3. Mizhnarodnyi dosvid serednostrokovoho biudzhetnoho planuvannia: Dosvid dlia Ukrainy. URL: https://feao.org.ua/wp-content/uploads/2017/06/FEAO_Sered_budget_planning_A5_05_web-2.pdf

Oleksandr Shashkevych
Ternopil National Economy University

IMPLEMENTATION OF IT AUDIT STANDARDS IN UKRAINE

First of all, we have to recognize that IT Audit is necessary as an element of internal control of government organizations. But nowadays it is absolutely absent in all state control systems in Ukraine.

By the way, implementation of IT Audit is one of the main strategic tasks of the State Audit Service of Ukraine. So, the main purpose of this paper is analysis of possibilities of establishing IT Audit Standards in practice of internal control for good governance and management of government organizations (GO) in Ukraine.

This paper emphasizes the importance of IT Audit, the control procedures that go beyond just individual applications, and covers overall organization of IT processes.

IT processes today cover many areas, ranging from an IT application to control a government organization's (GO) accounting general accounting ledger to numerous laptop and handheld systems and connections to the all-pervasive Internet. Today government executive should have a strong understanding of IT internal control techniques covering these many technologies and processes.

Robert R. Moeller in his work [1] considers that IT general controls cover all information systems operations and include:

Reliability of information systems processing. Good controls need to be in place over all IT systems operations. These controls often depend on the nature and management of the specific size and type of systems used.

Integrity of data. Processes should be in place to ensure a level of integrity over all data used in various application programs.

Integrity of programs. New or revised programs should be developed in a well-controlled manner to provide accurate processing results. These control issues include the overall process of application program development.

Controls over the proper development and implementation of systems. Controls should be in place to ensure the orderly development of new and revised information systems.

Continuity of processing. Controls should be in place to back up key systems and to recover operations in the event of an unexpected outage what

was once called disaster recovery planning and is often known today as continuity planning.

There is the necessity to implement the IT Audit Standards in control activity of the State Audit Service of Ukraine. This will help the government sector of Ukraine to approach the European Union's control standards.

We propose such typical structure of IT Audit Standards that is used by the Information Systems Audit and Control Association (ISACA) [2] with some differences.

Standard 1. Independence

Professional Independence. In all matters related to the audit, the Information System (IS) auditor should be independent of the auditee in both attitude and appearance.

Organizational Independence. The IS audit function should be independent of the area or activity being reviewed to permit objective completion of the audit assignment.

Standard 2. Professional Ethics and Standards

The IS auditor should adhere to the Code of Professional Ethics in conducting audit assignments.

The IS auditor should exercise due professional care, including observance of applicable professional auditing standards, in conducting the audit assignments.

Standard 3. Professional Competence

The IS auditor should be professionally competent, having the skills and knowledge to conduct the audit assignment.

Standard 4. Planning

The IS auditor should plan the information systems audit coverage to address the audit objectives and comply with applicable laws and professional auditing standards.

The IS auditor should develop and document a risk-based audit approach.

The IS auditor should develop and document an audit plan that lists the audit detailing the nature and objectives, timing and extent, objectives and resources required.

The IS auditor should develop an audit program and/or plan and detailing the nature, timing and extent of the audit procedures required to complete the audit.

Standard 5. Performance of Audit Work

Supervision – IS audit staff should be supervised to provide reasonable assurance that audit objectives are accomplished and applicable professional auditing standards are met.

Evidence – During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The

audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.

Documentation – The audit process should be documented, describing the audit work performed and the audit evidence that supports the IS auditor's findings and conclusions.

Standard 6. Reporting

The IS auditor should provide a report, in an appropriate form, upon completion of the audit. The report should identify the organization, the intended recipients and any restrictions on circulation.

The audit report should state the scope, objectives, period of coverage and the nature, timing and extent of the audit work performed.

The report should state the findings, conclusions and recommendations and any reservations, qualifications or limitations in scope that the IS auditor has with respect to the audit.

The IS auditor should have sufficient and appropriate audit evidence to support the results reported.

When issued, the IS auditor's report should be signed, dated and distributed according to the terms of the audit charter or engagement letter.

Standard 7. Follow-Up Activities

After the reporting of findings and recommendations, the IS auditor should request and evaluate relevant information to conclude whether appropriate action has been taken by management in a timely manner.

Standard 8. Irregularities and Illegal Acts

In planning and performing the audit to reduce audit risk to a low level, the IS auditor should consider the risk of irregularities and illegal acts.

The IS auditor should maintain an attitude of professional skepticism during the audit, recognizing the possibility that material misstatements due to irregularities and illegal acts could exist, irrespective of his/her evaluation of the risk of irregularities and illegal acts.

The IS auditor should obtain an understanding of the organization and its environment, including internal controls.

When performing audit procedures the IS auditor should consider unusual or unexpected relationships that may indicate a risk of material misstatements due to irregularities and illegal acts.

The IS auditor should design and perform procedures to test the appropriateness of internal control and the risk of management override of controls.

If the IS auditor has identified a material irregularity or illegal act involving management or employees who have significant roles in internal control, the IS auditor should communicate these matters in a timely manner to those charged with governance.

The IS auditor should advise the appropriate level of management and those charged with governance of material weaknesses in the design and implementation of internal control to prevent and detect irregularities and illegal acts that may have come to the IS auditor's attention during the audit.

The IS auditor should document all communications, planning, results, evaluations and conclusions relating to material irregularities and illegal acts that have been reported to management, those charged with governance, regulators and others.

Standard 9. IT Governance

The IS auditor should review and assess:

– whether the IS function aligns with the organization's mission, vision, values, objectives and strategies;

– the effectiveness of IS resource and performance management processes;

– compliance with legal, environmental and information quality, and fiduciary and security requirements;

– the control environment of the organization;

– the risks that may adversely affect the IS environment.

A risk-based approach should be used by the IS auditor to evaluate the IS function.

Standard 10. Use of Risk Assessment in Audit Planning

The IS auditor should use an appropriate risk assessment technique or approach in developing the overall IS audit plan and in determining priorities for the effective allocation of IS audit resources.

When planning individual reviews, the IS auditor should identify and assess risks relevant to the area under review.

Standard 10. Audit Materiality

The IS auditor should consider audit materiality and its relationship to audit risk while determining the nature, timing and extent of audit procedures.

While planning for audit, the IS auditor should consider potential weakness or absence of controls and whether such weakness or absence of control could result into significant deficiency or a material weakness in the information system.

The report of the IS auditor should disclose ineffective controls or absence of controls and the significance of the control deficiencies and possibility of these weaknesses resulting in a significant deficiency or material weakness.

Standard 11. Using the Work of Other Experts

The IS auditor should, where appropriate, consider using the work of other experts for the audit.

The IS auditor should assess and be satisfied with the professional qualifications, competencies, relevant experience, resources, independence and quality control processes of other experts, prior to engagement.

Standard 12. Audit Evidence

The IS auditor should obtain sufficient and appropriate audit evidence to draw reasonable conclusions on which to base the audit results.

The IS auditor should evaluate the sufficiency of audit evidence obtained during the audit.

Standard 13. IT Controls

The IS auditor should evaluate and monitor IT controls that are an integral part of the internal control environment of the organization.

The IS auditor should assist management by providing advice regarding the design, implementation, operation and improvement of IT controls.

In cause of implementation of IT Audit Standards in few years Ukraine will receive a modern and effective public internal control system.

Literature

1. Robert R. Moeller. Executive's Guide to COSO Internal Controls. Understanding and Implementing the New Framework. Hoboken, New Jersey: Wiley&Sons, Inc., 2014, P. 181-184.
2. IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals. URL: https://www.isaca.org/knowledge-center/standards/documents/it-audit-assurance-guidance-1march2010.pdf.

Iryna Sydor
Ternopil National Economic University

DIRECTIONS OF IMPROVEMENT OF INTER-BUDGETARY RELATIONS IN THE CONTEXT OF FINANCIAL ALIGNMENT OF TERRITORIES

In the conditions of economic instability, modernization of social political and economic relations, the issues of formation of effective mechanisms of state stimulation and regulation of economic activity in the region, aimed at counteracting the destructive influence of factors of internal and external environment and creating favorable conditions for ensuring economic growth in the country, are significantly relevant. In recent years, the system of intergovernmental budgetary relations in Ukraine has undergone significant transformations - from the traditional unsystematic and unreasonable mechanism of intergovernmental budgetary reallocation of resources to the establishment of a market-based system of budgetary regulation based on effective methods and instruments. The main tool for implementing the system of financial relations between local and central government is intergovernmental relations. Their effective implementation is an effective factor in the economic and political development of Ukraine. That is why they are constantly in the process of improvement, which is aimed at solving the