

INTOSAI EDP COMMITTEE
Performance Audit Seminar
Slovenia, 14 -16 May, 2001

**AUDITING IT INVESTMENTS –
RESOURCES SPENT ON IT PROJECTS
AND HOW TO CONTROL THEM**

Poland Lead Paper



Supreme Chamber of Control

AUDITING IT INVESTMENTS – RESOURCES SPENT ON IT PROJECTS AND HOW TO CONTROL THEM

Summary

The present paper presents information on public financial resources spent in various countries on information technology (IT) investment projects, with special emphasis on countries undergoing transformation of their political systems, and especially on Poland. The degree to which SAIs are interested in auditing the spending of these resources is discussed and the serious threats posed by improperly implemented IT investment projects are highlighted. The paper also contains organisational and methodological suggestions for SAIs on how to best prepare for audits of spending public resources on IT investment projects.

1. INTRODUCTION

The whole world is in the middle of an IT revolution. This revolution is especially dramatic in countries undergoing political and economic transformation. Here, the pace at which changes are taking place is the greatest and so is, in relative terms, their scale. The IT revolution reached these countries at the time when they were beginning to open up to market economy and undergoing the process of redefining the basic functions, methods and scope of activities of their state administrations (both governmental and self-governmental). Here, expectations concerning the improvement of administrative efficiency have mingled with the aggressiveness of IT

companies and with the relatively low level of technical preparedness for using IT among the administration staff. Hence, in these countries, the advance of information technology has usually been spontaneous and, judging by the example of Poland, not very efficient. At the same time, the dynamic development of the information society poses new challenges for the administration as well as for the economy and educational system.

Some people have the opinion that audits of IT investment projects should be performed according to the rules which SAIs have developed over the years of auditing conventional investment projects. This view is difficult to accept for a number of fundamental reasons. Let's consider as an example an investment project consisting in construction of a bridge over a river. All the basic functions such a bridge might fulfil can be counted using the fingers of one hand: road and rail transport, carrying pipelines for transporting water, sewage, gas etc., cable telecommunication. All these functions are obvious and generally accepted. Usually, analysing the need for constructing a bridge is also an easy task. The situation is different in the case of IT an investment project. The multitude of functions which may potentially be implemented, the diversity of reports which may be generated, the various ways of ensuring future development - all these factors make an IT investment project a far more complex task. In the case of countries undergoing transformation, where IT investment projects in the administration are usually pioneer projects in this field, an additional very important aspect is present, since regardless of whether the IT project is concerned with the activities of the entire unit or only of its part, it is necessary to first perform a thorough review of the mission, strategic goals and methods of the unit in question. In the case of institutions, which have functioned for decades basing on conventional methods, building an information system (or the foundations of an information system) often means redesigning and rebuilding the whole institution from scratch.

In these circumstances, it is difficult to overestimate the role of the SAI. SAIs should undertake audits of IT investment projects in a systematic and planned manner and not limit themselves to care for rational spending of public funds, but also encourage the development of good practice in initiating and implementing such investment projects.

2. Auditing IT investment projects by SAIs.

When preparing the present paper, the Supreme Chamber of Control (SCC) approached 24 Supreme Audit Institutions (Albania, Argentina, Armenia, Bulgaria, Brazil, Chile, Croatia, Cyprus, the Czech Republic, Egypt, Estonia, Ghana, Greece, Hungary, Kazakhstan, Kirgistan, Lithuania, Latvia, Portugal, Russia, Rumania, the Slovak Republic, the Ukraine, Venezuela) for information on audits of IT investment projects. In our questionnaire we focused on SAIs of countries undergoing transformation and those countries which have made particularly quick civilisation progress in recent years and hence witnessed a dramatic increase in public spending on IT. We did not send the questionnaire to highly developed countries (such as Canada or the UK). In particular, we asked for the following information:

Q. 1: How much do government institutions of your country spend on new information and computer systems as well as on modernisation and improvement of the existing ones in the years 1995 - 2000.

Q. 2: What were the big computer system projects of the value greater than 20,000 USD and how many of them were successfully implemented.

Q. 3: Does your country have some standards concerning the preparation and implementation of IT investment projects.

Q. 4: Did you carry out performance audits of such investments and what were the conclusions (number of reports made and the most important audit findings)

Q. 5: What kind of methodology do you use for these audits

Q. 6: What were the reasons of the projects' failures (if any)

Q. 7: Could you shortly describe your experience and basic principles applied during the preparation of audit programs concerning IT investment projects.

Q. 8: Do you have a special unit (division) for auditing IT investments.

We received answers from 9 SAIs (Cyprus, Estonia, Lithuania, Portugal, Slovakia, the Ukraine, Hungary, and Venezuela); however, only five SAIs provided relatively comprehensive answers. Obviously, such information does not permit us to

formulate generally applicable statements; however, it is sufficient to reflect upon and draw certain conclusions. The collected answers are shown on the Table 1 where:

a)

- Cyprus - 16 projects valued more than USD 20,000, 15 - successfully
- Estonia - there have been about 350 IT development projects in the public sector started between 1994-2000. The total costs of 200 of them are more than 20,000 EUR.
- Hungary - there no detailed - project data concerning capital IT systems expenditures that was spend by the budgetary institution. In the framework of the central government IT infrastructure development target program was 13 projects exceeding USD 20,000, and there was establishment and then modernisation of the operation of the Hungarian State Treasury among them.
- Latvia - in the course of 4 years (1997-2001) 238 projects were submits, and 122 projects were turned down. 10 projects are now in progress and the value each of them is greater than USD 20,000 it is Fe. Project of Development of Information Technologies at the State Revenue Service,
- Portugal - 53 big IT systems in the main points of public affairs along: Justice Ministry, Ministry for Internal Affairs. Ministry for Agriculture, Health Ministry, Ministry for Foreign Affairs, Finance Ministry, Ministry for National Defence, Presidency of the Council of Ministers
- The Ukraine - several projects were launched and executed from 1993 till 1997 such as Parliament, National Bank of Ukraine, Ministry of Economy, State Proper Fund, Antimonopoly Committee etc. Mostly projects were financed by the World Bank, European Bank of Reconstruction and Development, USAID etc without suitable state co-ordination

b)

- Cyprus - there are Laws and Detailed Regulations relating to the procurement procedure. The system purchased should meet international standards on hardware, software and product quality. ISO 9000 series, PRINCE and SSADM are used.
- Estonia - the guidelines of planning the costs for IT systems was complemented by Ministry of Finance every year until 1999. This established principles are no longer expedient nowadays when the primary needs for information processing have been fulfilled. In 2000 the government has initiated the reorganisation and improvement of investment planning and assessment.
- Hungary - Act XL. /1995 on Public Procurement and related other statutory regulations. ITB regularly prepares recommendations for government institutions on the IT Issues
- Latvia - Latvia State Standard 65-74,1996. Information Technology. Programme engineering. Documentation of software testing; Low "On public procurement", regulations of the Cabinet of Ministers and instructions of the Ministry of Finance
- Portugal - the general rules governing the co-ordination of the acquisition and implementation of the information technologies by Public Administration and the rules governing the leasing or acquisition of IT equipment or services are established by law. Their are under special responsibility of the Finance Ministry's Information Technology Institute.
- The Ukraine - the Law of Ukraine "On the National Program of Computerisation" that was passed in 1998. The State Committee of Communication and Computerisation is a State agency, which

is responsible for the state policy implementation in the sphere of computerisation.

c)

Cyprus

- project was too complicated to be effective, non-specific terms in the relevant contracts, lack of proper planning, poor specifications and user's needs analysis, inability to envisage at the initial stage of the project the project's size, changes in the legislation and changes in the circumstances requiring further alterations during the development stage.

Estonia

- during the preliminary audit the following reasons of projects' failure was found: the deadlines and planned costs are not kept, the lack of specifying the goal during implementation, the changes of reorganisation or legislation, too insufficient analysis of needs, missing of complex and systematic approach will setting the targets, lack of competencies among the management, insufficiency of monitoring and control over the projects

The answers received indicate that some of the SAIs did not have information on the sums spent by the state in connection with the introduction of new information systems in the period in question (Slovakia, the Ukraine), and in the remaining countries the sums spent on this purpose varied from 39,000,000 USD (Cyprus) to 700,000,000 (Hungary).

Tab.1. Answers the questions.

Quest. No:	Cyprus	Estonia	Hungary	Latvia	Poland	Portugal	Slovakia	The Ukraine	Venezuela
1. (USD)	39,000,000	about 56,000	about 800,000,000	(1997-2000) about 23,000,000	about 200,000,000	(1996-1998) about 500,000,000	No data	No data (about 72,000 in 1999)	No data
2.	see below ^{a)}	see below	see below	see below	see Paper	see below	No	see below	No
3.	Yes ^{b)}	Yes, but now it needs a lot of improvements	Yes	No	No	Yes	No	Yes from 1998	No
4.	No	Yes – 1	No	No	Yes –7	No	No	No	No
5.	Like for other audits	No – it is on the way.	No	No	Yes see Paper	Like for other audits	No	No	No
6.	Incomplete and non-specific terms ^{c)}	to insufficient analysis of needs ^{c)}	no data	no data	see Paper	not applicable	No	No	No
7.	No	no data	No	not yet - project team for Auditing IT Systems was set up.	see Paper	not applicable	No	No	No
8.	No: this is a responsibility of the Computer Service Section	no data	No	No	No	No; a project team for auditing IT Systems was set up.	No	No	No

It is worth to note, that e.g. according to data from the Ukrainian SAI, many projects vital for the interests of the State implemented between 1993 and 1997 were financed by the World Bank, the European Bank for Restructuring and Development, TACIS and USAID programmes, etc. These projects were concerned with computerisation of the Parliament, the National Bank of the Ukraine, the Ministry of Economy, the State Treasury, the Anti-monopoly Committee, the State Tax Administration, the State Statistical Office etc. They were not co-ordinated by the State and the Ukrainian Chamber does not have any data about them. This situation is not an exception and, as Poland's experience discussed below indicates, the SAI's mandate to audit the spending foreign aid plays a fundamental role in ensuring that this aid is well used.

In all countries which responded to the questionnaire, IT projects worth more than 20,000 EURO constituted the majority of projects (for example in Lithuania they constituted 200 out of 300 projects implemented in the period considered) and were concerned with issues vital for the proper functioning of the state, such as taxes, state banks, social security, maintaining records of state property, the judicial system and national defence.

Countries, to which the questionnaires were sent, seldom had detailed legal regulations concerning designing and implementation of information systems in the administration and in state entities. The only exceptions were: Portugal, where appropriate legal regulations concerning purchase of IT equipment and services had been introduced and where the Finance Ministry's Information Technology Institute was entrusted with the responsibility for promoting, development, application and operation of information systems and IT by the state administration; Latvia, where appropriate regulations have been in place since 1999; and Cyprus, which uses SSADM (Structured System Analysis and Design Method) for project planning and PRINCE (Project in Controlled Environments) for project management as governmental standards. Hence, the reasons for failure in the implementation of such projects, or for making very expensive adjustments, are mainly attributed to incomplete or insufficiently accurate analysis of the actual needs of the future user and to overlooking future changes in the legislation in the planning phase, which results in the need to introduce very significant changes in the development and

implementation phases of the final project. Poor responsiveness and insufficient understanding [between the contractor] and the future user are also important factors.

None of the SAIs that responded to SCC's questionnaire have conducted performance audits of development of information systems or developed auditing standards in this field (the only exceptions are: Latvia, where a five-year plan of implementation of international standards, covering information system auditing standards, but not IT investment project auditing, was prepared in co-operation with SIGMA experts and approved by the SAO Council on December 15, 1999; and Poland, where a method of auditing of IT investment projects has been developed). None of the SAIs has established within its structure a separate unit assigned with the task of auditing IT investment projects or IT systems.

Answers provided by the SAIs allow us to conclude that, in most cases, in countries, where changes associated with the IT revolution are particularly rapid, SAIs pay very little attention to sound spending of funds on IT investment projects. However, four performance audits of IT-applications, performed by the Portuguese Court of Auditors should be noted here as exceptions.

3. Auditing IT investment projects in Poland

Although 10 years have already passed since the beginning of the transformation, it would be difficult to describe the computerisation of public life in Poland as successful. The process of implementing IT went most smoothly, although not without problems, in the banking sector. However, despite numerous undertakings, computerisation of such important areas as the tax system, the customs system, social security, the state budget or the judicial system, has not been completed yet.

Poland's central administration alone spent about 200,000,000 USD (including 56,000,000 USD in foreign aid grants) on majors IT investment projects (worth over 20,000 EURO) in 1995-1999. Obviously, these sums do not represent all spending on IT in the public sector. Resources spent by entities subordinate to the state

administration, as well as by local governments and state-owned enterprises, such as the Polish State Railways [*Polskie Koleje Państwowe*], should be added to the above figures.

Foreign aid grants were mainly appropriated for the purchase of hardware and standard software, on development and extension of local, municipal and wide area networks as well as on financial support for public administration units implementing IT projects. These resources were spent among others on the following investment projects:

- National Labour Inspectorate – supporting tools (software) for development of elements of the SYSPIP information system, development of a document management system and training courses and IT equipment for inspectors – 747,000 USD;
- Ministry of Agriculture – integrated agricultural market information systems and land register system (GIS) – 1,390,000 USD;
- Chief Statistical Office – deliveries of hardware and software for modernising the CSO'S IT systems for statistical data processing and transfer as well as development and extension of local and wide area networks – 39,590,000 USD;
- Chief Customs Office – implementation of certain information systems supporting the Office's work – 5,670,000 USD.
- Ministry of the Interior and Administration – development of the Central Register of Vehicles and Drivers [*Centralna Ewidencja Pojazdów i Kierowców – CEPiK*] – 1,000,000 USD;
- National Fund for Environmental Protection - Regional Geographic Information System, financial support for other IT projects and purchase of IT equipment – 1,600,000 USD.

IT products financed out of these resources, with the exception of the CEPiK system, are being used for the intended purposes. The CEPiK system has not been approved for operation due to its non-compliance with the Constitution of the Republic of Poland.

Listed below are the largest IT investment projects financed by the central administration of the Republic of Poland out of the state budget in 1990 – 1999:

- Computerisation of the tax system in Poland (POLTAX System; USD 80 million)¹;
- Information systems for the customs administration (about USD 51 million);
- Computerisation of employment offices and of the welfare office network (USD 66 million);
- Maintaining science's IT infrastructure (value: about USD 47 million);
- Comprehensive information system for the Social Security Office (total cost: USD 200 million);
- Computerisation of the Polish Post [Poczta Polska];
- Computerisation of State Health Service Management Units.

3.1 SCC's audit of selected IT investment projects - key findings and recommendations; results of implementation of recommendations.

Computerisation of the tax system in Poland – the POLTAX System.

The contract for the implementation of the above investment project, concluded between the Ministry of Finance and a French contractor in 1990, covered designing, development, acquisition, start-up and maintenance of a modern and effective integrated computer system for handling income tax and value-added tax (VAT), meeting the needs of the Ministry of Finance. Furthermore, the contract provided that the Contractor would deliver the hardware and software and the necessary services. June 15, 1991 was set as the deadline for final acceptance of the system. The contract's net value was estimated at FF 162 million. The system was to consist of four applications. Between July 1990 and June 1995, the deadline for final acceptance of the system was extended eight times by amendments to the contract. Moreover, the price was also increased significantly, up to USD 80 million, despite a

¹ The value of 100 million USD refers to the contract. The total cost of the POLTAX System must include the immense cost of completing the system following termination of the contract; the Polish party covered this cost.

reduction in the scope of work. The Central Register of Tax-Payers and key user functions based on this register were excluded from the scope of the POLTAX System by annexes to the contract. Other simplifications were also made. When the Contractor completed the software for the POLTEX System, acceptance tests were carried out. The tests demonstrated that although the software had been developed in accordance with the basic document of the system design, it did not function properly and did not suit the user's needs. Hence, the software was not put into operation. In 1995, a team of Polish experts took over the work on the POLTAX System and has been working on it up till now.

The Supreme Chamber of Control has not audited this IT investment project as such; however, in the course of numerous audits of the activities of the Ministry of Finance, tax offices and tax chambers, performed in 1991-1994 throughout Poland, the SCC identified the basic flaws in the execution of the POLTAX System contract, finding the activities of the Ministry of Finance in this field to be inefficient and ineffective and naming those responsible for these flaws. Among others it was found, that:

the deadline for completion of the project, specified in the main contract, i.e. June 15, 1991, was unrealistic, as legal acts essential for proper implementation of the information system, i.e. the personal income tax act, the goods and services tax act and act on the register of taxpayers, were adopted by the Sejm [Lower House of Poland's Parliament] in July 1991, January 1993 and October 1995, respectively;

in implementing the contract, the Ministry of Finance made serious organisational mistakes; for example, it did not formulate a uniform concept of how the system should function ultimately; it gave up on checking the quality of the contractor's work by refusing to accept free-of-charge assistance in quality control offered by the governments of the US and Switzerland and not resorting to standard, professional and independent quality control on behalf of the MoF;

the MoF agreed to start the implementation of the contract from the delivery and installation of hardware, two years before work on application software began – a common example of gross wastefulness, which resulted in spending too much money (over 84%) too early as well as in losing the benefits connected with the

contractor's guarantee and in technical ageing of the equipment which was either lying useless in storerooms or was used for purposes other than originally intended. Deliveries of equipment were premature and not adequate to the actual requirements of the system and eventually resulted in the need to spend significant additional sums on building a new hardware base of the system. In 1995, the MoF signed an agreement terminating its contracts with the contractor, which made it impossible for Poland to claim the return of the sums spent on these contracts.

When auditing the implementation of the state budget and the activities of tax chambers in 1997-1999, the Supreme Chamber of Control found that the basic objective of the POLTAX System has not been achieved in full and recommended that the MoF implement the System in a form permitting it to handle the tasks of the tax administration in a comprehensive way. Two additional modules of the POLTAX System were implemented by the end of 1999; however, work on the system has not been completed yet and the scope of implementation of the system still does not permit the tasks of the tax administration to be handled in a comprehensive manner.

Information systems for the customs administration:

a) Information System for the Warsaw Airport Customs Office (ACO) – a pilot project for COs throughout Poland

The USD 700.000 contract for the development of the system was concluded in March 1992, and implementation was to be completed by August 1993. The main objectives of the project were i.a.: to computerise the procedures of the Warsaw ACO; to simplify the processes of intensive control and tax collection; to prepare the infrastructure of the ACO for eventual connection with the Main Customs System; to interface with the external organisation of the Airport; to develop software for data and statistical information management and matching; and to build the infrastructure necessary for transferring this data to the future central nation-wide system.

As of June 1997, the system that had been put into operation did not satisfy all the needs of the ACO.

The SCC conducted two audits of the execution of the contract for the development of this information system: in 1993 and in 1996. Upon completion of the 1993 audit, the SCC recommended to strengthen supervision over the implementation timeschedule and to conduct an analysis of the system's functionality with regard to the ACO's existing software and hardware. The audit performed in 1996 showed that the SCC's recommendations had not been implemented and that the Chief Customs Office had not met its commitments. In the SCC's judgement, the way in which the contract and an annex to the contract were implemented, i.a. the deficiencies and faults in the customs application and its documentation and months of delay in delivering final products – indicated that the contractor did not have sufficient technical expertise to develop the system.

According to the SCC, the reduction of the functional scope of the system, approved by the CCO in the annex to the contract, fell short of the original assumptions made by the CCO and could not have led to the intended end result, i.e. to full computerisation of the ACO.

b) Nation-wide Information System for the Customs Administration – „OSIAC”

The USD 50 million contract for the implementation of this investment project was concluded in February, 1995 and included i.a.: analytical work and design of the information system; delivery of equipment, i.e. hardware, system software, software tools and diagnostical software; development of applications and; integration of the information system as a whole. The investment project has never been implemented. After three years, the parties dissolved the contract without claiming against each other.

The SCC performed an audit of the execution of the contract for the development of the OSIAC System between November 1996 and June 1997. According to the SCC, the CCO had not been diligent in selecting the contractor. During the tender procedure, it failed to properly assess the German contractor's preparedness for the implementation of the project and selected a contractor, who did not have sufficient

expertise to develop the OSIAC System. The audit established that supervision of the works by the CCO was insufficient, that the CCO failed to properly co-ordinate its co-operation with the contractor and that the procedures provided for by the contract were neglected. The fact that the CCO was not diligent in these matters prevented it from successfully claiming contractual fines for improper execution of the contract. More importantly, several years have been wasted and so far, Poland's customs services do not have a comprehensive information system, which is extremely damaging for their effectiveness in a period of dynamic growth of trade.

c) Computerisation of the General Customs Inspectorate (GCI), a department within the CCO

In December 1994 the CCO concluded a contract for the development of a separate information system for the General Custom Inspectorate (GCI) by the end of June 1995. The value of the contract, including a later annex, was zł 3,7 million, and the value of an additional contract which followed was zł 272 thousand. In July, 1995 the contractor delivered hardware, equipment and software tools, which were not integrated into an operational Tele-information system, because the GCI did not receive a complete, operational Tele-information system from the contractor.

In the period between November 1996 and June 1997, the SCC conducted an audit of the execution of the contract for the development of the OSIAC System for the GCI. According to the SCC, the key factors in the failure to develop a system for the GCI were the lack of reliable assumptions and technical and organisational analyses as well as insufficient supervision by the Management of the CCO and incorrect methods of implementation. The Office had spent resources on IT products, i.e. software, hardware and auxiliary equipment and not gained a functioning Tele-information system supporting the activities of the GCI in return.

The SCC's audit findings allowed to establish that none of the above three projects concerned with computerising the customs administration, has yielded the intended result, i.e. an operational information system for the CCO. In the case of the second contract, the CCO made payments for the delivery of hardware, tele-information equipment, instrumentation, cabling and applications and software tools in the

amount of zł 5,3 million, i.e. about EURO 1,262 million, but did not receive an operating information system. The CCO failed to develop a uniform, general concept of rational implementation of IT investment projects. The CCO's employees responsible for co-ordinating works under the said IT projects failed to live up to the specific technical and organisational requirements of the tasks associated with those projects, especially tasks connected with proper and exhaustive analysis and development of comprehensive concepts of the systems as well as tender procedures, successful negotiating of non-standard, specialist IT contracts and effective supervision of the implementation phase. The audit findings led the SCC to formulate the following recommendations addressed to the Chairman of the Chief Customs Office:

With regard to the audit of the investment project a):

- To immediately implement the delivered application software, ensuring that it is fully utilised and to ensure full and proper utilisation of the hardware in possession of the ACO.
- To assess the actual feasibility of supplementing the application software so as to computerise the remaining tasks of the ACO.

With regard to the audit of the investment project b):

- To consider, in the light of contractual provisions, the undertaking of formal/ legal measures aimed at terminating CCO's contract with a contractor who proved to be unreliable and unable to perform the task;
- To exact payment of zł 3 million for the CCO on basis of an unconditional guarantee provided by a guarantor according to the provisions of the contract concluded with the contractor;

- To exact payment by the contractor to the CCO of the penalties due under the contract for late delivery.

With regard to the audit of the investment project c):

- To eliminate the causes of malfunctioning of the Tele-information system and render it fully operational.
- To insure computer equipment received as a result of implementation of the customs Tele-information system.

With regard to all three investment project contracts, the SCC recommended that the CCO prepare a detailed report on the implementation of these projects, including i.a.:

- evaluation of the performance of employees responsible for co-ordination and supervision of the individual contracts;
- evaluation of the Management's decisions concerning official and legal sanctions against persons responsible for irregularities identified in the tender procedure, negotiation procedure, implementation of the contracts and in payments made out of the CCO's resources for delivery of incomplete and malfunctioning information systems.

Acting on the recommendations of the SCC, the CCO terminated the contract with the contractor of the OSIAC System and received the sum of USD 800 thousand, due on basis of the unconditional guarantee, granted by the guarantor according to the provisions of the contract concluded with the contractor.

At that time, the audit of the CCO's IT investment projects was the largest audit performed by the SCC in this field. As a result of the audit two basic conclusions were made: one concerned the government administration and the second concerned the SCC itself. In order to reduce or eliminate fundamental errors and

irregularities associated with activities aimed at computerising state administration offices, the SCC considered it purposeful for **the Board of Ministers of the Republic of Poland or the Minister of Interior and Administration to adopt basic assumptions and procedural methods which would be binding for state administration bodies and their subsidiaries in initiating and implementing IT investment projects.** This recommendation was accepted for implementation; however, no such document has been issued up till now. **As a matter of fact, a regulation on this subject has been drafted, but it has not yet been published as binding legislation.**

The second principal conclusion is that the SCC itself recognised that it was not sufficiently prepared to conduct thorough audits of IT investment projects. Decisions to take appropriate measures were taken, with priority for development of a methodology of such audits. A methodological guide on this subject was prepared in co-operation with a consulting firm in 1998 (page 30).

Computerisation of the employment offices network and of the social welfare offices network – the ALSO Project

The contract for the implementation of the ALSO Project (value: USD 6 million) was concluded in 1992 and covered development of a general plan of computerisation, system design and supervision over the implementation and extension of the system. Sources of financing of the Project included a World Bank loan, the PHARE Programme and the budget of the Ministry of Labour and Social Welfare (MLSW).

Following a negative opinion on the implementation of the project, given by the SCC in 1994, the Ministry reviewed the implementation of the ALSO Project and, having identified numerous technical flaws, concluded that the usefulness of the work completed so far was negligible. As a result of this evaluation, implementation of the project in its original shape was discontinued and a decision to terminate co-operation with the contractor was taken. According to a new concept of continuation of the ALSO Project, adopted by the Ministry's management at the end of 1994, the entire project would be implemented by a team of Polish designers located at the IT

Office of the MLSW. It is worth to note that this was the second case of a large project during which it became necessary terminate a service contract with a foreign contractor.

The document determining the way of implementing the ALSO Project, approved by the management of the MLSW on December 27 1994, provided that the project would consist of three interrelated sub-projects, i.e. the Employment office System – PULS, the Social Welfare System – POMOST and the MLSW Support System.

An audit carried out by the SCC indicated that the PULS System met the acceptance criteria and could be put into operation; the contractual deadline for rendering the PULS system operational was November 30, 1999. The deadline for the implementation of the POMOST System has not been not met and system itself has failed tests. At present, the PULS System is being implemented in Employment offices (LOs) throughout Poland.

The audit performed by the SCC in 1996 indicated that key elements of the ALSO Project were being properly implemented by the Polish team and project objectives were consistent with the basic policies of the MLSW. However, it was also found that no strategic analysis had been performed prior to launching the ALSO Project. This concerns in particular the relevant functions of labour and social welfare offices, the scope of information necessary for performing these functions, the locations at which these functions are performed, information flow etc. The lack of a strategic analysis resulted i.a. in the failure of the management of the MLSW and the National Employment office (NLO) to decide on the method of servicing loans from the Labour Fund and `the State Fund for Rehabilitation of the Disabled, for the unemployed to start their own businesses and for employers to create new jobs. The lack of this decision made it impossible for the ALSO design team to develop the loan management and servicing module. The Project did not include development of a model of the software nor an obligation to use tools permitting to significantly simplify the process of agreeing the detailed design with the users and to facilitate testing the consistency of the product with the users' expectations.

The audit findings referred also to the schedule of implementation of the ALSO Project. According to the timeschedule of December, 1994, the Project was to be completed in July, 1996; however, this deadline was extended until the first half of 1998 (Employment office – February, 1998; Social Welfare Offices – May, 1998). At the same time, the duration of the individual sub-projects was significantly extended. Reasons for extending the time required to complete the individual subprojects included delays in selection and purchase of software for the LOs and SWOs. The process of procurement of hardware for the SWO component was also delayed.

One of the reasons for these delays in the implementation of the ALSO Project was the poor functioning of the unit responsible for co-ordinating activities connected with the World Bank loan and especially the poor handling of procurement of supplies and services and insufficient supervision of the deliveries. Another factor adding to the delays was the time taken by the management of the MLSW as well as the World Bank to make decisions approving the selection of suppliers of hardware and software.

In 1999, the SCC performed another audit, this time concerning utilisation funds, including the World Bank loan, for the implementation of a project called „Promotion of Employment and Development of Employment Services”, at the MLSW, the NLO and at 27 unit subordinate to the NLO. Examination of the implementation of the PULS and POMOST contracts revealed that both of them were behind the contractual schedule and delayed in relation to the delivery of computer equipment which had taken place in 1998. The PULS system was found to satisfy the acceptance criteria and was ready to be put into operation. According to the contract, this was to take place on November 30th, 1999. On the other hand, the contractual deadline for the completion of the POMOST system had not been met and the system had failed the appropriate tests.

The reasons for the delays were as follows:

- adoption of an unrealistic implementation timeschedule
- significant changes in the legislation and administrative structure of the country during implementation

- faults in the software and organisational problems, such as gaps in training programmes and flaws in the delivery of documentation and in installation of equipment at the users' offices

Comprehensive information system for the Social Security Office

Computerisation of the SSO is undoubtedly the largest project of this type in Poland and one of the largest in Europe. The value of the contract concluded to implement this task exceeds USD 200 million. In 1999-2000, the SCC audited the preparation and implementation of this project.

The need to develop a comprehensive information system for the SSO became apparent when the Sejm adopted the „Social Security Reform Programme”. In May 1996, the SSO prepared a document called „Comprehensive Information System for the SSO (CIS SSO) – Conceptual implementation plan”. The document stated that the implementation of the information system is a precondition for the implementation of the envisaged reform based on monitoring individual social security accounts. The document prepared by the SSO did not contain a definite concept of the CIS or any cost estimates; rather, it was a set of statements reflecting the SSO's expectations with regard to the future concept of the system. The document named factors which may negatively affect the implementation of the CIS, including i.a. lack of a unit within the institution, capable of undertaking the task; lack of expertise and impracticability of employing specialists; short implementation timeframe; impracticability of operating and modernising the system without external assistance and; lack of compatibility between existing local networks. These circumstances led to the decision to resort to a tender procedure and hire a contractor to design and implement the system.

On October 10th, 1997, a contract for the design and implementation of the CIS SSO and for delivery of operational software tools to the SSO was concluded with the Main Contractor (MC). According to the contract, a 19-module system was to be developed. The duration of the contract is set at 10 years, i.e. until October 10th 2007. The contract stipulates that this period may be extended by another 5 years, with regard to maintenance services connected with the CIS; however, both parties

have the right to refrain from this option. The contractual time for the implementation of the CIS SSO (i.e. design, development of modules and putting them into operation at the headquarters and all branch offices and inspectorates of the SSO) was 4 years and 4 months, i.e. from November 1st, 1997 until February 28th, 2002. The original contract was modified by two annexes, which significantly increased the scope of the project and changed the system's architecture.

In the SCCs opinion, the contract, and especially the annexes, which followed, contain solutions, which are detrimental to the system. An audit of the project carried out by the SCC revealed the following major deficiencies and irregularities:

1. The tender procedure to select the MC and contract the implementation of the CIS SSO was carried out despite the fact that there was no concept of the whole system, the relevant basic legal acts had not been adopted and no decisions had been made concerning the legal status of the SSO or the way of financing of the project.
2. The SSO breached the provisions of the Public Procurement Act during the tender procedure to select the MC and contract the implementation of the CIS SSO and by signing Annex 2 to the contract concluded on October 10th 1997.
3. The provisions of the contract with the MC did not safeguard the interests of the SSO in a satisfactory manner.
4. The contract with the MC stipulated unrealistic deadlines for the implementation of the CIS SSO.
5. Annex No 2 to the contract introduced the following fundamental changes concerning the subject of the contract:
 - the timeframe for the implementation of the social security reform was compressed and consequently, the deadline for putting the system into operation was also shortened

- the number of functions to be performed by the system was drastically increased, resulting in an increase of the number of modules from 19 to 216
 - the system's architecture was changed from decentralised to centralised
 - the number of control points was increased from 142 to 1091
 - the pilot implementation phase was cancelled due to time constraints; the annex also excluded any independent external auditors from participating in the acceptance of the individual outputs of the project
6. A centralised model of the CIS SSO was adopted, even though it had been rejected by independent experts in the negotiation phase; possible consequences of this include a collapse of the entire social security system in Poland, a delay in the implementation of the CIS SSO and failure of the social security reform.

Developed as a result of the audit carried out by the Supreme Chamber of Control in, the risks metrics related to the system implementation accordance with Annex 2 yielded the result of 86 points, placing the project in the area of extreme risk with the impossible to define margin of safety.

An external expert was asked to produce the risks metrics on the basis of "Principles and methodology of IT investment audits" (see Chapter 5.1). Risks related to the project implementation were assessed in five areas according to risk factors to which specific values were ascribed. The maximum score was 100 points.

The detailed analysis yielded the following risk values in particular areas:

1. Technical risk – 16 points (medium).

8 risk factors, e.g. clarity of requirements, complexity of telecommunications structure, up-to-date technology, were analysed.

2. Planning risk – 17 points (high).

4 risk factors, e.g. team qualifications and experience, critical time conditions, were analysed.

3. Profitability risk – 24 points (high).

6 risk factors, e.g. liquidity of costs, liquidity of requirements, relation to the institution's IT strategy, were analysed.

4. Organisational risk – 12 points (medium).

6 risk factors, e.g. territorial and organisational distribution, users' experience in co-operation with designers, the institution's size, were analysed.

5. External conditions risk – 17 points (high).

8 risk factors, e.g. a number of sub-suppliers, a necessity to hire additional personnel, dependence on alteration of existing laws, were analysed.

A maximum number of points was given to the factor "dependence on alteration of existing laws", which reinforces the view, built on the basis of previous experiences of the Supreme Chamber of Control, that the changeability of laws (natural in the countries undergoing the transformation of a political system) is one of the most important risk factors in the area of IT systems.

The grave errors made in the planning and implementation of the information system for the SSO resulted in budgetary losses amounting to about USD 2 billion in 1999 alone, in undermining public confidence in the SSO, which is a state institution, and in immeasurable losses incurred by entrepreneurs, who have to put up with all the deficiencies of the poorly designed and implemented system.

The audit demonstrated that the actual cost of the project would be about two times higher than originally anticipated.

In view of the audit's findings, the SCC instructed the Chairman of the SSO i.a. to take the following measures:

- to modify the way in which the project is organised and managed, i.a. by introducing dynamic management, so as to increase the chance of success in the implementation of the CIS SSO
- to identify interdependencies between the different tasks, critical task implementation deadlines and priorities and critical paths
- to develop alternative action plans which could be used if project implementation comes under threat
- to secure the funding necessary to implement the project
- to appoint an independent auditor so as to ensure proper project quality assurance
- to develop a detailed plan of financing the Project

4. Maintaining science's IT infrastructure

Major investment projects financed under this heading were concerned with:

- development and extension of local area networks (LAN) – USD 18.000 thousand,
- development of city area networks (CAN) – USD 17.000 thousand
- procurement of equipment of high-yield computer (HYC) centres for universities – USD 12.000 thousand,

Between October 1997 and February 1998, the SCC performed an audit at the Scientific Research Committee (SRC), covering i.a. performance of tasks associated with the development and maintenance of science's IT infrastructure. During the audit, regularity of disbursement of funds for high-yield computers was examined and the following was established:

- the SRC had directly spent funds appropriated for the procurement of high-yield computers in the amount of USD 14.000 thousand, thus violating article 15 point 2 of the Act on the Scientific Research Committee, which limits the SRC's mandate in this area to awarding grants to interested scientific and research and development institutions; technically, budget resources should be transferred to the account of the given unit.

- in the process of procurement of high-yield computer equipment the SRC had violated the provisions of the Public Procurement Act
- contracts had been concluded without due regard to formulating terms and conditions crucial for establishing the contractors' responsibility for delays, i.e. delivery deadlines had not been specified, which made it impracticable to apply provisions concerning daily penalties for delays
- the SRC failed to ensure proper supervision of the implementation of these contracts, even though very significant funds were involved. This is supported by the fact that the SRC did not have the full documentation required to confirm that the contracts had been implemented; this concerns in particular the results of equipment acceptance tests. Documents confirming that the equipment had been registered as fixed assets of the relevant institutions were also missing. These gaps in documentation began to fill in only during the audit. Without these documents, the SRC did not respond to delays in the execution of the contracts and in taking the equipment over by the relevant institutions, as in the case of high-yield computers. The delays were caused by the fact that, as pointed out earlier, the SRC had financed the procurement of equipment directly, without having sorted out the question of transfer of property rights to the HYC centres.

In view of the audit's findings, the SCC instructed the Chairman of the SRC to:

1. Harmonise its procedures of procurement of high-yield computer equipment for scientific and R&D institutions with the provisions of the Act on the Scientific Research Committee of January 12th, 19991 and the Public Contracting Act of June 10th, 1994 or to bring about appropriate amendments to these acts.

2. To finalise steps taken during the audit and aimed at resolving the issues of transfer of ownership rights to HYC equipment which the SRC had donated to the relevant institutions. List of important irregularities disclosed by the NIK in the course of audits of IT investments shows Table 2. This table clearly indicates that:

- Risk analysis, risk level or risk management schemes were not developed for any of the above mentioned IT investments.

- Investments where objectives and users requirements were not defined or incorrectly defined before start were concluded with total or partial failure.

- Lack of strategic analysis to be concluded before the IT investments were initiated made it impossible to correctly define investment aims and users requirements, or properly take into account the legal regulations necessary to define tasks that the IT investments were expected to perform.

It turns out that carrying out strategic analysis makes a necessary (though not sufficient) condition to complete the investment successfully, since it is the analysis results that determine the correct definition of subsequent IT undertakings as well as, among others, the way to monitor investment realisation and the deadline by which the investment should be completed.

Table No 2 List of important irregularities disclosed by the NIK in the course of audits of IT investments

	Type of irregularity disclosed								
	1	2	3	4	5	6	7	8	9
Name of investment	Lack of strategic analysis before starting investment	Incorrectly defined (or not defined at all) aim and users requirements	Lack of or amendments to legal regulations necessary for defining the tasks that the IT system should fulfil	Incorrectly defined (or not defined at all) mechanism of auditing investment realisation	Failure to meet investment contract conditions	Selecting incompetent contractor	Selecting unrealistic deadlines (for the whole of investment or its particular stages)	Failure to observe The Public Procurement Act	Total (T) or partial (P) failure to achieve the aim of investment
POL TAX	Y	Y	Y	Y	Y	Y	Y	*	I T/II P (**)
CCO	Y	Y	N	Y	Y	Y	Y	*	P
OSI AC	Y	Y	N	Y	Y	Y	N	N	T
GCI	Y	Y	N	Y	Y	Y	N	*	P
ALSO	Y	Y	Y	Y	Y	Y	Y	*	I T/II P (**)
SSO	Y	Y	Y	Y	N	N	Y	Y	P
SRC	-	N	N	Y	Y	N	N	Y	aim achieved

Y=yes, N=no,

(-) Not audited,

(*) Prior to Public Procurement Act coming into life

() I –investment implementation incomplete or failed**

II –investment started again in different shape.

4. Public Procurement and IT investments in Poland

The Public Procurement Act, which regulates the principles of contracting goods and services by public entities, has been in force in Poland since 1995. However, the results of various audits indicate that this act is not well adapted to IT investment projects. It's main weak points include the following:

- there is no precise definition of the term „domestic produce” with regard to information technology, which makes it very difficult to apply „domestic produce preferences” in practice
- the requirement that the public procurement procedure must result in defining the contract price makes it more difficult to develop large integrated computer systems.

Results of public contracting procedures are published in the Journal of the Public Procurement Authority. According to this source of information, 367 public procurement procedures took place in Poland in 1998-1999, resulting in contracts worth about USD 66 million in total. It is symptomatic that out of all these tender procedures only 39, worth USD 14 million in total, did not concern procurement of computer hardware, while information systems comprised only 4,3% of all supplies.

Our studies show that public projects have often been split by announcing in one budget year several smaller tenders concerning the same supply or service and selecting new contractors each time. For instance, in 1998 the Ministry of Education launched 8 tender procedures for supply of Internet classroom equipment for schools (worth USD 20 mln in total) and the Ministry of Health violated the Public Procurement Act by splitting the contract for supply of a nation-wide computer system for registering medical services between two suppliers. As demonstrated by the SCC's audits, systems supplied in this way are not fully integrated.

The above findings persuaded the SCC to conduct in 2001 a comprehensive audit of the government administration's spending on computerisation. The audit will cover budgetary resources as well as foreign aid funds.

5. Methodology of auditing public funds spent on IT.

Both answers to the questionnaire and own experience of the Supreme Chamber of Control let us pose a statement that the methodology of auditing public funds spent on IT may be most helpful for SAIs in countries which undergo dynamic system changes and IT revolution. The following circumstances support that statement:

1. Demand for IT in public service grows dramatically;
2. Administrations of countries (particularly those which undergo transformation) are not sufficiently prepared for efficient performance of such tasks;
3. Few administrations adopted central solutions aimed at rationalisation of IT expenditures
4. IT services market expands fast and is very aggressive, which along with paragraphs 1, 2, and 3 lets us make a statement that spending funds on IT is a high risk area for any inconsistencies.
5. SAIs (in particular in countries under transformation) usually underestimate the meaning of proper spending of funds on IT for the state;
6. SAIs are usually insufficiently prepared in terms of professional knowledge, personnel, and organisation to carry out audits of IT investments.

As far as the assessment of IT related public expenditures with the criterion of legality should present no problems, the assessment with the criteria of advisability, reliability, and economical management in this area can be a problem for many SAIs (including the SCC). The solution may be to establish a relevant methodology. The SCC took steps to develop such a methodology. This task was assigned to a specialised consulting company, which closely co-operated with the special workgroup in the SCC. As a result "Rules and Methodology of Auditing IT Investments" manual was written. The manual contains elementary knowledge about IT systems and serves as a methodological guidebook. SCC auditors had never been trained in information technology before, therefore auditors had to be taught basic ideas

on the subject. We did not aim to turn all auditors to IT experts, but just to allow them to feel confident in these areas, learn basic ideas, identify problems, and use external expert help. Relatively a lot of attention was paid to the audit of preparations to computerisation namely strategic planning and defining objectives of designed system. Another important area is taking care of quality of particular components of the system and risk management.

The general part of the manual addressed the issues of risk in IT projects. Factors that may lead to project crash were presented as well as factors, which add to the success of a project. The auditors were told to focus on:

- a) factors related to the “sociology of the project”, (experience of the managerial staff, experience of the client, qualification of project teams),
- b) technical factors (selection of system design and implementation technology, selection of programming tools, supervision over specification of requirements and scope of the system);
- c) factors related to project management (estimating work consumption, planning, tracking degree of work completion, and estimating expenses on project quality audit).

The statistical influence of main risk factors on dates of project completion was discussed as well as the introduction to issues of drawing up **risk metrics** for the project.

The second chapter of the manual describes issues of IT projects within the context of the Act on the Supreme Chamber of Control. The chapter describes relations between statutory tasks of the SCC and auditing IT projects. This is important as the SCC carries out audits pursuant to the following four criteria: legality, advisability, economical management and reliability, and each of these criteria should be related to specific nature of IT projects.

Elements of good practice were discussed at great lengths; they should be present in all projects of such type and lack of them is a serious signal that works on the system may be carried out improperly and may result in poor quality product. Rules of good practice were discussed with regard to areas such as project management, organisation of the team and design works, project scheduling, quality assurance plan, quality procedures, audit procedures, risk assessment.

A separate part of the manual tackled advisability of IT projects. The SCC believes that one of basic problems with completion of IT projects, in particular when actions of the ordered in the competitive market does not establish generally accepted criteria and priorities of IT investments, is to ensure advisability of actions namely to place the investment within the context of statutory activities and to ensure rational financial expenditures.

The auditors were introduced to the definition of IT project objectives, requirements specification, assessment of costs and benefits, policy of IT security.

The main part of the manual contains 46 audit tasks in eleven areas: audit of advisability, analysis of the project state, process audit, strategic planning, analysis of requirements, system architecture planning, system construction and tests, system introduction, system use, system modernisation. The problem was discussed in each chapter and detailed exercises for auditors were provided. Required qualifications of auditors were also enumerated, which may be of importance while using services of external experts.

5.1. Basic areas of IT audit

1. Audit of advisability.

Analysis of the scope of the task and cost and benefit scope analysis is recommended for this area. In particular the auditor should determine if and how:

- objectives and requirements for the system were developed,
- the scope of design works was documented and whether that scope was covered in the contract,
- cost analysis had been carried out,
- benefits from the project were defined in such a way so that a follow-up verification can be carried out.

2. Analysis of the project.

The purpose of this analysis is to define actual progress of works and identify possible threats to objectives of the project. This type of audit should be part of the routine for large IT investments. Within this area, the auditor should determine if:

- project organisation representing all parties involved in the project has been defined;
- there are reporting procedures for work progress and their up-to-date documentation;
- there are documented changes to the project along with the risk analysis for introduction of such changes;
- risk level of the project is adequate to expected benefits,
- high risk areas have certain emergency plans.

3. Risk metrics

The purpose of risk analysis is to determine such areas of an IT project which may cause excessive costs or delays in schedule, inadequate functionality or efficiency of the system, interruption of the project, result in dissatisfaction of the user or loss of trust to the institution. With such an analysis in hand we may identify risk factors and plan the project in such a way so as to fight them or have emergency scenarios in case of trouble. The tool used for this purpose is the **risk metrics**. It allows to review such typical risk factors and assign certain measurement to each such factor. When the measurements are summed up, we can classify risk of the project (e.g. specify whether project risk will be low, medium, high, or extreme). Obviously, assignment of relevant measurements is only estimated and required great experience. When the values of risk certificate are specified, the global influence of project risk on the budget and completion time can be estimated by e.g. adding the value of the so-called safety margin to the preliminary budget and completion time (just in case). The "Rules and Methodology of Auditing IT Investments" assume, according to *Jones, Capers, "Patterns of Software Systems Failure and Success", International Thompson Computer Press, 1996*, the following values:

- low - if the score is 10 – 40 points; safety margin 10%
- medium - if the score is 41-65 points; safety margin 15%;
- high – if the score is 66 – 85 points; safety margin 20%;

- extreme – if the score exceeded 85 points; **safety margin cannot be estimated.**

While performing audit of IT investment in the Social Security Office, the Supreme Chamber of Control commissioned drawing up of a risk metrics for that project (see Chap. 3.6.)

4. Process audit.

Process audit with risk analysis is the basic audits tools of the SCC for IT investment audits. The purpose of process audit is to identify practices used in the project and assess their compliance with standards set down in the contracts. Audit related tasks include:

- assessment of investment organisation from the point of view of clear division of competencies and ensuring the effectiveness of decision making process and solving critical situations;
- assessment of the quality system through analysis of documentation and practices related to planning and quality control;
- assessment of practised mechanisms of project management (reliability and keeping documentation up-to-date, budget check, quality control);
- assessment of applied production technology (adequacy to project description).

To achieve these objectives, the auditor should determine whether there is a document that specifies division of competencies in the institution, documented methodology of project design, current project quality assurance plan, current documentation of the project management.

5.2 Detailed tasks.

The “Methodology” also tries to define detailed important audit tasks for various stages of developing and implementing an IT system. Certainly, selection of detailed tasks depends on the current stage of project life and scope of the audit.

1. Strategic planning.

The basic product of this stage is the strategic information plan containing the following elements:

- definition of institution’s strategy (mission, objectives, SWOT analysis)
- definition of IT strategy (role of IT systems in supporting the strategy)
- preliminary specification of IT projects (objectives, scope, basic technological assumptions, and costs).

During the audit it has to be determined whether:

- representatives of strategic managerial level were involved in strategy development,
- IT strategy was defined and linked with general institution strategy;
- objectives and prerequisites for the system were defined,
- expected and verifiable benefits from the project were defined.

2. Requirements analysis.

The basic product at this stage is specification of system requirements. The Auditor should determine whether:

- complete documentation defining objectives and requirements of the system was drawn up;
- clear quality assessment criteria for various elements of requirements specification were defined and applied in practice,
- verification of requirements specification was carried out and documented by the ordered,
- possibility of development and modification of the specification is possible in the future.

3. System architecture design.

The product of this stage is system architecture comprising models of requirements, processes, data, or objects at the level of general system concept and the level of scope definition for particular applications. The auditor should determine whether:

- discussion on the alternative solutions of application and technical architecture was carried out and final solution recommendations were based on results of such a discussion;
- assessment of the scope and level of meeting user requirements by solutions proposed in the architecture;
- technical standards for development of various system components were defined
- possibility of development and modification of system architecture definition during project performance was ensured.

Performance of the aforementioned tasks requires expert knowledge and the auditor should seek such help in performing his duties.

4. System components design.

The product of this stage is specification of components, which may comprise elements such as database design, application design, multidimensional analyses model for decision support systems, tests plan.

The auditor is to determine whether:

- quality assurance system is documented and implemented;
- design documentation includes clear references to requirements specification that let determine how individual solutions fixed in project meet requirements defined at the analysis stage;
- there is documentation that specifies rules of testing for various elements from the aspect of meeting technical and system requirements.

5. System development and tests.

Products of this stage include:

- a set of tested applications ready for implementation,
- user documentation (if it is part of the contract),
- acceptance test documentation.

The auditor should determine whether:

- there is a test plan including all created system elements,
- there is a current documentation of tests for created system elements,
- updating and products versioning procedures are in place and carried out.

Performance of audit in this scope requires good knowledge of the rules of software test planning as well as expert knowledge of IT technologies applied in the project. Therefore the use of external expert help will be necessary.

6. System implementation

The basic product of this stage is a properly configured, ready to use IT system (or part thereof provided in the contract), which should contain all elements specified in the contract and schedule. Team of user employees should be trained. Basic documentation elements of this stage include:

- system set-up documentation covering typical workstations, network topology, database configuration, etc.
- system administrator manual,
- end user manual,
- user training materials.

The auditor is to determine whether:

- system implementation documentation is in place,
- there is schedule for delivery and installation of computer hardware,
- administrator and user training programme are in place and carried out.

7. Exploitation of IT system.

The basic product of this stage is documentation of errors and problems submitted by users and analyses of causes and results of system malfunctions. The auditor should first determine whether:

- user opinions are regularly gathered and analysed,
- there are documented and applied standards for system resource administration (access rules, back-ups, resource load audit),
- there is an efficient technical support team,
- there are system malfunction elimination procedures,
- analyses of causes and results of malfunctions and user notes are kept up-to-date and documented.

8. System modernisation.

This stage of IT investment consists in ensuring current adaptation of the system to changing user needs (e.g. changes in the legal system). As for the incremental model of an IT system, co-ordination of changes introduced to the implemented system increments along with other elements under design and construction is a serious problem. The basic product of the modernisation stage is documentation related to changes of the scope and requirements of the system and faults found during system exploitation. The auditor is to determine whether:

- system user opinions are regularly gathered and analysed,
- documentation of changes of requirements and system scope as well as cost and risk analysis for proposed changes is in place

“Rules and Methodology of Auditing IT Investments” manual also contains elements such as:

- basic terms glossary;
- list of professional literature,
- PN-ISO 9000-3:1994 “Guidelines for ISO 9001 application for preparation, delivery and use of software” standard,
- IT system typical documentation with a typical quality assurance plan;
- a typical project size estimate,
- a typical project risk metrics.

6. CONCLUSIONS

1. SAIs should carefully monitor public spending on IT investment projects.
2. Auditing public spending on IT investment projects usually requires a special methodology and auditors trained in applying it.
3. The audit methodology should highlight the issues of strategic planning, identification of project objectives and quality management.
4. SAIs should consider recommending to the central administration that it develop basic standards and procedures to be followed by the public administration in initiating, planning and implementing information systems
5. Accounts of major audits of public spending on IT (scope, methodology, key findings and recommendations) should be published in „Info-IT”.

Warsaw, January, 2001,