



PUBLIC AUDIT FORUM

Audit Implications of Electronic Service Delivery in the Public Sector

April 2001



Pulp used in the manufacture of this paper is
bleached by a totally chlorine free process
(TCF - Totally Chlorine Free)

THE PUBLIC AUDIT FORUM

Public sector audit has a key part to play in safeguarding public money, ensuring proper accountability, upholding proper standards of conduct in public services and helping public services achieve value for money.

The Public Audit Forum was established in 1998 by the national audit agencies: the National Audit Office (NAO), the Northern Ireland Audit Office (NIAO), the Audit Commission for Local Authorities and the National Health Service in England and Wales, and the Accounts Commission for Scotland. It was set up to provide a focus for developmental thinking about public audit.

The Public Audit Forum has a specific remit to build on the existing co-operation between the national audit agencies to enhance the efficiency and effectiveness of public audit, to provide a strategic focus on issues cutting across their work and to develop broadly consistent approaches to public audit.

MEMBERSHIP OF THE CONSULTATIVE FORUM OF THE PUBLIC AUDIT FORUM

Tim Burr

Deputy Comptroller and Auditor General
National Audit Office (**Chairman**)

John Ballard

Department of the Environment,
Transport and the Regions

Julie Barnaby

Department of Health

Robert Black

Auditor General for Scotland

Dr Peter Collings

Scottish Executive

John Dowdall

Northern Ireland Audit Office

Janet Eilbeck

PricewaterhouseCoopers

Martin Evans

The Audit Commission for Local Authorities and
the National Health Service in England and Wales

Brian Glicksman

HM Treasury

Ronnie Hinds

Audit Scotland

Lew Hughes

Auditing Practices Board

Gilbert Lloyd

KPMG

Caroline Mawhood

National Audit Office

Peter Makeham

Department for Education
and Employment

Andrew McCormick

Northern Ireland Office

Alan Meekings

District Audit

David Richards

National Assembly for Wales

Vernon Sore

Chartered Institute of Public
Finance and Accountancy

Eugene Sullivan

RSM Robson Rhodes

John Sweetman

Cabinet Office

Stephen Thornton

NHS Confederation

Norie Williamson

Convention of Scottish
Local Authorities

Penny Young

Consumers Association

David Corner

National Audit Office
(Secretary)

Contents

Foreword	2
Introduction	4
The Public Audit Forum’s contribution to the Modernising Government Agenda	6
How electronic service delivery affects audit	7
The effect of electronic service delivery on audit objectives	7
New risks and controls	8
Effects on audit evidence: authenticity and records management problems	9
Effects on audit evidence: the need for information security	10
Cross-organisational considerations: the need for continuity of control	10
How information security standards are relevant to audit evidence	11
Information security standards help establish reliability of records	11
Information security standards help auditors of different organisations to make use of each others’ work	11
Information security standard BS 7799	11
What auditors need to do in response to electronic service delivery	13
Contributing to clients’ understanding	13
Acquiring and maintaining appropriate skills	13
Willingness to embrace change	13
Contributing to the development of information security standards and policies	14
Working together	14
Conclusion	15
Appendices	16
A Useful Internet Links for Audit and Electronic Service Delivery Matters	17
B Electronic service delivery risk areas and the controls auditors expect clients to employ	18
C Transaction types	21
D Examples of security requirements and mechanisms of different types of electronic service delivery	23

Foreword

This paper sets out to explain the audit implications of the integrated electronic service delivery envisaged in the 1999 *Modernising Government White Paper*. In the public services, it is essential that electronic service delivery does not cause erosion of accountability. There is, therefore, a particular public sector audit need for some basic guidance on the audit implications of electronic service delivery, both for auditors and management.

The delivery of public sector services over electronic networks does not give rise to new audit objectives, but it does result in new risks that need to be addressed by management and assessed by auditors in their audit planning work.

Management needs to be able to convince interested parties, especially their auditors, that their electronic records are reliable; this entails demonstrating that the controls that protect the records are appropriate to the value of the records and that they are working consistently. From an audit point of view, this means evaluating the control environment that protects business information before using that information to form an audit opinion. 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 cast doubt on all the records affected by that control.

The adequacy and appropriateness of controls depends on the quality of the risk analysis 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. Standards, such as the BS 7799 security management standard, set out minimum standards for the security of information systems. If management can show that their control framework has been independently assessed against such public standards, then this will help to demonstrate that the controls in place are appropriate and that they are functioning. Information security standards are therefore a useful tool for helping ensure that information security and records management are good enough to provide reliable audit evidence within one organisation. They are also an especially important means of demonstrating continuity of control when information crosses organisational boundaries.

In addition to its effect on the work they undertake to form their audit opinions, 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 their skills in order to undertake effective audits. And they have an important role to play in promoting management's client awareness of best practice in building and maintaining secure and effective systems, including information system standards.

This is a fast moving area and work is in hand in several professional bodies to address developments; for example, the Auditing Practices Board is preparing a bulletin *E-business: Identifying Financial Statement Risks*. Readers may wish to visit the Public Audit Forum's website www.public-audit-forum and those of the organisations given at Annex A, to check for up to date information.

We are pleased to endorse this paper, prepared by a consultative forum that draws on the experience and expertise of public auditors, the bodies that they audit, the auditing profession and the wider community. We welcome views on the paper, which may either be sent to any of the addresses given below, or by email to james.bromiley@nao.gsi.gov.uk

The image shows four handwritten signatures in black ink, arranged horizontally from left to right. The first signature is 'John Bourn', the second is 'Andrew Foster', the third is 'Robert Black', and the fourth is 'John Dowdall'. The handwriting is cursive and somewhat stylized.

Sir John Bourn Comptroller & Auditor General and Auditor General for Wales, National Audit Office, 157-197 Buckingham Palace Road, London SW1W 9SP

Sir Andrew Foster Controller of Audit, The Audit Commission for Local Authorities and the National Health Service in England and Wales, 1 Vincent Square, London SW1P 2PN

Robert Black Auditor General for Scotland, 110 George Street, Edinburgh EH2 4LH

John Dowdall Northern Ireland Comptroller and Auditor General, Northern Ireland Audit Office, 106 University Street, Belfast BT7 1UE

Introduction

1. Government has 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, email and Internet forms. In the *Modernising Government White Paper*, the Government stated among five key commitments that:

“we will use new technology to meet the needs of citizens and business, and not trail behind technological developments.”

2. The Government's primary objective is the improvement of the quality of public service, while containing costs, by making full use of the benefits of electronic service delivery. The Government's commitment on “information age government” will result in many services becoming available in electronic form, with the intention that:
 - ◆ by 2005 all public services that are capable of electronic delivery will be available in this form;
 - ◆ public services will be available 24 hours a day, seven days a week where there is a demand;
 - ◆ people will be able to notify different parts of government of changes in circumstances in one electronic transaction.
3. The practical effect of electronic service delivery on people's lives can be seen from some of the developments currently under way, as shown in box 1.

Box 1: The effects of developments in electronic service delivery on daily life

The public being able to report crimes on-line: this will save the public time and inconvenience in travelling to, and waiting in, police stations. It will also save the police time in recording and filing reports, as much of this will be done by the public.

Farmers being able to apply for Common Agricultural Policy grants on-line: this will allow applications to be made, and processed, more quickly, so improving farmers' cash flows.

On-line VAT registration: this makes one of the tasks involved in setting up a new business more convenient.

Local authorities improving local land charges services by linking land and property information with an intranet: this reduces the delay people face when buying a new home by making searches faster. Also, as local authority staff can deal with a greater volume of searches, the service becomes less expensive.

4. The Government recognises that the structure of existing public sector information systems reflects 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. Delivering the *Modernising Government* vision will require systems that are geared to the convenience of the user. The Government plans to make public services easier to use by supplementing existing communication channels with call centres, the Internet, digital television and public access points in unconventional surroundings, such as information kiosks located in libraries, post offices, banks and supermarkets. The Office of the e-Envoy *e-strategy for the public sector*¹ and the supporting Information Age Government Champions papers² are intended to assist the realisation of these plans.

5. It is important to realise that the strategy and mechanisms for the delivery of electronic services to the public are at a fairly early stage and are evolving rapidly. The management of public sector bodies and their auditors may therefore find it useful to keep abreast of developments by monitoring the Internet sites listed at Appendix A.

1 <http://www.e-envoy.gov.uk/>

2 <http://www.e-envoy.gov.uk/> and <http://www.govtalk.gov.uk/>

The Public Audit Forum's contribution to the Modernising Government Agenda

6. The Public Audit Forum has made it clear in its paper *Implications for Audit of the Modernising Government Agenda* that auditors should support well-managed innovation. The Forum also commented on how auditors should be ready to embrace change (see box 2).

Box 2: Public Audit Forum comments on auditors embracing change

Auditors must support and encourage worthwhile change. Auditors at both national and local level have demonstrated their willingness and capacity to respond to the changing public service environment. They should now ensure that they understand the objectives and practical implications of the Modernising Government programme and respond constructively and positively to such initiatives in ways that are consistent with their professional standards and statutory duties.

Paragraph 14 of *Implications for Audit of the Modernising Government Agenda*, Public Audit Forum April 1999, available at <http://www.public-audit-forum.gov.uk>.

7. This paper builds on the Forum's earlier paper by explaining the audit implications of the integrated electronic service delivery envisaged in the 1999 *Modernising Government White Paper*³. It sets out auditors' expectations of the bodies they audit, and ways in which auditors can help their management meet them, by exploring:
 - ◆ how electronic service delivery affects audit;
 - ◆ how information security standards are relevant to addressing the effect of electronic service delivery on audit evidence requirements;
 - ◆ what auditors need to do in response to the development of electronic service delivery.

In the process, this paper builds on several themes raised in the Forum's *Implications for Audit of the Modernising Government Agenda* paper: the readiness of auditors as well as managers to embrace change; the need to maintain financial discipline, and the importance of co-operative working between auditors. It does not seek to provide advice on obtaining value for money from the exploitation of information and communication systems, but it does contain material that is relevant to value for money examinations.

³ Modernising Government, presented to Parliament March 1999, Cm 4310

How electronic service delivery affects audit

The effect of electronic service delivery on audit objectives

8. Auditors have been auditing computerised information 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 benefit claim and 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 effects of electronic service delivery are outlined in the case study in box 3.

Box 3: 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 reliability 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.

10. Where the audit remit extends to the examination of the regularity, or legality, of transactions, the auditor needs to consider whether electronic transactions conform to appropriate authority (comply with legislation and regulations). This is particularly the case where appropriate authority requires a physical signature or mark. The Electronic Communications Act 2000⁴ establishes a legal basis for electronic signatures so this particular concern should recede once there are

⁴ Available electronically from <http://www.hms0.gov.uk>

suitable legal precedents. Regardless of the legality of the use of electronic signatures the evidential 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 add to the weight of evidence.

New risks and controls

11. The new risks introduced by electronic service delivery need to be effectively managed in order to ensure the proper functioning of the bodies operating electronic service delivery systems, the legitimacy of their transactions and the reliability of their records. Some examples of the aspects of risk that need to be managed and associated controls are set out in Appendix B under the headings:
 - ◆ threats to accountability from anonymous processing;
 - ◆ vulnerability to amendment;
 - ◆ ease of duplication;
 - ◆ invisible processing;
 - ◆ remote access;
 - ◆ the existence of an audit trail;
 - ◆ reliance on third party service providers.
12. Auditors may expect management to assess risks in order to match the level of control to the threats faced by the system and the impact that would be caused by control failure. Excessive controls may render systems ineffective by deterring users or by making transactions too expensive. The progressive increase in the rigour of controls to be applied to classes of transaction presenting increasing risk is illustrated in Appendix C. Further information on controls and other security requirements that are appropriate to different types of electronic service delivery is at Appendix D.

Effects on audit evidence: authenticity and records management problems

13. Public sector bodies must keep adequate records in order to provide a basis on which to report to Parliament, 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 bodies must, in the first instance, be able to demonstrate that they are “authentic”.
14. “Authenticity” means that the evidence tendered is exactly what it purports to be. The need for authentic records is not new. What is new is the transition from paper records, authenticated by such as hand-written signatures, to electronic records where manual authentication is not applicable. Unlike paper records, electronic records are easy to create or alter without trace. The use of networks makes electronic records vulnerable to alteration while in transit, or by someone working from a remote location. This ease of alteration adds to the need to ensure authenticity.
15. Paper records may be subjected to a forensic examination of such distinguishing features as handwriting, ink, paper, embossing, etc., if there is doubt about their authenticity. But different authentication techniques are required for electronic records because those applicable to paper documents cannot be applied to electronic documents stored in electronic, magnetic or optical devices. It is not meaningful to scrutinise a printed or screen image of a signature on an electronic record, as the image of a signature can be readily copied and manipulated.
16. Closely linked to the question of authenticity is that of the availability of electronic records as evidence. The traditional management disciplines that apply to paper records are not always applied to electronic records, such as e-mail, with the same rigour, if at all. Lax record-keeping can exacerbate the problem of authenticity and result in:
 - ◆ **confusion** between different versions of an electronic record, as many users may take copies and amend them leaving a multiplicity of versions none of which is definitive;
 - ◆ **loss or destruction** of records that need to be retained, resulting from poor records management or users being unaware of retention requirements;
 - ◆ **loss of context** about who did what and when, stemming from the way that electronic documents are stored or the inability to navigate from one document to other related documents;
 - ◆ **inaccessibility** due to technical obsolescence or loss of associated encryption keys.

Effects on audit evidence: the need for information security

17. The broad solution to the problems of evidence posed by electronic service delivery is for organisations to ensure that records that may be needed for audit are identified and carefully managed. An information security policy is an essential starting point for achieving this. 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 records 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.
18. 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 authenticity of business records by reference to an acceptable and demonstrable standard of information security.

Cross-organisational considerations: the need for continuity of control

19. 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.

How information security standards are relevant to audit evidence

Information security standards help establish reliability of records

20. Information security standards can provide consistent frameworks for effective information security. They can provide the basis for the information security policies of individual organisations so reducing the amount of groundwork needed to establish such policies. If followed, they help ensure that electronic records can be relied on as evidence. Such standards are needed to govern the secure interchange of electronic documents between government and the public, as well as helping auditors rely on records.

Information security standards help auditors of different organisations to make use of each others' work

21. Where business activities span organisational boundaries, a single transaction may pass through many systems each with different management, controls and auditors. In such circumstances, a shared framework of control across organisational boundaries is a useful starting point for demonstrating continuity of control as the transaction passes between organisations and hence in establishing the reliability of the evidence generated.

Information security standard BS 7799

22. Where the delivery of services involves co-operation between central and local government and between the public and private sectors, it is preferable for all participants in the business process to share recognition of the same guidance. With this in mind, the Cabinet Office have recommended that public sector organisations work towards compliance with the British Standard on Information Security Management⁵ (BS 7799) since this standard is equally applicable to public sector bodies and their private sector partners.
23. BS 7799 includes a specification against which compliance with the code of practice may be assessed. It also has a certification scheme linked to it that bodies can use to obtain independent confirmation that their information security management system complies with the standard. To provide explanation and help ensure consistency of application, the British Standards Institute has published other guides, including the *Guide to BS 7799 Risk Assessment and Risk Management* (PD3002) and the *Guide to BS 7799 Auditing* (PD3004). BS 7799 has received widespread support and is being promoted for adoption as an international standard. In Government, the Cabinet Office⁶ Security Division is actively promoting its values among departments. The Standard and its supporting guidance is a strong candidate to form the basis of inter-organisational information systems auditing.

⁵ The British Standards Institute has an Internet site at: <http://www.bsi-global.com/index.html>

⁶ The main Cabinet Office Internet site is at: <http://www.cabinet-office.gov.uk/>

24. Other British Standards Institute documents that provide useful guidance on effective information technology service management include:

- ◆ **PD5000 (incorporating the earlier PD0008)** is an authoritative set of guidance for managing electronic documents and e-commerce transactions as legally admissible evidence.

- ◆ **PD0005**, *A Code of Practice for IT Service Management* provides guidance on the implementation of processes covering service design and management, software release, the management of incidents and problems, control of suppliers, change management and configuration management. An auditing specification to accompany the code of practice is being developed.

What auditors need to do in response to electronic service delivery

Contributing to audited bodies' understanding

25. The auditor has an important role to play in drawing clients' attention to the importance of information security standards such as BS 7799 and helping management to identify the control requirements associated with the effective management of electronic records (as outlined in Appendices B and C). 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

26. The implications of electronic service delivery mean that management and auditors need training and development to ensure that they understand the risks associated with electronic service delivery and the controls appropriate to manage those risks. Auditors dealing with electronic service delivery systems will, in particular, need to be familiar with relevant information security standards such as the BS 7799 information system security management standard. 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 specialist assistance and interpret the findings of specialists in the context of business risk.

Willingness to embrace change

27. The Public Audit Forum recognises that new ways of working will be necessary to achieve the development of robust and auditable electronic service delivery systems. It is keen for public sector auditors to be supportive of public bodies' efforts to exploit new service delivery channels effectively.
28. 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 integrity and availability 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.

Contributing to the development of information security standards and policies

29. Auditors can add value to the Modernising Government programme by participating in the development of information security standards and guidance. Such involvement will help to ensure the development of best practice guidance that meets the needs of both management and auditors.

Working together

30. As the development of information security standards has been pursued by a variety of organisations and, as yet, no particular standard has been universally adopted, there are variations in information management that hinder consistent audit coverage of transactions that cross organisational boundaries. Therefore, one particular area needing the contribution of auditors at the institutional level is the agreement of a common approach to the audit of 'joined-up' electronic service delivery so that auditors can take account of each others' work.
31. The need for co-operation is heightened by the increased 'joined-up' working envisaged under the customer focus of the Modernising Government programme. An example of such 'joined-up' working, is the development of electronic 'hubs'⁷ for local authority procurement. As purchases are made against agreed frameworks, senior staff no longer need to authorise most orders. Both the internal auditors and the appointed auditors of all the local authorities using the hub will be expected to agree an approach to testing the framework controls at the hub so that they can maximise efficiency and eliminate the unnecessary duplication of audit effort.

⁷ Internet-based forums holding the catalogues of suppliers and the buying requirements of many purchasers

Conclusion

- 32.** Electronic service delivery does not introduce new audit objectives, but it does introduce new 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.
- 33.** 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 standard with which management should be able to demonstrate compliance is set out in the British Standard on Information Security Management (BS 7799).
- 34.** In the context of electronic service delivery, auditors may contribute to the success of the Modernising Government programme by:
- ◆ contributing to audited bodies' understanding of the need for 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 they can work together more easily and take account of each others' work.

Appendices

Sources for Guidance

- A Useful Internet Links for Audit and Electronic Service Delivery Matters
- B Electronic service delivery risk areas and the controls auditors expect clients to employ
- C Transaction types
- D Examples of security requirements
and mechanisms of different types of electronic service delivery

A Useful Internet Links for Audit and Electronic Service Delivery Matters

Audit Commission	http://www.audit-commission.gov.uk/
Audit Scotland	http://www.audit-scotland.gov.uk/
British Standards Institute	http://www.bsi-global.com/index.html
Cabinet Office	http://www.cabinet-office.gov.uk/
Central Computer and Telecommunications Agency	http://www.ccta.gov.uk/
Chartered Institute of Public Finance and Accountancy	http://www.cipfa.org.uk/
Department of Trade and Industry	http://www.dti.gov.uk/
Cabinet Office guidance on e-government	http://www.govtalk.gov.uk/
ICAEW	http://www.icaew.co.uk/
Information Audit and Control Association	http://www.isaca.org
Institute of Internal Auditors	http://www.iaa.org.uk/home.html
INTOSAI	http://www.intosai.org/
Kablenet Government Computing News service:	http://www.kablenet.com/
National Audit Office:	http://www.nao.gov.uk/
Northern Ireland Audit Office	http://www.niauditoffice.gov.uk/
Office of Government commerce	http://www.ogc.gov.uk/
Office of the e-envoy	http://www.e-envoy.gov.uk/
Open Government index to public sector Internet resources:	http://www.open.gov.uk
Performance and Innovation Unit	http://www.cabinet-office.gov.uk/innovation/
Public Audit Forum	http://www.public-audit-forum.gov.uk/
UK Online citizen portal	http://www.ukonline.gov.uk/

B Electronic service delivery risk areas and the controls auditors expect clients to employ

This appendix lists the main areas of risk that are presented by electronic service delivery. Within each section, it outlines the types of controls that auditors expect to see to manage these risks.

Threats to accountability from anonymous processing

Computer users are, by default, anonymous. Individual users cannot be held accountable for their actions in systems that cannot identify and record their activities. As a result they are more likely to carry out unauthorised activities in such systems. Policies and controls that enforce individual identification and logging reduce this risk and electronic signatures appended to transactions can also be used to strengthen accountability.

Accountability reduces the likelihood of abuse of information systems and is particularly important in the context of the Internet as the potential for access is so great.

Vulnerability to amendment

Computer software and data is stored and transmitted in an intangible form and can be amended without trace. Effective controls are required to ensure that amendments are recorded and to prevent unauthorised amendments. Weak controls may result in the user being unable to rely on the authenticity of electronic records or computer-generated audit trails.

Software and data should be protected from unauthorised amendment by the use of physical and logical access controls. Physical access controls (locks, keys and guards) should be used to protect key sites but the increasing use of communications networks blurs the boundaries of sites to be physically protected. The use of open networks to deliver services makes strong logical controls very important since uncontrolled remote access lays system data and software open to abuse whatever physical controls protect the site where the information is held.

Logical access controls use hardware and software to restrict the actions that users can perform, detect unauthorised actions, trigger alarms and record system activity (who did what and when). Operating system controls usually enforce access control within a site but when data passes over open networks, continuity of access control cannot be assumed. The Internet should be considered a hostile environment for data, so important information should be protected using encryption and digital signatures as a precaution against unauthorised access or amendment.

Ease of duplication

Unlike paper copies, copied computer files can be made indistinguishable from the original. Where data has financial value, such as in electronic funds transfer systems, it is very important to apply controls to prevent and detect duplicate processing. Suitable controls include the assignment of sequence numbers to transactions and the routine checking of control totals.

Business managers should be aware of possible problems where negotiable instruments, such as bills of lading or deeds, are stored and exchanged via computers. In such circumstances, it may be appropriate to use a trusted third party to act as registrar and maintain records of the registered owners of negotiable instruments. On completion of a contract, the purchaser waits for confirmation that the seller had title to the instrument before authorising payment. This arrangement prevents electronic documents being traded twice.

Invisible processing

Transaction processing that occurs inside a computer network is effectively invisible. System input and output can be inspected but the exact internal processing that has been carried out may not be immediately apparent. This weakness can be exploited to facilitate the unauthorised insertion, amendment or deletion of data in the transaction stream. In an open communications system, the owners of the receiving and sending transaction processing system can use formal testing and change control procedures to gain assurance of the integrity of their own applications but cannot gain the same level of assurance about external systems through which transactions may pass.

Depending on the value of the transactions, steps taken to protect the integrity of the transaction stream might include the use of encryption to create a virtual private channel across the untrusted network, or the use of digital signatures and sequencing to protect individual transactions.

Remote access

Any system connected to an open network may be the target of attack by outsiders. System managers can make use of “firewalls” and access control to detect and record attempted unauthorised access and to help prevent unauthorised activities.

The existence of an audit trail

Both auditors and management need to be able to trace transactions back to their origins and forward through their processing cycle.

Where transactions take place through third-party networks, the integrity of the audit trail will depend on the capture of incoming and outgoing transactions data in addition to the implementation of controls to demonstrate that transactions have not been manipulated in transit.

A system generating an audit trail will typically need to be able to identify and log time, identities, actions and results. This implies having robust identification and authentication schemes, time synchronisation systems, data integrity protection and a logging system at the transaction level.

Reliance on third party IT service providers

Traditional information systems have been provided in one of three ways:

in-house: systems are owned by the organisation, and operated by their IT department;

facilities management: systems are owned by the organisation, but operations and maintenance activities are contracted out to a third party service supplier;

outsourced: both systems and IT staff are provided by a third party.

Where an external IT service provider is used, management should consider the security requirements, incorporate security requirements in the service level agreement and build in mechanisms that check whether the mandated security level is being met.

In an open network environment, this model breaks down because the application system owner will not know which other systems will be involved and a contractual relationship with owners of the other systems is unlikely. As a result, the application owner should assume no protection and then build an appropriate level of protection into the transaction processes that involve open network access. This might include encryption of application data and the use of digital signatures to protect the integrity of transactions.

C Transaction types

The Office of the e-envoy Call Centre Guidelines⁸ define classes of transaction that might be subject to different levels of authentication:

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: the 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., National 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

⁸ Published December 1999. Available from the Information Age Government Champions web site at: <http://www.e-envoy.gov.uk/>

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)

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:

Mother's maiden name

Random digits of a PIN number

Written proof of change of circumstances may be required by statute or may be a sensible 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

Benefit 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.

D 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 email. For example, local authorities publicise the opening times of libraries and other services through their 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, NHS general practitioners hold administrative information about their patients, such as names, addresses and appointment times, as well as medical information, such as treatment histories. The Government is committed to making 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 parallel 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 would be extremely embarrassing, so it is 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, unauthorised 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, new vulnerabilities arise:

- ◆ 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 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.

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 is 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 innately 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;
- ◆ lodgement of 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.