Working group "Audit Manuals"

Activity Report for the year 2003

March 2004

1. <u>BACKGROUND</u>

At the last meeting of the Hof the Supreme Audit Institutions of Central and Eastern European Countries, Cyprus, Malta, Turkey and the European Court of Auditors in Bucharest, Romania, it was agreed that active collaboration on the continuous development of Audit Manuals and effective and reliable audit techniques and methodologies remained of great importance to the participating SAIs, also with regard to EU accession. Consequently, it was decided to extend the mandate of this Working Group for another year and to invite the Working Group to continue in particular with the implementation of further workshops and the publication of newsletters in the year 2003. The Electronic Discussion Group (EDG) should continue to serve also as a library or archive of "audit manual" and "audit methodology" related material.

In a questionnaire from the workshops in 2002, the following topics were identified by SAI participants as topics of highest priority for possible workshops in 2003:

➢ Audit planning / Risk assessment

➢ Audit Sampling

➢ Audit of IT systems

➢ Using Computer Assisted Audit Tools

➢ Managing the Audit Process

➢ Audit of Procurement

➢ Audit of Revenues

From these topics the first three were chosen for the workshops in 2003 and after discussing with the hosts the following dates for the workshops were agreed:

1. Audit of IT Systems:
   11 – 13 June 2003 in Tirana, Albania

2. Risk Assessment in the planning phase:
   24 – 26 September 2003 in Antalya, Turkey

3. Audit Sampling:
   17 – 19 November 2003 in Ljubljana, Slovenia

In parallel to the implementation of the workshops, the co-ordinators of the working group, the European Court of Auditors and SIGMA[1], would publish further issues of the Newsletter. The Electronic Discussion Group (EDG) would also continue to be updated and reorganised and serve as library for documents of the working group.

---

[1] SIGMA is a joint initiative of the OECD and the EU, principally financed by the EU. See www.sigmaweb.org

2. **IMPLEMENTATION OF THE WORKSHOPS**

The workshops have been implemented as scheduled and they were attended by participants from all the SAIs of Central and Eastern European countries, Cyprus, Malta and Turkey together with representatives from SIGMA, the ECA, EUROSAI, ISACA, IFAC, and from a number of EU Member State SAIs (Austria, Denmark, Finland, France, Ireland, the Netherlands, Portugal, and the United Kingdom). The presence of leading technical experts from private sector standard setting institutions (ISACA, IFAC) as well as from private sector audit companies (Deloitte) was a new and positive element brought into the workshops in 2003.

Compared to last year, the participants of the workshops were very different depending on the subject. For the first one (IT Audit), which was a rather special topic, SAIs tend to send their IT experts. The second workshop (Risk Assessment) was then attended mainly by general methodologists that had participated already in the 2002 workshops. The last one (Audit Sampling) was attended by sampling experts as well as general methodologists. The participation of leading technical experts significantly contributed to the discussion of specific questions during plenary sessions and group exercises.

The hosting SAIs provided the logistical facilities, which were, like in 2002, of a consistently high standard. Modern presentation techniques as well as secretarial facilities proved to be essential for the implementation of such workshops as a lot of material has to be prepared, copied and disseminated during the workshops. After the work related discussions the hosts also organised a social programme that allowed the participants to get better acquainted with the hosting country.

All workshops followed the same basic structure as in 2002 and were divided into two parts: discussion of the theoretical concepts and then practical exchanges of experiences for the specific topic. For both parts presentations were combined and supported with interactive group discussions and exercises.

Evaluations of the workshops by the participants show high marks for the presentations and group exercises as well as for the organisation of the workshops. For all three workshops, the overall evaluation as well as the relevance of the workshop for the work of the participating SAIs was well above 4 (in a scale from 1 to 5, with 5 being the best possible assessment).

However, the sometimes heterogeneous composition of the participants resulted in different expectations. Participants who were not experts in the area were asking for a general overview for example about the different sampling techniques whereas the technical experts would have preferred to discuss the topic in more detail. If such technical workshops will be

organised in the future, it might be advisable to specify the expected results and the technical level needed from the participants more clearly. Thought will be given fin the future to having in addition to more general level workshops some master class type events for experienced practitioners..

3. <u>MAIN RESULTS OF THE WORKSHOP</u>

The first workshop on IT Audit was very much focussing on the COBIT model as this model is considered by INTOSAI as well as IFAC as leading model for any audit of IT systems. The participants were presented the different modules of the COBIT model like key concepts and principles, the COBIT Management Guidelines, the COBIT Auditing Guidelines as well as different ways of implementing the COBIT model. Experiences of SAIs in IT Audit showed that the COBIT model is not yet widely applied in SAIs and further training on this topic is needed. It showed also that these guidelines are very comprehensive and practical to perform audit of IT systems and their use is highly recommended.

The second workshop about Risk Assessment in the planning phase gave some very interesting presentations about how the risk assessments are carried out in the audit offices. The implementation of risk assessment techniques seems not to be carried out in a systematic way by all SAIs. In the light of the new IFAC standards this might well change and risk assessments will become much more important for all audits. This presentation about the new IFAC standards gave a very good insight into the future developments in this area and informed the SAIs already at a very early stage about up-coming changes.

The third workshop on Audit Sampling revealed that sampling is widely used in SAIs, although the methods are not always based on statistical sampling. The participants agreed that essential factors to be taken into account when planning an audit sample are the following: Audit objectives, resources available and staff knowledge of sampling techniques, population size and characteristics, materiality, risk assessment, confidence level. The workshop discussed also the interpretation of sampling results and it was concluded that the isolation of errors and the extension of the sample size were useful tools in some cases. However, the application of those tools has to be done with care and by respecting the underlying mathematical assumptions. The participants were also informed that at least in the private sector the MUS sampling approach will in the long term be replaced by more modern techniques (Bayes).

The outcome of the workshops from 2002 was in the meantime put on a CD and SIGMA has ensured that this material has been distributed to all SAIs. The same will be done in due course for the materials from the workshops in 2003.

4. THE ELECTRONIC DISCUSSION GROUP

Beginning of 2003 SIGMA redesigned its website and made the EDG better designed for use as library and archive of documents related to audit and the co-operation between SAIs. The new section of the EDG for the audit manuals library/archive has developed beyond expectations and is a significant repository and research tool for its members. Besides audit staff from candidate country SAIs also staff from EU Member State SAIs is users of the EDG.

5. NEWSLETTERS

One of the tasks of the working group was the publication of Newsletters in order to prepare the participants for the upcoming workshops and also to report on the results of those workshops as well as on other events.

In 2003 three Newsletters were issued, two regular ones in April and October 2003 and one summarising the results of the workshops in December 2003. The Newsletters are attached to this report. The Newsletters were disseminated widely within the SAIs of the Network as well as to SAIs from EU Member States. Further Newsletters are expected to be produced in 2004.

6. FUTURE PERSPECTIVES

In order to know more about the intentions of SAIs concerning the need for continuation of the work undertaken by the working group, the participants of the workshops were asked generally about their opinion and given the positive feed-back at those workshops, the ECA sent a more detailed questionnaire to all SAIs.

The outcome of this questionnaire was that 13 SAIs wanted to continue the activities of the working group. All but one of these 13 SAIs wanted to continue the working group with the full participation of the SAIs from the accession countries. The importance SAIs gave to this working group's work and, in particular, the workshops was also shown by the high number of SAIs that offered to host one of the workshops - in total six SAIs made this offer. Concerning the topics for future workshops, the priorities expressed by the SAIs were transferred into numerical values by giving the following points: 1 - very high, 2 - high, 3 - medium and 4 - low. The final table of topics, in order of priority is as follows:

(Number of SAIs)

Subject	Very high - 1 -	High - 2 -	Medium - 3 -	Low - 4 -	Average
Audit of EU funds	11	0	2	0	*1,31*
Audit of structural funds	9	1	2	0	*1,42*
Performance auditing	5	5	2	0	*1,75*
Financial audit	3	3	4	0	*2,10*
Audit of Procurement	4	3	5	1	*2,23*
Role of SAIs in the fight against fraud and corruption	2	7	2	2	*2,31*
Taxation and customs	2	6	4	1	*2,31*
Audit of Revenues	1	7	4	1	*2,38*
Accruals Accounting System in the Public Sector	4	2	3	4	*2,54*

Other topics proposed by SAIs were "Environmental Auditing", "Audit of Cohesion Fund", "Audit of Internal Control System", and "Systems Audit".

At the meeting of the Liaison Officers in Dubrovnik, on 19/20 February 2004, there was also general consensus that the continuation of the activities of the working group would be favourable for all SAIs. Given the interest raised by some SAIs from the present EU Member States, it was even envisaged to invite the SAIs from present EU Member States to all future workshops on a general basis and not only as presenter for specific topics.

The organisation of the workshops however depend very much also on the possibilities SIGMA could offer to again support and assist in the organisation and financing. In the past this was always a crucial factor and contacts have to be made with the EU Commission in order to seek for continued support in this area.

7. **CONCLUSIONS AND RECOMMENDATIONS**

o The workshops implemented in 2003 were again of a very high standard, both from the content and their organisation. The Workshops were highly effective in securing a transfer of useful technical knowledge and sharing of helpful practical experiences. The participation of presenters from private sector, standards setting and other institutions was very beneficial and enlarged the discussions during the workshops.

This additional element should be continued if the workshops will be organised also in the future.

o The participants and presenters from the Acceding, Candidate, Member and other States, and the ECA were of a consistent high standard and proved to be very helpful and useful.

o The SAIs of Albania, Turkey and Slovenia hosted the workshops in an excellent way and offered besides high standard technical facilities a warm hospitality to the participants.

o The Newsletter and the EDG were useful tools for preparing the workshops and disseminating the results.

o It was strongly wished by the SAIs that the Audit Manuals Working Group's activities should be continued and developed through 2004/5 along the lines and stated needs set out above.
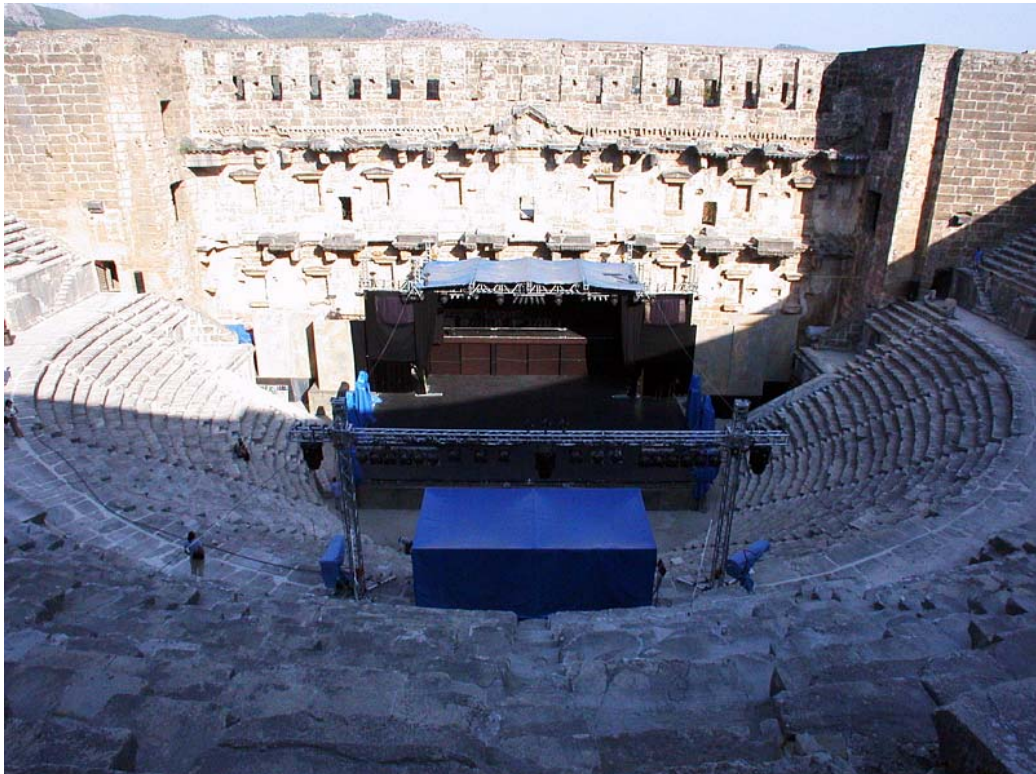
* * *

The Newsletter of the Working Group Audit Manuals

At the last meeting of the Presidents of the Supreme Audit Institutions of Central and Eastern European Countries, Cyprus, Malta, Turkey and the European Court of Auditors in Bucharest, it was agreed that the working group on Audit Manuals will continue its activities for another year. Those activities concern mainly the organisation of workshops and the publication of further Newsletters.

As in the past the Newsletters will cover the different topics chosen for the workshops and report about the outcome of the workshops as well. The Newsletters will also cover other aspects of our co-operation and may be used by any of your institutions as means of communication for matters related to our co-operation. The dates of publication will be loosely related to the workshops.

We hope that the publication of the Newsletter will be helpful in your work and we would be happy for a y contribution or comment you might have in t is respect.

Juan Manuel Fabra Vallés
President of the ECA

db

Towards Enlargement: Efficient and Effective Management and Control of European Union Funds

The Seventh Annual Meeting of the Presidents of the Supreme Audit Institutions (SAIs) of Central and Eastern Europe, Cyprus, Malta and Turkey and the European Court of Auditors (ECA) took place in Bucharest. The official meeting was chaired jointly by Mr Dan Drosu Şaguna, President of the Romanian Court of Accounts and Mr Maarten B. Engwirda, Member of the European Court of Auditors, responsible for the co-ordination of the audit of the pre-accession funds.

The heads of the Candidate Countries' national external audit institutions, representatives of the European Parliament and Commission, other national audit institutions (Albania, Croatia, Denmark, UK and USA), international audit organisations, SIGMA and the ECA met, with due respect to their own independence and constitutional and legal mandates to further improve co-operation and take practical joint steps towards further improving their methods and operational efficiency.

Mr Fabra Vallés, President of the ECA said in his message to the Presidents of the SAIs of the Candidate Countries: "One of the Union's principal requirements is for sound public administration which is capable of managing and scrutinising financial transfers from the EU budget. Together we need to ensure that the various programmes attain the desired objectives and help to improve its citizen's quality of life. This is one of the main challenges, which the applicant countries will have to face. *(see continuation on page 2)*

President's of the SAI's meeting, Bucharest 13-14 December 2003

Table of Contents

Towards Enlargement (contd 1)

In this connection, the Supreme Audit Institutions are called upon to play an essential role:

- Their reports serve as a basis for the democratic scrutiny of public expenditure by Parliaments; they help, in other words, to legitimise the use of public funds;

- Their audit work ensures that funds are used in accordance with the applicable rules and regulations; and

- Their observations and recommendations help managers to improve their performance and to ensure that the principles of sound financial management are observed."

Opening speeches were also given by Mr Şaguna and Mr Nastase, Prime Minister of Romania. Messages were given by Dr Michaele Schreyer, Member of the European Commission Mr Herbert Bösch, Vice-Chairman of the Budgetary Control Committee. Dr Franz Fiedler, President of the Austrian SAI and Secretary General of INTOSAI; and Mr Sergey Stepashin, President of the Russian SAI and President of EUROSAI.

SIGMA Head of Programme, Bob Bonwitt and Nick Treen (Principal Administrator, Audit and Financial Control) made a presentation on SIGMA's activities during 2002 and presented a paper summarising the results of their 2002 baseline assessment for public sector external audit (the presentation and paper are on the SIGMA web-site: http://www.oecd.org/sigma

nt/db

Forthcoming Audit Manuals Workshop

Following the decision by the Heads of the SAIs in Bucharest to continue the workshops in the area of Audit Manuals, it is planned to organise three workshops during the year 2003.

According to the priorities expressed by the participants of the previous workshops, the most relevant topics for these workshops are: IT Audit, Planning and Risk Assessment, and Audit Sampling. Many SAIs offered to host a workshop in 2003 and we are of course very happy for these generous offers, because the hosting of these workshops always requires some important human and financial resources. Among these SAIs we had to chose only three and taking into account that some SAIs have not had the chance so far to organise any event within the framework of our co-operation we have agreed to plan the following three workshops:

1. "IT Audit" in Albania (11 – 13 June);
2. "Risk Assessment and Planning" in Turkey (24 – 26 September);
3. "Audit Sampling" in Slovenia (17 – 19 November);

We hope that the dates of the workshops are convenient for the technical experts so that your institution can participate and contribute to the success of the workshops as last year.

The workshops will in principle follow the same structure as chosen last year because most of the participants were happy with it. This means that we will also invite representatives from international organisations and EU Member State SAIs to present some theoretical aspects of the topics as well as their national experience in implementing it. We are also looking for contributions from the group of your SAIs with regard to your experience in this matter. If you feel that your institution has a particular experience in implementing one of the above mentioned topics and if you would like to share this experience with your colleagues, we would be grateful if you would inform us about it so that we can foresee your presentation in the respective programme.

Concerning the first workshop on IT audit please read also the article about the COBIT model. This model and the related Audit Guidelines will be discussed further at the workshop and an expert from the Information Systems Audit and Control Association & Foundation (ISACA), who has developed this model and the Audit Guidelines will be present.

For more information on the programme please consult the EDG category, or contact Dieter Böckem by e-mail mailto:dieter.boeckem@eca.eu.int or Nick Treen at mailto:nicolasjohn.treen@oecd.org.

Regarding the administrative arrangements for the workshops, please contact for the:

Albanian workshop: mailto:esther.bright@oecd.org
Turkish workshop: mailto:mimi.bessarat@oecd.org
Slovenian workshop: mailto:annes.mcgoogan@oecd.org

db/nt

A Better Understanding of Corporate and Organisational Controls

Corporate governance and its requirements that good internal control should exist in an organisation, has led to organisations in both the public and private sector to taking a wider view of the whole control framework for which they are responsible. This has resulted in a move to providing an overall assessment of an organisation's control activities with the aim of giving an assurance as to the effectiveness of its internal control systems.

With this in mind, a number of frameworks have been established and adapted according to the individual characteristics of an organisation. Perhaps the one which has attracted the greatest following is the COSO framework of controls developed by a Committee of Sponsoring Organisations of the SEC in the USA.

In many ways the COSO framework is a much better tool for conceptualising control than the currently prevalent ex-ante and ex-poste description. It is proving to be particularly useful when drawing up standards for internal control and has been used by the EU Commission for this purpose and also by a number of Candidate Countries, e.g. Poland, Lithuania, Estonia.

The framework is built around five main control areas:

A. Control Environment;
B. Identification of Risks and Priorities for Control;
C. Financial Strategy and Management;
D. Control Activities;
E. Monitoring and Corrective Action.

This grouping provides a combination of **"soft"** controls such as establishing an environment in which control can survive and flourish alongside stricter more traditional types of **"hard"** controls over accounting and financial transactions. The main issues to be considered would be along the following lines:

A. Control Environment

1) A commitment by ministers, directors, management and staff to competence and integrity.
2) The communication of ethical values and control consciousness to managers and employees.
3) An appropriate organisational structure within which business can be planned, executed, controlled and monitored to achieve the organisation's objectives.
4) Appropriate delegation of authority which has regard to acceptable levels of risk.
5) A professional approach to financial reporting that complies with accounting practice.

B. Identification of Risk and Priorities for Control

1) Identification of key organisational risks in a systematic and timely manner.
2) Consideration of the likelihood of risks occurring and the significance of the likely impact on the organisation.
3) Establishment of priorities for the allocation of resources available for control and the setting of clear control objectives.

C. Financial Strategy and Management

1) Performance indicators that allow management to monitor the key business and financial activities and risks, and the progress towards objectives, and to identify developments that require intervention.
2) Information systems that provide ongoing identification and capture of relevant, reliable, and up-to-date financial and operational information from internal and external sources.
3) Systems that communicate relevant information to the right people at the right time in a way that identifies variance from plans and allows a prompt response.

D. Control Activities

1) Procedures to ensure complete and accurate accounting for claims and financial transactions.
2) Appropriate authorisation limits for claims and transactions.
3) Procedures to ensure the reliability of data processing and information reports generated.
4) Controls that limit exposure to loss of assets/records or to fraud and the risk of disallowance.
5) Procedures to ensure compliance with laws and regulations that have significant operational and financial implications.

E. Monitoring and Corrective Action

1) A monitoring process that provides reasonable assurance to directors and managers that there are appropriate control procedures in place for all significant business activities and that these procedures are being followed.
2) Identification of change in the business and its environment that may require changes to internal control systems.
3) Formal procedures for reporting weaknesses and for ensuring appropriate corrective action.
4) The provision of adequate support for public statements on internal control.

nt

Launch of new EDGS

We are pleased to announce the launch in March of two newly updated Electronic Discussion Groups, the restricted EDG: *SIGMA Supporting the Exchange of Experiences Concerning Public Sector External Audit and European Union Accession*; and the open EDG, *the Electronic Advisory Forum*.

We found that there was a need give a clearer overview of the work we do in the financial control and external audit area. We hope that you find the new EDGs more streamlined and user-friendly. The categories have been changed to better reflect what we do and there is an audit manuals library which will be regularly updated for your consultation.

Aivo Vaske from the Riigikontroll worked with us in March to support the updating and reviewing of the data in the current EDGs. Many thanks go to him for this useful work.

If you are not already a member and would like to join or if you have any questions or need any information concerning the EDG, please contact mailto:esther.bright@oecd.org; or mailto:nicolasjohn.treen@oecd.org

You can visit the new EDGs via our homepage: http://www.oecd.org/sigma

nt

Expert Working Groups for 2003

For 2003 the Expert Group on Quality in the Audit Process will continue its good work in this area (for their 2002 report see the web-sites of the Hungarian, Maltese or Polish SAIs; or the SIGMA homepage: http://www.oecd.org/sigma by preparing a draft auditing standard for quality.

The expert group on the Audit of Public Internal Financial Control systems will also continue, led by the Croatian SAI and supported by SIGMA. Other interested SAIs who would like to contribute to this work should contact Lidija Pernar mailto:pernar@revizija.hr or Nick Treen mailto:nicolasjohn.treen@oecd.org

Discussions are ongoing concerning the starting up of an Expert Group on Procurement Audit. Any SAIs interested in this should, in the first instance, contact Nick Treen mailto:nicolasjohn.treen@oecd.org

nt

SIGMA Papers No 33: Relations between Supreme Audit Institutions and Parliamentary Committees

The SIGMA Paper is drawn from a report on relations between Supreme Audit Institutions and parliamentary committees, prepared for the network of Presidents of the Supreme Audit Institutions of Central and Eastern Countries, Cyprus, Malta and the European Court of Auditors, as part of their efforts to prepare candidate countries for eventual membership of the European Union. It was written primarily for use by those organisations but SIGMA does believe it also has wider interest.

SIGMA has published this paper in the belief that the information it contains should be of broad interest to those involved in or concerned about this important set of relationships. The work of an SAI, and its relations with parliament are key factors in a strong chain of accountability and the effectiveness of public sector governance.

The original report will now also be presented by the Chairmen of the Maltese and Polish SAIs, Mr Galea and Mr Sekuła, to the Budgetary Control Committee of the European Parliament on 29 April 2003. The interest expressed by this Committee confirms the good work undertaken within the framework of the co-operation and will hopefully be reflected also in a number of national parliaments.

The European Court of Auditors and SIGMA will also attend the presentation.

You can find the paper on our web-site:

http://www.oecd.org/sigma

nt/db

Progress on PIFC Peer Assistance

SIGMA Peer Assistance for Public Internal Financial Control at the Ministry of Finance is ongoing at the moment in Slovakia, Slovenia and the Czech Republic.

Plans have been agreed with DGs Elarg and Budget and the countries concerned for SIGMA Peer Assistance to start in Poland and Hungary in May and June, respectively.

It is hoped to start the Peer Assistance in Romania in the autumn of 2003.

For further information, contact Nick Treen at nicolasjohn.treen@oecd.org, or François-Roger Cazala at mailto:francois-roger.cazala@oecd.org

nt

VII Meeting of the EUROSAI Training Committee (Lisbon 20-22 January 2003)

The EUROSAI Training Committee under the chairmanship of Mr Christophe Perron from the French Cour des Comptes met in Lisbon in order to discuss its training strategy and training activities. Concerning the training strategy first drafts for the Mission Statement were prepared as well as for the operational plan. These first drafts will be further elaborated until the next meeting, which will take place on 23 – 24 June in Poland. Concerning the other points discussed, the close relation between the workshops initiated by the ETC and IDI and the workshops of the working group "Audit Manuals" were pointed out by all participants. It was agreed that these activities will be closely co-ordinated between the ETC and the working group.

db

THE COBIT TOOL FOR IT SYSTEMS– AN EXECUTIVE OVERVIEW

The following text is an extract about the Control Objectives for Information and related Technology (COBIT). COBIT's mission and objective is to research, develop, publicise and promote an authoritative, up-to-date, international set of generally accepted IT Control Objectives for day-to-day use by business managers as well as security, control and audit practitioners. COBIT has been developed as a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners.

The COBIT model will be presented in more detail at the next workshop on IT audit from 11 – 13 June 2003 in Albania. The full text including the graphics as well as further material is available on the web-site of the Information Systems Audit and Control Association & Foundation (ISACA) at www.isaca.org.

OVERVIEW OF THE COBIT MODEL

Critically important to the survival and success of an organisation is effective management of information and related Information Technology (IT). In this global information society—where information travels through cyberspace without the constraints of time, distance and speed—this criticality arises from the:

- Increasing dependence on information and the systems that deliver this information
- Increasing vulnerabilities and a wide spectrum of threats, such as cyber threats and information warfare
- Scale and cost of the current and future investments in information and information systems
- Potential for technologies to dramatically change organisations and business practices, create new opportunities and reduce costs

For many organisations, information and the technology that supports it represent the organisation's most valuable assets. Moreover, in today's very competitive and rapidly changing business environment, management has heightened expectations regarding IT delivery functions: management requires increased quality, functionality and ease of use; decreased delivery time; and continuously improving service levels — while demanding that this be accomplished at lower costs.

Many organisations recognise the potential benefits that technology can yield. Successful organisations, however, understand and manage the risks associated with implementing new technologies.

There are numerous changes in IT and its operating environment that emphasise the need to better manage IT-related risks. Dependence on electronic information and IT systems is essential to support critical business processes. In addition, the regulatory environment is mandating stricter control over information. This, in turn, is driven by increasing disclosures of information system disasters and increasing electronic fraud. The management of IT-related risks is now being understood as a key part of enterprise governance.

Within enterprise governance, IT governance is becoming more and more prominent, and is defined as a structure of relationships and processes to direct and control the enter-prise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes. IT governance is integral to the success of enterprise governance by assuring efficient and effective measurable improvements in related enterprise processes. IT governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives. Furthermore, IT governance integrates and institutionalises good (or best) practices of planning and organising, acquiring and implementing, delivering and supporting, and monitoring IT performance to ensure that the enterprise's information and related technology support its business objectives. IT governance thus enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

IT GOVERNANCE

A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.

The COBIT tool for IT systems (contd)

Organisations must satisfy the quality, fiduciary and security requirements for their information, as for all assets. Management must also optimise the use of available resources, including data, application systems, technology, facilities and people. To discharge these responsibilities, as well as to achieve its objectives, management must understand the status of its own IT systems and decide what security and control they should provide.

Control Objectives for Information and related Technology (COBIT), now in its 3rd edition, helps meet the multiple needs of management by bridging the gaps between business risks, control needs and technical issues. It provides good practices across a domain and process framework and presents activities in a manageable and logical structure. COBIT's "good practices" means consensus of the experts—they will help optimise information investments and will provide a measure to be judged against when things do go wrong.

Management must ensure that an internal control system or framework is in place which supports the business processes, makes it clear how each individual control activity satisfies the information requirements and impacts the IT resources. Impact on IT resources is highlighted in the COBIT *Framework* together with the business requirements for effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability of information that need to be satisfied. Control, which includes policies, organisational structures, practices and procedures, is management's responsibility. Management, through its enterprise governance, must ensure that due diligence is exercised by all individuals involved in the management, use, design, development, maintenance or operation of information systems. An IT control objective is a statement of the desired result or purpose to be achieved by implementing control procedures within a particular IT activity.

Business orientation is the main theme of COBIT. It is designed to be employed not only by users and auditors, but also, and more importantly, as comprehensive guidance for management and business process owners. Increasingly, business practice involves the full empowerment of business process owners so they have total responsibility for all aspects of the business process. In particular, this includes providing adequate controls.

The COBIT *Framework* provides a tool for the business process owner that facilitates the discharge of this responsibility. The *Framework* starts from a simple and pragmatic premise:

In order to provide the information that the organisation needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.

The *Framework* continues with a set of 34 high-level *Control Objectives*, one for each of the IT processes, grouped into four domains: planning and organisation, acquisition and implementation, delivery and support, and monitoring. This structure covers all aspects of information and the technology that supports it. By addressing these 34 high-level control objectives, the business process owner can ensure that an adequate control system is provided for the IT environment.

IT governance guidance is also provided in the COBIT *Framework*. IT governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives. IT governance integrates optimal ways of planning and organising, acquiring and implementing, delivering and supporting, and monitoring IT performance. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

In addition, corresponding to each of the 34 high-level control objectives is an *Audit Guideline* to enable the review of IT processes against COBIT's 318 recommended detailed control objectives to provide management assurance and/or advice for improvement.

The *Management Guidelines*, COBIT's most recent development, further enhances and enables enterprise management to deal more effectively with the needs and requirements of IT governance. The guidelines are action oriented and generic and provide management direction for getting the enterprise's information and related processes under control, for monitoring achievement of organisational goals, for monitoring performance within each IT process and for benchmarking organisational achievement.

The COBIT tool for IT systems (contd)

Specifically, COBIT provides *Maturity Models* for control over IT processes, so that management can map where the organisation is today, where it stands in relation to the best-in-class in its industry and to international standards and where the organisation wants to be; *Critical Success Factors*, which define the most important management-oriented implementation guidelines to achieve control over and within its IT processes; *Key Goal Indicators*, which define measures that tell management—after the fact—whether an IT process has achieved its business requirements; and *Key Performance Indicators*, which are lead indicators that define measures of how well the IT process is performing in enabling the goal to be reached.

COBIT's Management Guidelines are generic and action oriented for the purpose of answering the following types of management questions: How far should we go, and is the cost justified by the benefit? What are the indicators of good performance? What are the critical success factors? What are the risks of not achieving our objectives? What do others do? How do we measure and compare?

COBIT also contains an *Implementation Tool Set* that provides lessons learned from those organisations that quickly and successfully applied COBIT in their work environments. It has two particularly useful tools—Management Awareness Diagnostic and IT Control Diagnostic—to assist in analysing an organisation's IT control environment.

Over the next few years, the management of organisations will need to demonstrably attain increased levels of security and control. COBIT is a tool that allows managers to bridge the gap with respect to control requirements, technical issues and business risks and communicate that level of control to stakeholders. COBIT enables the development of clear policy and good practice for IT control throughout organisations, world-wide. **Thus, COBIT is designed to be the breakthrough IT governance tool that helps in understanding and managing the risks and benefits associated with information and related IT.**

THE COBIT FRAMEWORK

THE NEED FOR CONTROL IN INFORMATION TECHNOLOGY

In recent years, it has become increasingly evident that there is a need for a reference framework for security and control in IT. Successful organisations require an appreciation for and a basic understanding of the risks and constraints of IT at all levels within the enterprise in order to achieve effective direction and adequate controls.

MANAGEMENT has to decide what to reasonably invest for security and control in IT and how to balance risk and control investment in an often unpredictable IT environment. While information systems security and control help manage risks, they do not eliminate them. In addition, the exact level of risk can never be known since there is always some degree of uncertainty. Ultimately, management must decide on the level of risk it is willing to accept. Judging what level can be tolerated, particularly when weighted against the cost, can be a difficult management decision. Therefore, management clearly needs a framework of generally accepted IT security and control practices to benchmark the existing and planned IT environment.

There is an increasing need for **USERS** of IT services to be assured, through accreditation and audit of IT services provided by internal or third parties, that adequate security and control exists. At present, however, the implementation of good IT controls in information systems, be they commercial, non-profit or governmental, is hampered by confusion. The confusion arises from the different evaluation methods such as ITSEC, TCSEC, IS0 9000 evaluations, emerging COSO internal control evaluations, etc. As a result, users need a general foundation to be established as a first step.

Frequently, AUDITORS have taken the lead in such international standardisation efforts because they are continuously confronted with the need to substantiate their opinion on internal control to management. Without a framework, this is an exceedingly difficult task. Furthermore, auditors are increasingly being called on by management to proactively consult and advise on IT security and control-related matters.

The COBIT tool for IT systems (contd)

THE BUSINESS ENVIRONMENT: COMPETITION, CHANGE AND COST

Global competition is here. Organisations are restructuring to streamline operations and simultaneously take advantage of the advances in IT to improve their competitive position. Business re-engineering, right-sizing, outsourcing, empowerment, flattened organisations and distributed processing are all changes that impact the way that business and governmental organisations operate. These changes are having, and will continue to have, profound implications for the management and operational control structures within organisations world-wide.

Emphasis on attaining competitive advantage and cost-efficiency implies an ever-increasing reliance on technology as a major component in the strategy of most organisations. Automating organisational functions is, by its very nature, dictating the incorporation of more powerful control mechanisms into computers and networks, both hardware-based and software-based. Furthermore, the fundamental structural characteristics of these controls are evolving at the same rate and in the same "leap frog" manner as the underlying computing and networking technologies are evolving.

Within the framework of accelerated change, if managers, information systems specialists and auditors are indeed going to be able to effectively fulfil their roles, their skills must evolve as rapidly as the technology and the environment. One must understand the technology of controls involved and its changing nature if one is to exercise reasonable and prudent judgements in evaluating control practices found in typical business or governmental organisations.

EMERGENCE OF ENTERPRISE AND IT GOVERNANCE

To achieve success in this information economy, enterprise governance and IT governance can no longer be considered separate and distinct disciplines. Effective enterprise governance focuses individual and group expertise and experience where it can be most productive, monitors and measures performance and provides assurance to critical issues. IT, long considered solely an enabler of an enterprise's strategy, must now be regarded as an integral part of that strategy.

IT governance provides the structure that links IT processes, IT resources, and information to enterprise strategies and objectives. IT governance integrates and institutionalises optimal ways of planning and organising, acquiring and implementing, delivering and supporting, and monitoring IT performance. IT governance is integral to the success of enterprise governance by assuring efficient and effective measurable improvements in related enterprise processes. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

Looking at the interplay of enterprise and IT governance processes in more detail, enterprise governance, the system by which entities are directed and controlled, drives and sets IT governance. At the same time, IT should provide critical input to, and constitute an important component of, strategic plans. IT may in fact influence strategic opportunities outlined by the enterprise.

Enterprise activities require information from IT activities in order to meet business objectives. Successful organisations ensure interdependence between their strategic planning and their IT activities. IT must be aligned with and enable the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining a competitive advantage.

Enterprises are governed by generally accepted good (or best) practices, to ensure that the enterprise is achieving its goals–the assurance of which is guaranteed by certain controls. From these objectives flows the organisation's direction, which dictates certain enterprise activities, using the enterprise's resources. The results of the enterprise activities are measured and reported on, providing input to the constant revision and maintenance of the controls, beginning the cycle again.

IT also is governed by good (or best) practices, to ensure that the enterprise's information and related technology support its business objectives, its resources are used responsibly and its risks are managed appropriately. These practices form a basis for direction of IT activities, which can be characterised as planning and organising, acquiring and implementing, delivering and supporting, and monitoring, for the dual purposes of managing risks (to gain security, reliability and compliance) and realising benefits (increasing effectiveness and efficiency). Reports are issued on the outcomes of IT activities, which are measured against the various practices and controls, and the cycle begins again.

The COBIT tool for IT systems (contd)

In order to ensure that management reaches its business objectives, it must direct and manage IT activities to reach an effective balance between managing risks and realising benefits. To accomplish this, management needs to identify the most important activities to be performed, measure progress towards achieving goals and determine how well the IT processes are performing. In addition, it needs the ability to evaluate the organisation's maturity level against industry best practices and international standards. **To support these management needs, the COBIT Management Guidelines have identified specific Critical Success Factors, Key Goal Indicators, Key Performance Indicators and an associated Maturity Model for IT governance.**

RESPONSE TO THE NEED

In view of these ongoing changes, the development of this framework for control objectives for IT, along with continued applied research in IT controls based on this framework, are cornerstones for effective progress in the field of information and related technology controls.

On the one hand, we have witnessed the development and publication of overall business control models like COSO (Committee of Sponsoring Organisations of the Treadway Commission—Internal Control-Integrated Framework, 1992) in the US, Cadbury in the UK, CoCo in Canada and King in South Africa. On the other hand, an important number of more focused control models are in existence at the level of IT. Good examples of the latter category are the Security Code of Conduct from DTI (Department of Trade and Industry, UK), Information Technology Control Guidelines from CICA (Canadian Institute of Chartered Accountants, Canada), and the Security Handbook from NIST (National Institute of Standards and Technology, US). However, these focused control models do not provide a comprehensive and usable control model over IT in support of business processes. The purpose of COBIT is to bridge this gap by providing a foundation that is closely linked to business objectives while focusing on IT.

A focus on the business requirements for controls in IT and the application of emerging control models and related international standards evolved the original Information Systems Audit and Control Foundation's Control Objectives from an auditor's tool to COBIT, a management tool. Further, the development of IT Management Guidelines has taken COBIT to the next level–providing management with Key Goal Indicators (KGIs), Key Performance Indicators (KPIs), Critical Success Factors (CSFs) and Maturity Models so that it can assess its IT environment and make choices for control implementation and control improvements over the organisation's information and related technology.

Hence, the main objective of the COBIT project is the development of clear policies and good practices for security and control in IT for world-wide endorsement by commercial, governmental and professional organisations. It is the goal of the project to develop these control objectives primarily from the business objectives and needs perspective. (This is compliant with the COSO perspective, which is first and foremost a management framework for internal controls.) Subsequently, control objectives have been developed from the audit objectives (certification of financial information, certification of internal control measures, efficiency and effectiveness, etc.) perspective.

AUDIENCE: MANAGEMENT, USERS AND AUDITORS

COBIT is designed to be used by three distinct audiences.

MANAGEMENT: to help them balance risk and control investment in an often unpredictable IT environment.

USERS: to obtain assurance on the security and controls of IT services provided by internal or third parties.

AUDITORS: to substantiate their opinions and/or provide advice to management on internal controls.

The COBIT tool for IT systems (contd)

BUSINESS OBJECTIVES ORIENTATION

COBIT is aimed at addressing business objectives. The control objectives make a clear and distinct link to business objectives in order to support significant use out-side the audit community. Control objectives are defined in a process-oriented manner following the principle of business re-engineering. At identified domains and processes, a high-level control objective is identified and rationale provided to document the link to the business objectives. In addition, considerations and guidelines are provided to define and implement the IT control objective.

The classification of domains where high-level control objectives apply (domains and processes), an indication of the business requirements for information in that domain, as well as the IT resources primarily impacted by the control objectives, together form the COBIT Framework. The Framework is based on the research activities that have identified 34 high-level control objectives and 318 detailed control objectives. The Framework was exposed to the IT industry and the audit profession to allow an opportunity for review, challenge and comment. The insights gained have been appropriately incorporated.

GENERAL DEFINITIONS

For the purpose of this project, the following definitions are provided. "Control" is adapted from the COSO Report (Internal Control—Integrated Framework, Committee of Sponsoring Organisations of the Treadway Commission, 1992) and "IT Control Objective" is adapted from the SAC Report (Systems Auditability and Control Report, The Institute of Internal Auditors Research Foundation, 1991 and 1994).

Control is defined as: the policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

IT Control Objective is defined as: a statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

IT Governance is defined as: a structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.

The COBIT model will be presented in more detail at the next workshop on IT audit from 11 – 13 June 2003 in Albania. The full text including the graphics as well as further material is available on the web-site of the Information Systems Audit and Control Association & Foundation (ISACA) at

www.isaca.org.

db

Agenda of events for 2003

Month	Day	Week	Event	Place
January	20 - 22	4	Meeting of the EUROSAI Training Committee (ETC) Board	Lisbon, Portugal
February	3-14	6	ETC: IDI Programme for SAIs of Phase I & II: Regional Audit Workshop for candidate countries SAIs	Nicosia, Cyprus
March	7	10	Meeting of the Task Force on Audit Activities (HU, FR, UK, ECA)	Paris, France
Mar/Apr	31-4	14	16. UN/INTOSAI Seminar	Vienna, Austria
April	29	18	Presentation of the report on "The relations between SAIs and Parliamentary Committees" to the Budgetary Control Committee of the European Parliament	Brussels, Belgium
May	12 - 13	20	Meeting of the NATO International Board of Auditors	Brussels, Belgium
May	21 - 23	21	Meeting of the Heads of SAIs from the 10 countries acceding the EU in 2004	Kraków, Poland
May	22 - 23	21	Meeting of the Liaison Officers of the EU Member States	Athens, Greece
May	26 - 28	22	EUROSAI Training event: Evaluation of Internal Control	Prague, Czech Republic
June	5 - 7	23	II EURORAI – EUROSAI Conference	Copenhagen, Denmark
June	11 - 13	24	Workshop "Audit Manuals": IT Audit (CEEC, CY, MT, TY)	Albania
June	23 - 24	26	Meeting of the EUROSAI Training Committee (ETC) Board	Poland
September	4-5	36	Annual meeting of the Baltic - Nordic SAIs	Estonia
September		39	Workshop "Audit Manuals": Audit Planning / Risk Assessment (CEEC, CY, MT, TY)	Turkey
October	6 - 7	41	Meeting of the Liaison Officers of the EU Member States	Luxembourg
October	7 - 8	41	Meeting of the Liaison Officers of Central and Eastern European countries, Cyprus, Malta, Turkey and the ECA	Luxembourg
October	13 -16	42	Meeting of the INTOSAI Governing Board	Budapest, Hungary
October	28	44	Meeting of the EUROSAI Governing Board	Rome, Italy
November	17 - 19	47	Workshop "Audit Manuals": Audit Sampling (CEEC, CY, MT, TY)	Slovenia
December		50	Meeting of the EU Contact Committee	

db

Unfortunately, Johannes Stenbæk-Madsen is no longer with us. He has left to join the World Bank after four years with SIGMA, and we wish him well in his new job.

Contributions to the next issues of the Newsletter are most welcome and should be send to nicolasjohn.treen@oecd.org or annes.mcgoogan@oecd.org

nt

NEWSLETTER ● October 2003

For the Working Groups of the Presidents of the Supreme Audit Institutions of European Union Candidate Countries, Albania, Croatia & the European Court of Auditors Produced by SIGMA and the European Court of Auditors

SIGMA

Support for Improvement in Governance and Management

A joint initiative of the OECD and the European Un ion, principally financed by the EU

Workshops, Expert Groups and Peer Assistance

It is with great pleasure that we hereby present this year's second issue of the Newsletter.

In this issue we continue to provide information about risk assessment. Three articles are related to this topic. Following the decision by the Heads of the SAIs in Bucharest it was planned to organise three workshops during the year 2003. Two have already taken place in Albania (IT Audit) and in Turkey (Risk Assessment and Planning). The Expert Groups on the Audit of Public Internal Financial Control systems and on Quality in the Audit Process continue their good work. Other SAIs have already joined or are expected to join these groups.

JUDr Lubomír Voleník died suddenly in June this year aged 53. The news came as a shock to us. He was a highly respected and fondly regarded President of the Czech Supreme Audit Office. We will miss him a lot.

New experts have joined or will join SIGMA soon. They will assist SIGMA activities on candidate countries.

Best wishes from SIGMA

Heads of SAIs at the Krakow meeting

Communiqué from the Meeting of the Heads of the SAIs of the EU Acceding Countries

The meeting was held in Krakow in May 2003 and discussed the following issues:

- New solutions and developments concerning audit methodology and its organisation.
- Preparation of SAIs human resources.
- Changes in the scope of audit – the audit of the EU funds before and after accession.

To find out more about what was discussed click here:
http://www.nik.gov.pl/english/documents/communique.pdf

Table of Contents

Forthcoming Audit Manuals Workshops

Following the decision by the Heads of the SAIs in Bucharest to continue the workshops in the area of Audit Manuals, it was planned to organise three workshops during the year 2003.

- The first workshop (IT-Audit) which hosted by the President of the Supreme Audit Office of Albania, Mr Mustafa Kerçuku, took place in Tirana from 11 – 13 June 2003. For further information, please contact Esther Bright at esther.bright@oecd.org

- The second workshop (Risk Assessment and Planning) took place in Antalya, from 24 – 26 September 2003. It was hosted by Mr Mehmet Damar, the president of the Turkish Court of Accounts. For further information, please contact Mimi Bessarat at mimi.bessarat@oecd.org

- The third workshop, which will be hosted by Dr Vojko Anton Antončič, President of the Court of Audit of Slovenia, will take place in Slovenia on 17-19 November 2003. It will focus on "Audit Sampling". Regarding the administrative arrangements for the Slovenian workshop and further information, please contact Esther Bright at esther.bright@oecd.org or to the Adviser to the President Nataša Skrt-Kos at Natasa.Skrt-Kos@rs-rs.si

-

According to the priorities expressed by the participants of the previous workshops, the most relevant topics for these workshops are: IT Audit, Planning and Risk Assessment, and Audit Sampling. Many SAIs offered to host a workshop in 2003 and we are of course very happy for these generous offers, because the hosting of these workshops always requires some important human and financial resources. Among these SAIs we had to chose only three and taking into account that some SAIs have not had the chance so far to organise any event within the framework of our co-operation we have agreed to plan the following three workshops:

The workshops follow the same structure as operated last year because most of the participants were happy with it. This means that we will also invite representatives from international organisations and EU Member State SAIs to present some theoretical aspects of the topics as well as their national experience in implementing it. We are also looking for contributions from the group of your SAIs with regard to your experience in this matter. If you feel that your institution has a particular experience in implementing one of the above mentioned topics and if you would like to share this experience with your colleagues, we would be grateful if you would inform us about it so that we can foresee your presentation in the respective programme.

Discussions have also started on whether a further programme of workshops will be undertaken in 2004.

For more information on the programme please consult the Closed EDG category, or contact Dieter Böckem by e-mail dieter.boeckem@eca.eu.int or Nick Treen at nicolasjohn.treen@oecd.org.

Progress on PIFC Peer Assistance

SIGMA Peer Assistance for Public Internal Financial Control at the Ministry of Finance is ongoing at the moment in the Czech Republic, Poland, Romania and Slovakia.

Peer Assistance in Hungary will begin towards the end of 2003 and Bulgaria is planned for early 2004, subject to agreement with DGs Budget and Elarg. At present it also seems very likely that a PIFC Peer Assistance will also be requested to take place in Estonia in 2004.

For further information, contact Nick Treen at nicolasjohn.treen@oecd.org or François-Roger Cazala at francois-roger.cazala@oecd.org or Joop Vrolijk at joop.vrolijk@oecd.org

Tribute to Lubomír Voleník

The news JUDr Lubomír Voleník, who died suddenly in June this year aged 53, was a highly respected and fondly regarded President of the Czech Supreme Audit Office.

The news came as a shock to those of us who knew him. We will remember him as a very professional and hardworking man, who was well respected not only in the Czech Republic and also within the wider SAI community. He was appointed President of the Czech Supreme Audit Office in July 1993. In addition to this role, he was also President of EUROSAI and Chairman of the Governing Board from 1996-1999.

He was an active and enthusiastic member of the Network of Presidents of the Supreme Audit Institutions of European Union Candidate Countries, Albania, Croatia & the European Court of Auditors. He was proud to be the host for the Meeting of these Presidents when they approved their report entitled the "11 Recommendations concerning the functioning of SAIs in the context of European Integration", now also known as the "Prague Recommendations".

We will all treasure memories of when the formalities were over, President Voleník would gladly get out his guitar or sit at the piano and start playing and organising the singing.

He worked hard to create and establish an effective SAI in the Czech Republic and to ensure a robust financial accountability process for the State. He showed a rare courage and determination to surmount obstacles in spite of his ill health.

Lubomír Voleník will be remembered for his power and humanity.

President Voleník leaves a wife, Ivana, two children and three grandchildren.

[Click here to see the article by President Voleník and published in the SIGMA PMF No 4 - 2000](#)

JUDr Lubomír Voleník, President of the Czech Supreme Audit Office

New staff in SIGMA

Joop Vrolijk arrived April 2003 on secondment from the Netherlands SAI, the Algemene Rekenkamer, to work on candidate countries. Ulrika Klingenstierna formerly from DG Budget B3 and the Swedish Riksrevisionsverket arrives in November 2003 to also work on candidate countries.

Jens Piontek from the German SAI, the Bundesrechnungshof, had a six week internship with SIGMA. He worked on the Risk-Assessment Workshop, the Slovak PIFC peer assistance and the expert group "Quality in the Audit Process".

Setting the framework for risk assessment – risk to the supreme audit institution

In deciding an SAI's work programme (which audits we should carry out and when planning its individual audit tasks (how should we carry out these audits?), the question of risk is (or at least, should be) at the centre of the SAI's thinking. However, risk in the audit context is neither a simple nor a single idea. In fact we need to consider many different types of "risk" to understand how they interact, to know how and when to assess them and finally to decide how to react to these assessments.

When everything is stripped down to the most basic ideas, three levels of risk can be identified. These are the:

- risk to the supreme audit institution;
- risk at the programming level;
- risk at the planning level.

These three levels are interlinked in a complex way and are only separated here to allow a closer examination of some of the key background considerations. In particular, the risk to the SAI will strongly influence (and may be a major element in) the assessment of risk at the programming level.

In effect, a proper understanding of the "risk to the SAI" will set the context and framework for the programming and planning risk assessments. So, what is this "risk to the SAI"? In essence, it is the risk that the SAI fails to fulfil satisfactorily the expectations of the users of its outputs. This, in itself, has at least three dimensions:

- not all expectations upon the SAI will be reasonable, taking into account its mandate, its traditional role and the resources and powers available to it;
- the SAI will never be able to meet the expectations of all the users of its outputs at all times. In particular, the expectation of Parliament, the press, audited entities and the general public will only very rarely, if ever, converge;
- expectations, and thus the potential role of the SAI, are continually evolving. For example, SAIs are increasingly being called upon to add value by helping audited entries to improve their management, rather than simply identifying errors and irregularities.

Managing the "risk to the SAI" may mean that the SAI's senior management must do three things at the same time. First, they may have to explain and justify to Parliament, the press and the public, the difference between all possible expectations and those expectations which are both reasonable and attainable, given the SAI's resources, legal powers and traditional role. Second, having defined and won acceptance for an agenda of reasonable expectations, they have to ensure the available resources and legal remits are fully exploited in the SAI's overall work programme and in its individual audits to meet these expectations to the fullest possible extent. Third, they may need to take a longer term view with the objectives of expanding the scope of reasonable expectations in the future by obtaining the necessary additional resources and legal mandates..

IFAC Exposure Draft on Audit Risk

The IFAC International Auditing and Assurance Standards Board (IAASB) issued in October 2002 an Exposure Draft on "Audit Risk – Proposed International Standards on Auditing and Proposed Amendment to ISA 200, Objective and Principles Governing an Audit of Financial Statements";

The IAASB believes the proposed standards will increase audit quality as a result of better risk assessments and improved design and performance of audit procedures to respond to the risks. The improved linkage of audit procedures and assessed risks is expected to result in a greater concentration of effort on areas where there is greater risk of misstatement.

The full text of the Exposure Draft as well as further material is available on the IFAC Web site: http://www.ifac.org/Guidance/EXD-Details.php?EDID=0002

!!!Newsflash!!!

SIGMA has a new Web site. You will find that it is new and improved and easy to find information that you may be looking for. The SIGMA open EDG – *Electronic Advisory Forum* and the restricted EDG – *SIGMA Supporting the Exchange of Experiences Concerning Public Sector External Audit and European Accession* can be found on the SIGMA homepage.

Please visit us at: www.sigmaweb.org

nt

SAI Peer Assistance

Mr. Mihkel Oviir, the Auditor General of the Estonian SAI, the Riigikontroll, has recently asked SIGMA to undertake a second Peer Assistance Review. It is expected that this will take place in early 2004.

Please contact Nick Treen for further information and details nicolasjohn.treen@oecd.org.

nt

Expert Working Groups for 2003

For 2003 the Expert Group on Quality in the Audit Process will continue its good work in this area by preparing a draft auditing guideline for quality (for their 2002 report either see the Web sites of the Hungarian, Maltese or Polish SAIs; or look on the new SIGMA Web site : http://www.sigmaweb.org/libpubs/pubextaudit.htm .The French SAI, the *Cour des Comptes* is also working with the group. Recent meetings were hosted by the Hungarian SAI in Budapest and by the Cour des Comptes in Paris.

The expert group on the Audit of Public Internal Financial Control systems will also continue, led by the Croatian SAI and supported by SIGMA. The SAIs of Slovakia and Denmark are expected to join this group soon. Other interested SAIs who would like to contribute to this work should contact Lidija Pernar pernar@revizija.hr or Nick Treen nicolasjohn.treen@oecd.org

Discussions are ongoing concerning the starting up of an Expert Group on Procurement Audit. Any SAIs interested in this should, in the first instance, contact Nick Treen nicolasjohn.treen@oecd.org

nt

Risk at the Planning Level – Audit Risk and its Components in Financial Audit Planning Antalya Workshop, 24-26 September 2003

In planning a financial audit, we need to assess the components of audit risk. During the workshop at Antalya, we will look at its various components and consider how (if?) we can assess them and what the implications are of this assessment. The basic theory is outlined in European Implementing Guielines No. 12, and, particularly, in Annex 2.

During the workshop we have briefly run through and explain the mechanics of the audit risk model. In short, the model suggests that each SAI defines the level of audit risk (AR) that it is ready to accept. This is composed of inherent risk (IR), control risk (CR) and detect risk (DR). Mathematically, the model suggests that:

$$\text{Acceptable AR} = \text{IR} \times \text{CR} \times \text{Acceptable DR}.$$

The acceptable level of AR is defined by our SAI. If we can measure IR and CR, we can determine the acceptable level of DR, detect risk. This, in turn, tells us the risk that we can afford to accept, when we take samples for substantive testing, of not detecting errors and/or irregularities. This is done by transforming the above formulae to give:

$$\text{Acceptable DR} = \frac{\text{Acceptable AR}}{\text{IR} \times \text{CR}}$$

This is all very neat and tidy. It gives financial audit a mathematical justification that seems to give it the status of a scientific process whose conclusions are incontestable although audit is not a scientific process.

In my view, we need to post some fundamental questions about the way in which this risk model is applied in practice. For example; how do we assess inherent risk and control risk?; how do these assess inherent risk and control risk/; how so these assessments fit into the overall objectives (mission statement) of the SAI?

<div align="right">

Neil Usher
Head of Section, ECA
Co-Chairman of Antalya Workshop

</div>

Agenda of events for 2003 and 2004

Month	Day	Week	Event	Place
October	6-7	41	Meeting of the Liaison Officers of the EU Member States	Luxembourg
October	7-8	41	Meeting of the Liaison Officers of Central and Eastern European Countries, Cyprus, Malta, Turkey and the ECA	Luxembourg
October	13 -16	42	Meeting of the INTOSAI Governing Board	Budapest, Hungary
October	27-28	44	Seminar for SAIs from Candidate Countries	Luxembourg
October	28	44	Meeting of the EUROSAI Governing Board	Rome, Italy
November	17-19	47	Workshop "Audit Manuals": Audit Sampling (CEEC, CY, MT, TY)	Ljubljana, Slovenia
November	24-25	48	Meeting of the EUROSAI Training Committee (ETC) Board	Copenhagen, Denmark
December	9-10	50	Meeting of the EU Contact Committee	Prague, Czech Republic
December	9-11	50	Meeting of the EUROSAI Working Group on Environmental Auditing	The Hague, Netherlands
April 2004			Meeting of the Presidents of the SAIs of the EU Candidate Countries, Albania, Croatia, Turkey and the ECA	Riga, Latvia

SIGMA Evaluation by PHARE

EMS – the independent evaluation and monitoring service of PHARE evaluated the work of SIGMA. The evaluation covered the Phare Multi-Country assistance to the public administration reform through the SIGMA Programme.

Main findings were that the SIGMA approach combined high profile expert intervention, a good operational approach and an opportunity for continuity. SIGMA was very relevant to Public Administration Reform, very efficient in terms of timeliness, overall cost and the extent and quality of intervention. It was effective; the immediate project objectives are achieved and twinning is supported. The SIGMA approach had good indications of impact and sustainability, including the high political commitment and support to SIGMA projects.

It was recommended that SIGMA continue working in transition period but should have an exit strategy for all activities. A wider use of SIGMA approach and techniques should be considered.

**Contributions to the next issues of the Newsletter are most welcome and should be sent to
nicolasjohn.treen@oecd.org or esther.bright@oecd.org**

NEWSLETTER ● SPECIAL ISSUE ● December 2003

For the Working Groups of the Presidents of the Supreme Audit Institutions of European Union Candidate Countries, Albania, Croatia & the European Court of Auditors
Produced by SIGMA and the European Court of Auditors

European Court of Auditors

Workshops of the SAI Working Group on Audit Manuals in Tirana, Antalya and Ljubljana

It is with great pleasure that we hereby present this year's final issue of the Newsletter. In this issue we cover the three workshops: the workshop on IT Audit on 11-13 June was hosted by the Albanian Supreme Audit Office (*Kontrolli i Larte i Shtetit*); the workshop on Risk Assessment on 23-26 September was hosted by the Turkish Court of Accounts (*TC Sayistay Baskanligi*); and finally the workshop on Audit Sampling on 17-19 November was hosted by the Slovenian Court of Audit (*Racunsko Sodisce*). We have again decided to make the information and recommendations, exchanged during the course of the workshops, available to as many of our colleagues as possible. We will also make all documents available on the SIGMA Closed EDG, to be found on our Web site www.sigmaweb.org as well as the Web sites of the hosting SAIs. We will also send to all Presidents, Liaison Officers and participants, past and present, paper copies of all the documents as well as a few extra papers with information about different practices and standards relevant under the theme of the workshop in question.

We hope that you will find the reading interesting and useful in your work as public sector external auditors.

Best wishes from SIGMA

The Hosts of the Workshops in Tirana, Antalya and Ljubljana

SIGMA would especially like to thank the hosts of the three workshops (***top to bottom***): Mustafa Kerçuku, President of the Albanian Supreme Audit Office, Mehmet Damar, President of the Turkish Court of Accounts and Vojko Anton Antončič President of the Slovenian Court of Audit for their generosity and excellent work in organising the workshops.

Mustafa Kerçuku

Mehmet Damar

Vojko Anton Antončič

Conclusions from Tirana, 11-13 June 2003
Workshop on Audit of IT Systems

President Mustafa Kerçuku, with co-chair Jan Pieter Lingen (ECA) and participants and speakers from Albania, and the Netherlands

The objective of the workshop was to facilitate the exchange of knowledge and practical experience between member state, acceding country and candidate country SAIs concerning current practices and standards for IT systems and the audit thereof, so as to encourage the application of better methods and procedures for IT Audit.

In addition, a Board Member of the Information Systems Audit and Control Association (www.itgi.org), presented COBIT (control objectives for information and related technology) explaining its key concepts, practical application and principles. A representative of the Chair of the EUROSAI IT Working Group (Algemene Rekenkamer) also informed the workshop of the new and important activities of this Group.

In essence the workshop encouraged the active and expert audit of IT systems and recommended the following specific actions:

- To carry out audits of significant and material IT systems in their countries.
- To make good use of the modern and effective IT audit tool – COBIT.
- To support and be active in the EUROSAI IT Audit Working Group and support its training and other activities.
- To further exchange practical and useful information between the workshop participants.
- To encourage IT audit training in their SAIs.
- To support staff who wish to train to become specialist IT auditors through the ISACA.
- To substantially revise the EU Implementing Guideline on IT Audit.

More photos from Tirana

Participants and facilitators from Bulgaria, Albania, Slovakia, Belgium, Croatia and the Netherlands

The workshop participants with their host, President Mustafa Kerçuku

Conclusions from Antalya, 23-26 September 2003
Workshop on Risk Assessment

Group work on risk assessment with participants and facilitators

The SAIs of the Acceding and Candidate countries as well as representatives from Albania and Croatia, met for three days in order to exchange experiences and discuss good practices for risk assessments carried out in the planning phase of an audit. Besides the above-mentioned SAIs, representatives from the Danish, Portuguese and UK SAIs also attended the workshop, which was organised by the Turkish Court of Accounts and chaired by SIGMA and the ECA.

The first important task of the workshop was to define the "risk" to be discussed in view of the different definitions that exist. Starting with a more general definition of risk used in the context of social science and the "Risk Management" of an enterprise, the "Audit Risk Model" was discussed in more detail and related to the other two definitions.

The presentations of SAIs in the area of risk assessments showed very different positions. Some SAIs apply risk assessments only in very limited cases because they are obliged to audit all transactions. Most of the SAIs do risk assessments in a general way and only in qualitative terms. The differentiation between inherent and control risk is not often made and criteria for risk assessments are not always clear. One SAI reported on its experience in applying a knowledge-based software to perform qualified risk assessments. All these risk assessments were carried out in financial audits and a new dimension was given by the experience of the UK NAO in performing risk assessments in VFM audits.

All these experiences were of course based on the existing standards in the area of risk assessment.

The presentation of the new IFAC standards that are expected to be adopted late 2003, however, changed the situation. According to this new standard, systematic audit risk assessment will be part of the General Principles governing a financial audit of financial statements and it will place the risk assessment at the planning phase in the core of every single financial audit. This assessment will be necessary and the audit documentation will have to show how the results of the assessment are followed through at each of the following stages of the audit.

Audit risk assessment will be made at two levels – the overall level of the financial statements and the Assertion (or Audit Objective) level. INTOSAI have commented that the list of assertions in draft ISA 500 needs to be expanded to include "regularity" and that direct references to internal audit should be included in the standard.

Workshop Host President Mehmet Damar

The risk assessment will be made based on a comprehensive understanding of the entity, covering the five aspects of the control environment and the five elements of internal control framework. Included in these is an assumption that the entity has a risk management programme and a system for the communication of performance results.

The understanding of the entity also extends to an appreciation of events and conditions outside the transaction processing system (the accounting system), that have an impact on the financial statements. It is expected that financial auditors must have an in-depth understanding of wider business risks of the entity, what in the public sector might be interpreted as the equivalent of "value-for-money" risk.

As it is possible that there are some risks that may not be mitigated solely by substantive tests, the draft ISAs appear to rule out the option of setting control risk high, eliminating tests of controls as a source of audit evidence and relying instead on mainly substantive tests.

Participants from the Turkish Court of Accounts The audit response to the overall assessment is likely to be strengthening the resources required for the audit, identifying potential difficulties from inherent risks that cannot be mitigated by substantive procedures and setting the overall level of audit risk/audit assurance required from the audit procedures.

The participants agreed that the exposure draft might have a number of implications for SAIs:

- The national audit law of SAIs.

- The financial audit methodology model of an SAI including the need to update audit manuals and guidance and the development of templates to assist implementation.

- Intensified involvement of senior auditors in field work and better documentation of risk assessments and risk assessment decisions.

- The need for additional training and briefing material.

- Intensified co-operation with internal audit services.

- The need of communicating the new approach and the added value to auditees and parliaments.

- The need for additional resources.

- Risks assessed to be clearly linked to audit tests.

In order to better assess the risks associated with business, SAIs might also recommend that auditees introduce "Risk Based Management" in audited institutions. In addition, there is the need to test institutional risk management processes as a key control.

Conclusions and Recommendations

Risk Assessment is at present used by SAIs in the planning phase of an audit in order to identify areas on which the audit work should focus. According to the "Audit Risk Model", risks identified refer to risks that the audit institution will give a positive opinion when in fact the area audited is subject of major irregularities, misstatements or weaknesses. The identification of those risks is linked to the system of internal control and the "risk management" in the audited institutions.

Co-chair of the Workshop, Neil Usher (ECA), discussing Group work with participants and facilitators

Audit techniques to identify risk can be both quantitative and qualitative, although the quantitative approach is not very often used at present. Developments in international standards will require, in the future, that risk assessment will not only be used in the planning phase, but will be a major tool of the audit itself. This will lead to a more important use of risk assessment techniques. Even if the available international audit standards will primarily be applicable for financial audits, risk assessments in performance audits will also become more

prominent and necessary. In order to comply with those international standards for financial audits, SAIs should seek to develop specific guidance and tools for risk assessments, both for financial and value for money audits. This guidance should clearly express the link between the risks identified and the audit approach used.

****

Conclusions from Ljubljana, 17-19 November 2003
Workshop on Audit Sampling

President Vojko Anton Antončič opening the workshop with co-chairs Colin Maynard (ECA) and Nick Treen (SIGMA)

Sampling represents a key tool for auditor to gain information and to draw a conclusion about the population without the need to examine the population in its entirety. Thus, audit sampling is the application of an audit procedure to less than 100% of the total population to obtain audit evidence about certain characteristics of the population.

Although the degree of the implementation of the audit sampling differs among participants' countries, it was unanimously accepted between participants that this instrument is highly effective and efficient increasing the quality of the audit work carried out by SAIs. Also, it was observed that the approach to audit sampling on the part of SAIs is relatively homogenous, planning being based on the audit risk model and the most used sampling technique being Monetary Unit Sampling (MUS), although it is not appropriate in all circumstances and the limits of this technique have to be taken into account.

There are two general approaches to audit sampling: statistical or non-statistical. Both approaches require the auditor to use professional judgement in planning, performing and evaluating a sample. Either approach to audit sampling, when properly applied, can provide sufficient evidence. The participants in the workshop considered a series of the most important advantages of audit sampling to be the following:

- saves time and money;
- increases consistency and transparency of audit work;

Julio Cabeca from the European Court of Auditors with colleagues from Poland, Latvia, Slovakia, Turkey, Malta, Romania and France during one of the group exercises.

- encourages to apply risk based approach;
- is an effective and efficient way of auditing large complex populations;
- meets the audit objective and provides defendable audit results;
- encourages dealing with and being familiar with, the data subject to audit;
- assures harmonisation and compatibility of methods.

All participants agreed that in most cases 100% testing is impracticable on cost grounds.

However, in some cases the auditor could test in full a relatively small group of items which are sufficiently important that an error in any one of them would have serious implications for the entire population. Usually, these are high value items or a group of transactions which are particularly risky.

The essential factors to be taken into account when planning an audit sample are the following:

- Audit objectives.
- Resources available and staff knowledge of sampling techniques.
- Population size and characteristics.
- Materiality.
- Risk assessment.
- Confidence level.

The first three of these factors have an impact on selecting the most appropriate sampling method, and the last four on designing the sample size.

For the auditor to draw valid conclusions, it is essential that a sample is representative of the population from which it is drawn. This means that the attribute being tested for should be expected to occur in the sample to the same extent as it appears in the population as a whole.

In designing the sampling strategy the auditor considers if it is necessary to stratify the population before sampling. The participants agreed that if certain types of transactions are more prone to error than other transactions, they should be treated as a separate population.

In the same time the auditor has to be aware of the risk of over-stratification of a population which leads to more audit work rather then simplifying it.

President Vojko Anton Antončič with Colin Maynard of the European Court of Auditors

Before extrapolating the results of a test sample the auditor should ensure that the extrapolation will only be made over the (sub-) population from which the sample was selected.

In interpreting the sampling results, the auditor reviews the materiality limit against the projected error and against the upper error limit. The accounts will be acceptable whenever the materiality level is above the upper error limit. However, this is not always the case. A number of other situations can arise. In some cases, the auditor is faced with a situation where the materiality limit is below the upper error limit or the projected error. After debating this concrete issue, participants reached the conclusion that the auditor should always analyse the nature and the causes of the errors. Following this analysis, there are two main actions the auditor could undertake: to try to isolate errors whose effect can be limited to only a part of the population and/or to consider extending the sample size.

In the first case, the auditor determines for which part of the tested population these errors may have had consequences. In doing this, the auditor defines a threshold in terms of risks and controls and may be able to isolate the errors in a relatively small part of the population, providing a rationale for accepting the "good" part in which the error causes are not valid. However, isolation of errors is a very time consuming approach and is not efficient in cases where the auditor finds multiple error causes. It is an efficient tool to reduce the upper error limit of the sampling result.

President Vojko Anton Antončič concluding the Workshop with discussions on using the results of audit sampling

Extending the sampling size may not be the best solution because it is likely that more errors could appear. Furthermore, sample extension will reduce the original planned confidence level. By expanding the sample size, the auditor will fail to meet the required assurance unless the originally planned sample size incorporated a cushion allowing the auditor to arrive at an acceptable result even if some errors are found. Extending the sample size proves to be an effective solution in cases where the materiality level is only slightly below the upper error limit.

When neither isolation of errors nor extending the sample size are applicable and the materiality level is below the upper error limit, the auditor should consider concluding that the accounts are not reliable and/or the underlying transactions are not, taken as a whole, legal and regular. In these circumstances the auditor should consider drafting an audit report with a qualified or adverse opinion.

The general conclusion of the workshop was that sampling enables the auditor to meet audit objectives in an effective and efficient way. Participants agreed that statistical sampling is usually to be preferred as it should normally be efficient and it provides objective, representative and defendable results. Where non-statistical sampling is used, the approach to planning sample sizes, selecting items for testing and evaluating results, should be rigorous enough to ensure that the results are sufficient and unbiased.

****

!!! NEWSFLASH !!!

If you would like to join the SIGMA restricted Electronic Discussion Group – SIGMA Supporting the Exchange of Experiences – Concerning Public Sector External Audit and European Accession please contact:
nicolasjohn.treen@oecd.org or esther.bright@oecd.org

LIST OF PARTICIPANTS

Workshop in Albania		Workshop in Turkey	
Name	**Country**	Besim DIKA	Albania
Alida HYSENI	Albania	Sonila PROSEKU	Albania
Kozma KONDAKCI	Albania	Majlinda MUSTAFAJ	Albania
Sali AGAJ	Albania	Polya PETKOVA	Bulgaria
Elvana TIVARI	Albania	Krasimir YORDANOV	Bulgaria
Nevila GEGA	Albania	Bozhana NENKOVA	Bulgaria
Hendrik CEULEMANS*	Belgium	Stefka MIHAYLOVA	Bulgaria
Boycho MISHLYAKOV	Bulgaria	Verica AKRAP	Croatia
Anguel SHISHKOFF	Bulgaria	Lidija PERNAR	Croatia
Lidija PERNAR	Croatia	Clelia PAPADOPOULOU	Cyprus
Verica AKRAP	Croatia	Chrystalla ASIMENOU*	Cyprus
Marios THEOPHILOU	Cyprus	Jan KINST	Czech Republic
Eva ROUSOVA	Czech Republic	Vera NOVACKOVA	Czech Republic
Tonis SAAR	Estonia	Rolf ELM-LARSEN*	Denmark
Pentti MYKKANEN*	Finland	Ines METSALU	Estonia
Raija HOLOPAINEN*	Finland	Kristjan MELLIK	Estonia
Zsofia HANGYAL	Hungary	Gyorgyi HAMORINE MAROTI	Hungary
Ferenc BORSOS*	Hungary	Zsofia HANGYAL	Hungary
Galina KANEJEVA	Latvia	Endre Istvan AKOS	Hungary
Einars PIRAGS	Latvia	Colm DUNNE	Ireland
Rimantas BRUZGULIS	Lithuania	Ilvija ATVARE	Latvia
Paul BORG	Malta	Aija FELDMANE	Latvia
Mantoine D'AMBROGIO	Malta	Galina KANEJEVA	Latvia
Joseph CILIA	Malta	Rimantas BRUZGULIS	Lithuania
Sandro BORG	Malta	Irmantas DOBILAS	Lithuania
Thomas WIJSMAN*	Netherlands	Michael CAMILLERI	Malta
Piotr MADZIAR	Poland	Paul BORG	Malta
Wieslaw OSTASZEWSKI	Poland	Andrzej POGODA	Poland
Ramona Florela PORADICI	Romania	Bozena SULKOWSKA*	Poland
Dumitru ALAMIIE	Romania	Elzbieta MATUSZEWSKA*	Poland
Maria KYSUCKA	Slovakia	Alberto Miguel PESTANA*	Portugal
Eda VEZIROGLU	Turkey	Ovidiu ISPIR	Romania
Jan Pieter LINGEN	ECA	Verdes AUREL	Romania
Dieter BOECKEM	ECA	Dragos BUDULAC	Romania
John EILBECK*	ECA	Maria KYSUCKA	Slovakia
Lage OLOFSSON	SIGMA	Zdenka VIDOVIC	Slovenia
Esther BRIGHT	SIGMA	Cevad GURER	Turkey
		Hulya DEMIRKAYA	Turkey
		Gul NOGAY*	Turkey
		Nevin ATAKAN	Turkey
		Marcus POPPLEWELL*	United Kingdom
		Neil USHER*	ECA
		Dieter BOECKEM	ECA
Main country and other presenters		Nick TREEN	SIGMA
		Jens PIONTEK	SIGMA
		Mimi BESSARAT	SIGMA

Workshop in Slovenia

Friedrich REISINGER	Austria
Nikolai CHERNEV	Bulgaria
Emiliya DZHARTOVA	Bulgaria
Anita MENICANIN	Croatia
Neda ROGOSIC	Croatia
Kyriacos PIERIDES	Cyprus
Vera NOVACKOVA	Czech Republic
Jan KINST	Czech Republic
Ludmila VOZABOVA	Czech Republic
Pille PODER	Estonia
Oie SOOVIK	Estonia
Martine LATARE	France
Gyorgyi HAMORINE MAROTI	Hungary
Zsofia HANGYAL	Hungary
Andy HARKNESS*	Ireland
Everita POLE	Latvia
Zaiga EGLITE	Latvia
Rita KENIAUSIENE	Lithuania
Carmel TONNA	Malta
Pierre Andre AQUILINA	Malta
Paul VAN BATENBURG*	Netherlands
Wieslaw OSTASZEWSKI	Poland
Marek SIKORSKI	Poland
Elena ACIOBANITEI DOICESCU	Romania
Nicoleta Ana DRAGOMIR	Romania
Victor DAN*	Romania
Maria KYSUCKA	Slovakia
Anica BRATANIC*	Slovenia
Zoran MLADENOVIC	Slovenia
Marjan PODGORSEK	Slovenia
Goranka KIRALJ	Slovenia
Natasa SKRT-KOS	Slovenia
Nevin ATAKAN	Turkey
Kate HENDERSON*	United Kingdom
Colin MAYNARD	ECA
Dieter BOECKEM	ECA
Julio CABECA*	ECA
Dragos BUDULAC*	ECA
Nick TREEN	SIGMA
Esther BRIGHT	SIGMA

Group Photo from Antalya

Group Photo from Ljubljana

Contributions to the next issue of the Newsletter are most welcome and should be sent to:
nicolas.john.treen@oecd.org or esther.bright@oecd.org