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 contribution or comment you might have in this respect.

Juan Manuel Fabra Vallés
President of the ECA

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)
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 Michaela 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)

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.mcoogan@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-post 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.
**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 Vasek 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

**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.

**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 Sekula, 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
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.

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

The EUROSAl 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.
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 enterprise 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, ISO 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 advantages 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.
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 outside 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](http://www.isaca.org).
## Agenda of events for 2003

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

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.