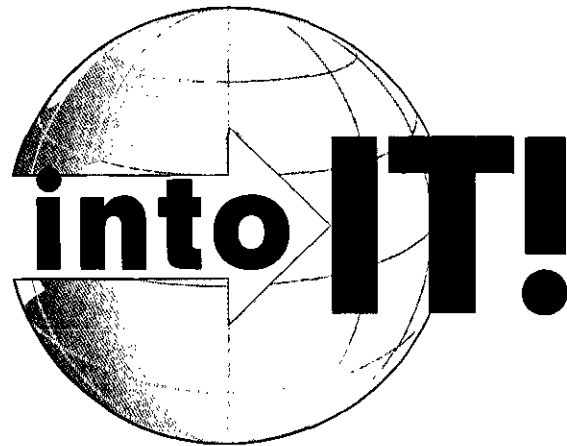


July 1995

Issue 2



The Intosai IT Journal

Country Focus Zimbabwe

**INTOSAI EDP
Directory**

**Developing Information
Technology Strategies**

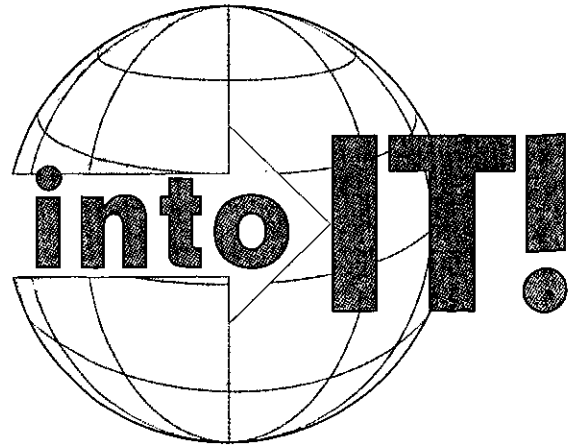
**Reviewing Information
Security**

**IT Audit Curriculum
for INTOSAI**

**INTOSAI and the
INTERNET**

**News from around
the world**





Contents

Editorial	2
Country Focus Zimbabwe	4
INTOSAI EDP Directory	9
Developing Information Technology Strategies	15
Reviewing Information Security	20
IT Audit Curriculum for INTOSAI	22
INTOSAI and the INTERNET	24
News from around the World	28

This is the second edition of *intoIT* - the IT journal of the INTOSAI EDP Committee. The journal is published twice a year, and aims to provide an interesting mix of news, views and comment on the use of IT in SAIs around the world.

Material in the journal is not copyrighted for members of INTOSAI. Articles from *intoIT* can be copied freely for distribution within SAIs, or reproduced in internal magazines, or for use on training courses.

The Editor welcomes unsolicited articles on relevant topics, preferably accompanied by a photograph and short biography of the author, and short news items for inclusion in future issues.

Contributions should be sent to Roger Goacher, Associate Director, National Audit Office, 157-197 Buckingham Palace Road, London SW1W 9SP, United Kingdom.

Editorial

The Chairman of the INTOSAI EDP Committee, Mr C G Somiah from India, details progress on projects sponsored by the Committee

In the first issue of *intoIT*, I outlined the Committee's goals and work programme. With the active participation of the Committee's members and the enthusiastic responses from the INTOSAI community, we have come a long way since then. I am happy to inform you that the Committee has already developed 5 products including this Journal. Two of these products - *intoIT* and the INTOSAI EDP Directory - should already be with you. Both these products are intended to facilitate sharing of knowledge and exchange of experiences. *intoIT* will be produced twice every year to start with, while the EDP Directory will be updated once every 3 years. This issue contains an article on the EDP Directory which will give you an idea about its contents and utility.

The INTOSAI Governing Board has already approved three other products of the Committee:

- i an Information System Security Review Methodology;
- ii a Guide to Developing IT Strategies in SAIs, and
- iii an IT Audit Curriculum for INTOSAI.

These products are being mailed to the INTOSAI members as exposure drafts for their comments, and are expected to be approved by the XV INCOSAI in Cairo this year. This issue carries a write-up about all these three products which will be available in all the INTOSAI working languages before the end of this year.

The Committee also produced a paper on funding which was originally intended to enable SAIs to present their case to various funding agencies for funding their IT programmes. The Committee has decided, after deliberations, to convert this guide to a paper captioned "Strengthening Legislative Audit Institutions in Developing Countries - A Catalyst to Enhance Good Governance" shifting the

focus to the importance of funding SAIs and not just their IT programmes. This paper has been handed over to the IDI for their use and is being carried forward by them. In a future issue of *intoIT*, we expect to feature an article on this paper.

The Committee organised a seminar in March 1995 at Stockholm on "Future Risks and Opportunities in the field of IT Performance Auditing". The seminar was well attended; representatives of 15 countries and the Board of Auditors of NATO attended. The seminar produced interesting discussions and the proceedings of the seminar will be circulated to all SAIs by July 1995.

At its recent meeting in Stockholm in March 1995, the Committee also reviewed two other products viz "Guide on Audit of Electronic Data Interchange" and "Reference List of Performance Auditing of Use of IT Systems". The Committee expects to circulate a research paper on "EDI and the paperless audit" to all the Committee members to appraise them of the implications of this new technology, and solicit their views and experience before formulating a Guide on the Audit of EDI. The Reference List which has been prepared already is also being modified and is expected to be sent to all INTOSAI members in 1996.

The Committee is presenting its work plan for the next three years to the XV INCOSAI in Cairo this September. In the forthcoming issue of *intoIT*, I should be able to share with you the plans of the Committee for the next three years.

As we progress with our work in the Committee, we have been increasingly realising the importance of *intoIT* as a fast and efficient way of disseminating information to the INTOSAI community about the developments in the IT field. These tend to be rapid and may also have significant implications for the way SAIs conduct their business. We hope to use this communication vehicle with increasing results in the years to come. We are very

gratified, therefore, with the response we have been receiving from the INTOSAI community to this Journal. You will notice that this issue contains a country focus article on the use of IT in the SAI of Zimbabwe, and news items from a number of different countries around the world. We hope that other readers will also start sending in information and articles about their experiences so that this journal serves its important goal of facilitating exchange of experiences and ideas among SAIs in the

field of IT and IT Audit. Our objective is to disseminate information to facilitate this process; therefore, we would urge you to freely use the whole or any part of this journal in your SAI's internal publications, journals, etc.

We look forward to your suggestions and contributions for improving the Journal.

Help wanted

As mentioned in the Editorial, the INTOSAI EDP Committee has been considering EDI and the Paperless Audit, and proposes to circulate a Research Paper on the subject to all SAIs.

The Office of the Auditor General of Canada is taking the lead on this research study, and the next edition of *intoIT* will contain an article on the work being done.

Canada would welcome SAIs views on the subject or details of their experiences. These should be sent to:

Mr Larry Meyers
Deputy Auditor General
Office of the Auditor General
240 Sparkes Street
Ottawa
Ontario K1A 0GA
CANADA

CD-ROMs

The INTOSAI EDP Committee has decided that the preparation of an IT-specific CD-ROM is not economically viable at present.

However, Canada has agreed to add IT-related information to the CD-ROM which it produces in English and French, and the UK will include IT-related material on their CD-ROM which is produced in English.

France is also considering producing a CD-ROM in French, which could include IT-related information.

Any enquiries about these information sources should be addressed to the SAI of the country concerned.

If any other SAIs produce, or are considering producing, CD-ROMs relating to the work of their organisation and containing IT-related material, would these please inform the Editor of *intoIT* so that he can publicise details in the journal.

Country Focus

Information Technology is having a significant impact on the operations of the Office of the Comptroller and Auditor General of Zimbabwe



Background

The Comptroller and Auditor - General of Zimbabwe

The post of the Comptroller and Auditor General (C&AG) is established under of Section 105 of the Constitution of Zimbabwe. The Supreme Audit Institution in Zimbabwe is known as the Office of the Comptroller and Auditor General (OC&AG).

The C&AG of Zimbabwe is appointed by the President and is not a civil servant. He holds office on such terms and conditions as fixed by the President. All other staff in the office, including the Deputy Auditors General, are civil servants. In doing their work, they act under the authority of the C&AG and enjoy the powers conferred on him in the exercise of their duties.

Under Section 106(6) of the Constitution of Zimbabwe "The Comptroller and Auditor General shall not be subject to the direction and control of any person or authority other than Parliament" in the exercise of his functions.

Duties of the Comptroller and Auditor General

The duties of the Comptroller and Auditor General include the following:

- to examine, enquire into, and audit the accounts of all Accounting Officers;
- to satisfy himself as to the safeguarding of all public moneys and State property;
- to audit all, or at his discretion contract out the audit of, the accounts of Designated Bodies (Parastatals) with effect from 16 July 1993;
- to carry out Value for Money Audits both in Central Government and Designated Corporate Bodies;
- to grant credit on the Exchequer Account;

- to prepare memoranda for the Committee of Public Accounts;
- to prepare and submit reports and do any other duties required of him by any statute.

Types of Audits conducted by the C&AG

The C&AG is mainly involved in three types of audits:

- Financial Audits - audits that report on the financial statements of both Government Departments and Parastatals;
- Value for Money Audits - audits that report on the economy, efficiency and effectiveness of the use of an organisation's resources;
- Specialised Audits - investigations initiated mainly by Parliament.

The C&AG's Report

The C&AG is required to report each year on the results of his examination of all financial statements which he audits. He always reports on any qualifications of his audit certificate.

The C&AG has to report on and, where applicable, certify the accounts he audits every financial year. In addition to his annual report, the C&AG also prepares special reports as and when necessary. Since the office started conducting Value for Money audits, results of such audits are presented to Parliament.

Organisation and structure of the Audit Office

The policy and overall operations of the Audit Office are vested in the Policy Committee made up of the C&AG, the two Deputy Auditors-General and one Deputy Manager responsible for Parastatals. The power of final decision rests with the C&AG. The main body of the office comprises nine Directors of Audit, and sixteen assistant Directors of Audit who

head the various audit sections of the office. Below them come Senior Auditors, Auditors and Audit Assistants.

Eleven of the sections carry out financial audits of Central Government and Parastatals. Three sections carry out Value for Money Audits. The 'IT' section is mainly a service section involved in the computerisation of the Audit Office. It assists the various sections in their use of computers. It also audits the various computer systems used by Government Departments.

Goals and objectives of computerisation

The objectives of computerisation in the OC&AG is to ensure that the C&AG carries out his duties in a more economical, efficient and effective way. The computerisation can be broadly divided into two main areas - automation of the audit process and automation of the administration and accounting functions.

Automation of the Audit Process

The main objectives of audit automation are to:

- perform better quality audits;
- perform audits in less time thereby meeting the statutory deadline for the C&AG's report;
- increase audit coverage;
- produce performance reports, management letters, plans and other reports in less time.

Automation of the Administrative/Accounts Routines

The main objectives of computerising the administration and accounting routines are to:

- provide timely and accurate information for management, thereby facilitating decision making;
- prepare reports needed by Treasury and any other parties in time;
- be able to retrieve information on both accounts and personnel issues timeously;
- perform work using minimum required resources.

To achieve these objectives, a set of guidelines was devised to facilitate a planned and structured implementation of EDP.

Activity Areas

Automation of the audit

EDP is supporting work in different audit areas:

Word Processing

WordPerfect is used in the Office. This allows the auditor or the audit manager to

Audit Phase	Activities	Documents	Tools
Preparatory	Planning the audit work	Audit Plans	Wordprocessing Spreadsheets IDEA
Examination			
Current Examination	Internal Control Evaluation	Report on Current Examination	Wordprocessing Spreadsheet
	Compliance and substantive tests	Working papers	Database IDEA
Final Examination	Substantive tests Analytical Review	Report on Final Examination Working Papers Memorandum Audit Report	Word processing Spreadsheet Database IDEA

write his own reports, memos and audit programs. Documents can be retained, updated and printed for the audit with a minimum effort and cost. Every officer is now using WordPerfect 5.1. This wordprocessing package is used to produce:

- staff performance reports;
- special reports;
- audit programs;
- audit working papers;
- memos;
- management letters;
- standard forms;
- circulars.

The introduction of computers and wordprocessing to all audit sections, accounts and administration departments has greatly reduced the work load of the typing pool.

Spreadsheets

The Microsoft Excel spreadsheet is used for a variety of functions, including:

- analytical review of client data;
- production and analysis of various schedules of data;
- preparation of financial statements which feature in the Comptroller and Auditor-General's report;
- audit project planning, budgeting and monitoring.

The introduction of Excel enabled the 1992/93 C&AG's Report to be produced within the Office, for the first time. The accounts department is also using Excel for:

- control of asset inventory;
- forecasts of expenditure;
- salaries forecasts;
- expenditure commitment control;
- reconciliations.

Data Analysis

A software package called Interactive Data Extraction Analysis (IDEA), developed by the Auditor General of Canada is now being used for audit purposes within the Office. Using this software the auditor now carries out:

- data extraction. This enables the auditor to extract certain sets of data which meets his/her criteria;
- displaying or printing the auditors query results as standardised or as customised reports;
- data analysis;
- file management.

IDEA is currently used to analyse Government expenditure. The Government Computing Service Department provides a monthly file containing details of transactions for all Government ministries and departments. The IT section distributes this data to the various audit sections.

Audit sections used IDEA on a pilot basis during their interim audits to analyse the Government expenditure transaction files for the 1992/93 financial year. The transfer and subsequent analysis of salaries and wages data is also being trialled.

Automation of the Administrative/Accounts Routines

Before the accounts and administration functions were computerised there were many problems in creating or updating records due to the volume of transactions and the amount of paper work involved.

The following activities have been automated:

<i>Activities</i>	<i>Documents</i>	<i>Tools</i>
<i>Budgeting</i>	<i>Plans and budgets</i>	<i>Wordprocessing Spreadsheets</i>
<i>Maintenance of various Registers, eg Commitment Suspense Accounts</i>	<i>Updated Registers Schedules of Outstanding Amounts</i>	<i>Spreadsheets</i>
<i>Maintenance of Personnel Records; Assets, Files</i>	<i>Staff schedules, Reports and Extraction</i>	<i>Database Spreadsheet Wordperfect</i>
	<i>Asset Schedules</i>	

Accounts

IT is now being widely used in the Accounts Department for a variety of functions including the following:

- control of asset inventories;
- forecasts of expenditure;
- salaries forecasts;
- expenditure commitment control;
- reconciliations

All the above routines are now fully automated and are being done timeously.

Administration

IT is now being used in the Administration department mainly for controlling personnel records. A database for all personnel records has been created. It is now easy and faster to access, add or update any information relating to personnel issues.

Hardware/Software

At present the office is equipped with 26 ICL 386 desktop computers, 20 386 AST laptops and 10 486 AST laptops. We also have nine printers - three laser printers and six dot-matrix printers.

The office uses MS-DOS as its operating system on stand alone PC's. Other application packages being used are Harvard Graphics, Word for Windows and Norton Utilities.

Responsibilities

To spearhead and speed up the whole computerisation process in the office, a three-tier EDP structure was formed in the office:

- Computer Committee - Guidelines;
- Information Technology - Technical and User Support
- Keyperson - Local Support

Computer Committee

The Computer Committee membership is composed of representatives from the IT section and other sections. The IT section Director is the chairperson of the committee. The duties of the committee are:

- to determine the general development and priorities regarding the use of computers for audit;
- giving feedback on the support being given by the IT section.

IT Section

The IT section was formed in April 1991 to spearhead the computerisation of the office. Its responsibilities are as follows:

- assessment of needs and procurement of hardware and software;
- acquiring data from Central Computing Services and distributing it to sections for use with IDEA;
- provision of technical and user support;
- arranging courses for competence building in computers;
- audit of computerised systems;
- software research and development and programming;
- virus management;
- network administration and management;
- computer security;

- training;
- computer maintenance.

Key Persons

It was envisaged that the demand for services to audit teams would continue to increase as the use of computers in the office gained momentum. This would overburden the IT section and create a backlog of work. The solution was to decentralise the activity by the development of 'keypersons' at different sections who serve as local agents for the introduction and further use of computers.

The keypersons also act as the middlemen between their sections and the IT section. They are expected to bring their section's needs and proposals for development of computerisation to the attention of the IT section. 16 keypersons representing the 16 audit sections have so far been trained in their roles as keypersons.

User Group	Type of Training
<i>Information Technology Section</i>	<i>MS-DOS Advanced MS-DOS Technical Support WordPerfect Excel DBase Basic DBase Programming IDEA Network Administration & Management Virus Management Computer Auditing Security Management</i>
<i>Keypersons</i>	<i>MS-DOS Basic Technical Support WordPerfect Excel DBase IDEA</i>
<i>Financial Auditors</i>	<i>WordPerfect Excel DBase IDEA</i>
<i>VFM Auditors</i>	<i>WordPerfect Excel DBase IDEA</i>
<i>Accounts / Administration</i>	<i>WordPerfect Excel</i>
<i>Management</i>	<i>Management Information Systems WordPerfect Excel DBase IDEA</i>

Training

Training for each user group is as shown in the box on the previous page.

The above training is being conducted both in-house as well as externally and it is an on going process.

The Future

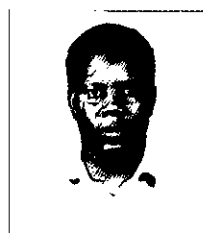
Currently an exercise is in progress to connect all the PCs in the office to a network. This will enable sharing of information between users and devices like printers. It is also envisaged that in future the ratio of PC to Auditor will be 1:1 and computer literacy in the office will be 100%.

Authors of this article



Mr A Chanakira

Mr A Chanakira joined the OC&AG in 1983 as an Auditor and rose through the ranks to his current position as Assistant Director - IT. He is in charge of the computer systems



Mr D Marimwe

Mr D Marimwe joined the office in 1990. He is now a Senior Auditor responsible for computer support services and computer audits within the public sector.



Mr A Gumbo

Mr A Gumbo joined the office in 1989. He transferred to the IT section from Financial Audit in 1993, and is now responsible for computer support services within the office.



Mr J Manyeruke

Mr J Manyeruke transferred from the Central Statistical Office to the OC&AG in 1992. He is now responsible for computer support services within the office.

The INTOSAI EDP Directory

Mr Chandramouli of the Indian Audit Office reports on the compilation of a significant information basis for all SAIs

Few modern developments have impacted on SAIs in the way that Information Technology (IT) has. The rapid advancements in IT pose a plethora of problems and provide new opportunities for all institutions, more so for SAIs who are influenced considerably by the changes in their auditee-institutions. The difficulties faced by the audit community in facing these challenges and the recognition of the importance of co-operative efforts in harnessing IT found expression in Berlin in 1989 during the XIII INCOSAI. The INTOSAI Standing Committee on EDP Audit was formed in 1992 to meet the aspiration of the INTOSAI community for a joint effort to harness IT.

Besides promoting the discussion and dissemination of standards and guidelines, a major goal of the Committee is to provide information and facilities for SAIs to exchange experiences and to facilitate co-operative ventures among SAIs. To fulfil this mandate and to create an information base for its work, the Committee conducted a multi-lingual survey between the end of 1993 and the first half of 1994; the survey was intended to identify:

- the status of SAIs in the use of Information Technology;
- the IT-related resources available to SAIs; the levels and types of IT-related skills available in, or needed by, SAIs;
- the status of SAIs in the audit of Information Technology;
- the expertise available in SAIs in auditing Information Technology; and
- SAIs access to, or need for, funding for bilateral or multilateral co-operative efforts related to IT.

The response to the survey was overwhelming; many SAIs have offered to share their software, training course-ware and other resources with other SAIs. The majority of the information, painstakingly furnished by 108 SAIs, has been collated, analysed and presented in the INTOSAI EDP Directory. The Directory is one of the

products through which the Committee expects to provide members, from time to time, with useful information about the IT-related activities and resources of other SAIs and pave the way for mutually beneficial bilateral and multilateral partnerships!

Contents of the Directory

The 336-page Directory is organised into 5 sections:

- **Introductory Section:** This contains the organisation of the Directory, the sources of information for the Directory and the list of SAIs who responded to the survey.
- **Profile of SAIs:** This section contains an SAI-wide collation of information, presented in a standard format for easy reference.
- **Topic-wise Information:** This section is organised topic-wise, to enable SAIs looking for particular types of information, assistance or association to seek out suitable partners or identify appropriate sources of information.
- **Analysis of responses:** This section contains a descriptive analysis of some important IT aspects of SAIs. Illustratively, this section highlights the IT strategies followed by SAIs who use IT relatively extensively, the typical use of common software packages for audit purposes, the type of assistance that would be available to SAIs seeking to build up the IT function, etc.
- **Appendices:** The appendices include (i) the addresses of SAIs including their membership of Regional Working Groups of INTOSAI and (ii) the survey questionnaire.

Profile of SAIs

This section is expected to provide an idea of the IT status of each SAI, including some important information relating to IT audit:

- The hardware base of the SAI is specified, with the types (PCs, minis, mainframes) and quantities. The operating system (DOS, Windows, UNIX, etc) is also shown.
- The software packages commonly used by the SAI are indicated under various categories like spreadsheet (Lotus 123, Excel, etc.), database (dBase, Foxpro, etc.), word processor (Word, Wordperfect, etc.), desk-top publishing (Page-maker, Ventura, etc.), flowcharting (ABC Flowcharter, Visio, etc.), graphics (Freelance, Harvard Graphics, etc.), project management (Microsoft Project, HPM, etc.), communication (Procomm, etc), electronic mail (cc-Mail, Microsoft Mail, etc.), text retrieval, etc. The operating system and how the SAI uses the software for various audit activities are also mentioned.
- The audit software that each SAI uses are shown according to the main function they perform viz. downloading from mainframe computer, data extraction and analysis, sampling, etc. In addition, the types of audits - financial attest, VFM, security evaluations, etc. - the SAI uses such software and techniques for are also spelt out.
- To provide an idea about the IT-skilled personnel resources of the SAI, information is provided about (i) the size of the IT Department, (ii) the type of persons employed in that Department (Audit Directors/Managers, Auditors, Professionals, Specialist, etc.) and (iii) the extent of IT and IT Audit literacy and proficiency among the personnel employed by the SAI.
- The types of IT-related training courses organised by the SAI for different categories of personnel are indicated to enable other SAIs to determine sources for training material, assistance, etc.
- Though the survey questionnaire contained several matters relating to IT audit, some key information about the IT audit function of each SAI is provided: (i) the extent and types of IT environments encountered among auditees by the SAI, (ii) the periodicity of survey of auditees IT systems, (iii) the SAIs involvement in systems under development including consultation prior to introduction of IT-based systems, and (iv) the types of IT audits conducted, IT audit techniques employed, deployment of IT professionals, etc.

Topic-wise information

This section contains information on a number of topics, collated from the responses of the SAIs, and presented in a series of tables with short explanations at the beginning of each table. This section provides (i) general information to all SAIs about IT audit practices and tools, (ii) specific information that will enable SAIs to work out bilateral or multilateral arrangements relating to setting up the IT or IT audit function, designing, developing or organising IT training, etc., and (iii) a basis for exchange of software and IT literature among SAIs.

Sharing Software: Many SAIs have offered to share their software with other SAIs either free of cost or against payment. This software is grouped in the Directory under the following broad categories:

- Audit Automation Software (offers from 12 SAIs).
- Office Automation Software (offers from 18 SAIs).
- Audit Software for different types of audits - financial attest audit, performance audit, security evaluations, etc (offers from 4 SAIs).

These tables also provide information about the name of the software, the operating system and hardware needed for running them, the function of the software (audit planning, audit management, resource management, payroll, etc.) and the terms of supply (free, royalty fee, on payment, etc.).

Direct Training Assistance: Many SAIs have offered assistance to other SAIs for IT training by (i) taking trainees on their regular training courses, (ii) organising special courses for other SAIs, and/or (iii) providing on-the-job computer-related training.

- Regular Training Courses: 12 SAIs have offered to take persons from other SAIs on their regular courses, for a variety of courses including word processing, database management, programming, audit interrogation and statistical sampling. Most of the SAIs are offering this free of cost. The number of slots in each course so available is also indicated in the Directory in most cases, and ranges from 2 to 30 per course.
- Special Courses: 11 SAIs have come forward to organise special courses for other SAIs on topics like word processing, spreadsheets, data base management, audit interrogation (IDEA, ACL),

mostly for 1 week each. In most cases, the SAIs have offered to run the courses both in their own country and in the country of the requesting SAI, depending on the latter's needs. They have also indicated the approximate duration of the courses, the terms of payment (free or on payment), and the location at which the courses would be organised

- On-the-job training: 15 SAIs have offered to provide such training to other SAIs.

Other forms of assistance for training: 22 SAIs have offered to assist other SAIs by providing faculty for computer courses, assisting in designing courses, developing or sharing course-ware, providing case studies, etc. The terms of assistance viz. on payment, free of cost, etc. are also shown in many cases. 12 SAIs have also come forward to sponsor symposia and conferences relating to EDP auditing.

Expert Assistance: 21 SAIs have indicated willingness to assist other SAIs by sparing their experts either to advise them regarding setting up the IT function or by assisting in EDP Audits. In most cases, SAIs have offered both types of support.

Financial Assistance: SAIs have offered financial assistance to other SAIs in several forms.

- 11 SAIs have offered to depute experts at their own cost to assist other SAIs. In all, 42 SAIs have offered to depute experts at their own cost, provided the recipient SAI would bear stay and other local expenses.
- 8 SAIs have funding arrangements for entertaining officials from other SAIs for training, conferences, symposia, etc. 3 SAIs have funding for training, coaching, research, etc.

Audit Software: This is one of the most important segments of the Directory. The users of audit software have been classified into 3 broad categories.

- Classified by techniques: 49 SAIs are listed who use audit software for downloading, data extraction and analysis, and sampling. 24 SAIs use software for Risk Analysis or other aspects of audit. In all these cases, the name of the software and the operating system are specified. The popularity of IDEA and ACL is clear from these tables.
- Classified by types of audits: 29 SAIs have indicated the use of audit software for financial attest audit, 12 SAIs for performance audit, 10 SAIs for security evaluations and 10 SAIs for other types.

Wherever known, the name of the software, its main function and the hardware needed for using the software are also shown. Besides the widespread use of IDEA and ACL, several SAIs appear to be using popular packages like Lotus 123 and Excel for such audits.

- Classified by audit automation activity: 76 SAIs are listed as using software for one or more audit automation activities like planning, management, control and reporting. Names of software along with operating system have been indicated wherever known.

Guidelines: Many SAIs have guidelines for developing application software, assessing their hardware and software requirements, selecting vendors for hardware and software, post-warranty maintenance contracts, EDP systems management, data security and auditing EDP systems. The availability of such guidelines in 59 SAIs is indicated in the Directory along with the SAIs willingness to supply copies and the language in which the documentation is available. 37 SAIs have confirmed that they follow or have evolved guidelines for auditing IT systems; nearly all of them have expressed their willingness to provide a copy thereof.

IT Audit Reports: 37 SAIs have indicated that they have IT audit reports relating to financial attest audit (18 SAIs), performance audit (20 SAIs), security evaluations (22 SAIs) and other types of audits (8 SAIs). In most of these cases, the language and the electronic format (Word, Wordperfect, etc) in which the reports are available have also been shown; if not available in electronic format, this has also been indicated. SAIs can contact these SAIs to get copies, depending on their areas of interest. Many SAIs have already offered to supply abstracts in English of such documentation.

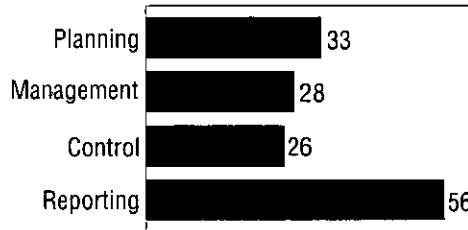
Research Activities: Several SAIs are engaged in IT-audit related research in such areas as Electronic Data Interchange (EDI), Electronic Funds Transfer (EFT), Networks, Expert Systems, etc. Many SAIs have expressed willingness to participate in research with other SAIs. For instance, 35 SAIs have indicated that their auditees use or plan to use EDI or EFT; these SAIs can contact the 9 SAIs who are researching EDI audit or the 4 SAIs researching EFT audit. SAIs currently engaged in research can identify potential research partners from the large number of SAIs who have expressed willingness to deploy their resources for such research. SAIs already engaged in research and SAIs wishing to participate in research have been listed according to the area of research.

Analysis of Responses

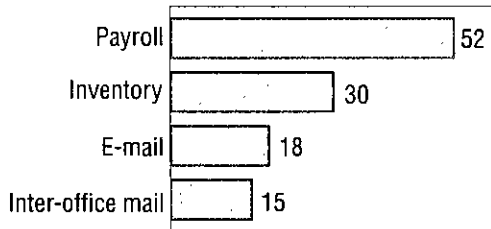
While the other sections give SAI-specific information, this 9-page section of the Directory contains an analysis of the responses of SAIs to certain questions concerning IT strategy, IT Audit Practices, etc. Some of these are reproduced or extracted here.

Automated Applications: The applications that are typically automated by various SAIs were broadly categorised as Audit and Office Automation in the survey questionnaire; responses to these two questions showed that reporting is the most commonly automated audit application followed by audit planning, while the payroll and inventory feature most among office automation.

Audit Automation



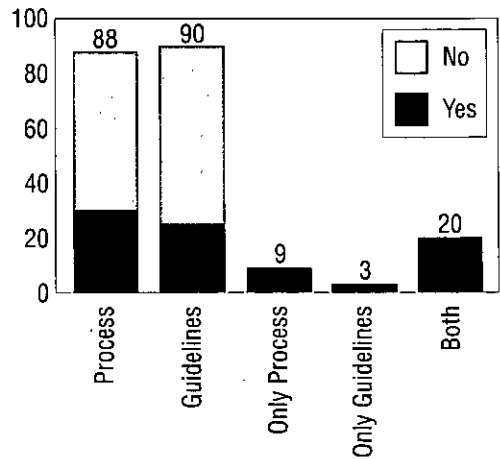
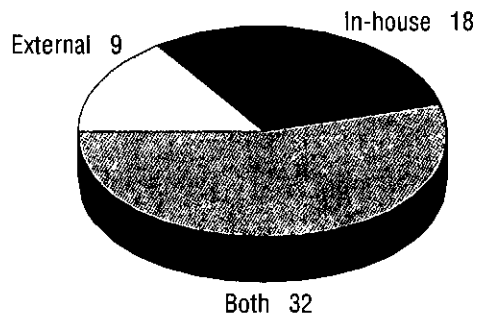
Office Automation



Software Development: SAIs were requested to indicate whether they develop their application software in-house, with the help of external agencies or through a combination of both. They were also asked to state whether they had any prescribed process and guidelines for development of application software. Their responses, summarised at the top of the next column, show that the majority of SAIs do not have a prescribed process or guidelines for software development.

IT Strategy: 56 SAIs have formalised their strategy with a clearly stated policy while 38 stated that they have not. While 44 SAIs have also established a Steering Committee for planning and regulating IT activities, 48 SAIs have not done so. The majority of the SAIs (53) have a separate IT Department; in 42 cases, the IT Department reports to the top management. The IT department generally has both hardware and software experts, though software experts are more common. In nearly 50% of cases, it also

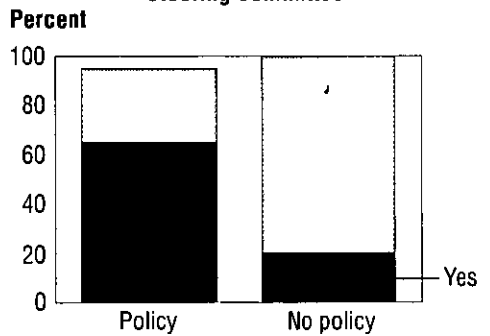
Source



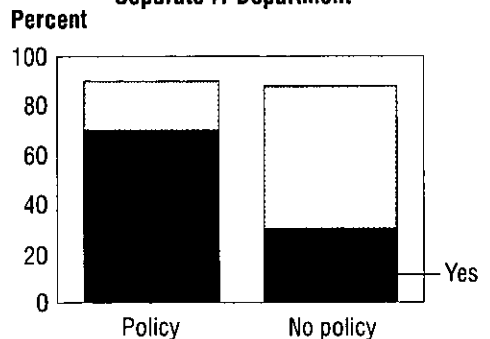
comprises qualified EDP Auditors. Most SAIs have said that the separate IT department is a combination of a service department and a specialist computer assistance group.

The following figures show that SAIs who have a formal IT policy or strategy are more likely to have a steering committee and a separate IT Department:

Steering Committee



Separate IT Department



Of the 56 SAIs who have a policy, 22 also have guidelines for EDP Systems Management and 30 for Data Security. A few SAIs have such guidelines even though they do not have a formal policy.

Computerisation among auditees: the extent of audits in which SAIs typically encounter IT Systems varies widely. For convenience, SAIs have been grouped broadly under four heads, depending on the volume of IT auditees that they encounter. A number of responses to the survey questionnaire have been analysed with reference to this categorisation; for example, the usage of audit software and professionally qualified IT auditors, types of IT audits conducted and their timing, IT audit techniques used, etc. How far the tasks of these SAIs are facilitated by a standard development methodology and whether the (mandatory) training on IT for their staff is a matter of policy, are also depicted below to facilitate conclusions being drawn.

Audit Techniques: In their choice of type of testing - compliance testing, direct substantive testing or a combination of both - those favouring one or the other are equal in number (12 SAIs) but the majority (43 SAIs) prefer a combination of the two. The combination of the two methods is also clearly the most used technique.

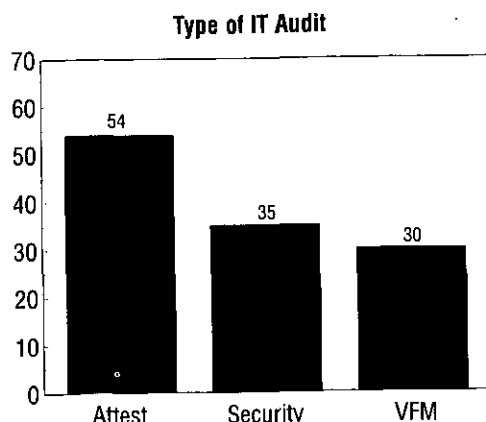
Interestingly, SAIs with high percentage of IT auditees prefer direct substantive testing over compliance testing.

Software Tools: Nearly 50% of SAIs use audit software for at least one type of IT audit. The use of audit software for security evaluations is more prevalent among SAIs with larger population of IT auditees, while its use for VFM audits is almost totally concentrated among SAIs with very high percentage of IT auditees. In general, the use of audit software is more widely prevalent among SAIs which have a larger hardware base.

Percentage of Auditees	0-10	11-25	26-50	51-75	76-100
No. of SAIs	30	7	8	8	14
Users of audit software	11	6	3	4	12
Have qualified IT auditors	8	3	3	0	8
Where auditees use standard methodology for system development	6	1	3	4	5
Prescribe mandatory IT training	5	3	4	1	11

IT Audit Practices:

Types of audits: Amongst the types of audits involving the use of IT, Financial Attest audit is the most widely prevalent, followed by security evaluations. This trend is common to all categories of SAIs though the percentages are high for SAIs who have more than 75% IT-auditees.



Use of audit software: Amongst the uses of audit software, financial attest audits clearly outnumber VFM audits and security evaluations.

Involvement during development of IT systems: In most countries, auditees are not required to consult the SAI before introducing IT-based systems. However, a number of SAIs do get involved during the development phase of the IT systems of auditees, primarily with a view to providing an audit trail for themselves. Some SAIs even approve the systems design and see no difficulty in this arrangement. Some get involved to ensuring adherence to standards or to embed audit modules.

Timing of IT audit: The majority of SAIs undertake IT audit during the normal audit cycle though some do so at the design stage or after testing.

IT audit personnel: SAIs seem to prefer using both IT experts and generalist auditors for conducting their IT audits. The practice of engaging IT professionals (consultants) for assisting the IT audit teams is also widely prevalent (21 SAIs).

Guidelines for IT audits: 37 SAIs have stated that they either have evolved or follow guidelines for auditing IT systems; 46 SAIs replied that they do not have such guidelines. The proportion of SAIs using such guidelines is higher among the SAIs who have more IT auditees.

Training: 24 SAIs feel that their training facilities are adequate for their needs while 47 SAIs feel that they are not sufficient. 41 of the 47 SAIs have expressed the need for assistance from other SAIs. Conversely a number of SAIs have offered training assistance to other SAIs as already highlighted.

Appendices

The addresses of SAIs, with contact telephone and facsimile numbers, has been included for easy reference. While every effort has been made to collate the responses of SAIs carefully, the survey questionnaire that was circulated has been included as an Appendix so that SAIs interpreting the contents of the Directory can study the responses in the context of the questions in the questionnaire. Further, the Directory has been prepared using a major part of, but NOT all the responses to, the questionnaire. So, SAIs

who may need information implicit in the questionnaire but not included in the Directory could approach SAI-India for matters of particular interest to them. The INTOSAI EDP Audit Committee has already been using such information for its projects.

Conclusion

The compilation of the Directory was a mammoth effort to which several SAIs contributed greatly, including those who responded to the survey by devoting considerable effort. We are grateful to all of them. The task of the EDP Audit Committee will be greatly facilitated by this Directory. However, the Committee will also be hampered by the lack of information about the SAIs who did not respond. The table below lists the SAIs who responded to the survey. May I take this opportunity to request those who have not responded, to kindly send in the information about their SAI to SAI-India at the following address, so that we can update the Directory:

Principal Director (Research &
International Relations)
Office of the Comptroller &
Auditor General of India
10 Bahadur Shah Zafar Marg
New Delhi-110002, India
Facsimile: (91)-11-3315446

The Directory was mailed to all SAIs in January-February 1995 and contains a copy of the questionnaire.

Algeria	Greece	Montserrat	St Kitts & Nevis
Antigua	Grenada	Myanmar	Saint Lucia
Australia	Guyana	Namibia	St Vincent & The Grenadines
Austria	Hong Kong	Nauru	Sultanate of Oman
Barbados	Hungary	Nepal	Suriname
Belgium	Iceland	Netherlands	Swaziland
Bermuda	India	New Zealand	Sweden
Bhutan	Indonesia	Norway	Switzerland
Botswana	Iraq	Pakistan	Tanzania
Brazil	Ireland	Panama	Thailand
Brunei Darussalam	Israel	Papua New Guinea	Togo
Canada	Italy	Paraguay	Tonga
Cayman Islands	Japan	Philippines	Trinidad and Tobago
China	Jordan	Poland	Tunisia
Cyprus	Kiribati	Portugal	Turkey
Czech Republic	Korea Puerto	Rico	Uganda
Denmark	Kuwait	Romania	United Arab Emirates
Egypt	Lebanon	Saudi Arabia	United Kingdom
El Salvador	Luxembourg	Seychelles	USA
Estonia	Malawi	Sierra Leone	Vanuatu
Ethiopia	Malaysia	Singapore	Venezuela
European Communities	Malta	Solomon Islands	Western Samoa
Finland	Mauritania	South Africa	Zambia
France	Mauritius	Spain	Zimbabwe
Germany	Mexico	Sri Lanka	

Argentina, Colombia and Yemen have also sent responses.

Developing Information Technology Strategies

SAIs often experience difficulties in formulating their IT Strategy. Steve Doughty of the UK NAO discusses a new guide which may help

Background

In October 1993, the INTOSAI EDP Committee agreed that, as part of its work to support and promote the development and transfer of knowledge, it should produce a good practice guide on developing IT Strategies in SAIs. The United Kingdom took the lead in producing the guide, and a draft was considered by the Committee in August 1994, and then submitted and approved by the INTOSAI Governing Board in October. By the time you read this, the guide should be available.

The guide is primarily aimed at senior management concerned with directing development of an IT Strategy. But the issues which arise in considering such a strategy concern all staff to some degree. Staff are involved as providers of information, recipients of information, direct users of systems, or through their audit work as reviewers of systems of audited bodies.

This article focuses on three areas of interest. Two are for people who are relatively new to the world of IT:

- why have an IT Strategy?
- how small bodies, with no existing IT, can get started.

The third, for those more familiar with IT systems, considers:

- how bodies with an existing investment in IT should tackle changes in IT strategy and migration to new systems.

Why have an IT strategy?

The work of an audit institution is just like a business, and goes far beyond the provision of audit services. To be successful the audit office must develop

policies to meet the changing environment in which it operates. It must also demonstrate best practice by managing its audits economically, efficiently, and effectively; by managing and motivating staff to perform at their best; and by properly managing and controlling other resources and support activities.

Sustained business success can only be achieved if the right information is available when key decisions are required. To ensure this the information needs to be organised into "information systems". These systems may be manual, technology assisted, such as a card index system, computerised, or a combination of all three.

To ensure that the right information is available when required systems must be planned so that:

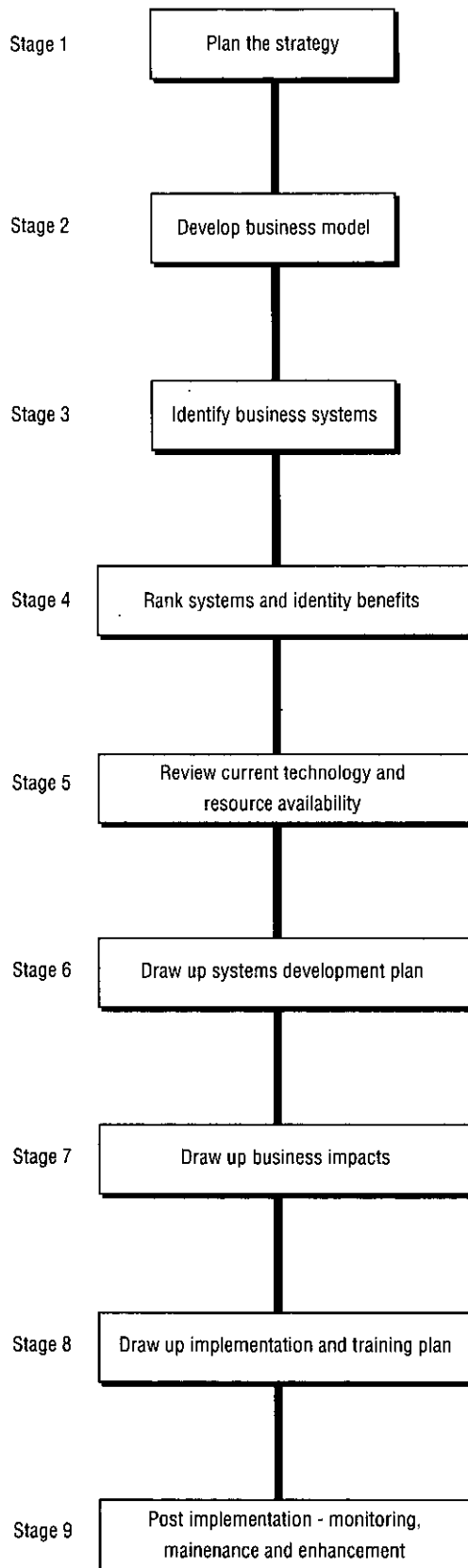
- the aims and objectives of the business are understood;
- information requirements are clearly set out which support achievement of aims and objectives;
- the systems needed are defined;
- the role of IT in supporting systems is clear;
- policies, priorities and development and implementation plans are agreed;
- resources needed to implement the strategy are provided;
- potential impacts, such as the effect on organisation and culture are identified, and the evolving strategy is managed and reviewed. The purpose of an IT strategy is to bring all this information together into a plan that makes the best use of both information and technology needed to support the business, but at



Steve Doughty



Steve Doughty joined the NAO in 1986 from the Ministry of Defence. Until recently he was the manager of Finance. He has just taken on a new role as the project manager of a team developing and implementing new IT systems.



the same time takes account of constraints such as the availability of resources. Information Technology is here to stay, and will continue to improve at an ever increasing pace. All organisations, of whatever size, need an IT strategy to ensure that best use is made of the funds available. It is all too easy to spend lots of money on computers and software without realising the full benefits. For example, one small element of a strategy review is to ensure that standards are adopted that allow data from different systems be integrated when necessary or passed between different users. But without it, the added value to be gained from data integration and exchange, probably at no extra cost, would be lost.

The most important factor is that using a structured method to develop an IT strategy allows a high level business approach to be adopted that ensures that resources are committed in line with business objectives, rather than on pure technical considerations. Quite often, the main benefits of a strategy initially have nothing to do with IT. A formal strategy review means that the organisation is forced to consider overall aims and objectives and results is a statement of direction which may not have been clear previously. Only then can there be a commitment to developing the role of IT in the organisation to support it.

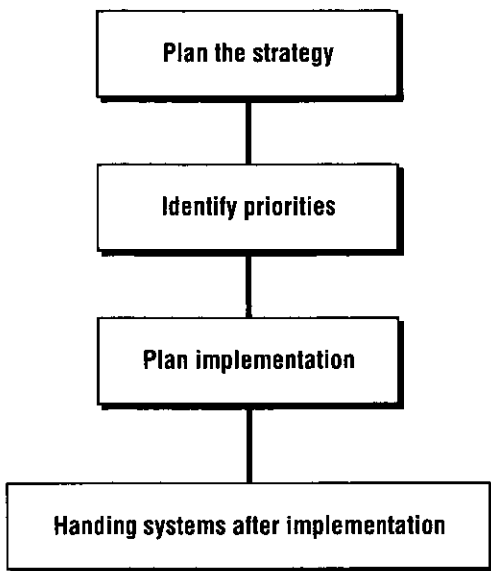
Undertaking an IT strategy will lead to a better understanding of the business so that objectives may be achieved more efficiently and effectively. But it is important to make sure that the strategy is appropriate for the size of body under consideration.

The next section of this article covers what might be appropriate for a very small SAI with no existing IT.

How small bodies should get started

For a small audit office, without any existing IT, the first step might be to buy a few personal computers and to implement office systems such as word processing and spreadsheet. But even then, a logical and systematic approach is essential. Limited resources make it vital that best value is obtained from what is available, and in order to do so a strategy must be planned in a systematic way.

In these circumstances it might be appropriate to streamline a full IT strategy review into 4 stages:



Stage 1 - Plan the strategy

The main elements of this stage are:

- appoint a senior management sponsor;
- decide who is going to undertake the strategy review;
- draw up a timetable; start with a review of the business of the audit institution, not the technology available.

Stage 2 - Identify priorities

The outcome from this stage should be a clear statement of proposed systems and priorities. To achieve this it is necessary to:

- agree a set of main business objectives and functions, ensuring that there is a full understanding of the business;
- consider whether improvements could be achieved by other means, for example, by using manual or card index systems;
- consider whether some of the functions which are candidates for computerisation could be managed better by someone else who already has or is developing computer systems, for example, a bureau;
- consider the benefits of enabling technology, such as office automation - stand alone PCs with word processing and spreadsheet software - and whether this would be a good introduction to computers and information technology. A focus on user awareness and education may well be a first priority.

- other potential computer systems can be ranked according to their corporate objectives, but there is little point in putting a great deal of effort into evaluating systems of lower priority until the organisation has the skills or resources available for implementation;
- ensure that proposals have senior management approval and that the resources to develop, implement and support the strategy will be available.

Stage 3 - Plan implementation and training

Key points for this stage are to:

- consider package solutions - they may not meet requirements precisely, but are much cheaper to support;
- train at least one member of staff to act as "an intelligent purchaser" and to act as trouble-shooter. This will help cut through some of the gloss from manufacturers and salesmen, and will reduce dependence on expensive external resources;
- ensure that all users will receive adequate training to get them started - even with standard word processing and spreadsheet packages. The IT strategy is likely to fail if users are afraid of, or uncomfortable with, using computers or they do not know what is expected of them;
- get senior management approval to the plan and a specific commitment for resources to implement it.

Stage 4 - Handling systems after implementation

The final stage of developing the strategy is to plan what will happen after implementation. The main features are to:

- plan for maintenance of both hardware and software;
- plan for monitoring the use of the IT implemented to ensure that the expected benefits are being achieved;
- plan for enhancements - to meet user requirements once they have become familiar with what computers can do, to meet technological change, and to implement other planned systems as resources become available;
- keep the documentation produced as part of the strategy review up to date to reflect changes as they arise;

- ensure resources are available to keep the system running and that the organisation are not over reliant on a small number of key staff who may decide to market their newly acquired skills elsewhere;
- review and update the overall strategy periodically.

Limited resources may mean everything desirable cannot be achieved immediately or even in the foreseeable future, but the review will have revealed what should be done, established priorities and set out the path for achieving those most important.

Developing a Strategy for migration - how to implement major strategy or systems changes

This section offers some advice to SAIs who are considering migrating existing systems. This is more likely to be the case in larger bodies.

Plan the strategy

First of all, if you don't have an IT strategy, this is the time to undertake a full review! The procedures in the Guide mentioned at the beginning of this article sets out each of the stages in some detail. The nine main stages are shown in the graphic at the end of this article. The remainder of this section of this article offers some brief comments on the key points.

A senior management sponsor must appoint a steering committee, who in turn appoint a project team.

Review existing systems and data

An existing IT strategy should be reviewed and updated. The business model (Stage 2) should be updated, and key business information systems identified (Stage 3). Some of these may already exist, but others may be new requirements. A review of current technology and data (Stage 5) is needed to ensure that for existing systems the project team fully understand the fund of experience, understanding (or possible misunderstanding), skills, problems and opportunities that currently exist.

The project team will need to review and document existing systems, the hardware, software and any communications network, documentation quality, complexity, interfaces to other systems etc, and evaluate key problems. This review should focus on how IT is already being used, and how it is managed and being

delivered to users. The review should highlight issues for senior management's attention such as:

- whether IT is seen by users as a necessary evil, a scarce resource, or an aid to their work. This indicates the overall value placed on existing systems by users, and whether business objectives are achieved;
- whether the existing systems are considered easy to use and provide a rapid response to users. Do they provide information on-line, or do users have to wait for daily, weekly or monthly batch runs to obtain the information they require? What is the demand for on-line access to the information held?
- whether the existing systems can cope with the demand placed upon them. Are there complaints about lack of flexibility, usability, accuracy, response times etc?
- the proportion of resources devoted to maintenance, and the extent to which technology, rather than user demands, is driving system changes;
- technical support availability, and the wider availability of the skills needed for maintenance (eg does the system rely on the skills of one person who could not easily be replaced?);
- the degree of data duplication, and data that is collected but not needed.

Relating existing systems to the new business model

The project team should also relate the functions of the existing systems to business objectives to highlight any gaps in functionality. This helps ensure that the proposed new system meets the needs of the business and does not simply replicate what currently exists.

Migration options

If the existing system does not satisfy the current business requirements there are three main options for migration:-

- use existing technology but enhance functionality
- upgrade technology and enhance functionality
- replace.

The choice depends on how quickly the existing technology will become obsolete, whether it can handle new requirements, the replacement costs, the resources available, or a combination of all these factors. There is no hard and fast rule for the decision, which will depend on the individual circumstances of each case.

But in reaching a decision, SAs should bear in mind that the cost of hardware is relatively cheap compared with the costs of developing bespoke systems. A particularly significant cost of replacing systems, and one which is often underestimated, is the cost of re-training users, even when package solutions are adopted.

The ideal solution might be a progressive upgrade in stages which allows upgrade and re-training costs to be spread over a suitable period. But this is not always

possible if hardware is obsolete or will soon become so, or a major change in functionality is required beyond the capability of the existing system.

The objective here - as part of an overall systems development plan (Stage 6) - is to present the Steering Committee and Senior Management with options for migration, drawing up the advantages, disadvantages, risks, upheaval, costs and availability of skilled resources necessary for each. Costs must be comprehensive and include the costs of transition. Maintaining both new and old systems for lengthy periods can be expensive and must be weighed against the risks involved if the new system fails. And the review must take account of the effect on and costs of any changes needed to linked systems.

Developing a migration plan

The chosen options - as with other approved proposals in a systems development plan - should be reflected in a business impacts assessment (Stage 7) and implementation and training plan (Stage 8).

For systems to be migrated, systems development and other plans should include data capture, data conversion, data

loading and validation, user training, preparing training materials, acceptance testing and parallel running where appropriate. Particular care is necessary in planning how the switch over from the existing systems will occur and what fallback to existing systems will be provided if problems arise - for example, the period of parallel running needs to be extended until the new system has been proved. Examining these issues before the systems development plan is finalised and approved ensures that problems do not arise late in the development cycle which are costly to resolve - for example it is easy to overlook or underestimate the additional effort which may be needed to capture and validate new data outside the scope of the existing system.

Data converted from an existing system will need to be checked to ensure that it has been captured correctly. Acceptance testing is likely to reveal a number of anomalies within the data. Each must be investigated to correct data and assess the implications of the error or inconsistency uncovered, and plans must allow adequate resources for this work.

Planning post implementation activity, monitoring, maintenance and enhancement

Migrated systems should be included in a plan for post implementation activity (Stage 9). The agreed plan should include tasks to ensure that expected benefits are delivered, and that the overall strategy is further reviewed and updated periodically.

And finally!

The success of any IT strategy review - large or small - will not only be measured by number of computers purchased or systems successfully implemented. More important is that all involved will have a much better understanding of the objectives of the business of the audit office and how the various supporting functions work.

Reviewing information security: A practical approach



To meet the challenge of reviewing information security, Guy Dumas of the Canadian Audit Office proposes a practical approach based on a draft model recently adopted by the INTOSAI EDP Committee

Guy Dumas



Guy Dumas joined the Office of the Auditor General of Canada in 1980 and is currently Director of VFM Informatics. Over the past six years, he has been involved in security matters at the OAG and in government departments.

Why Is Security So Important?

Our government institutions have become so dependent on technology that auditors find it increasingly important to look at the security of information technology (IT) systems. Their concern centres on the confidentiality, integrity and availability of the information carried by these systems. The main factors are the sensitivity and the value of that information to government organisations and to the public they serve.

A Challenge for Most SAIs

There are three issues that prevent many SAIs from getting more involved in the field of IT security: first, the size and complexity of the task; second, a perceived lack of adequate resources; and third, seemingly complex review methodologies.

To say that the task is not formidable is to bury one's head in the sand. The technology is fast evolving toward greater integration and more sophistication. Networks now link systems that used to be remote and isolated.

In a national context, systems are spread over wide areas, often in distant locations and, in some countries, over a number of time zones.

The greatest inhibitor for SAIs is the perception that they lack adequate resources to carry out the task in the first place. Information technology security easily comes last because there are, it seems, so many other more pressing

matters. In the area of information technology, security is an area of specialisation in itself. And there is the problem of funding the effort.

Overshadowing these issues, there is also a problem of methodology. The methodologies proposed today, and there are many, usually rest on very complex and lengthy review processes based on a quantitative evaluation of the security risks. Most models propose a monetary evaluation of the risks and countermeasures. They require the integration of monetary values and probability factors for every threat to every information asset, whether hardware, software or data. These methods usually come with software tools of various levels of quality and ease of use. The task of reviewing information security with these tools takes on an added dimension of difficulty.

The Proposed Method - Background

The information technology security review methodology, as approved in draft by the INTOSAI EDP Committee in New Delhi, India, in August 1994, is based on a two-tier approach. The first tier is a method developed by Bart Burron and Guy Dumas for use at the Office of the Auditor General (OAG) of Canada. The methodology benefits from work done in Canada by the Royal Canadian Mounted Police. The second tier is a manual method from the UK National Audit Office that uses quantitative analysis techniques. The full two-tier methodology is described in greater detail in a draft guide, "INTOSAI, Information

Technology Security Review Methodology, August 1994", that will be presented for final approval at the XV INCOSAI in Cairo later this year.

How Does This Methodology Work?

The first tier of the methodology takes a management view of information security. The information that is processed or carried by the information systems is more important than the technology that supports that information. Instead of attempting to measure precise expected annual losses, the first tier of the methodology uses "informed" value judgements on the security risks of the application under review. Applications can include Accounts Receivable, Payroll, collections of Lotus spreadsheets, collections of word processing documents or sub-categories of such collections. For each application, some standard threats are rated high, medium or low risk. In parallel, business impacts are also rated as high, medium or low. Using a simple matrix, the results of these two assessments are combined to provide a final overall security exposure level for each application. Appropriate priorities and recommendations can then be presented to management.

As adopted by INTOSAI, the methodology offers SAIs a second tier of risk assessment, using quantitative methodologies. However, this step is taken only if such a requirement exists for the SAI in question or if more in-depth justifications are required to support recommendations to management.

What's In It For SAIs?

The methodology is simple, does not require extensive resources and can be used by staff who have a basic knowledge of information technology and of security principles. In short, it is cost-effective and can be used by all SAIs.

In most cases, the use of the first tier of the methodology is sufficient to quickly determine the level of security risk for any given application and, ultimately, for the whole organisations information. Depending on the seriousness of the risks, recommendations can be made immediately to management in terms it understands. In cases where

recommendations need to be made for expensive or complex countermeasures, more demanding quantitative methodologies can be used, if management needs such analysis to accept the recommendations and if the SAI has the needed resources.

In general, SAIs can perform a first-tier security analysis with existing resources and simple techniques. As used at the OAG and proposed to INTOSAI, the methodology uses simple tools such as pre-printed forms produced in WordPerfect and Lotus. For SAIs that have access to microcomputers, the electronic forms can be used to tabulate the results of the assessments for each application. If needed, SAIs can also use database software to create repositories of results for further analysis.

Information technology experts are a scarce resource in most SAIs; experts in information technology security are even more so. The INTOSAI approach allows staff who are knowledgeable in management controls and sufficiently aware of information technology to make reasonable judgements about the security risks that affect the information. Based on the sensitivity of the information, as determined by the owners of that information, the staff perform the assessment and submit their security review report.

Conclusion

The INTOSAI methodology is cost-effective because there is no absolute need for information technology experts; and pencil and paper or, if available, standard office microcomputer applications can be used. The first tier of the methodology is straightforward and simple enough that training can be limited to a careful reading of the manual, on-the-job training and judicious supervision. Most of all, it gives SAIs the opportunity to obtain timely results and sufficient evidence to support solid recommendations to management. The first assessment can be carried out on the SAI's own Office. As well as providing for a more secure Office, it offers a good opportunity for training staff in information technology security reviews. More demanding and costly quantitative security review methodologies are used only when necessary.

An IT Audit Curriculum for INTOSAI



The ability to audit IT systems is now essential for most, if not all, SAIs. Martin Pflieger of the United Kingdom NAO discusses the new INTOSAI IT Audit Curriculum which is intended to help SAIs assess their training requirements. He also outlines the INTOSAI EDP Committee's plans to develop a comprehensive training package which SAIs can use

Martin Pflieger



Martin Pflieger is an Assistant Auditor General at the NAO. He is responsible for all central technical and support services for the office, including IT policy and implementation.

Introduction

The bodies or institutions we audit are increasingly reliant on IT systems for the efficient and effective delivery of public services. Increasingly SAIs are unable to audit expenditure or income, or the regularity of transactions, without a review of the underlying IT systems. Moreover, the investment in new technology is substantial and there is considerable scope for bad project management and inefficient systems, so auditors need to appreciate and audit these risks as well.

The INTOSAI IT Audit Curriculum

Against this background, in October 1993 the INTOSAI EDP Committee recognised the importance of defining the IT audit skills needed by staff in SAIs. They gave priority, in their work programme, to the development of a high level curriculum which would focus on the core competencies required by an IT auditor. The Committee agreed the curriculum at its meeting in September 1994 and it was endorsed by the INTOSAI Governing Board at its meeting last November.

The Curriculum recognises that it is neither feasible nor desirable to require all auditors to have a deep knowledge of IT and of IT audit. The curriculum is, therefore, based on three levels of IT audit skills.

In practice, SAIs may choose to organise their IT audit function along different lines. Some might allocate the different tasks of IT audit between generalist auditors and

specialists in a way which best suits their circumstances; others might prefer to have all IT audit tasks carried out by specialists. The modular structure of the curriculum is intended to promote common standards in each of the areas covered, whilst being flexible enough to accommodate SAI's different approaches to IT audit.

Scope of the Curriculum

The curriculum aims to specify the main tasks of IT audit in six different areas. However, individual SAIs might, through their statutory role or choice of audit approach, not undertake some tasks or place less emphasis on others. In effect, the curriculum provides a menu from which each SAI can choose. The six areas are:

- Planning, progressing and reviewing of IT Audit.
- Assessing controls in IT systems. Computer-assisted audit techniques (CAATs).
- Auditing IT systems under development or procurement.
- Performance audits of IT systems and functions.
- Special assignments.

Making Training Available To SAIs

The EDP Committee recognise that in many countries there are already a wide range of IT audit training courses available commercially. In some cases, this training is linked to the Certified Information Systems Auditor (CISA) programme offered by the Information Systems Audit and Control Association (ISACA): Level 2 of the INTOSAI curriculum corresponds broadly to the CISA standards. The Committee also acknowledges the considerable efforts of the IDI in delivering basic IT audit training (Level 1) at Regional level, although the Committee notes that this training will be less available in future as IDI shifts its emphasis from direct training to helping regional groups strengthen their training capability.

However, at its meeting in Stockholm in March 1995 the Committee agreed that there was a need to make available to SAIs comprehensive training material on a consistent basis. Subject to approval at the INCOSAI meeting later this year, the Committee have therefore decided to develop the course-ware (trainer's packs, lecture notes, slides, handouts, case studies and reading lists) for Levels 1 and 2 by the end of 1997. Level 3 needs are likely to be met through short workshops, symposia etc rather than formal training. The material will be developed in English, though the Committee is willing to work with regional groups subsequently to translate it where necessary.

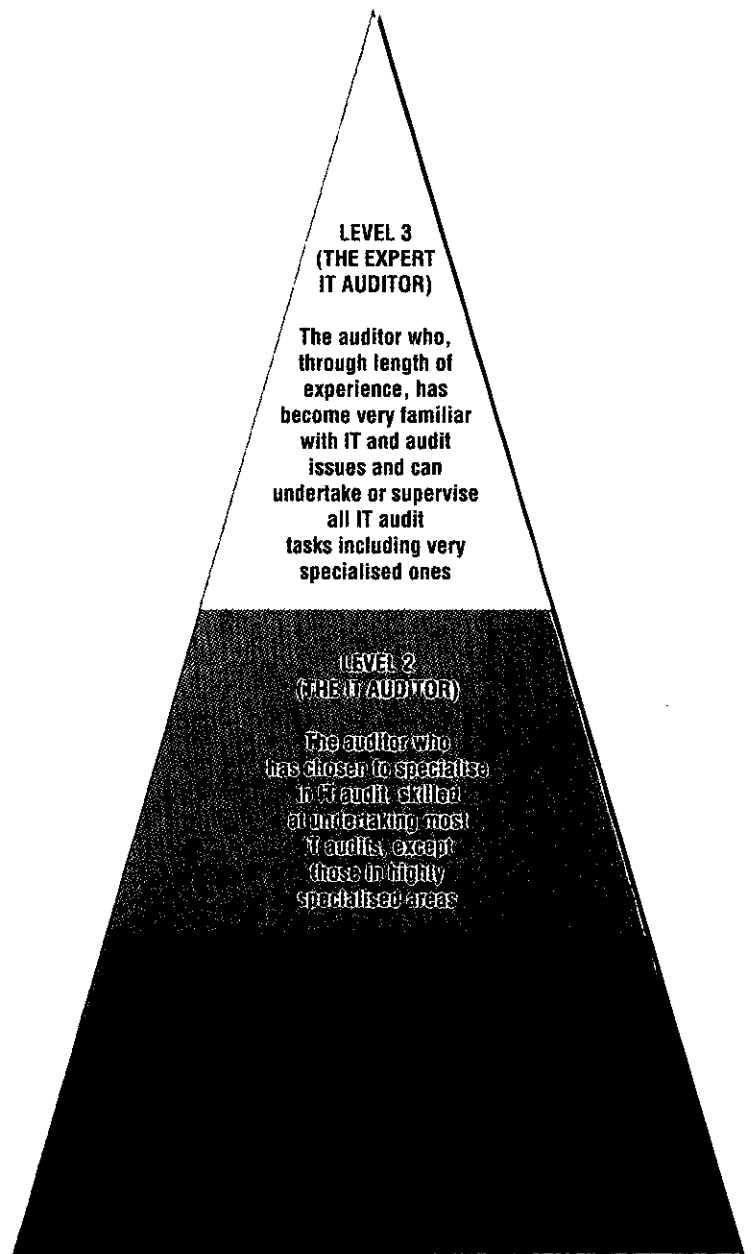
Once the course-ware is available, there is the question of delivering training courses. The EDP Committee does not have the resources to fund course delivery. Rather, its aim is to provide individual SAIs and regional groupings with the material to organise and run their own training.

Funding for training courses is crucial and the Committee envisage that Regional Groups and SAIs working together will be able to identify funding for training activities. As Mr Somiah noted in his editorial, the Committee has been working on a guide to funding to help SAIs bid for funds from donor agencies and this guide will be distributed via IDI shortly.

Experienced lecturers and tutors are also essential; the INTOSAI EDP Directory identifies those SAIs willing to provide expert assistance. The EDP Committee is willing to work with Regional Groups to help provide the experienced trainers to make most effective use of the training material now under development. There may also be scope for strategic partnerships, on a bilateral basis: for example the SAIs of India and the United

Kingdom are working together on a UK-funded project to train over 200 specialist IT auditors in the Indian Audit Office.

I hope that all SAIs will recognise the merit, and challenge, of developing this training material. If SAIs have good quality training material which they would like to share with the EDP Committee, please send it to me so that we can build it into the new course-ware. On the other hand, if SAIs or Regional Groups have ideas for, or are planning IT audit training events and need assistance, please contact Mr Somiah, the Auditor General of India, myself or your region's representative on the EDP Committee.



INTOSAI and the Internet



SAIs are increasingly taking advantage of communications developments. The INTOSAI Secretariat discusses a project to link SAIs to the 'superhighway'

Introduction

At its 38th meeting held in Vienna in March 1993, the INTOSAI Governing Board appointed a study group, co-ordinated by the German Federal Court of Audit (FCA), and comprising as members the United States General Accounting Office (GAO) as well as the INTOSAI General Secretariat, which is under the direction of the Austrian Court of Account. The study group's mandate was to explore available options for the further development and improvement of communication among the Supreme Audit Institutions and to submit relevant proposals to the Governing Board of INTOSAI.

On the basis of this mandate, the following projects were initiated and a report thereon submitted at the INTOSAI Governing Board's 39th meeting in Cairo in October 1994:

- a brochure on INTOSAI designed to provide, in condensed form, a survey of the responsibilities and objectives of INTOSAI;
- a membership directory compiled by the General Secretariat and published by the International Journal of Government Auditing (IJGA) for distribution at the XVth INCOSAI in Cairo and updated annually, and
- a Calendar of Events published in the IJGA announcing major events organised by INTOSAI and regional working groups.

While the projects named above are based on printed material, the General Secretariat has assumed yet another task, namely

- reviewing the feasibility of using EDP-based data transmission as a means of communication among SAIs.

This article discusses in more detail:

- the starting point
- the status of the project as of spring 1995, and
- further continuation of the project of electronic communication among SAIs.

Starting point

The start of electronic communication between SAIs dates back to the early nineties. Beside electronic mail facilities installed between the SAIs of the United States (GOA), Canada (OAG) and Australia (ANAO), electronic data links were set up between the INTOSAI General Secretariat and GAO as well as the International Journal of Government Auditing, which has its offices at the same location. The objective in establishing this link was not only to provide a facility for transfer of electronic mail between these two agencies but also to enable fast and economical transmission of ready-for-press documents in the run-up to the XIVth INCOSAI 1992 in Washington, D.C.

Prior to this, electronic data communication had already been used for transmitting the German edition of IJGA to the IJGA office for printing after translation from the English, and preparation for printing by the Austrian Court of Account, as shipment of disks through express delivery services had proved impractical. In view of the advantages inherent in electronic data transmission, the IJGA and the General Secretariat started considering, at a very early date, how this specific solution might be developed into a wider application of the technology for the benefit of as large a number of SAIs as possible.

This plan was assisted by rapid technological progress and the establishment, in the mid-nineties, of

Internet as the most widely available computer network (linking, for example, almost all universities world-wide).

Status of the project as of spring 1995

Access to Internet

The Internet address at which the General Secretariat can be reached from March 1995 is:

rh.into@magnet.at

Subscribers to pilot operations

Some SAIs had obtained access to the Internet even earlier. These SAIs have agreed to conduct electronic communication with the General Secretariat on a trial basis. A list of these SAIs and their Internet addresses is provided at the end of this article.

Other subscribers

The General Secretariat requests all SAIs not listed in the annex but interested in taking part in pilot operations and being in possession of an Internet address to inform the General Secretariat accordingly.

The Internet cannot be accessed direct but only through private providers, clubs, or government agencies. Also, most of the universities have access to Internet.

Experience to date

First experience gained in the practical implementation of data communication between SAIs and the General Secretariat via Internet has shown that electronic mail (E-mail) can be handled quite conveniently in the form of messages, which are the least common denominator for the different platforms (DOS, MacOS, Next, and Windows). There have been difficulties, however, in several cases with an expanded use of E-mail, i.e. where files had been attached to simple messages. In such cases it is advisable to agree with the other party in advance on the software to be used in creating the attached file (a specific text processing, spreadsheet, database, or graphics software) as well as the type of data compression and transmission protocols employed. A special problem in INTOSAI with its five working languages is transmission of country-specific special characters.

Integration of Internet into the in-house network

The General Secretariat accesses Internet by means of "FirstClass - Software" and is thereby integrated into the electronic communications system of the Austrian Court of Account. This means that no extra procedures are required for sending or receiving Internet messages.

Some of the SAIs, however, do not - or not yet - have such facilities. They therefore have to follow a special selection procedure to establish contact with the Internet interface, which some users describe as rather cumbersome. In some SAIs where employees had been assigned personal Internet addresses (similar to telephone extensions) it was found that messages addressed to employees currently absent from the office were read out and acted only on their return.

Summary E-mail

Summarising the above one may say that experience gained to date with the transmission of E-mail between the General Secretariat and SAIs via Internet has been encouraging. Nevertheless, the following points should be borne in mind:

- If E-mail is sent only occasionally to the General Secretariat or other SAIs it should be confined initially to simple electronic messages (with no files attached).
- In cases in which files were attached difficulties were occasionally experienced when the parties to the exchange were working from different platforms (DOS, MacOS, Next, and Windows): while recipients were able to read the electronic message they were sometimes not able to open the attached files. It is therefore suggested to await further developments in the required software before using the Internet for routine communication among SAIs with different platforms. Until then, it will not be possible to rely on it as a partial replacement for other means of communication such as fax messages.
- Also, some organisational arrangements will be required at SAIs to ensure that messages sent via Internet are passed on even in the absence of addressees (similar to technical and organisational solutions already incorporated in advanced private branch exchanges which, in the absence of an employee, forward calls to another extension or to a switchboard).

- Despite the above reservations E-mail will certainly be a definite option for the future because of its obvious benefits including, specifically, the possibility of processing incoming text. Internet might thus be used most effectively in assisting the work of the INTOSAI Standards Committee and working groups where an exchange of documents ready for direct editing by members would be very helpful indeed.

Further continuation of the project

The General Secretariat is planning to start pilot operations on the World Wide Web in early summer 1995 as an effective means of presenting INTOSAI. For this purpose, the database of the INTOSAI General Secretariat will be linked with a server that will hold a selection of INTOSAI documents of general interest. A so-called "Hypertext" search system will enable access to these documents, which can then be read out on the SAI's PCs. In the initial phase these documents will be available only as full text versions in the format "WordPerfect 5.1 PC Document".

The following documents are planned to be made available for these pilot operations:

- a fully updated INTOSAI Membership Directory;
- INTOSAI Statutes in English, French, German, and Spanish;
- INTOSAI Auditing Standards for Government Auditing in English, French, German, and Spanish and

- the most recent INTOSAI Circular in English, French, German, and Spanish.

As a next step, and after clarification of preliminary questions, the following documents are planned for incorporation:

- a fully updated INTOSAI Calendar of Events showing upcoming major events;
- the results and interim results of the work of INTOSAI Standards Committees and working groups and
- available bibliographies relating to government auditing.

Inclusion of Arabic, the fifth INTOSAI working language, is currently not possible for technical reasons.

A number of SAIs have meanwhile agreed to take part in such WWW pilot operations. Other SAIs who are interested in connecting to the WWW - INTOSAI server are invited to advise the General Secretariat of their Internet addresses. It is currently planned to allow access to the INTOSAI WWW server only to Internet subscribers (SAIs) that are registered with the General Secretariat.

The domain name under which the INTOSAI WWW server can be accessed will be communicated in good time to subscribers participating in pilot operations.

List of Internet addresses of SAIs in E-mail pilot operations:

Australia - Australie - Australien - Australia

Australian National Audit Office

Tel: ++61 (6) 203 -7300

Fax: ++61 (6) 203 -7777

E-mail: AG1@ANAO.GOV.AU, CC: WINKSS@ANAO.GOV.AU

Austria - Autriche - Österreich - Austria

Rechnungshof (Austrian Court of Audit / Cour des Comptes de l'Autriche /

Tribunal de Cuentas de Austria)

Tel: ++43 (1) 711 71-8456

Fax: ++43 (1) 712 94 25

E-mail: RH.INTO@MAGNET.AT

Canada - Canada - Kanada - Canadá

Bureau du Vérificateur Général du Canada (Office of the Auditor General)
Tel: ++1 (613) 992-3086
Fax: ++1 (613) 957-4023
E-mail: JADSHEAD@HOOKUP.NET

Norway - Norvège - Norwegen - Noruega

Riksrevisjonen
Tel: 0047 (2) 234 21 51
Fax: 0047 (2) 234 2128, 34 22 32
E-mail: ELINFA@OSLONETT.NO

Sweden - Suède - Schweden - Suecia

Riksrevisionsverket (The Swedish National Audit Office)
Tel: 0046 (8) 690 4000
Fax: 0046 (8) 690 4100
E-mail: GORAN.STEEN@RRVSWEAUDIT.POSTNET.SE

United States of America - Etats-Unis d'Amérique - Vereinigte Staaten v. Amerika - Estados

Unidos de América
International Journal of Government Auditing
Tel: ++1 (202) 512-4707
Fax: ++1 (202) 512-4021
E-mail: 75607.1051@COMPUSERVE.COM

The first issue of intoIT was published and circulated in January 1995. It contained articles on:

- *The use of IT in the Indian Audit Office;*
- *The Use of IDEA in the Swedish Audit Office;*
- *Text Retrieval in the UK Audit Office;*
- *The Canadian Audit Office's 'Audit Briefcase; and*
- *IT New from Japan, Kuwait, Sweden, the UK and Zambabwe*

A small number of copies of Issue 1 are still available from the Editor of intoIT at the address on the contents page of this issue.

The 3rd issue of intoIT will be circulated in January 1996. It will feature articles on:

- *the use of IT in the Japanese Audit Office*
- *a report on the IT Audit Symposium in Sweden in March 1994*
- *Planning and Monitoring Audits and Resources*
- *EDI*
- *and IT audit news from SAIs around the world.*

Contributions for that issue must be received by the Editor of intoIT by the end of July 1995. The deadline for contributions for the 4th issue of the journal is December 1995.

News from around the World

ECUADOR



The Comptroller General of Ecuador is currently undertaking an institutional strengthening programme, financed by the Inter-American Development Bank. Amongst other initiatives, this programme is considering improvements in internal control and auditing and accountability practices. The results will serve as a guide to government auditing and contribute to strengthening auditors' knowledge, developing their skills in applying current Standards, and especially to improving the audit approach.

To demonstrate the importance attached to this initiative, the Controller has published the Guía de Control No. 17 (Control Manual No.17), which contains:

- rules for internal control;
- principles, policies and technical standards of accounting;
- auditing policies;
- generally accepted auditing standards in the public sector;
- technical rules for contracting with private firms for audit services;
- a summary of the application of IT in audit.

The section on IT provides details of the computer applications already developed and operating in the Contraloría General:

- 1. Inventory of Bodies for Audit Planning;
- 2. Annual Control Plan;
- 3. Monitoring of Work in Progress;
- 4. Summary of Permanent Audit File;
- 5. Register of Audit Reports;
- 6. Register of Engineering Studies;
- 7. Register of Special Examinations;
- 8. Auditing Questionnaires and Audit Programmes;
- 9. Standard Recommendations;
- 10. Register of Contracts with Audit Firms;
- 11. Technical Specifications for Civil Works.

FRANCE

The information service of the French Cour des comptes provides the banque de donnes internes (BDI) for the magistrates of their SAI. This is a computerised database of all documents produced by the Cour des comptes during the year.

The database contains summarised information on Reports, with keyword searching to help those looking for specific information. However, judicial acts made by the court are held on the database in a full-text format. This enables searching of the entire text of an act with full word-by-word indexing.

The database is a very useful tool for magistrate auditors.

The BDI currently contains 24,000 documents, largely dating from 1970 to the present day. Implementation began in 1992 and was completed in 1994. By the end of 1994 an average of 1,500 documents per month were being accessed. The technical requirement for using the database is a 486 microcomputer operating under SCO-Unix.



KUWAIT

The State Audit Bureau of Kuwait has established a new IT Centre and a Training and Development Centre.

The objectives of the IT Centre are to:

- develop work procedures and computer systems for document storage, and train staff in their use;
- produce periodic plans for the computer and technical resources required for such systems, within the financial budgets allocated to the State Audit Bureau for this purpose;
- formulate the specifications, technical standards and procedures to be followed when contracting to purchase, computers, their accessories, software and other equipment for document storage systems;
- provide scientific assistance and technical advice to the different departments of the Bureau when using the computers available to the Centre. To encourage the use of the information systems developed and operated by the Centre, as these are the central information bank for the State Audit Bureau of Kuwait;
- collect and classify information related to the computer systems used by the State Audit Bureau, and also the applications used and technical staff handling this information. This will provide information for planning purposes to interested institutions of the State of Kuwait.

The Training and Development Centre will:

- prepare plans and formulate and present training programmes for State Audit Bureau staff locally and overseas;
- supervise the execution of staff training programmes and then prepare and provide reports on the outcome of the programmes.





NETHERLANDS

The Netherlands Court of Audit has released the results of four specific IT audits during 1994. These audits concerned:

- the IT planning of the Netherlands Royal Navy. The audit results showed that the plans were out-dated and did not adapt to current organisational developments due to the altered political goals;
- the security of the data-communications network of the Ministry of Agriculture and Fisheries. The audit pointed out that a lack of risk analysis and system classifications could have a negative impact on the integrity and availability of (financial) data distributed over this wide- area network;
- the quality of the organisation and processing of environmental data flows needed for policy making on environmental issues. The audit showed that there were few guarantees that the data processed was valid and complete, due to a lack of co-ordination between the governmental bodies and agencies involved;
- the access security to the system for Intra Community Transactions at the Ministry of Finance for checking the VAT involved in trade transactions between member states of the European Union. Proper access security was not always guaranteed, and uncertainty arose about the security measures taken by other member states using this system.

Contact person: W.A.M. van Westing



SIERRA LEONE

The Development of Information Technology

Over the last two years the Auditor General's Department of Sierra Leone has greatly improved its operational systems. Developments have been made possible through the Public Sector Management Support Project under the World Bank Assistance Programme to the Sierra Leone Government.

The Department became a beneficiary agency under the World Bank Project, and this resulted in a series of developments including the acquisition of desktop computers, laptops, electrical typewriters and other modern equipment. With the acquisition of computers, the Department was able to develop and improve its initial Information Technology strategy. A fair number of Department staff are already computer literate, and other staff are given full opportunities to improve their skills.

As part of the Project two consultants, working with internal staff, created a Personnel Database for the Department. This Database can be queried to produce pertinent information at short notice. A Contracts Database has also been created to assist the monitoring and scrutiny of Works and Supplies Contracts entered into by the Government.

There are plans to computerise the entire Pensions Division of the Department, which is responsible for verifying gratuities and pensions (retirement benefits) for civil servants in the whole country. It is also hoped to computerise shortly the Registry Division, which issues all Audit Reports and correspondence.

The Auditor General of Sierra Leone, Mrs Ade O Caulker, takes a serious personal interest in the rapid development of IT systems. Massive changes in the accounting systems of the Treasury of the Auditor General's Department are presently in progress. Personal emoluments and other expenditure is currently being computerised to provide a centralised system of accounting. Delphi Financial software, developed by the Midland Software Corporation, has already been installed. The Department, which has the mandate to audit the accounts of the Accountant General, will recommend the urgent development of software to enable the proper auditing of the Country's accounts maintained by the Accountant General.

SWEDEN

The Swedish National Audit Office hosted a Symposium on IT audit issues in Stockholm in March. The main themes of the seminar were:

- performance audit of client IT;
- the audit of developing IT systems;
- a risk-based approach to financial audit;
- the audit challenge posed by client use of electronic trading;
- and auditing societal effects of IT.

The seminar was followed by the 4th meeting of the INTOSAI Standing Committee on EDP audit. The next issue of intoIT will contain a full account of the Symposium and further information on the work of the EDP Committee.



UNITED KINGDOM

IT Strategy

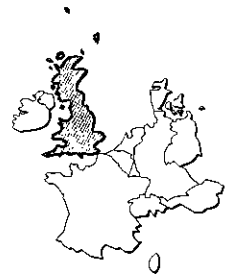
The UK National Audit Office (NAO) has recently completed a major review of its IT Strategy. The review was carried out by an in-house team and external consultants. It:

- considered developments within the IT industry and assessed the implications on the NAO IT Strategy;
- considered the opportunities for the implementation of additional IT facilities;
- assessed the implications of introducing new facilities on existing systems; considered whether changes would offer real benefits to the NAO; and the costs associated with change.

Following the review, the NAO has agreed revised proposals for the next five years. These will involve:

- the migration of its existing character-based systems, run largely on central mini computers, to Windows-based systems operating in a client / server environment, to provide greater operating flexibility in the future;
- the replacement of the currently used Office Automation software - Uniplex - with Microsoft Office. This will provide enhanced Word-processing, Spreadsheet, Personnel Database and Graphics tools to end users on their desktop;

The enhancement of centrally run Planning and Monitoring Systems for Audits and Resources, and Document Management Systems, to take advantage of the greater facilities offered by Windows; and the enhancement and redevelopment of Financial and Value for Money Audit Support Systems to provide improved tools for audit staff working both in their office and away from their desk. This main elements of the new IT Strategy will be introduced over the next three years and will cost an additional £1,120,000 over the lifetime of the Strategy.



Audit Reports

The NAO has recently issued two Audit Reports on the use of IT in Government:

IT Security in Government Departments

This Report examined and compared IT Security in a variety of Government Departments and Agencies. It concluded that a number of worthwhile actions had been taken since 1991 to respond to security concerns. However, Departments and Agencies still had some way to go on issues such as IT security training, awareness programmes and contingency planning, and that hacking, theft and viruses continued to pose threats to IT security. In particular the NAO found that:

- between 1990 and 1994 there were 36 cases of reputed computer fraud in central government with a total value of under £250,000;
- departments reported 655 hacking incidents in 1993-94, a rise of 140 per cent over the previous year, although the proportion of successful hacking attempts fell from 51 per cent to just 17 per cent in the same period. Almost all of these incidents were caused by departmental staff obtaining unauthorised access to official information;
- departments reported 562 virus incidents in 1993-94, an increase of more than 300 per cent since 1991-92, but a growing proportion of viruses were detected and prevented from spreading; and
- theft of IT equipment continued to be a major problem, with portable computers and printers being the main targets. 433 incidents were reported by departments in 1993- 94, costing a total of £1,200,000.

The Report made a number of recommendations for improvements in IT Security Risk Assessment, security training, contingency planning and incident reporting.

Market Testing of IT in the Inland Revenue

This Report examined one of the largest exercises to out-source computer services previously provided by a Government Department in-house IT team. In May 1994 the Inland Revenue signed a 10-year contract with a commercial firm . Under the contract - which is valued at around £1 billion over 10 years - the company took over the work, assets and some 1,900 staff of the Department. The Inland Revenue estimates the new arrangements could result in cash savings of about £225 million over 10 years at 1994-95 prices.

The NAO found that contractual safeguards provide, as far as possible at this stage, reasonable safeguards to protect the interests of the Department, taxpayers and staff. The Report highlights the scope and nature of the contract negotiations, and the conditions built into the contract to safeguard the various stakeholders interests.

On the future management of the contract, the NAO found that strong control and management procedures had been established. However, it is not yet possible to determine how effective these processes will be during the lifetime of the contract. The NAO intends to re-examine the situation in the future, and review the contract management arrangements, including the achievement of benefits, and the regulation and control of the contract charges.