



APPROVED BY THE
AUDITOR GENERAL'S
Order No. V-65 of 27 April 2006

METHODOLOGICAL RECOMMENDATIONS FOR INFORMATION SYSTEMS AUDIT

INTRODUCTION

Public auditors obtain part of the needed data from computerized accounting and management systems. Auditors need to evaluate audit risk and reliability of the received information (audit evidence), therefore it is **important to know how the audited entity controls information systems**. Information received by auditors is not primary; it is obtained after a complex process of data processing during which errors may occur. Errors may be made due to human factor, e.g., when entering data, due to programmers' errors etc. Errors may be random and intentional. Like any other assets, IS are vulnerable, e.g., they may be damaged or stolen. Data and programmes which are in the computer are intangible, therefore they may be accessed or changed without leaving any visible trace.

IS development, installation, and maintenance costs should also be properly audited. It is purposeful to evaluate economy, efficiency, and effectiveness of IS development, installation, and maintenance.¹

Also, audit methods have to be continually developed taking into consideration progress of science and technology.²

This document seeks to explain purpose of IS audit and its performance in the National Audit Office of Lithuania (NAOL). Annexes to this document are of recommendatory nature, and they are freely interpreted by auditors during audits.

¹ INTOSAI Lima Declaration of Guidelines on Auditing Precepts.

² Ibid.

Concepts and abbreviations

| | |
|-----------------------------|---|
| SAI | Supreme Audit Institution |
| CAAT | Computer Assisted Audit Tools (Data Analysis Software) |
| COBIT | Control Objectives for Information and Related Technology |
| INTOSAI | International Organisation of Supreme Audit Institutions |
| IS | Information Systems |
| ISACA | Information Systems Audit and Control Association |
| IS Audit | Part of Public Audit Process Related to Information Systems |
| IS General Controls | It is systems software and physical procedures composing the general control environment of an institution or organization |
| ISO | International Standards Organisation |
| IT | Information Technologies |
| ITIL | Information Technologies Infrastructure Library (Internationally Accepted Set of Best Practices for Managing IT Services Developed in the UK) |
| Application Controls | Control of the Concrete Computerized Function |

Regulation of IS audit in the Supreme Audit Institutions

INTOSAI Lima Declaration of Guidelines on Auditing Precepts, Section 13, Part 3 and Section 22.

INTOSAI Auditing Standards, Items 51 b), 86, 144 and 153.

European Implementing Guidelines for the INTOSAI Auditing Standards. Guideline No. 22.

Commission Regulation (EC) No 1663/95 of 7 July 1995 laying down detailed rules for the application of Council Regulation (EEC) No 729/70 regarding the procedure for the clearance of the accounts of the EAGGF Guarantee Section and the associated IT Systems Security Guidelines.³

³ IT Systems Security Guidelines No VI/661/97 REV.2 for Paying Agencies approved by the European Commission DG Agriculture on 19 February 1998.

1. GENERAL PRINCIPLES

1.1 Definition of IS audit

IS audit is a process of evidence collection and evaluation allowing to decide whether a computer system (information system) ensures assets' security, data integrity, as well as helps to efficiently seek organizational goals and rationally use the resources.⁴

1.2 Areas of IS audit

Application of IS audit may be divided into two areas:

- Evaluation of internal control,
- Evaluation of IS in terms of economy, efficiency, and effectiveness (hereinafter - 3Es).

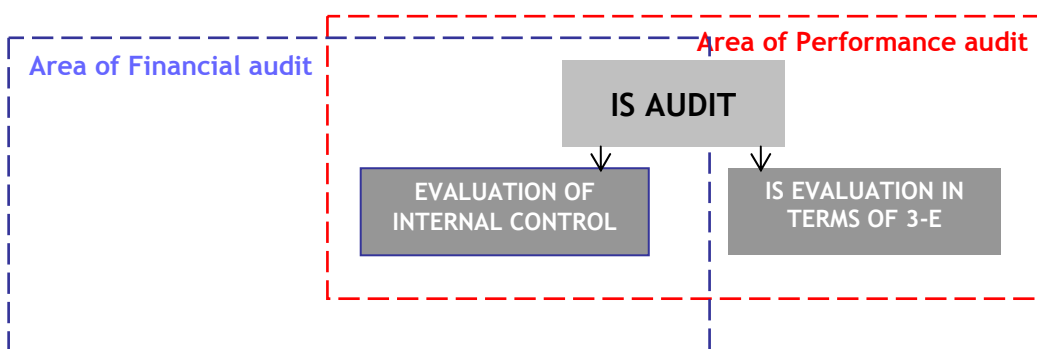
Public Auditing Requirements, Point 70.

Internal control shall mean the entire set of controls established by the management of a public legal entity in order to provide reasonable assurance that the operations of the public legal entity are legal, economic, efficient, effective and transparent, that the strategic and other plans are implemented, that assets are safeguarded, that financial information and reporting are reliable and exhaustive, that contractual liabilities to third persons are satisfied and that all identified risks are managed.

In order to avoid problems of IS management and security protection general IS control methods were developed. Generally IS audit is meant to evaluate such control. Evaluation of the audited entity's internal control is an area of financial and performance audits; therefore **IS audit is a constituent part of financial and performance audits.**

Evaluation of IS in terms of economy, efficiency, and effectiveness is a separate IS performance audit conducted following Performance Audit Manual (Figure 1.).

Figure 1. Areas of IS audit



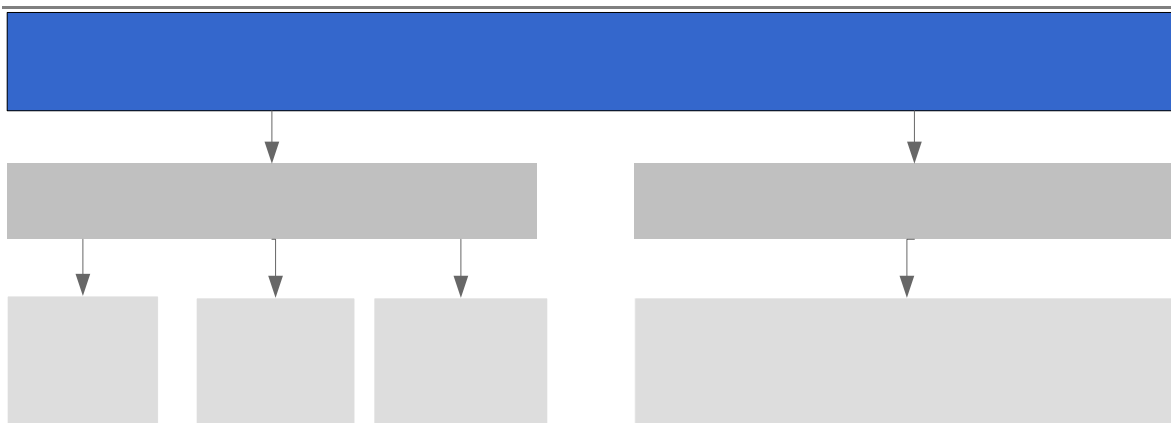
⁴ Weber, Ron (1999), „Information Systems Control and Audit“ p. 10

1.3 Types and objectives of IS audit

Types of IS audit:

- Audit of IS general controls,
- Audit of application controls
- Audit of IS development controls
- IS performance audit.

Figure 2. Types of IS audit



Objectives of IS audit:

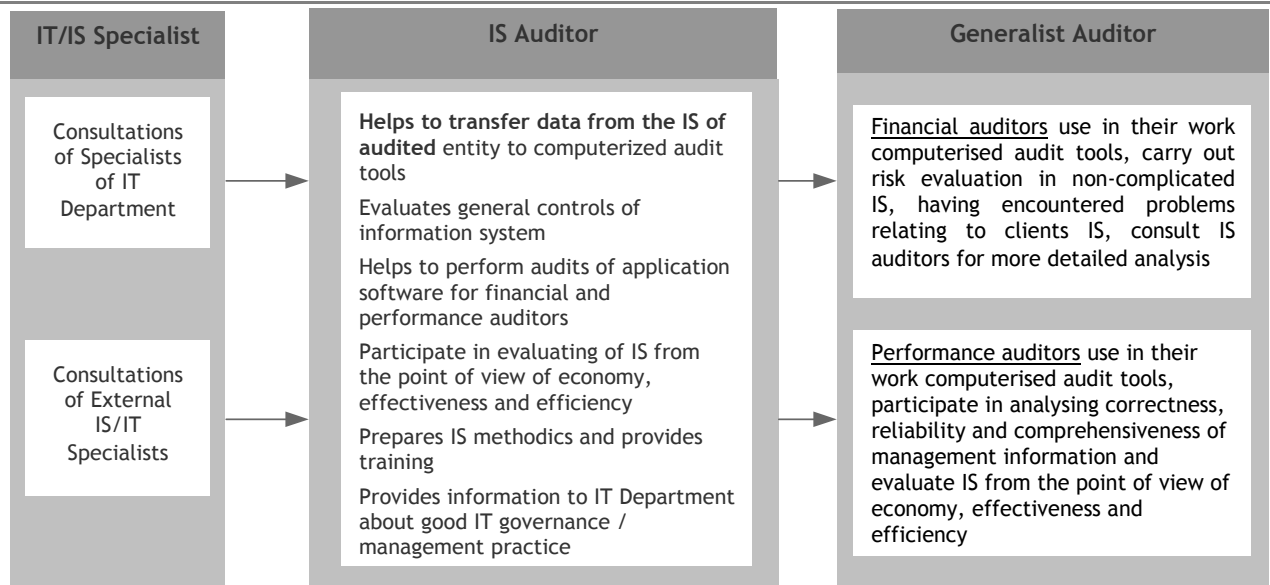
- **Audit of IS general controls** is to evaluate internal control which covers all information systems of an organization.
- **Audit of application controls** is to evaluate a control related to data input, processing, protection, and obtaining in the specific applications (e.g., *Navision Financials*, *LABBIS* etc.).
- **Audit of IS development controls** is to evaluate management and control of IS development from the beginning of its conception until its legitimation; covering IS change management;
- **Objective of IS performance audit** is to evaluate issues related to IS in terms of efficiency, economy, and effectiveness.

1.4 Cooperation of public auditors

In terms of IS audit INTOSAI distinguishes three levels of auditors (interaction of these levels in the National Audit Office of Lithuania is presented in the Figure 3.):

- Public auditors conducting financial and performance audits (hereinafter - general auditors),
- IS auditors,
- IS/IT specialists.

Figure 3. Division of functions when performing IS audit



IS audits performed by general auditors are limited to medium complexity evaluation of IS general control and accounting programmes (e.g., *Navision Financials*, *LABBIS* etc.).

IS auditors perform audits of general control of complex IS (e.g., IS of the State Social Insurance Fund Board of the Republic of Lithuania, Customs' IS etc.), IS development audits, and IS performance audits.

IS/IT specialists provide specialized guidance on particular issues.

Table 1.

| Type of IS audit | Evaluation of complexity of IS* | Audit is performed by | Performing the audit it is recommended to follow |
|-------------------------------------|---|-------------------------------------|---|
| 1. Audit of IS general controls | Simple | General auditors | Annex 2 |
| | Medium complexity (computerized accounting systems) | General auditors | Annexes 2, 7 |
| | Complex (information systems of the state) | IS auditors | Annexes 2, 4, 5, 7 |
| 2. Audit of application controls | | General auditors | Annex 3 |
| 3. Audit of IS development controls | | IS auditors | Annex 4, Part 10 Design and maintenance of systems and partly Annex 4, Part 8 Management of communications and working procedures |
| 4. IS performance audit | | IS auditors Performance auditors | Performance Audit Manual |

* Evaluation of IS is performed using questionnaire from Annex 1.

During financial or performance audits (in cases stipulated in this document) general auditors may ask for help from IS auditors or IS/IT specialists. In such cases Audit Department Director (Deputy Director) applies to Head of the structural unit of the NAOL which performs IS audits. In case of need external IT/IS specialist may be invited.

Having performed IS audits general auditors present results (copy of a document) of evaluation of IS general control to structural unit of the NAOL which performs IS audits.

1.5 IS audit is performed following:

- Public Auditing Requirements;
- Financial and Performance Audit Manuals;
- International standards of Information systems audit and Control Association ISACA and guidelines of Information system audit of this Association;
- European Implementing Guidelines for the INTOSAI Auditing Standards. Guideline No. 22.
- These methodological recommendations.

2. PROCESS OF EVALUATION OF IS INTERNAL CONTROL

Audit is performed upon an assignment following the procedure established by the Auditor General or as a separate stage of financial or performance audit.

Internal control evaluation of IS is performed in the following order:

- First of all, evaluation of IS general control is conducted in a particular audited entity, and maturity of IS general control is identified;
- Having performed evaluation of IS general control, evaluation of particular application software control is conducted;
- Annual summary on IS internal control is prepared;
- IS performance audit is carried out in the audited entity if potential IS economy, efficiency, and effectiveness problems are identified. Strategic planning of IS performance audit uses data obtained evaluating IS general control.

2.1 Audit of IS general controls

Auditor should not consider computer processed and (or) transferred information of the audited entity reliable until he has proper supporting evidence. Such evidence could be

obtained after getting assurance that internal control procedures of the system operate securely and properly.

Audit resources of IS general controls

Detailed evaluation of general control procedures for IS may require profound knowledge of IS audit and rather a lot of resources. Auditors who want to conduct a comprehensive audit of IS general control may need a specialist help; however, comprehensive IS audit is not always justifiable. General auditors need to decide when it is necessary to ask for help from IS audit specialists. To this end they need to use IS complexity evaluation questionnaire from Annex 1. in which complexity evaluation criteria of information systems are pointed out. According to their complexity, information systems are divided into simple, medium complexity, and complex.

- In audited entities which have introduced **simple** (not complex) IS, audit of the IS general control should be conducted by general auditors. Auditors should at once, without IS internal control evaluation, understand that simple (primitive) computerized accounting systems are subject to great risk. (Example 1.).

Example 1.

In most cases auditors get data in the form of tables (worksheets). Tables could be prepared using software application, e.g., accounting is managed with a help of electronic worksheets (*MS Excel* or similar software). Analysis showed⁵ that almost 80% of worksheets contain mistakes in the programmed formulas. When concrete data is important for an audit it should be crosschecked. In such case it is recommended to obtain full copies of documents on a diskette, CD, or DVD in order to be able to check all or part of the formulas. Audit in IT environment can use CAAT.

- Internal control audit of **medium complexity** IS is also performed by general auditors. They may ask for help with particular issues of IS auditors (see part 1.4). When evaluating it is recommended to use questionnaire which is presented in the Annex 2. This questionnaire points out standard questions. Copy of the filled questionnaire should be submitted to an IS auditor (see part 1.4).
- **Complex** general internal control audit of the state's IS is conducted by IS auditors. Complex audits of the state's IS are included into the annual Public Audit Programme.

Performing of audit

Audit of IS general control may be divided into three stages:

1. Analysis of IS general controls;
2. Testing of IS general controls;
3. Evaluation of IS internal controls.

⁵ See Audit Manual of European Court of Auditors

Analysis of IS general controls

Evaluating IS general controls of an organization (when performing audit of IS general controls it is recommended to use questionnaire from the Annex 2) an auditor should identify:

- Who in the management of an audited entity is responsible for IS;

Communicating with managers of various levels of an organization it is purposefull to find out as to how the managers supervise IS processes, i.e., it is purposefull to get to know the monitoring system of an organization and its operation. It is recommended to point out what actions were taken by managers when they had identified that IS performance had not satisfied legal acts and internal procedures. It is also purposefull to take note of the fact whether the applied control procedures are regularly (e.g., at least once a year) revised, and efficiency of the existing procedures as well as the need for new ones is regularly evaluated.

- How IT processes are organized in an audited entity;
- How internal audit of information systems is carried out (an auditor may use results of internal auditors if the quality of their work is reliable);
- Whether IS risk is evaluated in an audited entity; if there is an evaluation methodology, and whether this evaluation is documented;
- Whether IS and information security strategies, policies (regulations), procedures, rules, project specifications are documented, and whether an audited entity follows the above mentioned documents;

Auditors should learn which standards, methodologies, or other documents regulating to IT area are used by the audited entity. Legal acts⁶ of the Republic of Lithuania recommend following LST ISO/IEC 17799:2002 standard „Information technology. Practice code for information security management. (Equivalent to ISO/IEC 17799:2000)“. Audited entity may also choose LST ISO/IEC TR 13335 standard „Information technology. Guidelines for security management of information technology (equivalent to ISO/IEC TR 13335:1996)“. Standard questionnaires were developed for auditors according to the above mentioned standards (Annexes 4 and 5). These questionnaires list standard questions (which may be freely chosen by an auditor). However, assessment of compliance with the above mentioned standards is rather complicated, therefore it is recommended to use help of IS auditors.

- Identify whether IS comply with legal acts;

Auditor has to analyse or identify the main indicators of IS activity (indicators, if the management of the audited entity has not identified such). Part of IS activity is regulated by legal acts, therefore is it recommended to use the questionnaire prepared according to legal acts of the Republic of Lithuania (Annex 6). This questionnaire presents standard questions. Legal acts and questions have to be chosen by an auditor taking into consideration the topic of public audit.

- Evaluate other material information related to the use of information systems.

Example 2.

Auditor establishes that there is an inappropriate password policy in the organization, i.e., employees has his own passwords but they are openly written on stickers which are placed on computers; colleagues use each others' passwords. Division of responsibilities is formal, in reality it is not implemented (an accountant uses his own password, senior accountant who controls the others has his password, however, it is known to his colleagues).

Situation: the above mentioned risk factors provide for possibilities for abuse, i.e., to carry out operations which should be carried out only by senior accountant in his computer without informing him. In the existing environment there is a medium probability of such a situation (controls do not really function), impact for the organisation can be considerable (data could be fabricated).

⁶ Government Resolution No. 952 of 4 September, 1997 Concerning Data Protection in the State and Local Government Information Systems (Government Resolution Edition No. 2105 of 31 December, 2002).

Example 3.

Auditor identifies that all the information (data bases) is contained in servers, however, backup copies are not made. Servers are placed in premises which are located under the sanitary unit, and usually there is a concrete ceiling.

Situation: the above mentioned risk factors provide for preconditions that in case of the leakage in the server's premises information contained there could be lost without possibility to recover it. In the existing environment such probability is considerable (leakages in sanitary units occur quite often), impact is also considerable (data could be lost).

Testing of IS general controls

Audit of IS general controls is not limited to the review of documents regulating assurance of internal control. Auditor has to make sure that control measures identified in legal acts, IS policy, procedures, rules, and any other documents are really operating. To this end environment observation may be performed (e.g., observation of passing through the control post, entering the computer premises, workstations etc.) or interviews may be carried out (e.g., with managers of units, users who have different permissions, system administrator etc.). It is purposeful to make sure that having made themselves familiar with control procedures employees understand and implement them, and provide reasoned suggestions on their development to the management. It is recommended to define potential situations emerging of which may be determined by risk factors. For evaluation of the general controls it is purposeful to select **5-10** samples of every examined process (e.g., giving IS user rights, management of IS changes etc.) and to recheck them. In some cases sample size may be increased or decreased.

Evaluation of IS internal controls

Having performed analysis and testing of documents of IS general controls, an auditor evaluates status of internal control of information system. If sufficient internal control procedures are provided for and operate, and they are monitored, internal control may ensure information security (confidentiality, integrity, and accessibility)⁷. Internal control may be evaluated using Capability Maturity Model⁸ (Annex 7.). IS capability maturity may be identified evaluating all the IS internal control (giving one common score) or evaluating control of separate IS processes (giving scores for separate processes).

Making final decision on reliability of the audited data, auditors have to evaluate the fact that data reliability may increase due to duplication of some data in paper versions.

⁷LST ISO/IEC 17799 standard „Information technology. Practice code for information security management. (equivalent to ISO/IEC 17799:2000)“

⁸ Capability Maturity Model is developed using the Annex IT Systems Security Guidelines of the Commission Regulation (EC) No 1663/95 of 7 July 1995 laying down detailed rules for the application of Council Regulation (EEC) No 729/70 regarding the procedure for the clearance of the accounts of the EAGGF Guarantee Section

Results of audits of IS general controls may be used when planning IS performance audits (see Part 3).

2.2 Audit of application controls

During the audit it is usually sought to evaluate if the application controls is sufficient, if all the entries into information system are accurate, comprehensive, made in time, and people making and processing these entries are properly authorized.

Audit resources of application controls

During the audits of application software control technical IS issues are usually not analysed, therefore such audits would have to be performed by general auditors. In cases when technical issues arise, IS auditors may be asked for help.

Performance of application controls audit

Audit of application controls may be divided into three stages:

1. Analysis of documents of application controls;
2. Testing of application controls;
3. Evaluation of application controls.

Analysis of documents of application controls

Auditing application controls the following aspects are taken into consideration:

- Organization and documentation,
- Data entry,
- Data processing,
- Data transferring,
- Data output,
- Master data (data with little fluctuation, e.g., Litas/Euro exchange rate, VAT, depreciation standards).

Performing audit of application software it is recommended to use questionnaire from **Annex 3** presenting standard questions which may be freely chosen by an auditor.

Testing of application controls

Evaluating application controls an auditor should perform 1-2 comprehensive monitorings of the system operation - from data entry to obtaining of result. Making a decision about

reliability of this control, an auditor should make sure that the control was operating efficiently during all the audited period.

Evaluation of application controls

Having performed analysis and testing procedures of application controls, an auditor estimates as to how reliable applications is.

Results of audits of application controls may be used planning IS performance audits (see Part 3).

2.3 *Audit of IS development controls*

During the audit of IS development controls it is examined whether IS development, installation, legitimation, and changes are properly controlled.

Audit of IS development controls may be also an object of IS general controls audit.

Audit of IS under development may violate independence of a public auditor, therefore in each individual case it has to be thought over whether it is worth conducting such audit. In order to mitigate this risk, it is suggested to limit oneself to evaluation of IS development controls, and not of the effectiveness and efficiency of the systems themselves.

Audit resources of IS development controls

IS auditors.

Audit performance

Performing audits of IS development controls the following aspects should be taken into consideration:

- **Management of IS development:**

Auditor has to evaluate IS design standards, programming standards, testing procedures, all the IS documentation, confirmation of system's users before implementation, incorporation of internal audit, division of duties between developers and operators.

- **Management of IS changes:**

Auditor has to evaluate monitoring and training, authorization for changes, as well as documentation, passwords security, making backups of IS data, physical protection of data, rotation of positions, testing procedures, and confirmation of changes.

- **Management of IS implementation:**

Auditor has to evaluate IS testing and documentation, security of software and its carriers, division of duties among programmers, operators, and users.

IS development controls in an audited entity may be also evaluated during audit of IS general controls (see Part 2.1).

Audit of development of the developed IS is conducted following Performance Audit Manual.

3. AUDIT PROCESS OF EVALUATING IS IN TERMS OF 3Es

Audit is performed upon an assignment following the procedure established by the Auditor General.

Evaluation of IS in terms of 3Es is an area of performance audit. Audit is conducted following performance audit principles.

IS performance audit may be started on the grounds of audit results of IS general control and application software control, as well as IS performance problems identified during the Strategic Study, and development possibilities.

Public Auditing Requirements, Point 57.2.

Performance audit shall cover:

efficiency audit of the use of financial, human, and other resources including information systems; study on performance indicators and monitoring system; follow-up study on audited entity activities while eliminating detected shortcomings, as well as any other study considered by auditor as significant and appropriate for improving performance of the audited entity;

IS performance audit resources

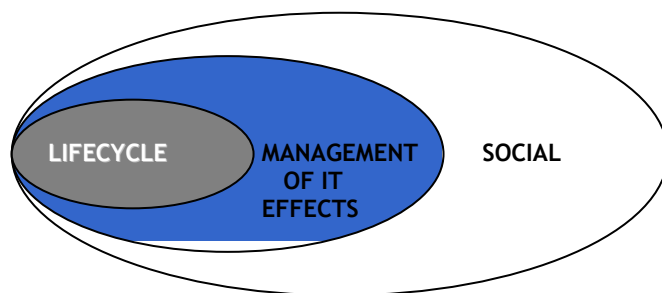
IS auditors and other public auditors; joint teams may be organized.

Performance of audit

Carrying out IS performance audit an auditor follows Performance Audit Manual.

IS performance audit may be divided into three stages (Figure 4.)⁹:

Figure 4. Stages of IS performance audit



1. IS development (IS performance audit in different stages of IS development)

During the audit IS acquisition and development is evaluated in terms of efficiency and economy. IS implementation, as well as exploitation, management, and systems updates are analysed. Issues related to IS quality and security may be analysed.

2. IS management

During the audit decisions made for IS use and the developed plans, as well as quality of the primary information used in decision-making are evaluated.

3. IS impact on the society.

Among many other issues, importance and quality of IS services are evaluated during the audit.

⁹ Introducing Performance Audit of the Use of EDP. A list of references. A Project within the INTOSAI Standing Committee on EDP Audit, The Swedish National Audit Office, 1995.

4. INFORMATION SOURCES

- ISACA IS audit standards, guidelines, and procedures,
- LST ISO/IEC 17799 standard „Information technology. Practice code for information security management. (equivalent to ISO/IEC 17799:2000)”,
- LST ISO 13335 standard „Information technology. Guidelines for security management of information technology (equivalent to ISO/IEC TR 13335:1996)”,
- COBIT Guidelines for Information Systems Audit,
- Sections relating to information systems audit of the Audit Manual of the European Court of Auditors,
- COSO Internal Control Assessment Model,
- USA GAO Internal Control Management and Assessment Methodology,
- ITIL - IT Service Management Methodology for Information Technology Infrastructure.