP it is essential to designate formal responsibilities for information security management.

6.38. In 51% of the audited institutions, there was no responsible persons or unit designated to carry out information security management. Due to the broad, varied range of activities related to managing information security, it is mandatory to designate people or units formally to perform these tasks.

6.39. Each organization must formally designate a responsible party (unit or person) to be responsible for information security in its area of activity, in a way similar to the guidelines in item 6.1.1 of norm ISO/IEC 27002:2013.

6.40. Another document very important to adequate management of information security is the Access Control Policy (ACP).

6.41. It was found that 44% of the audited institutions have no formally approved and published document that institutes an access control policy. The ACP must be established, documented, and critically analyzed based on information security and business requirements.

6.42. The rules for access control and the rights of each user and group of users must be clear in the ACP, considering controls for logical and physical access together, according to the business needs to be met.

6.43. The SAIs must recommend to the institutions that they audit to develop and formally approve an access control policy to the organization's information and IT resources, based on the business needs and the organization's information security, similar to the guidelines of section 9.1.1 of norm ISO/IEC 27002:2013.

6.44. In addition to the critical situation encountered in a significant number of the audited institutions, it was found that 49% of them have no risk management process for information security. The process of managing information security risks includes the assessment and/or evaluation of risks, the treatment of each risk, the definition of acceptable risk, the communication of the risk to the monitors and the critical risk analysis of information security.

6.45. The SAIs must recommend to the audited institutions that they define and implement a risk management process for information security, in a similar manner to the guidelines in norm ISO/IEC 27005:2008.

6.46. Another aspect of negligence in a significant number of the institutions audited is managing the continuity of IT services. It was found that 54% of the audited institutions had not implemented a process to provide IT service continuity. The process of managing continuity of IT services seeks to prevent IT services from interrupting the organization's activities and to keep the most critical information available according to the level of service required.

6.47. The SAIs must recommend to the audited institutions that they audit, develop and carry out a process to manage continuity of IT services, in a similar manner to that prescribed in docket DSS04 – COBIT 5 Continuity Management.

6.48. As a nearly direct consequence of the lack of a management process for IT services continuity, it was found that the majority (59%) of the audited institutions have not approved and published a Plan for Business Continuity (BCP). The purpose of the BCP is to prevent interruption of business activities and to protect critical processes against failure or important disasters, assuring its return within a defined time period.

6.49. The SAIs must recommend to the audited institutions that they audit, develop and carry out a process to manage continuity of IT services, in a similar manner to that prescribed in docket DSS04 – COBIT 5 Continuity Management.

7. Conclusions and Challenges

7.1. The main objective of this coordinated audit is to assess the situation of IT governance in the OLACEFS member countries, based on audits carried out in institutions representing various areas of public administration in each country. A total of 41 audits in public institutions of 11 different participating countries used the same planning matrix.

7.2. In order to define the areas of IT governance to be audited and to organize the work, four large areas were selected to focus the field audit: IT Structure and Governance, IT Planning, IT Contracting and Information Security.

7.3. With reference to IT structure and governance, it was found that, despite the fact that around two-thirds (66%) of the audited institutions have implemented structures and mechanisms, there are still many deficiencies. Of the audited institutions, 46% of the mechanisms were defective, and in 44% of them there was no IT committee and 7% of the committee representatives did not have an adequate profile to achieve a positive result from the activities. The conclusion is that there are problems in the majority of the institutions, which demand improvement on the IT governance structures.

7.4. With respect to IT planning, it was found that 39% of the institutions have not implemented an IT planning process, and that almost 2/3 of them have not produced IT strategic planning documents. It must be stressed that the absence of an IT strategic planning document leaves the institutions without a tool to follow up and support medium and long term projects, common in the IT area, which can cause discontinuity in these projects and the consequent waste of resources.

7.5. Of the four areas analyzed, IT contracting was the most organized and had fewer formal deficiencies. This finding, nevertheless, does not mean that contracting is being carried out in an effective and efficient manner. In practically a third of the organizations (34%), there was no process implemented for contracting IT. Moreover, in 39% of the evaluated institutions, the IT contracting process is not monitored. Also, IT contracting management process is not followed by 29% of the institutions. Greater control over IT contracting is necessary.

7.6. Regarding information security, it was found that it had the lowest score of the four focused areas in the present audit, as there were 13 different findings and some of them had significant numbers of appearances. Among these cases, we highlight the lack of plan for business continuity plan, in 59% of the institutions audited; the absence of an IT service continuity process in 54% of them, and failure to designate people or units responsible for information security management in 51% of the institutions. Most importantly, two of the basic information security processes, information security and continuity management, have still not been implemented in over half of the audited institutions. Moreover, essential documents and processes have not been developed or implemented in almost half the institutions audited, which further reinforces the need to pay attention to information security. The lack of a risk management process was detected in 49% of the audited entities, absence of an inventory asset program in 46% of them, lack of an information security committee in 46% of them, absence of a policy for information security in 46% of them and lack of an access control policy in 44% of the audited institutions.

7.7. Given the scenario presented, we highlight that the IT governance situation in the OLACEFS member countries is very heterogeneous in many respects. For example, the IT contracting issue, in addition to the natural differences among the countries participating in the audit, is somehow regulated by necessary norms, which, on one hand, represents some development, despite being far from the ideal. In the same condition are the aspects that use good practices as a main reference, that is: IT governance structures, IT planning and information security. These demand more attention. The aspect in which the IT governance situation is more critical is information security.

7.8. On this point, the greatest challenge for the SAIs is to raise the awareness of the audit institutions about the importance of IT governance and the benefits that could be obtained by improving its degree of maturity. It is important, even urgent, to invest resources to implement or enhance: the IT committees; the IT planning

process; strategic IT planning; monitoring the IT contracting process; the business continuity plan; the designation of a responsible person or unit to manage security information; a risk management process; an asset inventory process; an information security committee; and a policy for access control.

7.9. In conclusion, it was observed that the SAIs can and must act as inducers of the process to enhance IT governance in the public administration of the OLACEFS member countries. For that reason, if these activities are performed in a consistent y permanent way, the results will be promising, taking into account that there could be general improvement in all aspects. This fact will have repercussions for public administration services and will bring benefits to both the countries and their citizens.

8. References

8.1. Norma ISO/IEC 27002:2013, Code of practice for information security controls;

8.2. Norma ISO/IEC 27005:2008, Information Security Risk Management;

8.3. Norma ISO/IEC 38500:2008, Corporate Governance of Information Technology; y

8.4. Cobit 5, Framework for the Governance and Management of Enterprise IT.

9. Participants

9.1. The organization of the work was undertaken by auditors from the Federal Court of Accounts Brazil (TCU). The 41 audits were carried out by 52 auditors of the eleven different supreme audit institutions:

- The General Auditor's Office of the Plurinational State of Bolivia;
- The Federal Court of Accounts of Brazil;
- The General Auditor's Office of the Republic of Chile;
- The General Auditor's Office of the Republic of Costa Rica;
- The General Auditor's Office of the Republic of Ecuador;
- The Federal Court of Accounts of the Republic of El Salvador;
- General Auditor of Accounts of the Republic of Guatemala;
- Federal Court of Accounts of the Republic of Honduras;
- The General Auditor's Office of the Republic of Panama;
- The General Auditor's Office of the Republic of Paraguay;
- The General Auditor's Office of the Republic of Peru.

10. Acknowledgments

10.1. The Secretariat for International Relations (SERINT) of the TCU for all its support, professionalism, and the quality of the work carried out during the process.

10.2. The Inter-American Development Bank (IDB) for the financial support.

10.3. The International Affairs Department of the Auditor General's Office of the Republic of Costa Rica for its generosity in organizing the workshop held in San Jose in March 2015.

10.4. The international areas of the other SAIs who have helped in carrying out the activities of this coordinated audit of IT.