Summary and conclusions from the 4th Working Seminar on Performance Auditing

The major theme for the seminar was performance auditing on e-Government. This main subject was divided into three sub-themes: risk assessment, effectiveness in a client-oriented perspective and challenges when auditing e-Government.
 The goals set up for the seminar were
* to inspire Supreme Audit Institutions (SAI) in their performance audits within the e-Government area to strengthen and increase their control initiatives
* to provide an opportunity for sharing experience and further learning on e-Government auditing among the SAIs
* to help auditors become better acquainted and develop communications
* to improve efficiency and quality on Auditing e-Government

The seminar opened with an introductory speech describing what e-Government is and general trends within the e-Government area.

Thereafter three lead papers and eleven country papers were presented.

Sub-theme 1: Risk Assessment of e-Government projects

Four papers were presented under this sub-theme: The SAI of Slovenia's lead paper "Risk Assessment of e-service projects" and three county papers from respectively Sweden, Oman and USA.

The purpose of the presented paper from Slovenia was to provide a template for approaching risk assessment of e-government projects. This was done through offering a definition of risk assessments especially related to management of e-government projects.

There could be many different approaches for dividing the risks. Based on experience from similar projects, Slovenia has chosen to divide the risks and controls in the following five categories:

* Business Imperative / Motivation to Change

* Project Structure & Approach

* Technology

* People

* Project Management & Control

Under the business (motivation to change) category the important aspects of legal readiness and citizens readiness and accessibility are treated. These are aspects of unique importance to risk assessment of many e-Government projects.

In the spring of 2003, the former Swedish National Audit Office (SNAO) made a materiality and risk analysis of the Government's management and controls of the process of transition to e-Government/24-hour government agencies (24/7 agencies). In addition to the Slovenian risk categories the SNAO found the following main risk areas from a government administration point of view:

- Risks related to the overall management and controls of government agencies' work on e-Government
- Risks related to the current "fashion" of investing in e-Government. What are the forces behind the concept of e-Government and what is their purpose?

The country paper from USA explored how GAO used the Crystal Ball software for determining uncertainty using a Monte Carlo simulation technique in conjunction with a cost estimation spreadsheet to define the uncertainty with the cost of various scenarios for border control using biometrics.

In the discussion several questions were raised. Poland found the presented risk template very similar to the COBIT framework[1], and raised the question of the relationship between this particular framework and auditing e-Government. USA claimed that the main difference is that auditing e-Government requires far more attention and focus on the users (i.e. more client-oriented). Slovenia agreed upon this statement and pointed out the idea to make use of the COBIT framework, but to add other elements of special importance to risk assessment of e-Government when this is appropriate. Slovenia also emphasized that the risk template offers a less voluminous framework compared to the COBIT standards, and that risk assessment of e-Government might benefit from this.

Netherlands raised an important question concerning risk assessment at different levels of e-Government solutions. In general, framework as for instance COBIT, could prove to be quite useful at the project level, but fail to detect risks attached to the program level.

Sum-theme 2: Effectiveness in a client oriented perspective
Two papers were presented under this sub-theme: The SAI of Canada's lead paper "Auditing Government On-Line - the Canadian Government Experience", and the SAI of Norway's countrypaper "Performance audit on public e-procurement in Norway".

In the lead paper the SAI of Canada shared its methodology and approach when auditing E-Government issues. The paper discussed the recent experience in auditing the Canadian e-Government initiative (Government On-Line)[2] using concepts and approaches developed for the audit. The SAI of Canada identified some good practices and lessons learned that might add value to other SAIs planning similar audits in the future.

The following five lines of inquiry were chosen for the Canadian audit: (1) Strategic planning; limited to assess whether the government had established adequate plans and strategies to achieve its GOL objectives for 2005. (2) Funding; limited to assess the funding framework and whether the policy goals are being met. (3) Pathfinder/pilot projects; assess to which extent nine GOL projects contributed to the Government's overall GOL objective. (4)

---

[1] COBIT has been developed as a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners.

[2] Government On-Line (GOL) refers to making many government services available to citizens electronically, using Internet technology.

Governance; assess the governance strucucture. (5) Common secure infrastructure; assess the compatibility between Secure Channel and other applications.

Some of the key findings in the Canadian paper were: (1) Although the Government did have a well-developed vision, the outcome was vague and difficult to measure. (2) The full cost of the GOL initiative will be much greater than the $ 880 million funds allocated to the central agency. (3) The review of the nine GOL projects showed that these were align with the overall GOL objective, but also that the GOL initiative faces major challenges such as maintaining financial sustainability, transforming services, and marketing on-line services to encourage the public to use them. (4) The GOL initiative is a complex project, and the Government should strengthen its current GOL governance structure to provide more control over all aspects of government services to achieve full service transformation. (5) The audit concluded that the success of Secure Channel was at risk from a number of factors. In addition to difficulties in achieving compatibility between Secure Channel and other applications, there was no comprehensive business case, and a number of legal and privacy issues were yet to be resolved.

The SAI of Norways country paper described a performance audit on the government's investment in e-commerce through a public sector marketplace – a project organized as a four-year programme. The paper gave an introduction to the programme and a description of key audit questions, methods used and findings and assessments of the audit.

The audit focused on the effectiveness of the programme and possible reasons for the insufficient achievement of goals.

The audit revealed that the effectiveness of the Norwegian e-commerce programme was poor in terms of achievement of goals. However, the objectives were set in the dot-com era, when there was widespread optimism about the opportunities afforded by e-business, and a comparison with nine other public sector marketplaces in other countries showed that only two of these had a higher turnover.

In the discussion after this session a number of questions were raised. The SAI of India raised a question concerning the reliability of survey data as evidence in performance audits. The debate indicated that the praxis among the SAIs in collecting and using this type of data differ. This was partly due to the auditors professional background and competence, and the SAIs mandate.

Some SAIs stated that the findings in the Canadian and Norwegian papers supported the assumption that auditing e-Government to some extent will correspond with established methodology used in performance audits. On the other hand, as other SAIs pointed out, methodology that covers the "e" and the relationship between the e and governance can also be critical when auditing e-Government.

Sub-themes 3: Challenges when auditing e-government

India had the lead-paper under this sub-theme, and stressed the importance of developing special skills and targeted methodology when doing performance audits on E-government. Training in theese areas both within and across SAI`s could be of significant value.  India also advised the SAI`s to develop normative standards based on best practice when auditing E-

government. The best practice approach could be of great value because of the fact that technology and system implementation issues are to a large extent similar and irrespective of the nations maturity in IT-implementation. India also high-lighted examples from it`s own experience doing E-government audits.

The country-papers under sub-theme 3 from Russia, Pakistan, Japan and China, discussed a large variety of issues. The SAI of Russia gave in its presentation an overview of an ambitious program – "Electronic Russia" to implement up to date infrastructure of electronic information system within government bodies in Russia ensuring more effective interaction. The program covers nine years (2002-2010), and about 2,5 billion US dollars will be invested within the Federal target program framework. The paper also discussed general problems when organizing performance audits of E-government projects. One of the essential problems to the active implementation in Russia is represented by legislation imperfection and shortcomings in the current budget system.

The country paper from Pakistan presented the SAI`s work in connection with the certification of Financial Management Information Systems in Pakistan. The main purpose of the paper was to underline the increased responsibility of the SAI`s around the world in the wake of the increased use of integrated financial information systems. It is envisaged that in due course the SAI`s would be expected to combine the results of financial attest with findings from the audit of information systems. The paper also gave an overview of the system testing methodology developed for verifying a countrywide integrated financial management system. The paper from Japan gave some suggestions on the expert knowledge, techniques and methods required to audit E-government. In its paper Japan advises the SAI`s to use a large variety of techniques including the skills to design, make and operate relevant software. The Chinese paper gave an overview of the development of E-government in the country. The government of China has determined that E-government shall be a major aspect of IT-systems in China. The paper also presented some of the challenges when introducing audits on E-government, for example the methodology challenge.

In the discussion after the session several questions were raised. The Indian assumption that Audits on E-government requires certain skills and methodology was debated and questioned. Several countries argued, partly based on their own experience, that it was not a necessary condition to develop specific skills and methodology in order to be able to do performance Audits on E-government. Standard VMF-approaches can be excellent tools in a large variety of audits on E-Government. The different roles the SAI`s could perform when doing E-government Audits were also discussed. The position of the United States on this matter was that it was possible for the SAI`s to combine a process-oriented approach towards E-government projects and at the same time retain the SAI`s independence.

Conclusions from the seminar

E-Government is a transformation of service delivery within government agencies, as well as between government and citizens and other users such as businesses and non-governmental organizations. In general this means changes in the way governmental work is organized as well as in how communication is effected. The governmental agencies might need to redesign their business process when implementing E-government. This means that the SAIs have to face new challenges since the audit object has been enlarged.

A major theme running through both presentations and discussions at the seminar was the question of whether there are any differences in the audit approach and methods to be used in auditing e-Government compared to auditing IT-projects and programs in general. There proved to be a general consensus that auditing e-Government to some extent will be different, but this does not mean that there is a need to change the methodological approaches completely. A wide approach to risk assessment would be preferable, and in particular, audit criteria related to users and legal readiness need to be revised and supplemented. The SAIs have to face the challenges of obtaining information from citizens and other users of e-Government. For some SAIs this might involve changes of attitude and policy.

The first sub-theme was presented from many different perspectives. SAIs have collected a lot of experience in assessing risk. The presentations under first sub-theme showed that templates for classifying and assessing risk can be used as a basis for auditing e-Government by SAI's.

However the discussion indicated that templates for classifying and assessing risk presented by Slovenia and Sweden could be supplements to the COBIT standard and other similar approaches, mainly because these templates could be targeted especially towards e-governance. Furthermore they could be more focused on challenges addressed in the e-service programs, for example the client readiness, legal readiness and the need for integration between IT and the business strategy.

An audit of e-Government can be carried out on different levels; the SAIs can audit a project, a program or the governmental policy for implementing and managing e-Government. Several delegates underlined the fact that the main focus should be on governance and business process redesign rather than on implementing the IT-system. However, some speakers said that in order for e-Government services to reach the end user, it is crucial that the IT-infrastructure including the basic administrative systems are integrated, implemented and function well. The SAIs have different approaches when auditing these basic systems. Some SAIs certify the systems, while others audit the results of the system test or the output from the system.

Several delegates recommended that audits of e-government should be carried out at an early stage. Auditing E-Government covers a wide area of topics such as governmental policy, planning, technology, knowledge and business processes; giving advice at an early stage is preferable for improving the results and obtaining value for money. However, the opportunity to audit E-Government can be essentially limited by a SAI's mandate.

The seminar noted several other challenges when auditing e-Government. The e-Government projects and programs share the same weaknesses as other IT-projects, for example budget overload, lack of time and lack of integration.

The presentations showed that even advanced e-Government countries are far from reaching their main objectives within mature e-Government programs. The discussion indicated that many of the risk factors demonstrated in the templates (Slovenia and Sweden) have not been fully addressed in the e-Government programs, and this might explain some of the weaknesses in the cases presented at the seminar.

Another reason might be that the Government's strategy for implementing e-Government is not based on sound analysis. A number of international studies by private and public sector organizations have been released in the past few years assessing both the progress that several

countries have made in providing services via the Internet, and their capacity to develop on-line services. The results of these studies may have led some governments to prioritize e-Government projects without having performed the necessary planning and risk analysis.

Lack of audits and evaluations can lead to increased risks of repeating mistakes because important experience and knowledge have not been analyzed and reported or communicated to the interested parties, such as Parliament, Government and practitioners. It is therefore important to develop performance audits within the area of E-government.