- ***Record Keeping Guidance***

The purpose of this note is to set out guidance that will encourage appropriate standards for record keeping by businesses offering services or products via the Internet. The guidance is equally applicable to transaction-based taxes (GST/VAT) and direct taxes that make use of aggregated transaction information. It is aimed specifically at record keeping requirements for e-commerce although its principles apply equally to all computerised record keeping.

Centre for Tax Policy and Administration

Tax guidance series

Tax Administration Guidance – Record Keeping

Record Keeping Guidance

Caveat
Each revenue authority faces a varied environment within which they administer their taxation system. Jurisdictions differ in respect of their policy and legislative environment and their administrative practices and culture. As such, a standard approach to tax administration may be neither practical nor desirable in a particular instance.

The documents forming the OECD Tax guidance series need to be interpreted with this in mind. Care should always be taken when considering a Country's practices to fully appreciate the complex factors that have shaped a particular approach.

Introduction

1. To facilitate the growth of 'electronic commerce' the OECD Forum on Tax Administration has been developing guidance papers[1] to assist revenue authorities and businesses in creating more consistent practices across borders. Electronic Commerce (e-commerce) represents a broad range of technologies and practices that automate business transactions through largely paperless mechanisms. It largely encompasses domestic and cross-border transactions in and between both private and public sectors.

2. The purpose of this paper is to set out guidance that will encourage appropriate standards for record keeping by businesses offering services or products via the Internet. It was produced by Government and Business representatives from the Forum on Tax Administration Electronic Commerce Sub-Group and the Compliance Information and Documentation Technology Advisory Group. The teams agreed to adopt an approach based on an identified mutual need for Government and Business auditors to gain assurance in the operation of e-commerce computer systems, and for these requirements to be based whenever possible on the use of available commercial records.

3. The guidance is equally applicable to transaction-based taxes (GST/VAT) and direct taxes that make use of aggregated transaction information. It is aimed specifically at record keeping requirements for e-commerce although its principles apply equally to all computerised record keeping.

Taxation Framework Conditions

4. At the 1998 Ottawa Ministerial Conference on Electronic Commerce the OECD was tasked by Governments with progressing the Taxation Framework Conditions to govern the taxation of electronic commerce that it had drawn up with input from over 40 countries and international organisations.[2] This guidance note is part of ongoing work to transform the agreed taxation conditions into practical administrative measures.

5. The opening paragraphs of the Taxation Framework Conditions note:

> *"Electronic commerce has the potential to be one of the great economic developments of the 21st Century. The information and communication technologies which underlie this new way of doing business open up opportunities to improve global quality of life and economic well being. Electronic commerce has the potential to spur growth and employment in industrialised, emerging and developing countries.*

---

1 See documents at http://www.oecd.org/EN/documents/0,,EN-documents-101-nodirectorate-no-27-no-22,00.html

2 On 8 October 1998 at Ottawa, the OECD issued a set of Framework Conditions to govern the taxation of electronic commerce. These conditions were drawn up in co-operation with several countries outside the OECD (Argentina, Brazil, Chile, China, Chinese Taipei, Hong Kong (China), Israel, Malaysia, Russian Federation, Singapore, South Africa), the Centre for Inter-American Tax Administrators (CIAT), the Commonwealth Association of Tax Administrators (CATA), the European Union, the World Customs Organisation, and the business community. They were welcomed by Ministers at the October 1998 OECD Ministerial Meeting.

Revenue authorities have a role to play in realising this potential. Governments must provide a fiscal climate within which electronic commerce can flourish, weighed against the obligation to operate a fair and predictable taxation system that provides the revenue required to meet the legitimate expectations of citizens for publicly provided services." [3]

6. OECD governments and others[4] have endorsed neutrality, efficiency, certainty, simplicity, effectiveness, fairness and flexibility as the taxation principles that should guide Governments in relation to the taxation of electronic commerce.

7. The Framework conditions explicitly address the approach revenue authorities should take to record keeping requirements:

Tax administration, identification and information needs

(ii) Revenue authorities should maintain their ability to secure access to reliable and verifiable information in order to identify taxpayers and obtain the information necessary to administer their tax system."[5]

8. The Taxation Framework Conditions also recognise ongoing developments in areas such as Internet governance where Revenue authorities, individually and through international fora, such as the OECD, may need to play a role if they are to succeed in implementing the taxation principles.

9. The Taxation Framework Conditions were developed further in a discussion paper on the taxation issues that was also released at Ottawa. Implementation Options 15 of that paper noted:

"Revenue authorities may consider expressing their views on information requirements to appropriate bodies developing standards or protocols for electronic commerce.

a) Revenue authorities have, wherever possible, used or adapted commercial developments for taxation purposes so as to avoid the creation of a separate and burdensome tax regime. However, modifying systems after they have been finalised is costly and should be avoided where possible. Revenue authorities could co-operate with business initiatives to create protocols for trade that facilitate electronic offers, delivery, payment and documentation and express their views in a timely manner to the bodies developing such protocols or standards so that they can be developed, taking into account the views of Revenue authorities.

b) Further, private sector groups aiming at the introduction of new technical standards or protocols for electronic commerce could co-operate by contacting Revenue authorities, e.g. through the OECD, at an early stage to enhance a constructive dialogue designed to find mutually acceptable solutions".

---

3 From: *Electronic Commerce: Taxation Framework Conditions*, Introductory paragraphs 1 and 2. http://www.oecd.org/daf/fa/E_COM/framewke.pdf

4 In addition to the 40 countries and international organisations that were involved in the preparation of the Taxation Framework Conditions, they were also adopted by APEC (Asia-Pacific Economic Co-operation) countries at a joint OECD-APEC meeting in November 1998 and were endorsed by APEC Finance Ministers in May 1999.

5 Available at: http://www.oecd.org/daf/fa/E_COM/framewke.pdf

10. Since 1999 the OECD has been working with revenue authority delegates and businesses representatives through several Technical Advisory Groups (TAGs) set up to assist the OECD Working Parties in progressing the Taxation Framework Conditions. The initial results of this work were reported in the OECD publication 'Taxation and Electronic Commerce: Implementing the Ottawa Taxation Framework Conditions' (available as an e-book at: http://www1.oecd.org/publications/e-book/2301011E.PDF).

11. More detail on the work of the OECD Working Parties and the Technical Advisory Groups can be found in the following reports:

- Professional Data Assessment TAG (http://www.oecd.org/pdf/M000015000/M00015523.pdf),
- Consumption Tax TAG (http://www.oecd.org/pdf/M000015000/M00015515.pdf),
- Working Party No 9 [Consumption Taxes] (http://www.oecd.org/pdf/m00022000/m00022378.pdf), and
- Forum on Strategic Management (http://www.oecd.org/pdf/M000015000/M00015520.pdf).

12. This paper builds on the above OECD reports and also the work of the Council of the European Union, as detailed in Directive 2001/115/EC[6].

Costs of Compliance and Administration

13. Governments, through their tax administrations, generally seek to minimise the long term operating and compliance costs of their tax systems while at the same time keeping the tax compliance costs of taxpayers as low as possible. This means striking a balance between the costs borne by business in complying with tax regulations and the costs borne by the revenue authority in running the system. These two types of tax system operating costs are linked inextricably but not necessarily inversely, *i.e.* as one rises the other falls.

14. Enforcing compliance via frequent checks, substantive audits and prosecutions is an expensive way of ensuring adequate compliance levels, so most revenue authorities attempt to maximise 'voluntary compliance' where the taxpayer is encouraged to co-operate and actively comply with the tax regulations. This reduces the cost of administering the tax system but is only practicable when the requirements of the tax system are well understood, relatively easy to comply with, and generally accepted by businesses.

15. As is noted in the Tax Guidance Series General Administrative Principles paper GAP001 'Principles of Good Tax Administration':

> *"Voluntary compliance is promoted not only by an awareness of rights and expectations of a fair and efficient treatment but also by clear, simple and "user-friendly" administrative systems and procedures. Voluntary compliance is enhanced when it is easier for taxpayers to do so.*
>
> *When compliance is not achieved on a voluntary basis, revenue authorities must identify and address the risks associated with non-compliance by developing strategies targeted at those risks[7]. Voluntary compliance is maximised when revenue authorities are aware of major developments and trends in the business and legislative environment, and are responsive to their implications on tax administration and compliance. Good revenue authorities identify and assess compliance risks and develop strategies targeted at addressing those risks. These strategies*

6 On simplifying, modernising and harmonising the conditions laid down for invoicing in respect of Value Added Taxes covered by the Directive 77/388/EC (the Sixth Directive). It can be found at: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32001L0115&model=guichett

7 See GAP003 Risk Management and GAP004 Compliance Measurement

include education, service, marketing, profiling risk, auditing, general anti-avoidance efforts, prosecution and proposals for legislative change."

16. Voluntary compliance with tax record keeping requirements is best enabled where such requirements integrate with pre-existing business record and accounting systems. Providing such systems are reliable, Revenue authorities' administrative compliance costs are likely to be minimised.

17. With large businesses this approach is often made possible by the robustness of their internal control systems and procedures, and the activities of the auditors acting on the behalf of shareholders. Small to medium sized enterprises (SMEs) can sometimes have relatively significant compliance costs and difficulties in understanding and complying with tax requirements. The ability of these small and medium businesses to create, record and maintain adequate records as an integral part of their normal operations may be somewhat limited, although the ongoing development of accounting software packages aimed at small businesses has ameliorated this issue to some extent

18. While the development of e-commerce and electronic record keeping has changed the nature of business internal control systems, and in some cases weakening audit trails, it has also encouraged the use of audit techniques such as computer assisted audit techniques that can significantly improve audit coverage and productivity. However, the net effect of these two contrasting influences on compliance and administrative costs will vary by business and tax administration.

Issues

The changing business environment

19. Internet based e-Commerce is changing the way in which business is being conducted, particularly for SMEs who now have access to international markets on an unprecedented scale and can operate in ways that due to cost and complexity were previously the preserve of large businesses. This means that businesses will encounter a number of different regulatory requirements in each jurisdiction, and their internal controls will assume a greater importance if transactions are to be processed and recorded correctly by each participant.

20. E-commerce has also allowed the creation of new business models used by small and large businesses alike, such as electronic procurement, electronic marketplaces, the development of systems integration between businesses that were previously discrete, and the introduction of the electronic shop front (web shop) that creates in turn a need for increased integration between front end, back office, and security systems. It has also encouraged multi-national enterprises (MNEs) to centralise in one place those computerised accounting systems that service their trading locations worldwide. This makes it increasingly common for records relating to transactions made within a particular jurisdiction to be held outside that jurisdiction.

21. The ability for business to trade completely electronically in conjunction with new business methods and models means that auditing fundamentals such as the availability and nature of audit evidence are also subject to change. This propensity to change through technological advancement also means that record-keeping requirements should be kept under review by tax authorities and also be flexible enough to meet the opportunities presented by these changing business practices.

Authentic and reliable records

22. Legitimate businesses endeavour to create authentic and reliable accounting records in support of their functions and activities, and protect the integrity of these records for as long as required. There is a general consensus in this area between legitimate businesses and revenue authorities, albeit to the extent that

businesses will only want to maintain such records for as long as it is considered essential for their own activities or as otherwise prescribed by law. This implies that a business have at least three fundamental objectives for keeping records:

- To enable a business to control its activities, safeguard its assets, and monitor profitability thus informing its strategic direction. This is integral with the creation and maintenance of an audit trail of transactions on a historic and current basis in line with good business practice.
- To satisfy external auditors, company directors, shareholders, creditors, investors and other interested stakeholders that the records reflect a true and fair value of the business.
- To enable a business to meet various statutory requirements, including requirements for both Revenue authorities and external auditors.

23. These objectives apply to all types of commercial activity where a business is required by law to keep, maintain and produce its records to a Revenue authority for examination in order to verify a tax declaration, or to fulfil other statutory obligations under company law, such as to publish its annual accounts. In this connexion, ISO 15489 published in October 2001[8] observes that

> *"All organizations need to identify the regulatory environment that affects their activities and requirements to document their activities. The policies and procedures of organizations should reflect the application of the regulatory environment to their business procedures. An organization should provide adequate evidence of its compliance with the regulatory environment in the records of its activities".*

24. Businesses need reliable information in order to manage their operations in an effective and cost efficient manner. These management information needs within a business are generally fairly consistent across the organisation, even when it spans multiple jurisdictions, so as to minimise information costs while maximising reporting comparability. If record keeping requirements are made more consistent across jurisdictions then the overall systems compliance cost is likely to be reduced.

25. Revenue authority record keeping requirements should be in accordance with the business objective to control their own activities, and should seek to impose minimal burdens by allowing whenever possible the use of commercial records to meet statutory tax requirements. For e-commerce these requirements should also be in support of the OECD Taxation Framework conditions by facilitating the creation and maintenance of reliable and verifiable records that can be trusted to contain a full and accurate representation of electronic commerce transactions. Revenue authorities also need to examine records in order to collect the right amount of tax at the right time within their jurisdiction. Other stakeholders requiring reliable information include shareholders, banks, creditors, customers and other regulatory authorities.

26. On the basis of the financial documents and statements, potential and existing business shareholders decide whether to invest equity in business; banks decide whether to provide loans or other financial means; and suppliers and customers decide whether to undertake transactions. These other stakeholders may need assurance that the financial documents and statements of the business reflect economic and legal reality. Auditability of the financial statements is a prerequisite for this assurance and the statutory audits performed by private auditors for public and private companies will normally provide needed assurance to stakeholders.

---

[8] ISO/TR 15489-1 Information and Documentation – Records Management – part 1: General

Assurance Challenges

Audit evidence

27. The ultimate objective of the auditor is to gain a satisfactory level of audit assurance from the system under examination in order to form an audit opinion. The manner in which this is achieved varies according to the tax regime involved and the audit methodologies followed by individual tax administrations. However, a universal factor in all methods is the use of accounting records kept and maintained by a business, in accordance with its own accounting polices; general accountancy principles; and for all statutory reasons, some based on company law and the record keeping requirements of their tax authority.

28. An auditor must consider the available audit evidence as part of the assurance process leading to an audit opinion. This evidence can be obtained from a number of sources including accounting records, financial records and other documents and systems; and from the use of techniques such as inspection, observation, analytical reviews, and compliance and substantive testing. E-commerce systems increasingly contain audit trails that are wholly electronic and contain data of increasing volume and complexity. These systems pose challenges to auditors who may have previously relied on paper –based trails with their inherent look, feel and authenticity.

29. Some e-commerce transactions may not generate any paper records. The resultant electronic records may be more easily altered or destroyed than their paper equivalents, leaving no record of such actions. Auditors may therefore need to test system controls in order to validate audit evidence, including confirmation of transaction details with third parties. In the paper-based systems found in conventional commerce, documents from an external source are usually regarded as inherently possessing higher degree of credibility as audit evidence than internal documents even before internal controls are applied during transaction processing. However, in electronic commerce the credibility of any external electronic document used as audit evidence will depend less on its origins and form and more on the nature, source and reliability of both the internal controls during processing and the additional measures applied to ensure its integrity. In the absence of internal controls and additional measures, an auditor may regard any external electronic record produced as audit evidence as being no more than an internal electronic record.

Internal controls

30. Sales and purchases systems, whether manual, computerised "off-line", or Web-based have their origins in traditional accounting and stock control models, and share common objectives such as to deliver goods and services at minimal cost to the business; identify and collect monies owed efficiently; and pay suppliers correctly. Information from systems, including from both internal and external sources, is used to control business processes. In a traditional environment paper documents are often used to distribute control information whereas in an e-commerce environment this information is generally exchanged electronically.

31. The policies and practices designed to provide management with reasonable assurance that their goals have been met are known as internal control procedures. Internal control procedures aim to ensure the orderly and efficient conduct of business including ensuring that business can comply with the various legislative requirements of the jurisdictions it operates in.

32. An early stage in obtaining audit assurance is the examination and testing of internal controls with supporting audit evidence. Internal controls should perform preventative, restorative and corrective functions, *i.e*. to prevent errors or to otherwise detect and reverse an error that has been processed through

to the accounts in order to ensure the integrity of transactions. Internal controls in computerised accounting systems should also be concentrated in the following areas of activity:

- Access controls to ensure that only authorised users can access and process data according to the permissions given.
- Data capture controls to ensure that the right data gets into the system
- Processing controls to ensure that the data remains correct throughout processing
- Standing data controls to ensure that criteria used to process the data are correct
- Security controls that maintain the integrity of the processed data
- Output controls to ensure that system output is in the correct format and that the recipient undertakes any required action.

33. The use of electronic records means that proof of these internal control processes having occurred may be held electronically. These control records will also require some form of mechanism to validate their authenticity and reliability over a period of time. The very nature of an electronic environment changes the way of undertaking tests of internal control procedures, yet regardless of their form internal controls and their associated documentation must be adequate to provide reasonable assurance that assets are safeguarded and that transactions are properly authorised and correctly recorded in the accounting records. An important element for the successful operation of internal controls by an e-commerce business is the sufficiency of transaction information data elements exchanged in electronic form between businesses to allow these controls to be performed at the same level as in a paper based environment.

34. The majority of businesses worldwide are classified as SMEs[9], and issues of internal controls and the reliability and authenticity of supporting documentation are particularly pertinent in these cases. Many internal controls that are routinely applied by large businesses may not be practical or cost-effective for SMEs. SMEs often display a particular weakness of ineffective or non-existent separation of duties that can compromise their overall internal control procedures, and may also make it difficult for an auditor to detect unrecorded amendment and deletion of records. This means that sometimes the only methods available to the auditor to obtain the necessary audit evidence will be through substantive test procedures or by reference to evidence held by third parties, including records located in other jurisdictions. However, in situations where adequate internal controls may not be in place, the auditor may not have sufficient assurance that any external electronic documents are credible, and therefore cannot rely on this documentation to verify the results of substantive tests. This means that both a systems audit approach and use of substantive testing may be compromised unless these documents possess sufficient authenticity and reliability as audit evidence. In these cases sufficient levels of reliability and authenticity are best achieved by the application of appropriate technologies to the electronic record, including the development of software with specific design features that maintain the integrity of accounting records.

Records and technology

35. The multitude of technologies that may be encountered when examining system records over a period of time presents the auditor with a number of difficulties such as multiple hardware and operating systems, data held on obsolete media, data compression etc. Auditors will therefore need additional technological resources in order to access such records and view them in a readable format. Although this is potentially more of a problem when restoring archived records, similar difficulties may be encountered for records in a

[9] It should be noted that the criteria to classify an enterprise as a small or medium sized business might differ from jurisdiction to jurisdiction.

current financial period if the audit trail is spread over a number of systems each containing accounting systems that save records in a proprietary format.

36. A particular difficulty may be encountered when examining Enterprise Resource Planning systems or other systems that use tables in a relational database. These systems do not record or retain individual transactions as such, but rather the components of individual transactions are retained in multiple tables linked by transaction identifiers or by other similar means. To recreate transactions from an earlier period for tax auditors may present business with a number of difficulties particularly if the system has been changed or the software upgraded. Some ERP vendors are aware of these problems and have begun to incorporate programs that allow the production of audit trail information on demand. In the case of other systems, the use of a standard audit file to record transactions at the time of creation offers a credible solution.

Audit file

37. The traditional approach of physically viewing the document with its transaction details and control information is no longer viable for wholly electronic e-commerce systems, leading to increased substantive testing of transaction information, often by use of computer assisted audit. The use of these techniques may also offer increased effectiveness and efficiency to business and auditors alike, and a key enabler in this process is the incorporation of a standard audit file into software packages and ERP systems. This would allow auditors ready access to data thus gaining greater efficiency in audit coverage and productivity, while at the same time reducing compliance costs for business that would otherwise need to devote resources to produce the data in a readable format. The method of creation, whether at the time of every transaction or on demand by an auditor, will be a matter for each tax authority.

38. It should however be recognised that the audit file approach does not preclude the requirement for businesses to keep records in accordance with conditions laid down by revenue authorities. While a standard audit file will in most cases facilitate the full range of substantive tests there will be cases where additional data is required from businesses by auditors. This could for instance apply in particular business sectors where non-invoice data is used. The requirements for such a file are discussed in the OECD Tax Guidance Series document "Transaction Information Guidance" (TAG002). Tax administrations should work together with other organisations towards developing a specification for a standard international audit data file that meets the requirements of all parties operating e-business.

Requirements for record keeping

Principles

39. This section examines some of the basic principles associated with record keeping by businesses for tax purposes. Requirements relating to the keeping of specific records are not identified, as individual revenue authorities may place a different emphasis on the importance of each record type and tailor their regulatory requirements accordingly.

40. The OECD Taxation Framework conditions for e-commerce state that revenue authorities need to maintain their ability to secure access to reliable and verifiable information in order to identify taxpayers and obtain the information necessary to administer their tax systems. Access to reliable and verifiable information held in e-commerce systems is also a key concern for private sector auditors, both internal and external.

41. Businesses in turn should create reliable and verifiable records that allow it to determine its tax liability, including any claim for a refund of tax, and then maintain these records as required by legislation. These records should possess sufficient levels of authenticity, integrity and usability to form part of a

satisfactory audit trail enabling auditors to verify the accuracy or otherwise of the tax return. This remains true for both electronic and paper-based transactions.

42. The records created by e-commerce systems and their content are likely to be broadly similar to other trading models, in line with the similarity of business objectives across general commerce. However, e-commerce can also generate additional records containing information specific to this type of business activity, either during transaction processing (*e.g.* web logs) or as a result of security measures to preserve the authenticity and integrity of the resultant record (*e.g.* digital signatures). An additional factor in an e-commerce environment is the transitory nature of some records that may be considered material for tax purposes and which may therefore necessitate adoption of a different audit approach such as remote and current period audits. These additional records form an important part of the audit trail for e-commerce activity and will be of considerable value to auditors, both Government and private.

43. The underlying principle for record keeping is that all documentation, in whatever format, that forms part of the audit evidence must provide auditors with reasonable assurance that transactions are properly authorised and recorded in the accounting records. This will also enable the business to monitor profitability; safeguard its assets; and inform its strategic direction.

Reliability of records

44. A reliable e-commerce record is one whose contents can be trusted as a full and accurate representation of the transaction. In order to achieve the appropriate level of trust, the record should also display sufficient levels of authenticity, integrity, and usability[10].

45. A feature of e-commerce systems is the creation and retention of records and documents that are wholly electronic, and as a result may be regarded by auditors as being potentially less reliable than their paper equivalents. This perceived loss in reliability can often be overcome by the use of techniques that provide additional levels of assurance. For example, within the European Union, the Invoicing Directive[11] obliges Member States to accept invoices sent by electronic means provided that the authenticity of origin and integrity of the contents are guaranteed by means of:

- An advanced electronic signature[12]. (Member states may however ask for the advanced electronic signature to be based on a qualified certificate and created by a secure-signature-creation device[13]); or
- Electronic data interchange (EDI)[14] when the agreement relating to the exchange provides for the use of procedures guaranteeing the authenticity of the origin and integrity of the data. (but

---

10 ISO 15489 Information and documentation – Records management. Part 1 General.

11 Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view of simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax. This can be found at:

http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32001L0115&model=guichett

12 See article 2 (2) of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

13 See article 2 (6) and (10) of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

14 As defined in article 2 of Commission Recommendation 1994/820/EC of 19 October 1994 relating to the legal aspects of electronic data interchange.

note however that a Member State may also require production of an additional summary paper document).

It should be noted that the Invoicing Directive also allows Member States to accept electronic documents, such as invoices, that are guaranteed by other means approved by the jurisdictions.

46. There is a growing trend for SMEs to use electronic mail (e-mail) to send and receive order and invoice information. In the case of these and other invoice creation systems, sufficient levels of reliability must be obtained by other means. For example, control documents generated in a sales ordering process could be used to support the authenticity of the origin and integrity of the invoice provided the business can demonstrate a high level of integrity in their electronic and other internal control system over time. The use of these types of techniques can enable both private and tax auditors to obtain levels of assurance with respect to the reliability of invoices and, eventually financial statements, to the same degree as in a traditional paper environment.

47. A survey among OECD members has shown that some jurisdictions[15] have already introduced specific requirements to ensure the reliability of electronic documents. A review of these requirements indicates that countries have adopted different approaches. Many countries have passed legislation that recognises the equivalence of electronic documents as evidence when they make appropriate use of electronic signatures based upon electronic certificates. However in many other countries there is a lack of availability of electronic certificates that meet a sufficient level of integrity.

Security

48. The application of security services in conjunction with appropriate technologies to both the system used for e-commerce and the records held therein is a key requirement in achieving reliable records kept and maintained to a satisfactory standard (but note that in cases of fraud involving the deliberate omission or destruction of records kept outside of normal accounting systems it does not matter whether the records are in an electronic format or not).

49. Annex A describes a range of services that can be applied to electronic records, and Annex B examines the technologies and mechanisms involved.

Storage considerations

50. If an auditor requires the examination of documentary evidence of internal controls or source documents for transactions outside of the current period, it may be necessary to retrieve these documents from an archive. The auditor must have the assurance that an archived record is capable of being verified as an original, meaning that the record being produced is identical to the one on which the original e-commerce transaction was based. This is particularly important for electronic records that may be held in an accounting system in a simplified format that precludes their retrieval with full original detail, *e.g.* consolidated data fields.

51. The maintenance of electronic records for use as audit evidence therefore becomes of significant importance to both private and public sector auditors. Short-term maintenance focuses on the availability and use of the system audit trail to gain assurance on processing during the current accounting period; long-term maintenance focuses on archive procedures including retaining of audit trails and maintaining integrity of data thus ensuring the continued reliability and verifiability of the electronic record.

---

[15] For example, Switzerland and members of the EU.

52. It is important to ensure that the digital record is readable and usable even after the passage of an extended period of time. Storage over a long period raises the possibility of problems arising such as data loss; data unintelligibility; or even unavailability of suitable equipment or software to display a now obsolete data format.

53. Annex C explores a range of issues and technology-based methods for storing data over a long period of time.

Data protection and privacy

54. Businesses should observe the data protection and privacy laws applicable in the jurisdiction in which they are located. Data stored in other jurisdictions but produced in the home jurisdiction should be maintained to the same standards in this regard.

Legislative frameworks

55. In many jurisdictions the legal basis for record keeping and maintenance is based on considerations more applicable to paper records. In order for these Revenue authorities to meet the OECD Taxation Framework conditions, they will be required to re-examine their legislation in this area. This process is already underway in some countries for other reasons, such as the placing of e-commerce on a statutory footing, and the implementation of the EU Invoicing Directive for Member States by 1 January 2004. This section sets out broad guidance for legislative requirements that will assist tax authorities in meeting these conditions.

56. Revenue authorities should seek to ensure that legislation, such as data privacy provisions, do not compromise or prejudice the imposition, collection or recovery of taxation and other Government imposts by creating avoidance or evasion opportunities.

57. The establishment of legislative frameworks while being of benefit primarily to tax authorities and their auditors will also benefit e-commerce businesses and their auditors by setting standards for record keeping that will meet their requirements.

Access to systems and data

58. The wholly electronic environment of e-commerce and the transitory nature of on-line transactions mean that Revenue authorities will need enhanced access to computer systems and to obtain assistance from anyone concerned with their operation if they are to successfully administer their tax systems to the same level as before. Access should encompass the systems used for e-commerce; supporting systems documentation; the data associated with each transaction or group of transactions; and any file interrogation facilities. The distributed nature of some e-commerce systems, including networks that cross tax jurisdictions, means that access to data remotely should also be a facility available to revenue authorities.

Maintenance of records

59. All records, including source documents that originate in paper format, may be retained electronically provided security measures to prevent subsequent alteration are applied. Original paper documents and records should be copied accurately to provide an authentic image of the original, and this image must be displayable on demand in a readable format. Data received electronically should normally be kept electronically, although a transfer to paper format could be allowed provided controls to guarantee completeness and accuracy of the data are in place.

1. Additional records generated by computer systems such as digital signatures and the keys needed to verify these including decryption keys should also be kept and maintained to the same standard as other archived data records.

2. The authenticity and integrity of the content of source documents and electronic records must be preserved throughout storage through the application of suitable technologies. Also the readability and usability of data should be preserved, in particular, when data is transferred from one set of storage media to another.

Period of retention.

3. In common with other businesses, e-commerce businesses are required to keep records and accounts of all goods and services that they receive or supply in the course their business.

4. Maintenance of records for a particular length of time is likely to be a statutory requirement determined by the legislation applicable in a particular jurisdiction. Revenue authorities should recognise the burdens placed on businesses if they are required to store data for long periods. It should be noted that greater consistency of record keeping requirements, including retention periods, between jurisdictions could decrease overall business compliance costs.

Production of records

5. Where taxpayers produce their records for examination by Revenue authorities, any regulatory framework should ensure that such records are presented in a reasonable time and in a readable format, acceptable to the Revenue authority.

Records held by third parties

6. Where the documents and records relating to e-commerce transactions are held or maintained by a third party, regulatory frameworks should ensure that the business engaged in those transactions are not be relieved of their responsibility for the upkeep, retention and production of those documents or records, regardless of who physically maintains the records.

Records located in other jurisdictions

7. The growing business trend to maintain accounting and data storage systems in one country to service their locations worldwide should not present revenue authorities with difficulties provided access, readability, usability and evaluation of the data relevant for tax purposes can be assured at all times. To appropriately respond to this trend revenue authorities should work with Businesses to develop administrative and legislative frameworks and cost effective techniques for remote access to records including consistent formats and access methodologies.

8. Wherever the records are maintained, the taxable person still has responsibility to make data available for inspection in each country where that taxable person has a liability to tax. The maintenance of records in another jurisdiction should thus not relieve business of the requirement to produce records when and where needed for the effective administration of the tax system.

9. For example, within the EU, the Invoicing Directive gives the possibility to taxable persons to store their invoices in another Member State provided that on-line access to the records can be guaranteed. It should be noted that:

- The Directive also grants Member States with the right of access, download and use of electronic invoices stored by their taxable persons in another jurisdiction,

- There is, within the EU, a legal framework for mutual assistance in cases of non-compliance.

Use of electronic records as evidence

10. Revenue authorities should ensure that both e-commerce and tax legislation allows for the use of electronic records and systems as evidence in criminal and civil legal matters. For example, that such legislation provides for –

the legal recognition of

- Electronic contracts,
- Electronic writing,
- Electronic signature,
- Original information in electronic form,

in relation to commercial and non-commercial transactions and dealings and other matters;

- The admissibility of evidence in relation to such matters; and
- The accreditation, supervision and liability of certification service providers and the registration of domain names.

Conclusions

11. E-commerce can be highly beneficial to businesses of all sizes in reducing costs, creating marketing opportunities, and improving customer service. The electronic nature of the audit trail also offers opportunities for audit efficiencies through the application of computer-based audit techniques.

12. E-commerce also poses a number of record keeping challenges to businesses, Revenue authorities, and auditors (both private and public sector) who are otherwise more familiar with paper-based systems. Legitimate businesses will endeavour to create authentic and reliable accounting records in support of their functions and activities, and protect the integrity of these records for as long as legally required. Revenue authorities should seek to implement the OECD Taxation Framework conditions for e-commerce and maintain their ability to secure access to reliable and verifiable information in order to identify taxpayers and obtain the information necessary to administer their tax systems. Revenue authorities also need to examine business records in order to collect the right amount of tax at the right time within their jurisdiction.

13. Revenue Authority record keeping requirements should be in accordance with the business objective to control their activities, and should impose minimal burdens by allowing whenever possible the use of commercial records to meet statutory tax requirements. For e-commerce these requirements should also be in support of the OECD Taxation Framework conditions by facilitating the creation and maintenance of reliable and verifiable records that can be trusted to contain a full and accurate representation of electronic commerce transactions.

14. A significant feature of e-commerce is that it allows many SMEs to routinely trade across jurisdictional boundaries. These SMEs will encounter different regulatory requirements and may incur additional compliance costs; likewise tax administrations may also incur additional administration costs when attempting to enforce compliance. Increased consistency in record keeping requirements for e-commerce transactions is one method of reducing these costs for businesses and Revenue authorities alike and should be encouraged.

15. Electronic audit trails that feature software based internal controls and records containing document entries that may only have been created, verified and stored electronically require a different approach both from business, their auditors (both internal and external) and revenue authorities. The importance of this is not only to support business and revenue authority objectives, but also to safeguard systems and infrastructures that are potentially open to misuse. To meet these objectives, increase audit efficiency, and also provide safeguards requires the application of security and technology countermeasures in conjunction with the establishment of appropriate business and legal frameworks. One aspect of the countermeasures needed to protect the overall integrity of e-commerce businesses are record keeping guidelines issued by revenue authorities that reflect the concerns of auditors from both the private and public sectors.

16. The increase in audit efficiency and productivity that is available to both revenue and business auditors with electronic records will be greatly enhanced by the use of a standard audit file containing transaction data elements that are agreed and accepted by all parties. Use of such a file also provides business with a corresponding opportunity to reduce compliance costs.

17. Implementation of these guidelines by Governments may require legislative change in countries where current legislation is primarily based on the requirements for the creation and maintenance of paper records.

Guidance

1. **Revenue authorities *are encouraged to* work with relevant government regulatory agencies, business associations and other organisations, such as accountancy bodies, developers of accounting software and private auditors, to <u>develop</u>:**

    - Record keeping requirements in support of the OECD Taxation Framework conditions to facilitate the creation and maintenance of reliable and verifiable records that can be trusted to contain a full and accurate representation of electronic commerce transactions.

    - Record keeping requirements that allow, to the fullest extent possible, the use of commercial records to meet statutory requirements.

    - Common specifications for technology based and non technology based techniques providing sufficient assurance for all parties with respect to the authenticity and integrity of transaction information that is created, transmitted, recorded and maintained.

    - A specification for a standard audit file that meets the requirements of all parties operating e-businesses or using a computerized accounting system.

    - More consistent approaches to access and retention periods for electronic records that take account of technological developments, commercial practice, and the minimum requirements commensurate with good governance of the tax system in such an environment.

2. **Revenue authorities are encouraged to work with relevant government regulatory agencies, business associations and other organisations, such as accountancy bodies, developers of accounting software and private auditors, to ensure that:**

- An appropriate regulatory framework exists to allow the creation, transmission, retention and access to electronic records and for their use for evidentiary purposes.
- An appropriate level of access is available to revenue authorities and private auditors that includes:
    - A range of access options to computer systems and supporting documentation for revenue auditors
    - Timely access to electronic records in a readable format
    - Access to electronic records held in other jurisdictions. These records should be maintained to the same standard as in the jurisdiction where the business is located.
    - Access to electronic records held by 3rd parties.
- Appropriate assistance from anyone concerned with the operation of the system is available to auditors.
- Records should be produced for examination within a reasonable time, and in a readable format.
- Adequate storage and procedures for retrieval of electronic records exits. In particular they should ensure that:
    - All material data is stored including (where held) electronic signatures and certificates and related keys for signature verifications. If data is encrypted, keys and recovery procedures should also be appropriately maintained to ensure revenue authorities are provided with decrypted data in a readable format.

- Transaction data received in electronic format should be stored as received; or if converted to another format then documentation relating to the conversion process should be maintained. The authenticity and integrity of the content of source documents must be preserved throughout the required period of storage through the use of electronic or other controls.
- The usability and readability of data must be preserved through the required retention period, in particular when data is transferred from one storage system to another.
- An audit trail for tax relevant electronic records is maintained throughout the required period of storage.

- The burdens, including those related to retention periods, placed on businesses storing data are reasonable.

3. Revenue authorities should closely monitor developments in record keeping methods and technologies.

4. Revenue authorities should closely monitor developments in record keeping methods and technologies.

History

April 2001: The FSM (now FTA) Electronic Commerce Sub-group forms a team to analyse the issue of record keeping requirements.

March 2003: This exposure draft is released for comment. The paper is to be published as part of the "Tax Guidance Series" from the Centre for Tax Policy and Administration.

Compatibility

The principles in this document are compatible with those contained in:

- Electronic Commerce: Taxation Framework Conditions
  OECD October 1998

- GAP001 Principles of Good Tax Administration
  Centre for Tax Policy and Administration, OECD May 2001

- TAG002 - Transaction Information Guidance
  Centre for Tax Policy and Administration, OECD March 2003

Contact

For further information please contact Mr. Richard Highfield, Centre for Tax Policy and Administration.
Tel: +33 (0)1 45 24 94 63; Fax: +33 (0)1 44 30 63 51

Further reading

A number of publications are available to help the reader when implementing security and PKI procedures in the e-Commerce environment:

Fred Piper, "Digital Signatures - Security and Controls", 1999, Information Systems Audit and Control Foundation, Rolling Meadows, IL, USA

Deloitte & Touche and Information Systems Audit and Control Foundation,"E-Commerce Security - Public Key Infrastructure, Good Practice for Secure Communications," 2000, Information Systems and Audit and Control Foundation, Rolling Meadows, IL., USA

Deloitte & Touche and Information Systems Audit and Control Foundation, "E-Commerce Security - Trading Partner Authentication, Registration and Enrolment," 2001, Information Systems and Audit Foundation, Rolling Meadows, IL, USA

Deloitte & Touche and Information Systems Audit and Control Foundation, "E-Commerce Security - Enterprise Best Practice," 2000, Information Systems and Audit Foundation, Rolling Meadows, Il., USA

Deloitte & Touche and Information Systems Audit and Control Foundation, "E-Commerce Security - Business Continuity Planning," 2002, Information Systems and Audit Foundation, Rolling Meadows, Il., USA

ANNEX A – SECURITY SERVICES

A1. Authenticity

Authentication is the means of assuring that remote people or organisations are who or what they claim to be. These services provide assurance of identity, *i.e.* when someone or something claims to have a particular identity an authentication service provides a means of confirming or refuting this claim. In the e-commerce environment, reliable authentication is needed to for access control; to determine who is authorised to receive or modify information; to enforce accountability; and to achieve non-repudiation.

A2. Reliability

Reliability in terms of electronic records refers to the reliability of the data after being archived for an extended period of time (also in the context of "transaction integrity" as defined in AGS 105616). Unlike paper documents, digital data and e-records cannot be read directly by the human eye, and therefore problems which may arise during an extended storage time will not be readily detectable, *e.g.* degradation of the storage media causing the data become to illegible; the storage device or operating system becoming obsolete causing data to become irretrievable, *etc*. Reliability services for e-record retention should focus on measures that could be taken against anticipated circumstances.

A3. Confidentiality

Confidentiality is an information security objective that ensures information is not disclosed or revealed to unauthorised persons. The main technologies for achieving these goals are communications security and computer security. Confidentiality, along with integrity and availability, are attributes inherent in the information security process that can be applied to systems and networks to gauge their overall security status. For a system or network to possess confidentiality means that the information contained, transformed, or transported by the system or network cannot be read or retrieved by unauthorised entities. For accounting record retention, security measures must be implemented to ensure that information contained in electronic records cannot be read or retrieved by unauthorised entities or individuals.

A4. Data Integrity

These services protect against the threat that the value of a data item might be changed or the integrity of the data be compromised. Data integrity services also protect against creating or deleting data items, such as complete messages, without authorisation. As record retention for revenue authority purposes could span a long period of time, there is a need to take intentional countermeasures or implement security measures to prevent alteration. In the case of paper documents, minimal security measures are required to ensure data integrity as these documents inherently possess characteristics that make alteration difficult, *e.g.* the quality of the material; consistent aging of the ink to be visible etc. This is in sharp contrast to data held electronically which may be altered in the absence of security measures without detection.

---

[16] Australian Accounting Research Foundation, 2000, Auditing Guidance Statement 1056, *Electronic Commerce: Audit Risk Assessments and Control Considerations*, August, paragraph 44.

Current technologies must be capable of providing continuous protection over a long period of time as forgery techniques for both paper documents and electronic data advance as time progresses. In the case of paper documents, it is possible to match the auditor's detection techniques with those of the forger over time. The security of electronic documents, however, is wholly dependent on how well the security element originally added can withstand attempts at forgery. This leads to a situation where those trying to breach security can take time to develop new methods of attack, while those responsible for security must rely on technology available at the time the security measure is added.

Any recommended method should mitigate against the risk regarding a loss of traceability. It is impossible to forge a paper document perfectly since it contains analogue elements. However, it is theoretically possible to do so in the case of digital data, and if the added security is eventually breached then the integrity of the data will remain seriously compromised, and ultimately invalid. It is therefore especially necessary to evaluate each method in advance to measure the long-term integrity offered for data against its long-term durability against attack.

The correct approach to ensure long-term durability against attack is to entrust the record (or its hash value) to a third party. In this case, technology would be utilised mainly to ensure the legitimacy of operations by this third party rather than ensure the integrity of a document. This approach mitigates against the risk that a successful attempt at forgery could be untraceable, making it impossible to validate the content of the document as original.

Data integrity measures can also be incorporated into software used for e-commerce to make it difficult to amend or delete historical records as an alternative to the use of third party services. The software would feature security measures such as use of system logs and database integrity checks.

A5. Key management

The nature of a public key means that confidentiality is not required when distributing the key. It is, however, essential that the integrity of the public key be maintained and proper backup procedures followed to enable recovery of a copy of a secret or private key should it be lost or become otherwise unobtainable. In the case of message encryption, which requires a particular key for decryption, loss of the key will mean loss of the message. The concept of key recovery is that someone must hold copies of sensitive keys and release them under appropriate circumstances. Key escrow is a key recovery system in which a third party such as a government body or a private entity (escrow agent) typically holds keys in trust.

Key management controls in relation to the issuer or certifying authority must be established to ensure that the security of the keys and the underlying system is not compromised. Consideration must be given to the use of appropriate key management handling, use and storage practices, including

- Appropriate backup and storage of encryption and decryption keys
- Appropriate policies in relation to the use of encryption
- What can be encrypted, how, when, why and for how long
- Authorisation procedures
- Appropriate internal key management as for the certifying authority

While some governments have sought to mandate the use of particular systems, the use of encryption is not yet a routine occurrence in the business world. Business and their auditors should therefore consider other methods to safeguard the security and integrity of accounting data.

A6. Non-Repudiation

Non-repudiation is a safeguard against one party to a transaction or communication activity falsely denying that the transaction or activity occurred. It does not prevent the threat of false repudiation, but rather ensures the availability of sufficiently strong evidence to support the speedy resolution of a dispute. In the e-commerce B2B or B2C environment, an audit trail offers supporting evidence.

Successful non-repudiation measures are primarily dependent on the integrity of the third party used to store the transaction record. However, in cases where the third party does not retain these records, storage of the record concerned will become the responsibility of either party to the electronic transaction or to another intermediary. If storage were to be transferred to another intermediary, it would become necessary to take appropriate security measures such as time stamping or digital signatures.

As suitable framework for developing non-repudiation services in respect of e-commerce is the ISO non-repudiation model17. The essential elements of this model are as follows:

- ***Evidence of the origin of the message and verification***. This shows that the originator created the message (electronically signed record). The sender (person signing the record electronically) has to create a proof of origin certificate using the non-repudiation service. The electronically signed record can be sent to another party (receiver of the electronically-signed record or another application for further processing) using the non-repudiation delivery authority service. In case of dispute, the sender can later retrieve this evidence.
- ***Evidence of message receipt***. This proves that the message (electronically-signed record) was delivered. The recipient must create and send a proof of receipt certificate using non-repudiation delivery authority services. The sender receives this evidence and stores it using the non-repudiation storage service; it can later be retrieved if there is a dispute.
- ***Transaction timestamp***. The timestamp is generated by the non-repudiation service as part of the evidence that an event or action took place.
- ***Long-term storage facility***. This is used to store the certificates of origin and receipt. If there is a dispute the adjudicator uses this storage facility to retrieve the evidence. Depending on the length of storage it might be necessary to address software and hardware migration concerns as part of the design of this facility.
- ***The Adjudicator***. The Adjudicator is used to settle disputes based on stored evidence if either sender or receiver of electronically signed records makes false claims.

---

[17] Part 1: General Model ISO/IEC JTC1/SC27 N1503, November 1996; Non-repudiation Part 2: Using symmetric techniques ISO/IEC JTC1/SC27 N1505 November 1996).

ANNEX B - ELECTRONIC RECORDS: TECHNOLOGIES AND MECHANISMS

There are a number of technologies that can be can be applied to electronic records to give the same levels of authenticity and reliability as paper; to ensure data integrity, verifiability, and readability; and recoverability of archived accounting records. This section builds upon the final reports of the PDA TAG (DAFFE/CFA(2001)41) and Technology TAGs that examined these mechanisms.

B1. Electronic Certificates

As reported by the Technology TAG, there is general agreement that electronic certificates (and electronic signatures) show the most promise for identification of parties in the future. Electronic certificates are electronic documents attesting to the binding of public keys to an individual or entity, and allow verification of ownership. They employ on key pairs, one of which is public and the other private. The private key is used to encrypt a document while the public key is in turn used to decrypt a document. This private key needs to be secured to preserve its integrity. Electronic certificates are issued and managed by Certification Authorities. A Certification Authority is a trusted third party organisation or company that guarantees the individuals or organisations granted these unique certificates are in fact who they claim to be.

There are two types of electronic certificates used in e-commerce. Client side certificates are used on e-commerce servers for B2B transactions and allow web sites to identify themselves to users and to encrypt transactions with visitors such as their business partners. Client side certificates also help server users know that they are communicating with a particular host and not an impostor. Server side certificates are used to implement the Secure Socket Layer (SSL), which is the most common method of providing a secure channel between a user's web browser and the host. When a server displays SSL identification, users know that they are dealing with a legitimate source. Information passing between the browser and the host is then encrypted after a certificate sent from the host to the browser is authenticated. Note that for B2C transactions that are usually paid by credit card or a financial prepay service a digital certificate is not required. It would be in any case impractical to obtain authentication for a large number of individual consumers.

B2. Electronic Signatures

The electronic signature signing process can provide proof of integrity and authentication and in many jurisdictions now has the same effect as a handwritten signature on a paper document, i.e. it achieves non-repudiation. Messages used in e-commerce transactions, such as invoices, are often affixed with electronic signatures. Electronic signatures are frequently used in electronic certificates to authenticate the attestation in a certificate.

A legitimate electronic signature supports non-repudiation since only the claimant knows the private key whereas the receiver of the message was able to decrypt it using the claimant's public key.

However, electronic signatures alone cannot verify legitimacy after an extended period of time and it becomes necessary to employ additional measures. One method is to archive data affixed with an electronic signature after notarisation. After verifying the record as being original, it will attach a time

stamp to certify that the records have been verified. Although it is possible to certify the verification of data using electronic signatures, time stamping is a better method in terms of long-term durability.

B3. Message Digests and Hash Function

A message digest is a string of digits created by applying a one-way hash function to a block of data. One-way hash function technology cannot be deciphered like code, as its key length is almost infinite. For example, the key length of one of the frequently used hash functions, MD5, is 128 bits (~1038) and the key length of another frequently used hash function, SHA-1, is 160 bits (~1048). If the block of data is changed, the message digest will not be the same when applying the one-way hash function. For this reason, the use of message digests and one-way hash function can readily detect any alteration of the original document that may arise during an extended period of time since it is computationally infeasible to change a block of data and for it to agree with the message digest.

B4. Encryption

Encryption technology utilises a key pair applied to data that directly represents information such as a message. This data is known as plaintext, and is transformed by encryption into unintelligible data called cipher text using the receiver's public key. The receiver will decrypt the cipher text data using their own private key, resulting in the regeneration of the original plaintext data. Encryption can be used to secure archived electronic records.

The Technology TAG examined the then current use of encryption methods, reporting that the most common encryption methods use key-based algorithms. The two main types of key-based algorithms are symmetric (secret-key algorithms) and asymmetric (public-key algorithms) systems. In most secret-key algorithms, the encryption and decryption keys are the same. These algorithms require that the sender and the receiver agree on a secret-key before they can communicate securely. If the key is publicly divulged then anyone could encrypt and decrypt messages. Public-key algorithms are designed so that the encryption key is different from the decryption key. The decryption key is also known as the private key and is kept by the message receiver, whereas the encryption key, commonly known as the public key, is available to anyone. The advantage of public-key algorithms is increased security and convenience. Private keys never need to be transmitted or revealed to anyone. Secret-key algorithms require the secret key to be transmitted, creating the risk of interception. A disadvantage of public-key algorithms is that it is significantly slower than many of the secret-key algorithms.

B4. Time Stamping

Time stamping means that each document is, at the time of its presentation to a Time Stamping Authority (TSA) "stamped" using special procedures so that it can be proven later that the document really was written at that time and verify its contents as unchanged. Many of the time stamping technologies are incorporated into message digest and encryption techniques to strengthen the process and overcome some of the shortfalls of encryption 18

This method is technologically simple and highly durable against attack, meaning that users can focus on ensuring the integrity of the TSA itself.

---

[18] Ford, Warwick and Baum, Michael S., '*Secure Electronic Commerce,*' Prentice Hall PTR, 1997, New Jersey, USA

B5. Notarisation

The Technology TAG advise that according to the ISO, notarisation is the registration of data with a trusted party that allows the later assurance of the accuracy of its characteristics such as content, origin, time and delivery. 19 A notary service can provide proof that something was not backdated. The notary receives the data and electronically notarises the message digest of that data (but not its content) which implicitly acknowledges the message was received at a particular time. Therefore, the document must have been in existence at that time and could not be created later and backdated. There is in practice little difference between notarisation and time stamping.

[19] See ISO SC 27 Standing Document no. 6 '*Glossary of IT Security Technology*' available from http://www.jtc1.org

ANNEX C - ARCHIVAL ISSUES

If an auditor needs to examine documentary evidence of internal controls or source documents for transactions outside of the current period, it may be necessary to retrieve these documents from an archive. Maintenance of records for a particular length of time is likely to be a statutory requirement determined by the legislation applicable in a particular jurisdiction.

The auditor when reading an archived record must have the assurance that it is capable of being verified as an original, meaning that the record being produced is identical to the one on which the original e-commerce transaction was based. It is important to ensure that the digital record is readable for humans even after the passage of an extended period of time as, unlike paper documents, digital data cannot be read directly. Storage over a long period therefore creates the possibility of problems arising such as data loss; data intelligibility; or even unavailability of suitable equipment to display what may have become an obsolete data format.

The technology utilised in e-commerce transactions is diverse and continually advancing, as are the message formats used. It would be ideal from an audit standpoint if these records could be standardised into one specified format. However, this technological diversity and its ceaseless advancement makes a solution based solely on technology an unrealistic objective. There are therefore a number of basic requirements that must be fulfilled in order for an archived record to be successfully used as audit evidence:

C1. Integrity of the data stored

The following methods should be adopted in order to maintain data integrity when records are retained over a long period of time:

- Records that exist individually as object files, such as Rich Text and XML files prescribed as unique based on the bit string, will retain integrity if it can be ensured that the bit string is not altered during the time of retention.
- Encryption of the archived file and secure archival of the encryption keys for decryption at the time of retrieval. Archival of a key and its binding is required if an assured copy of a key might be required in the future. For example, as evidence of the validity of an old electronic signature for non-repudiation purposes, such archives must be very well protected as the integrity and in some cases the confidentiality of the key must be maintained. In some cases, when physical security of a key is impractical, and in particular when it needs to be communicated from one place to another, the key must be protected by other means such as assignment to a trusted party; use of dual-control system where by a key is split into two parts with each part being entrusted to a separate person; and environmental controls for purposes of communication or intermediate storage or protection during communication by confidentiality and/or integrity services such as by encryption under another key. It should be noted that all keys have a specified life cycle. However, most of the PKI systems permit one further use of the key under the recovery mode even if the life cycle duration has passed.

- When individual records exist only within a database management system (DBMS), the record extracted into universal file format data becomes the basis for verifying it as the original record and the database itself become the original, *i.e.* data backed-up over a fixed period becomes the original version. Because database files are often large, back-up methods utilising a combination of full and "amendment only" backups would probably be utilised.

In summary, the first method thus described would likely to be adopted expressly for the purposes of auditing. However it requires supporting information to be available and therefore has shortcomings. The second method can be applied to any files provided key management and file recovery procedures are clearly defined. The third method requires strong internal controls over the information systems accessing the database in order to ensure integrity. It also requires the storage of large amounts of data. Ultimately the choice of methods will be a matter of policy for an organization.

C2. An environment to display the contents.

In order to ensure that the data will be displayable even after the passing of an extended period of time, the records should be in a universal format such as Text, Rich Text or XML, rather than a specialised format. If XML is used, it is necessary to store data inclusive of its style information (XSL). If a specialised format is used then in order to ensure the readability of data it becomes both necessary to store the data together with its displaying environment (software, OS, DBMS, hardware, etc.), and to take measures to verify the legitimacy of that environment. It is preferable for both the parties storing the displaying environment and the parties verifying its legitimacy that the display environment be compact software such as a simple viewer. However, if the display requirements were for a very large system then it may become necessary for the company storing the environment to maintain what may become an obsolete system even if its own systems are replaced and upgraded. This is likely to be a heavy burden on the business involved.

C3.Third party archives

When the archiving of the record is commissioned to a third party, the assurance level of data integrity depends on the credibility of that party. If appropriate technologies and procedures are applied to records to the extent that unauthorised alteration is theoretically impossible then this will effectively guarantee long-term integrity. In particular, the use of an external time-stamping service would not only relieve the third party of the need to prove the legitimacy of its operations but also ensure legitimacy of the record itself.

C4. Long –term storage

A number of considerations must be taken onto account when storing records on electronic media:

- The point at which the storage media used in archiving electronic records begins to degrade must be taken into consideration. Ideally, the manufacturer's recommended length of time for retaining records will match the length of time required by statute for retention of a record.
- The storage conditions for the media, again as recommended by the manufacturer, and whether the mechanism for reading the chosen medium is likely to still be in existence after a long period of time. This can be facilitated by use of a general rather than a specialised medium. However, it may in all cases be wise to keep spare mechanisms to mitigate against obsolescence.

C5. Key management

In cases where data is archived in an encrypted form to prevent information leakage, *etc.*, there would be a need to make backups of the keys or to manage the keys so that the data could be decrypted with certainty.

C6. Data backup

To ensure that data to be archived is not lost by accident, it is desirable for backup procedures to be implemented. These procedures should include periodic checks of the magnetic media used for the archive to ensure it can still be restored over the passage of time. A widely used and established medium such as CD-ROM is preferable.

The use of physical media allows identification, albeit not perfectly, to identify when something was created, or to find traces of alteration. Although it would not be easy to detect alteration, and equally there would be variations in the estimation of when the data was created depending on the storage environment, it may be safely assumed that because the authenticity of the data is ultimately verifiable, this will act as a deterrent against alteration of data. However, in fact because it is a very simple method, it is not infallible as a measure to ensure integrity, and should only be used in conjunction with another method. A further important security consideration would be for a trusted third party to have custody of the data.

In summary, archive procedures should ensure the integrity and readability of electronic records after an extended period. Digital signatures should be secured using encryption and hash functions; encryption keys should be secured by storage with an independent party. An independent party should secure the encryption keys, and for these to be readily retrieved for file decryption; and time stamping should be secured using the hash function to assure the hash totals.