Fédération des
Experts Comptables
Européens

Risks and Audit Implications of Electronic Service Delivery in the Public Sector

February 2004

A Discussion Paper from the FEE Public Sector Committee

This paper is based on:

- A UK Public Audit Forum publication (April 2001) on the implications of electronic service delivery for local and national government; and
- A Guideline of the Information Technology Committee of IFAC (March 2002) on e-public services and the accountant: risk management from a managerial perspective.

CONTENTS

EXECUTIVE SUMMARY

The public sector is under increasing pressure to take advantage of electronic media. The electronic era is capable of transforming the way in which public bodies carry out business, deliver services and communicate with citizens. Activities like procurement can be carried out more rapidly and economically, whilst citizens can benefit from quick access to information and reduced paperwork when dealing with public bodies. The provision of public services through the Internet (e-public services) provides significant opportunities for the implementation of new and cost-effective service delivery models. However, along with these major advantages the advent of the e-era does create risks, which require special attention, firstly by management, but also by external auditors. For external audit it is important that all auditors have an awareness of such risks rather than just audit specialists in information systems.

The delivery of e-public services requires modern computerised information systems (IT systems). In turn reliance on IT systems requires an integrated evaluation of the organization of processes and IT implemented for this purpose. Where IT systems are used it is important that management makes appropriate arrangements to manage the ensuing risks. Consequently, management should assess IT risks and implement IT controls that operate effectively to help ensure that an IT system performs reliably. Information reliability depends on IT system reliability and IT system reliability depends on IT controls. Information generated by an IT system will be reliable where that system is capable of operating without material error, fault or failure during a specified period. This also applies to accounting information.

If elements or parts of the IT system of a public sector entity are used to process transactions or to present information on transactions that may be relevant to accounting and financial reporting, information reliability becomes a key risk factor. The reliability of a bookkeeping system as well as the reliability of preparation of the annual financial statements are management's responsibilities. Where public services are delivered using electronic networks management is responsible for the reliability of the electronic records; this entails demonstrating that the controls that protect the records are appropriate to the value of the records and that these controls are working consistently. From an audit point of view, this means evaluating the control environment that protects business information before using that information to inform an audit report. In a paperless system, evidence of the continuous operation of controls is more important than individual transaction records. This is because the failure of a control, or lack of evidence of its operation, will have an impact on all the records affected by that control rather than just a proportion of them.

From an audit point of view, the risk of a potential impact on a very large number of records means that the evaluation of the control environment that protects financial information against the risk of material errors is a key issue.

The adequacy and appropriateness of controls depends on the quality of the risk analysis and risk assessment that underpins the selection of controls for particular types of electronic record. Comparative analysis of controls can help determine whether they are in line with best practice. Industry standards on technical aspects set out minimum requirements for the security of information systems (e.g. Code of Practice for Information Security Management ISO/IEC 17799:2000).

Furthermore the IFAC Guideline "E-Business and The Accountant: Risk management for Accounting Systems in an E-Business Environment" provides principles which may be used to evaluate whether processed accounting information is reliable when using IT. This IFAC guideline addresses information security appropriate to accounting processing. These security requirements can also go some way to ensuring the privacy of information.

The audit implications of integrated electronic service delivery are significant. The delivery of e-public services does not change audit objectives, but it does result in new risks that need to be assessed by auditors in their audit planning and when performing the audit. For example a complex IT system with several sub-systems will lead to the adoption of risk oriented and process oriented audit approaches. Moreover, tests of internal controls in a computerized information system require special audit methods and the performance of computer-assisted audit procedures. There is, therefore, a particular need for some basic awareness by auditors of the audit implications of electronic service delivery in the public sector.

In addition to its effect on the work they undertake for audit reporting, the development of electronic service delivery has several other implications for auditors. They need to be aware of information system security risks, controls and standards and to maintain and update their skills in order to undertake effective audits. In addition, they have an important role to play in promoting management's client awareness of best practice in building and maintaining secure and effective systems.

INTRODUCTION

1 Governments have been using computers to help deliver services for several decades. But now more radical changes in public service are achievable through the use of multiple media to deliver services directly over open networks through voice, fax, e-mail and Internet forms. It is expected that these changes will be able to meet the needs of citizens and business, and not trail behind technological developments in the private sector.

2 A primary objective of any government is the cost efficient improvement of the quality of public service in accordance with legal requirements. Making full use of the benefits of electronic service delivery can go a long way to achieving this aim. A commitment to "information age government" will involve initiatives appropriate to individual jurisdictions. Objectives might include:

- Increasing the number of public services that are capable of electronic delivery by particular target dates;
- Allowing citizens to pay for licences and make taxation payments via the Internet;
- Making public services available 24 hours a day, seven days a week, where there is a demand;
- Allowing citizens to notify different parts of government of changes in circumstances in one electronic transaction.

3 These objectives can be achieved by the provision of public services through the Internet (e-public services). Existing public sector information systems reflect the needs of their operators rather than their users – the public and businesses. This results in inconvenience for users, and fragmented and inconsistent pockets of information. In order to improve the position public sector bodies might plan to make public services easier to use by supplementing existing communication channels with the Internet. Against this background it is essential to identify risks and opportunities of the different E-public services models.

4 The basic service model is the utilization of the Internet for information purposes. Websites used for browsing – e.g. for information on government services that is not specific to an individual such as the opening hours of public offices or tourist information. Information is conveyed in only one direction, which means that the Internet user can only read the data on the website, but cannot interact with the site other than to move from page to page.

5 A more advanced service model enables the user to interact with the website. An example is where farmers can apply for Common Agricultural Policy grants on-line: this will allow applications to be made, and processed, more quickly thereby improving farmers' cash flows. In this model information is exchanged in both directions, since the website both captures and displays data.

6 The service model reaches the e-commerce stage where a website's functions allow the procurement of goods and services that lead to the conclusion of financial transactions. Citizens are able to place orders for goods and services, which may be paid by credit card.

7 The service model with the highest complexity is the complete integration of the e-public service system within a public entity's business processes. The internet-based purchase of goods and services leads to interactions with other parts of the entity's IT system. For example, a purchase order initiated by the e-public services system may automatically trigger the movement of goods from the warehouse system to the delivery department and lead to data being recorded in the management information system, including the accounting system, and to transactions with suppliers. Hence, the e-public services system becomes an integral part of the entity's IT system.

HOW ELECTRONIC SERVICE DELIVERY AFFECTS AUDIT

The effect of electronic service delivery on audit objectives

8 Auditors have been auditing computerised information systems (IT systems) for many years and have adapted their approach to deal with risks relating to electronic data processing. But the use of the Internet, and other media, to deliver services raises new issues for management and auditors.

9 Electronic service delivery does not introduce new audit objectives, but it does introduce new risks (or changed levels of existing risks) and new forms of business records. New risks need to be managed and so require new controls. Electronic service delivery therefore has a two-fold effect on audit. Firstly, auditors must test the effectiveness of new controls if they are to rely on them in the course of providing their opinions and reporting on risk. Secondly, where audit evidence takes electronic form, such as computerised transfer payment records, auditors must take steps to ensure that they can rely on this evidence. This second consideration itself involves controls, so the two effects cannot be wholly separated.

The effect of electronic service delivery on the audit approach

10 The complexity of the service delivery model can affect the audit approach. In deciding on the design of the risk-driven audit approach, the organizational structure and the structure of operation and controls of the public sector entity being audited is crucial. When the design of controls is focused on a single computer application or computer system there is a danger that risks arising from the exchange of data between computer systems are not evaluated and that the technical context of the computer systems may not be adequately considered (e.g. the data exchange between the e-public service system and the accounting system). This may lead to controls being considered effective with respect to one separate computer system or application, even though these controls could be by-passed deliberately by, for instance, manipulating the upstream or downstream computer system or application.

11 From an auditor's perspective, the complete integration of the e-public service system within a public entity's business processes is a significant risk. This service delivery model contains complex business processes whose sub-processes involve several functional areas with non-integrated computer systems. In this case, it should be ensured that sufficient consideration is given to the data flow between the computer systems and the technical context of the computer system surrounding sub-systems.

12 Furthermore where a business process spans organisational boundaries there is a need to ensure continuity of control. If the managers involved have different views on control objectives and the means to achieve them, continuity of control will be more difficult to achieve and maintain. Consistency of information security across organisational boundaries becomes increasingly important as the number of organisations and the importance of exchanging data increases. The need for continuity and consistency of controls across organisational boundaries makes shared control standards particularly important.

13 In order to test the controls the auditor should determine whether the entity has responded to the identified inherent risks in the IT system by establishing effective internal controls. From the auditor's perspective internal controls and internal control systems are effective when they prevents inherent risks in the IT system from causing material error, fault or failure during a specified period.

14 A material prerequisite for the assessment of the effectiveness of controls is the auditor's assessment of the appropriateness of management's evaluation of IT risks in the context of the implementation of the IT strategy.

15 All policies material to the identification and analysis of IT risks relevant to accounting should be investigated to understand how management arrives at its assessment of risks and decides on the establishment of internal controls to limit the potential effects of these risks. Beyond this, the auditor should determine how management identifies all risks that may affect the reliability of accounting data and the presentation of financial information and how the consequences of these risks, in terms of their probability of occurrence and their quantitative effect, are assessed.

16 To test the effectiveness of the internal controls, the following steps are required in the audit areas defined in audit planning:

- Documentation of the IT system as the basis for the auditor's understanding of the internal controls and the internal control system;

- Testing the design of the internal controls (test of design);

- Testing the operation of the IT controls (test of operation).

17 The purpose of tests of design is to assess, whether the stipulated controls are appropriate and effective to the extent intended. The specific controls (i.e. input, output and processing controls) and their interaction are the subjects of this test. Typical audit procedures for tests of design include reviewing documents, making inquiries, observing activities and work processes.

18 Tests of operation are conducted for those controls of the IT system that the auditor has found to be adequate in the test of design. The purpose of tests of operation is for the auditor to asses whether the controls established are effective and contribute to the limitation of IT risks. The final assessment of the effectiveness and continuous application of the controls on the basis of the tests of operation should be adjusted to reflect any insights gained during the course of the audit.

19 Additional audit techniques are considered for tests of operations beyond the audit procedures already applied in conducting tests of design. The auditor may also assess the effectiveness of controls by means of:

- Analytical procedures;
- Assessing controls using re-performance or the auditor's own tests of control; or
- Using the work of third parties.

20 Tests of operation are supported by programs to assess the effectiveness of controls, such as testing the configuration of operating systems or assessing access rights to program libraries. The tools to test the effectiveness of controls include, among other items, the program controlled generation of test cases to examine input, processing and output controls. The use of computer-assisted audit techniques is particularly advantageous in those cases in which vouchers are only transmitted, generated and stored in electronic form or in which there is a very high number of transactions. Hence, the nature and extent of computer assisted audit techniques should be determined as part of risk-driven audit planning after taking into account the electronic service model used by the public sector entity.

WHAT RISKS ARISE FROM ELECTRONIC SERVICE DELIVERY?

21 As discussed above electronic service delivery generates new opportunities as well as new risks. The risks include those relating to technology, software, transaction authentication, electronic and digital signatures, legal provisions relating to electronic documents, and personal information privacy. These risks need to be effectively managed in order to ensure the proper functioning of the entity's IT operating system for electronic service delivery (IT risks), the legitimacy of their transactions (legal risks) and the reliability of their records and their information (risks for the reliability of accounting information).

IT risks

22 Since electronic service delivery invariably involves the use of the Internet, the most important risks associated with electronic service delivery are IT risks. The following IT risks can be distinguished: IT infrastructure, IT application, and IT business process risks.

23 IT infrastructure risks relate to the adequacy of the IT infrastructure for information processing. For example, hardware may be susceptible to malfunction. IT infrastructure risks are addressed by a security concept geared to the needs of the entity and by technical and organizational controls defined on this basis. Typical IT infrastructure risks include:

- Inappropriate physical security measures that do not prevent theft, unauthorized access or improper disclosure of information;
- Vulnerability to overheating, water, fire and other physical risks;
- Inadequate or improper emergency plans and procedures;
- Absence of adequate back-up procedures;
- Inadequate configuration and monitoring of firewalls against intrusion attempts;
- Inadequate encryption.

24 IT application risks result from:

- Bugs and errors in IT applications;
- Uncoordinated or undocumented program changes;
- Inadequately designed input, processing and output controls in IT applications;
- Inadequate procedures to ensure software security in connection with the security infrastructure (inadequate access authorization concepts and data back-up and restart procedures).

25 The expression “IT business process risks” is primarily a private sector term. However, it is used here to refer to risks that arise where analyses of security and information processing do not include all the processes of the public sector entity, but just certain parts. Such risks may arise from:

- Lack of data flow transparency;
- Inadequate integration of systems;
- Deficient reconciliation and control procedures in interfaces between sub-processes arising from the exchange of data between two subsystems.

26 In this situation, there is a risk that IT controls, such as access rights or data back-up procedures, will only be effective for the sub-processes, but not for the aggregated processes. Typical IT business process risks in an electronic service delivery environment include:

- Transaction data are not transmitted efficiently, completely or accurately from the electronic service sub-system to the accounting application;
- Safeguards only protect a sub-system from unauthorized or unapproved transactions and thereby allow transaction data to be modified by one of the downstream IT sub-systems;
- Improper or inadequate access control mechanisms may make it difficult or impossible to effectively manage access controls for all IT sub-systems integrated into the process of the public sector entity;
- Access protection that responds to a single IT application integrated into the process of the public sector entity could be bypassed deliberately by manipulating the upstream or downstream IT sub-systems;
- Back-up measures are only effective for the electronic service sub-system and hence for the sub-process, but not for the entire IT process;
- The design and implementation of interfaces between the electronic service sub-system and downstream IT sub-systems may not be appropriate.

Legal risks

27 Management is responsible for ensuring that electronic service delivery operations are conducted in compliance with applicable laws and regulations. The global nature of the Internet and international business creates additional legal problems (including national and international issues related to commercial law, tax law, criminal law, civil law and data protection). Against this background the European Directives on electronic commerce (2000/31/EC) and distance selling (97/7/EC) are important steps in the harmonisation of legal requirements. They contribute to the proper functioning of the internal European market by ensuring the free movement of services and goods between Member States. Consequently management has to ensure that the electronic service delivery systems are performed in accordance with the requirements of these EU Directives as implemented at the national level.

28 In general, public sector entities do not operate in other jurisdictions. However, if they do, they should be aware that, despite the best efforts of international rule-making bodies, applicable laws and regulations will vary across national boundaries. Some of the relevant legal issues include:

- Protection of intellectual property, including patent, copyright, and trademark laws;
- Enforceability of contracts with Internet Service Providers;
- Ownership of software by a software vendor or the right of a software vendor to sell software licenses.

29 In some jurisdictions public sector entities are required to make an assertion on the legality of transactions. Subsequently auditors are required to give a view on this assertion. In such cases management and auditor need to consider whether electronic transactions comply with legislation and regulations. This is particularly the case where the appropriate authority requires a physical signature or mark. Legislation might establish a legal basis for electronic signatures so this particular concern should recede once suitable legal precedents have been established. Regardless of the legality of the use of electronic signatures, the value of digitally signed transactions is critically dependent on the adequacy of the security environment in which the signature is applied. Factors such as the identification and authentication of users and the proper generation and management of cryptographic material affect the extent to which digital signatures enhance assurance.

Privacy risks

30 A public sector entity’s management is responsible for ensuring the privacy of personal information obtained through electronic service delivery activities e.g. on-line tax registration or on-line crime reporting. Although privacy and security of information are highly related, secure electronic delivery service systems do not automatically provide assurance that privacy is not being abused or violated.

31 The collection of “personally identifiable” information must comply with the requirements of the EU Data Protection Directive 95/46/EC. Thus, management will need to establish the way in which this Directive has been implemented at a national level in order to ensure that the data collection methods comply with domestic data protection legislation. In the case of service delivery outside the EU, management should be aware that there are no universally accepted definitions as to what constitutes the ownership and privacy of information. Therefore it is important to develop and publish a privacy policy as an essential part of security policy.

32 Consequently it is important that management assesses the legal requirements in countries where their customers, suppliers or service providers are located to determine the degree of privacy that the law requires. Under the safe harbour principles of the European Union, an entity should inform individuals why private information about them is being collected.

Risks for the reliability of accounting information

33 In an e-public service environment, commercial activity generated by an entity's website is automatically interfaced with the entity's "back office" systems, such as the internal reporting system, the inventory management system and the accounting system. An e-public service activity becomes relevant to the accounting system, if the activity – in particular e-public service transactions – affect assets or liabilities, result in expenses or income, or lead to events requiring disclosure in the financial statements or other reports.

34 Public sector entities must keep adequate records in order to provide a basis on which to report to legislatures, local electorates and the general public on the stewardship of public funds. Regardless of the form of records, auditors need to gather sufficient, relevant and reliable evidence to support their opinions. For records to be adequate, public entities should apply key principles for accounting information security and for appropriate accounting information processing. The next section discusses these principles.

WHAT PRINCIPLES FOR RELIABLE ACCOUNTING INFORMATION SHOULD BE FOLLOWED?

Principles for accounting information security

35 A prerequisite for reliable information in the books and records and hence the financial statements is secure accounting data and information. For the purposes of this document, data are defined as the basis for information. Since data are processed using IT applications and the underlying IT infrastructure when obtaining accounting information, IT applications and the underlying IT infrastructure are also aspects relevant to accounting information security.

36 Management is responsible for establishing the prerequisites for accounting information security. To achieve this, an appropriate security concept to ensure the required degree of information security can be developed, implemented and maintained.

37 A security concept comprises management's assessment of the security risks resulting from the use of IT. The security concept is an essential starting point for the implementation of information security policies. Such policies encompass the sum of policies and procedures that protect information against unauthorised disclosure, manipulation, unavailability and destruction. The main steps are:

- Identifying information and recording management risks and addressing them in corporate policy;
- Translating policy into appropriate controls that generate evidence of their effectiveness;
- Including control requirements in information system specifications and contracts.

38 IT systems are more likely to yield reliable accounting information when they meet the following security requirements:

- Integrity
  This requirement is fulfilled for an IT system when data and information are complete and accurate, systems are complete and appropriate and all of these are protected against unauthorized modification and manipulation. Appropriate testing and release procedures are typical means by which the integrity of data, information and systems can be ensured. Technical measures to achieve this include firewalls and virus scanners. The reliability of IT-aided accounting processes is improved when the IT infrastructure and the data, information and IT applications are used in a specified configuration and only authorized modifications are permitted.
- Availability
  Under this requirement, the public sector entity ensures the constant availability of the hardware, software, data and information to maintain business operations and also that the hardware, software, data, information and the requisite IT organization can be made operable within a reasonable period of time (e.g., after an emergency interruption). It is therefore important to establish appropriate back-up procedures for emergencies. In addition, the ability to convert digitally maintained books and records into human-readable format within a reasonable period of time is essential.

- Confidentiality
  This requirement means that data obtained from third parties not be transmitted or disclosed without authorization. Organizational and technical measures, like encryption technologies, include instructions to restrict the transmission of personal data to third parties, identify and verify the recipient of data, and to delete stored personal data after a certain length of time.

- Authenticity
  This requirement relates to the traceability of a business transaction to the individual who initiated it. This can be done by using an authorization procedure. When data or information are exchanged electronically, it is important that the other party be identified or identifiable – e.g., by using digital signature procedures. It may be convenient to use shared external or independent facilities (e.g., trust centres) for this purpose.

- Authorization
  This requirement means that only certain persons, appointed in advance (so-called authorized persons), may access certain data, information and systems (e.g., password protection) and that only authorized persons can use the rights defined for this system. This includes reading, creating, modifying and deleting data or information or the administration of an IT system. Useful methods to achieve this are physical and logical security procedures. Organizational arrangements and technical systems for access protection are essential to segregate incompatible duties. Biometric systems will become more common in future to supplement ID cards and passwords.

- Non-repudiation
  This requirement is defined as the ability of IT-aided procedures to bring about desired legal consequences with binding effect. It should be difficult for the person initiating the transaction to deny its validity on the grounds that the transaction was unintended or unauthorized. The use of public key systems can help prevent repudiation.

Box 1: Outline of the effects of electronic service delivery
Case study of a local authority procuring goods and services electronically

The authority keeps electronic records of specifications, standard orders, individual purchase orders, invoices and payments. It has established arrangements with an electronic procurement 'hub' (an Internet-based forum that contains the catalogues of a range of suppliers and buying requirements of other organisations). It has established access controls to its purchasing records so that only authorised people within the authority can amend the records and undertake transactions. Similarly, the authority has access controls to prevent unauthorised remote access to its purchasing systems. The system provides an audit trail by means of an electronic log of all changes to the records it contains. This records the electronic identities of all people making changes to the records, and the times and nature of the changes.

The authority's auditors may test the access controls for two reasons: firstly, to ensure that the system is robust so that the authority has reasonable precautions in place against loss of function and financial loss; secondly, to help ensure that they can rely on records produced by the system to form an opinion on the accounts. The auditors may also test the efficacy of the electronic log in order to establish the liability of the electronic records.

In addition to testing the system controls, the auditors may test a sample of transactions as recorded by the system. In doing so, they will be placing reliance on their system controls testing.

Principles for appropriate accounting information processing

39 Auditors who are unable to rely on electronic records may have to qualify their opinions on accounts, drawing attention to the absence of reliable business records. In requiring sound electronic records management, the auditor is seeking no more than that required for prudent business management. It is therefore in management's own interest to be able to demonstrate the reliability of business records by reference to acceptable and demonstrable principles.

40 The principles for appropriate accounting information processing are fulfilled where the e-public service system and the entire IT system safeguards meet the following general criteria for the input, processing, output and storage of information and data about e-public services transactions:

- Completeness;
- Accuracy;
- Timeliness;
- Assessability;
- Order;
- Inalterability (logging of alterations).

41 The completeness criterion refers to the extent and scope of processed transactions, i.e., the recipient of transactions determines that all transactions are input completely into the IT system.

42 In accordance with the accuracy criterion, processed information should accurately reflect transactions, i.e., recorded transactions should reflect the actual events and circumstances in conformity with the applicable financial reporting framework.

43 Under the timeliness criterion, e-public services transactions should be recorded on a timely basis, i.e., as soon as possible after the transaction has occurred. When some time elapses between the occurrence of a transaction and its recording, further appropriate action may become necessary to determine completeness and accuracy of the entry recorded.

44 Under the criterion of assessability, each item and disclosure in the financial statements should be verifiable in that it can be traced back to individual entries in the books and records and to the original source documents that support that entry. Furthermore, the criterion of assessability implies that an expert third party should be able to gain an insight into the transactions and position of the entity within a reasonable period of time.

45 In an accounting system, accounting entries should be organized in both chronological order (a journal function) and by nature (e.g. by type of asset, liability, revenue or expense – a ledger function). Transactions and their recording should be identifiable and be capable of conversion into human-readable format in a reasonable period of time.

46 In accordance with the criterion of inalterability, no entry or record may be changed after the posting date such that its original content can no longer be identified, unless the change to the original content can be identified by means of a log of such alterations. Therefore, alterations of entries or records should be made such that both the original content and the fact that changes have been made are evident or can be made evident. For program-generated or program-controlled entries (automated or recurring vouchers), changes to the underlying data used to generate and control accounting entries would also be recorded. This applies, in particular, to the logging of modifications of settings relevant to accounting or the parameterization of software and the recording of changes to master data.

47 Before accepting a transaction for processing, it would be useful to verify the following:

- All transaction details have been entered by the citizen;
- The authenticity of the citizen;
- The availability of the services to be supplied;
- The reasonableness of the inquiry, for example, to identify an unusually large amount resulting from an input error, or to identify erroneous duplicate orders;
- The pricing structure applied, where appropriate;
- The method of payment or credit worthiness of the citizen;
- The non-repudiability of the transaction in that the author thereof cannot later deny having entered into it.

48 In an electronic service delivery process, evidence of transactions often cannot be furnished by way of conventional vouchers – nor should it be. Despite this fact, transactions should continue to be supported by appropriate documentary evidence (i.e., the source document entry function).

49 Appendix A provides guidance on the adequacy of criteria for a functioning accounting system and highlights:

- Source Document Entry Function;
- Journal Function;
- Ledger Function;
- Documentation; and
- Retention Requirements for E-Business Transactions.

WHAT ELSE SHOULD AUDITORS DO IN RESPONSE TO ELECTRONIC SERVICE DELIVERY?

Contributing to audited bodies' understanding

50 The auditor has an important role to play in drawing clients' attention to the importance of information security standards, principles for reliable accounting information and in helping management to identify the control requirements associated with the effective management of electronic records. The progressive increase in the rigour of controls to be applied to particular classes of transaction is illustrated in Appendix B. Further information on controls and other security requirements that are appropriate to different types of electronic service delivery is provided at Appendix C.

51 Early audit involvement can help management avoid the expensive process of 'bolting-on' controls as an afterthought or suffering the consequences of insecure, unreliable or ineffective business information.

Acquiring and maintaining appropriate skills

52 The implications of electronic service delivery mean that auditors need training and development to ensure that they understand the impact of electronic service delivery on the audit. The level of skills and knowledge will vary with the complexity of the e-activities of the public sector entity. In the course of the audit planning the auditor has to consider whether the personnel assigned to the engagement have appropriate knowledge. Depending of the significance of the effect of electronic service delivery on the financial statements this knowledge may require an understanding of the risks involved and the controls appropriate to manage those risks. Most auditors will not require detailed technical knowledge of the mechanisms involved in electronic service delivery, but their understanding should be sufficient to enable them to recognise risks, evaluate controls, identify the need for the assistance of an expert and interpret the findings of the expert in the context of risk.

Willingness to embrace change

53 New ways of working will be necessary to achieve the development of robust and auditable electronic service delivery systems. This will require public sector auditors to be supportive of public bodies' efforts to exploit new service delivery channels effectively.

54 Auditors will need to adapt their audit approach in the light of electronic service delivery. Where auditors need to rely on electronic evidence, it will be particularly important for them to ensure that management is aware of the controls that need to be built into systems to protect the reliability of electronic records. Auditors should remain independent of the implementation and operation of the systems that they audit, but they can still draw on their knowledge and experience to provide advice to management on developing secure and effective electronic service delivery solutions.

CONCLUSION

55 Electronic service delivery does not introduce new audit objectives, but it does introduce new or modified risks- IT risks and legal risks. Managers and their auditors need to be aware of these risks and ensure that adequate controls are introduced to manage them. Where an audit relies to any extent on these controls to provide assurance, or assesses risk to the system, the controls will need to be audited.

56 The records produced by electronic service delivery systems also have audit implications. Ensuring that authentic records are available for auditors to rely on is more complex with electronic records than it is with paper documents. Clients therefore need to implement sound records management and information security in order for auditors to meet existing audit objectives. The minimum principles with which management should be able to demonstrate compliance should be set out in a public information security policy.

57 In the context of electronic service delivery, auditors may contribute to government modernization by:

- Contributing to audited bodies' understanding of appropriate controls and information security, and in particular, making clear their expectations in these areas;

- Ensuring that they maintain their professional knowledge to a level that will enable them to understand the strengths and weaknesses of controls in an electronic service delivery context;

- Embracing change by adopting an audit approach that reflects the changed risks introduced by electronic service delivery;

- Assisting the formulation and promulgation of standards on information system security and electronic service delivery;

- Agreeing common approaches to the audit of 'joined-up' electronic service delivery so that auditors can work together more easily and take account of each other's work.

APPENDICES

A: THE CRITERIA FOR A FUNCTIONING ACCOUNTING SYSTEM

B: TRANSACTION TYPES

C: EXAMPLES OF SECURITY REQUIREMENTS AND MECHANISMS OF DIFFERENT TYPES OF ELECTRONIC SERVICE DELIVERY

D: USEFUL FURTHER SOURCES

APPENDIX A: THE CRITERIA FOR A FUNCTIONING ACCOUNTING SYSTEM

Source Document Entry Function

According to the criterion of assessability, an expert third party should be able to gain an insight into the transactions and position of the entity within a reasonable period of time. Achievement of this objective requires that each transaction be supported by appropriate documentary evidence. This presupposes an audit trail from the original document to the financial statements and vice-versa. This source document entry function provides evidence for an entity's management accounting and financial reporting.

For automatically generated e-public services transactions, the source document entry function may also be satisfied by demonstrating that the accounting process itself links the specific transaction with its entry. Process evidence can usually be furnished by the following:

- Documentation of the program's internal entry generation rules;
- Evidence that these generation rules have been subject to an authorized modification procedure (including access protection, application control, testing and release procedures); and
- Evidence that entries have actually been made in accordance with these rules.

How the source document entry function is actually implemented depends on the structure of e-public services processes. When a transaction is recorded, the entry of at least the following information is important:

- A sufficient description of the transaction (a description of the transaction or a key representing such a description);
- The amount entered or details of quantity and value which determine the amount entered;
- The date of the transaction (voucher date, accounting period);
- Confirmation (authorization) by the person responsible for keeping books of account.

The time at which a transaction is deemed to have been posted also depends on a decision by the person obliged to keep the books of account in accordance with the entity's policies. Transactions are generally deemed to have been posted when they have been authorized, recorded and stored completely and accurately in an orderly fashion on a timely basis and in a form that can be processed. To achieve this, the details of the transaction may be supplemented by:

- Account coding (both sides of the accounting entry);
- Order criterion (e.g., voucher number);
- Posting date.

It is also important that an entry's authorization be defined and documented for e-public services transactions. In addition to globally standardized remote data transfer systems (S.W.I.F.T., EDI, and EDIFACT), individual contractual arrangements between contracting parties may also be used. The rules for generating and checking entries are generally set out clearly in the process documentation. Programs that have been released are ordinarily protected against unauthorized and undocumented modification. Evidence of authorization is provided by the documentation of the automated authorization procedures applied.

Journal Function

The journal function provides that all transactions posted into the books are recorded completely and in an understandable manner in chronological order as soon as possible after they have occurred (usually in a journal). While the purpose of the source document entry function is to demonstrate the existence of a transaction and the authorization to process it, the objective of the journal function is to demonstrate that transactions have actually been processed, and that processing took place in a reasonable time.

In a journal function, entries are stored in an analyzable form (itemized) in the e-public services applications upstream of the accounting system. In addition to process documentation, a control and reconciliation system may be used to demonstrate that the entries stored in non-accounting applications are identical to those in the general ledger and sub-ledgers.

In a journal function, the records stored are protected against modification or deletion. If vouchers are entered into intermediate files so that corrections can be made after having checked them, the lists generated from such files are classified as data entry logs and not as journals because the transactions have not yet been authorized.

A journal contains evidence of the transactions with all of the information required to fulfil the voucher function – if necessary by using references to further information stored elsewhere.

Journals may be saved for statutory retention periods by printing them out on paper or storing them on machine-readable data carriers. If a journal is stored as a printout, the completeness of the printed list can be shown by, for example, having consecutive page numbers or totals brought forward. When journals are stored on data carriers, it is important that the underlying process allow the conversion of the journals into human-readable format throughout the retention period.

Ledger Function

The ledger function provides that transactions recorded in chronological order in the journal are also organized by type of asset, liability, revenue or expense in accounts. In accounting systems, the journal and ledger functions are usually combined. In integrated software these functions may be supported by automatic account assignment processes.

The ledger function presents transactions separately for the general ledger and sub-ledgers, generally with the following information:

- Name of account;
- Entry identifier;
- Credit and debit totals and balances;
- Entry date;
- Voucher date;
- The account representing the other side of the accounting entry;
- Voucher reference;
- Entry description or code.

Furthermore, it may be useful if the following information is presented by the ledger function:

- Credit card approval number;
- Packet information to substantiate receipt, etc.;
- Digital signature information to enforce the contract.

Documentation

A prerequisite for the transparency of IT system is adequate procedural documentation that contains a description of all of the elements of the system needed to understand the e-public services process. An expert third party is able to assess the appropriateness of complex procedures only if he or she has access to informative documentation to supplement input data and processing results. It is important that documentation created to understand an e-public services process be adequately maintained so that the appropriateness of the processing of the accounting information can be assessed.

Procedural documentation consists of user documentation and technical system documentation. User documentation contains the information that is needed for the proper use of all IT applications. In addition to a general description of the tasks covered by an IT application and an explanation of the relationships between the different application modules, user documentation describes the nature and meaning of the input fields, the program's internal processing procedures (especially automated processing procedures) and the procedures for generating reports.

When standard software is used, the documentation supplied by the manufacturer is supplemented by a description of any adjustments that have been made to the application and documentation of the user's internal control system (e.g., parameterization and the use of input fields or code systems).

The main objective of technical system documentation is to ensure the secure and orderly operation of the IT. In addition, the technical system documentation ensures that the program developer can service IT applications. The nature and scope of technical documentation depends on the complexity of an IT application. The methodology and formal structure of technical documentation is within the discretion of the program developer. Given the large number of programming languages, documentation that refers only to the program source code is not adequate to ensure the transparency of e-public services and the accounting system. The documentation allows an expert third party to understand program processing – especially the processing functions and procedures – within a reasonable period of time and without knowledge of the programming language.

For example, technical system documentation contains information about the following:

- The purpose of a software module in connection with other modules;
- Data organization and structures (structure of data records or tables in databases);
- Modifiable elements of tables that are used to generate entries;
- Programmed processing procedures, including the input and processing controls in place;
- Programmed error routines;
- Keys;
- Interfaces to other systems and the specific data exchanged;
- Edit routines and the actions initiated (e.g., halt processing, create an error message, etc.).

Technical system documentation is generally supplemented by documentation of the proper application of the system. This relates to:

- Back-up processes;
- Business continuity processes, including ISP processes
- Processing verification (processing and reconciliation logs);
- Description of the procedures for releasing new and modified programs;
- List of available programs with evidence of the program version.

Retention Requirements for E-Business Transactions

Typical storage techniques are optical storage (microfilm), electronic storage (storing data in digital form on magnetic data carriers) and digital optical storage (storing an optical image on electronic media).

Technical storage processes depend on how documents are stored. Coded documents (CI = Coded Information) can be distinguished from non-coded documents (NCI = Non-Coded Information). CI documents can be analysed directly with the aid of IT and include, for example, business correspondence received electronically or files that can be printed out. NCI documents comprise analogue information carriers (e.g., paper) that cannot be analysed in their original form using IT, but which have to be digitalized prior to storage, for example, by scanners. The result is a digital image (bitmap or other digital image formats) that can be displayed on the monitor and printed out. To make it possible to locate an image, it is given an index designation that is stored separately from the document.

CI documents can be stored immediately and their contents analysed by, for example, searching for account numbers in an archive file containing statements of account. A typical example of this filing method is the COLD (Computer Output on Laser Disk) process. An additional printout of a CI document does not increase its evidentiary value, because the storage process itself satisfies the source document entry function. Business correspondence received electronically (for example via EDI, S.W.I.F.T. or e-business communications or transactions) should be stored in the format in which it was received as if it were an original document.

NCI storage systems can be categorized into gross imaging and net imaging systems. Gross imaging stores complete images. This process is, therefore, suitable for incoming and outgoing documents. In net imaging, recurring information on a document (e.g., the letterhead) is filtered out and is not stored. This process is suitable for storing standardized incoming documents or outgoing documents, provided that the net image can be combined with the filtered information when the document is reproduced.

Optical storage systems on non-rewriteable alternate storage media represent common storage processes for data carriers. When the digitalized documents are unalterable, the evidentiary force of the books and records is preserved by way of coordinated technical (e.g., unalterable storage media) and organisational (e.g., access protection and back-up procedures) measures and the proper implementation of document management systems within the existing organization of the entity.

The related technical and organizational requirements include:

- Inalterability of a digitalized document;
- Back-up copies of files;
- Organizational arrangements for the digitalization procedure to monitor completeness and reproduction quality; and
- Indexing processes that allow the digital document to be matched to the transaction.

APPENDIX B: TRANSACTION TYPES

Classes of transaction that might be subject to different levels of authentication have been defined as the following:

Class 1: provision of information on government services that is not specific to an individual

Examples:
Provision of leaflets, oral information, tourist information by post.

Identification:
No identification of the individual is required and should not be requested. Provision of material through the post requires name and address, but there is no reason for verification.

Class 2: disclosure of personal information by government to an individual

Examples:
Pension forecast, dates of payments, tax liability, payment values.

Identification:
Random permutation of a minimum of two pieces of personal information from, for example:

Full name
Address
Postcode
Date of birth
Identification number (e.g., Social Insurance Number or Tax Reference, as appropriate to the service)

Plus a piece of information only likely to be known by the caller, for example:

Mother's maiden name
Random digits of a PIN number

Class 2a: disclosure of personal information to government by an individual that could affect payments to, or liability of, the individual

Example:
Change of circumstances (address, name, marital status), income details for tax assessment

Identification:
Random permutation of minimum of two pieces of personal information from, for example:

Full name
Address
Postcode
Date of birth
Identification number (e.g., National Insurance Number or Tax Reference, as appropriate to the service)

Plus a piece of information only likely to be know by the caller, for example:

Random digits of a PIN number

Written proof of change of circumstances may be required by statute or may be a sensible anti-fraud prevention activity. In the case of benefits payments, a site visit may be necessary.

Class 3: payment for a government service by an individual

Example:
Purchase of TV licence

Identification:
Valid credit or debit card details
This may be in addition to identification of Class 2a, depending on the service, e.g., purchasing books may only require card details, paying for a TV licence would require Class 2a identification.

Class 4: payment to an individual by Government

Example:
Transfer payment

Identification:
Any innovative arrangements will require identification appropriate to audit and risk assessment requirements. With the emergence of new technologies and processes, this class will be kept under review.

Class 5: initial registration for a service by an individual

Example:
Passport application, driving licence application

Identification:
Any innovative arrangements will require identification appropriate to audit and risk assessment requirements. With the emergence of new technologies and processes, this class will be kept under review.

APPENDIX C: EXAMPLES OF SECURITY REQUIREMENTS AND MECHANISMS OF DIFFERENT TYPES OF ELECTRONIC SERVICE DELIVERY

Public information delivery

Description

Many public sector bodies already deliver information electronically through their web site and by e-mail. For example, the opening times of libraries and other services can be publicised in web sites. Some public bodies provide information through telephone call centres. There is scope for public sector bodies to deliver more publicity material through web sites and perhaps digital television.

Security requirement

There have been high profile incidents where public bodies have had their web pages “hijacked”. In cases where the legitimate contents of a web page have been corrupted or replaced, this causes significant disruption of the organisation affected and embarrassment.

It can be equally embarrassing if a public information system fails. There have already been cases of public sector information systems being brought down due to inability to cope with demand, poor design and by deliberate overloading via the Internet.

There is therefore a requirement to protect both the integrity and availability of public information systems and the services based on them.

Security mechanisms

The availability of public information services electronically depends both upon the availability of an information source and on a communication channel between the customer and the information source. The most basic responsibility of the owner is to ensure that there is a tried and tested business continuity plan to restore service delivery in the event of the failure of the primary system. The sophistication of the business continuity plan should reflect the likely impact of service unavailability.

The confidentiality and integrity of the information held on a web site can be protected by access controls based on a firewall and the operating system of the web server. The owners of public information systems should be able to demonstrate that they have considered the risk of unauthorised alteration or disclosure of their information and that they have evidence that the controls in place are meeting their requirements.

One type of attack on Internet sites involves first rendering the legitimate site unavailable and then causing enquiries to be diverted to a site under the control of the attacker. The primary defence against this sort of attack is to protect the legitimate public information system from being attacked through the Internet. Where public information is of vital importance additional technical measures might be employed to provide a user of the service with assurance that the service is being delivered by a legitimate system.

Personal information

Description

The public sector holds substantial quantities of personal information. For example, doctors in the public sector hold administrative information about their patients, such as names, addresses and appointment times, as well as medical information, such as treatment histories. Governments should make it easier to update personal information held by the public sector.
Achieving this might be done in several ways such as:

- Central storage of core personal information;
- A central personal information submission point with automatic onward submission of any changes to personal information systems held by other bodies;
- Use of information stored on a personal data storage device such as a smart card;
- Automated form filling using a personal information assistant that stores basic personal information locally.

Security requirement

Abuse of personal information held by public sector bodies is potentially extremely damaging to the privacy of citizens and to the sound reputation of public bodies. It may also expose the public sector body to the risk of legal action under data protection and human rights legislation. It is therefore important to control and record attempts to read or modify personal information.

The integrity of services based on the personal information submitted requires both secure information distribution and agreed data definitions.

Security mechanisms

There is a parallel here with the provision of banking services over the telephone and Internet. In both cases, the bank concentrates its efforts on setting up the account and then bases the security of subsequent interactions on secret information, such as account numbers and passwords, agreed when the account was set up.

Telephone banking relies upon interactive questions and answers to assure the call centre operator that they are talking to the right customer, and the customer that they are talking to a bank representative. The privacy of the conversation is assumed.

Internet banking cannot assume privacy of the interaction between the customer and the banking system as messages between the two can be intercepted, read and then discarded or altered. Banks have responded to this by using encryption to protect transactions made over the Internet.

Public Sector Procurement

Description

Buying goods over the telephone is well established in the private sector and buying goods over the Internet is becoming more widespread.

Security requirement

It is difficult to formulate a security requirement that would cover the whole range of public procurement as the range in value of transactions is so large. But both large and small transactions should involve:

- Separation of duties (requisition, authorise, order, accept, pay);
- An end user;
- An authorised buyer;
- An approved seller;
- Receipt of goods and services;
- Payment;
- Audit trail from the point of request through receipt of goods to payment and hence the accounts.

Security Mechanisms

Enforcement of separation of duties relies upon setting up individual's authorised roles and a means of identifying individuals and mechanisms to prevent loss of audit trail, unauthorized actions, payment before goods are received, and inaccurate accounting.

The identification of individuals in an online transaction environment involves having a set of user identifiers and then verifying that an individual using an authorised identifier is actually the person they claim to be. The depth of the authentication of a claimed identity should reflect the impact that could be caused by abuse of the authorised actions of the claimed identity.

For personal transactions over the telephone, the usual pattern is for the buyer to use a credit card. When a purchase is made the buyer quotes numbers from the face of the card. All this proves is that the buyer has seen the card and knows the name of the authorised holder, the card number and expiry date. Checks may extend to asking for the card billing address. Control depends on the cardholder controlling physical access to the card and checking the charges made against the card to those that they have authorised. For small transactions this system has been widely used in the private sector for years with a certain tolerated level of abuse. Use of the telephone allows higher value transactions to be recorded and later used by the seller both as evidence of the order made and, via voice analysis, to demonstrate the identity of the person placing the order. An additional control that can be linked to credit card transactions is the restriction of delivery to the cardholder's address.

If the transaction is made over the Internet, there are new risks:

- Information is exchanged in textual form that can, by default, be read or altered in transit;
- Text typed by one person is indistinguishable from text typed by someone else.

The most common countermeasure to eavesdropping is to negotiate a private link using encryption of the information passing between buyer and seller. Users are usually required to set up an account with a password that holds personal information that can be verified by the seller online. When the account is used over the Internet the seller loses the opportunity to record the conversation in a way that would be useful for voice analysis in the event of dispute, but (s)he has evidence that the buyer knew the account name, password and card details. In addition to the online interaction, it is usual for the seller to send confirmation to the buyer by email both as a shared record of the transaction but also to test the validity of the email address given by the buyer.

In the public sector context, similar models can be used by issuing approved buyers with cards with a credit limit appropriate to their authorised purchase level.

Within the buying organisation, accountability for electronic transactions may be based on traditional paper forms or the use of electronic “forms” to record requisition, authorisation, purchase, receipt and payment.

Where electronic forms are used, accountability will require that individuals have a unique electronic identity and that they can be held accountable for use of their identifier. In practice, this usually means that users log on to the corporate system using their identifier and password, and that their actions are subsequently constrained by the profile associated with their identifier. Accountability for transactions is usually based on the argument that the system controls render it impossible for a third party to pretend to be someone else or alter transactions entered by someone else. The strength of this argument depends on the security features of the system controls over the identification and authentication of individuals.

Accountability can be strengthened by the use of digital signatures but these are not widely used at present, as they require a supporting infrastructure that is still not widely available. Use of digital signatures provides additional assurance of the identity of the transaction originator as well as the integrity of the transaction itself. Where transactions are particularly sensitive or have to pass through hostile environments, such as the Internet, digital signatures can play a very useful role in building an appropriate security model.

Licences

Description

Acquiring passports, licences and certificates is a class of transaction that affects a large proportion of the population. Electronic application and distribution could replace the current pattern of form filling followed by a postal exchange. In particular, recent global events have emphasised the importance of properly controlling the issue of passports.

Security Requirement

Licences, certificates and passports need to be demonstrably authentic at the point of use. This has led to elaborate stationery incorporating features that are difficult to forge. If the paper form of licences were to be replaced by electronic equivalents then a similar degree of assurance of authenticity would need to be delivered by technical controls.

The process of obtaining a licence would be speeded up and simplified if an electronic licence could be applied for and issued electronically, printed on plain paper with a normal printer and checked using a hand held scanner.

The security requirement lies in the ability to demonstrate that a licence is genuine and that the details on it have not been altered since it was issued.

Security Mechanisms

Electronic licences can include a digital signature applied by the licensing authority that can be checked to demonstrate both validity and integrity.

Printed certificates might include a bar-coded “digital signature” that can only be applied using encryption keys held by the issuing authority. The licence itself would be issued as an image incorporating the bar-coded information. Checking the authenticity would then entail a software utility for electronic licences or a scanner for printed licences.

Form filling

Description

Many interactions between citizens and the government consist of obtaining a form, filling it out, posting it to the relevant authority and receiving a postal response. Examples include submitting tax returns and claiming benefits.

There are many attractions to filling out standard forms electronically including:

- The process is quicker;
- Answers can be validated locally and common mistakes eliminated;
- Processing electronic forms is more efficient than processing paper forms.

Security Requirement

Individuals are held accountable for the accuracy of the information that they submit on paper forms. In the event of dispute, the signed paper form is produced as evidence of the information supplied.

Paper forms are fairly difficult to amend without leaving evidence of the amendment. But electronic forms are comparatively easy to amend and the change is, by default, invisible, so the use of electronic forms requires a new mechanism to demonstrate that the form remains the same as it was when the applicant filled it in.

Security Mechanisms

A number of options have been used in existing applications:

- Printing out a copy of the form for retention by the applicant;
- Relying on the access controls of the systems that handle the form to stop unauthorised changes - this is difficult to demonstrate convincingly;
- Lodging copies of forms with third parties as evidence of what was submitted.

Digital signatures are an obvious candidate for the protection of electronic forms. The value of a digital signature depends on the robustness of the signature mechanism and the careful management of cryptographic keys, but these problems are not insuperable. The main problems with the use of digital signatures are that there is no standard digital signature mechanism or supporting infrastructure in widespread use, and very few members of the public have been issued with the means to apply them.

APPENDIX D: USEFUL FURTHER SOURCES

COMPUTER ASSISTED AUDIT TECHNIQUES

Guidance on this topic has been produced by INTOSAI, the international organisation for national level audit offfices. The guidance is available from:http://www.nao.gov.uk/intosai/edp

THE COBIT OPEN STANDARDS FOR IT SECURITY

These standards are available for free download from: http://www.isaca.org/ct_dwnld.htm

They include:

- Management Guidelines,
- Executive Summary,
- Framework,
- Control Objectives,
- Implementation Tool Set.

CODA GUIDE TO CHOOSING A FINANCIAL SYSTEM

CODA Group, a leading global provider of financial accounting software has developed a guide for companies selecting a financial system. The interactive guide will help customers to reduce expensive consultancy evaluation fees by providing a framework for selecting a financial accounting solution from all vendors, up to the point of the first product demonstration. The guide is available to download free from www.coda.com and is available in multi-lingual versions.