OECD

Centre for Tax Policy and Administration

CTPA

Centre for Tax Policy and Administration

Tax guidance series

Tax Administration Guidance – Business Identification

Business Identification 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. The purpose of this paper is to encourage appropriate standards of identification for businesses offering services or products via the Internet. 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.[1] This guidance note is part of ongoing work to transform the agreed taxation conditions into practical administrative measures.

2. 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.*
>
> *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."* [2]

3. OECD governments and others[3] 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.

4. From the revenue authority viewpoint, expectations about the adequacy and accuracy of business identification on the Internet, were explicitly expressed in the Ottawa Taxation Framework conditions.

> ***"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."*[4]

---

1 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.

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

3 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.

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

5. The Taxation Framework Conditions also recognised that there are ongoing developments in areas such as Internet governance where revenue authorities both individually, and through such international fora as the OECD, may need to play a role if they are to succeed in implementing the tax principles.

6. The Taxation Framework Conditions were developed further in a discussion paper on the taxation issues that was also released at Ottawa. Implementation Options 10 and 12 of that paper noted:

> ***"10. Revenue authorities may consider encouraging business practices that identify businesses engaged in electronic commerce***
>
> *Revenue authorities recognise that many businesses will provide information on their web sites and other electronic places of business which can be used to accurately identify the business and its physical location, (e.g. registered trading name, a physical or mailing address, telephone and facsimile numbers etc.) so as to engender consumer confidence amongst other things. As this is the type of information which Revenue authorities have traditionally required of businesses, it would be helpful if it is provided as a matter of common business practice.*
>
> …
>
> ***"12. Revenue authorities may consider making their views on user identity known to other bodies with a role in determining the identity of parties engaged in electronic commerce***
>
> *Revenue authorities will need to keep themselves informed about developments in bodies such as those dealing with the Internet domain name system and involved in issuing or setting standards for digital certificates or other technological means by which taxpayers may identify themselves for electronic commerce. Revenue authorities could make their views about the identification of parties engaged in electronic commerce known to these bodies.*
>
> *Alternatively, revenue authorities may collectively, through international organisations such as the OECD, hold themselves out to provide guidance to parties developing identification standards or protocols for electronic commerce."*[5]

Issues

The importance of accurate identification of business enterprises

7. Income and Consumption (VAT or Sales and Use) taxes form the basis of most tax systems in the world. The accurate identification of business enterprises is a critical foundation of these tax systems. Simply put: without such mechanisms taxation systems are at significant risk.

8. In the conventional commercial environment revenue authorities rely on being able to identify the taxpayer to obtain access to verifiable information about the taxation affairs of that taxpayer.

9. In the case of direct taxes, such as income tax, the accurate identification of the taxpayer ensures that they pay tax on their income and not that of someone else. Accurate identification thus ensures that double taxation or unintentional non-taxation is avoided. With consumption taxes, the accurate identification of the business assists in ensuring that the right jurisdiction gets the tax and that the taxpayer is not double taxed or unintentionally untaxed.

10. The development of global electronic commerce introduces a new element into the accurate identification of businesses for both consumers and regulatory authorities – the physical business is no longer directly observable. In an electronic commerce environment a business may only be identifiable by

---

5 From: *Electronic Commerce: A Discussion Paper on Taxation Issues,* http://www.oecd.org/daf/fa/E_COM/discusse.pdf

its domain name (*e.g.* www.businessname.com) and the correspondence between a domain name and the location of where the business activity is undertaken is generally non-existent.

11. This is particularly the case with generic top level domains (gTLD) such as .com and country code top level domain (ccTLD) names such as, for example, the .cc[6] domain [Cocos (Keeling) Islands – an Australian Territory] – that are open to global rather than jurisdictional business registrations.

12. Several revenue authority surveys[7] have found that approximately 15% of domain-named business sites could not be traced to a registered business entity or person. In the case of commercial web sites operating off an Internet service provider's resources (*e.g.* www.ISPname.com/businessname.html) the non-traceability level is substantially higher.

A shared concern

13. Revenue authorities, consumer groups, businesses, intellectual property organisations[8], business registration authorities, law enforcement agencies and the Internet's co-ordination bodies (such as the Internet Corporation for Assigned Names and Numbers [ICANN[9]]) all have interests in improving the identification information on commercial web sites. The growth and stability of electronic commerce, particularly business to consumer, depends to a significant degree on adequately and appropriately addressing these concerns in a manner that ensures that accurate holder and contact data is provided, and is publicly accessible, for all commercial web sites.

14. Just as conventional businesses are required to identify themselves adequately, commercial web sites should also be required to provide accurate, verifiable and accessible contact data. Indeed requiring such data should be seen as part of the responsible process of providing a trustworthy environment in which electronic commerce can flourish. It should be noted that revenue authorities only seek to have access to Internet based information to the same degree that they have access to information in relation to other forms of commerce.

Business identification on the World Wide Web

15. There are basically two complementary mechanisms for publicly identifying businesses trading on the Internet: *Self-identification* and *WHOIS data*.

---

6 See http://www.enic.cc/about/quick_facts.html for additional details about the cc domain.

7 See for example: *Tax and the Internet: Second Report*, Australian Government Publishing Service, Canberra, 1999, ¶ 6.2.11. Also available at: http://www.ato.gov.au/content/Businesses/ecommerce_Tati2.htm

8 See, for example, the draft document issued by the World Intellectual Property Organisation (WIPO) in February 2001: "ccTLD Best Practices for the Prevention and Resolution of Intellectual Property Disputes". Available at: http://ecommerce.wipo.int/domains/cctlds/bestpractices

9 ICANN is a non-profit corporation that was formed to assume responsibility for the IP address space allocation, protocol parameter assignment, domain name system management, and root server system management functions previously performed under U.S. Government contract by IANA and other entities. ICANN has contractual agreements with domain name registrars for the generic top level domains (.com, .net, .org etc). ICANN has been seeking to establish best practice arrangements with registries for country code top level domains (eg .com.au, .net.ca, .co.uk etc).

Self Identification

16. This is identifying information that a business provides about itself on its web site. While most businesses provide such information as a matter-of-course some unfortunately do not. For example, a 1999 study by Consumers International found that almost 30% of web sites did not provide a physical address for the business. Only 7% provided a business registration number, 74% a phone number and 86% an e-mail address.[10] A more recent study indicated that 12% of sites ***still*** do not indicate their geographic address while the number providing some telephone or e-mail contact had increased to just over 95%.

17. Businesses trading on the Internet should identify themselves adequately by displaying:

- The legal name of the business and, where it differs, the name under which the business trades;
- The principal physical addresses for the business;
- The e-mail address or other electronic means of contact, telephone number; and, where applicable,
- An address for registration purposes and any relevant government registration or license numbers.

18. Ideally this information would be found in a logical and easily located part of the web site such as the '**contact us**' or '**about us**' page.

WHOIS data

19. The second mechanism for obtaining identifying information about businesses trading on the Internet is via the WHOIS[11] database maintained by gTLDs and most ccTLDs. This is identifying information that a

---

10 Source: 1999 http://www.consumersinternational.org/campaigns/electronic/e-comm.pdf and 2001 http://www.consumersinternational.org/CI_Should_I_buy.pdf with similar findings from several Revenue authority surveys.

11 See http://www.icann.org/registrars/ra-agreement-17may01.htm for the agreement that accredited registrars have agreed to. Note Section 3: "Registrar Obligations" and in particular Sub Section 3.3 "Public Access to Data on Registered Names" which details the requirement to make available WHOIS data. Sub section 3.7.8 notes that a "Registrar shall abide by any specifications or policies established according to Section 4 requiring reasonable and commercially practicable (a) verification, at the time of registration, of contact information associated with a Registered Name sponsored by Registrar or (b) periodic re-verification of such information."

See http://www.apnic.net/db/world_whois.html for a WHOIS lookup of IP numbers.

See http://www.uwhois.com/domains.html for domain name lookups.

See http://www.visualware.com/visualroute/livedemo.html for an 'approximate' location of an IP number/domain name. (Note that the last hop may be inaccurate as it is based on WHOIS data rather than geographically known IP addresses.

holder of a domain name provides to the registry[12] about themselves. The information provided consists of the following fields, some of which repeat:

Domain ID
Domain Name
Sponsoring Registrar ID
Domain Status
Registrant, Administrative and Technical Contact Information including

Contact ID Contact Name Contact Organization Contact Address, City, State/Province, Country Contact Postal Code Contact Phone, Fax, E-mail	Repeat fields

Trademark Name
Registration Date
Country of Registration
Registration Number or other designation
Right to Use Information
Nameservers associated with this domain
Domain Registration Date
Domain Expiration Date
Domain Last Updated Date

20. WHOIS data is a critical source of information that assists in accurately identifying the registrants/holders of domain names. In some instances it is the only information that is available to identify the operators of commercial web sites. As such its reliability is a key concern to revenue authorities and other regulatory agencies.

21. The current institutional arrangements with the domain name registration authorities[13] are not consistently applied and in many cases the registries provide a simple fee-for-listing service. Few, if any, integrity checks are carried out. Even where the information is accurate, it often dates quickly and is rarely updated. Of serious concern is that some ccTLD registries do not record relevant WHOIS data or fail to make it publicly available when not legally prevented from doing so. The associated registration information that can be accessed by a WHOIS lookup of the domain name can therefore be unreliable or unavailable.

22. Currently most registries work on a policy of 'notification and correct' basis for maintaining the integrity of WHOIS data[14]. Under this policy a registry is obliged to seek correction of data if it becomes aware, generally by notification, that the WHOIS data is incorrect or falsified.

---

12 See http://www.internic.net/origin.html for a listing of gTLD registrars by jurisdiction. This excludes ccTLD registrars and registries that are not specifically accredited by ICANN. See http://www.icann.org/registrars/accredited-list.html for a listing of accredited gTLD registrars. See http://ecommerce.wipo.int/databases/cctld/output.html for details of ccTLD WHOIS availability.

13 Network Information Centres – see http://www.iana.org/cctld/cctld-whois.htm for a listing.

14 See http://www.icann.org/registrars/ra-agreement-17may01.htm Sub section 3.7.8: The "Registrar shall, upon notification by any person of an inaccuracy in the contact information associated with a Registered Name sponsored by Registrar, take reasonable steps to investigate that claimed inaccuracy. In the event Registrar learns of inaccurate contact information associated with a Registered Name it sponsors, it shall take reasonable steps to correct that inaccuracy."

23. While such a policy keeps registry costs to a minimum, it does place the entire onus and cost on the consumer and regulatory authorities to detect and notify the registry of the incorrect information. There is no real incentive in such a system to ensure that registries collect and pass accurate data into the WHOIS database.

24. The work-to-date of ICANN and related parties in attempting to establish quality standards in relation to WHOIS is recognised and welcomed by revenue authorities and other regulatory agencies. It is noted that the integrity of the WHOIS data could be improved by incorporating some appropriate pre- and post-registration data verification mechanisms, particularly where it is alleged that the business is located and controlled outside the home jurisdiction of the registry.

25. A range of possible mechanisms can be used for WHOIS data validation. These vary significantly in their ease of implementation, marginal cost and strength. While such verification mechanisms are possible now, the practicality of these proposals for existent registry modes of operation requires further analysis. The experience of registries in undertaking ex-post verification is that it has a high cost relative to the cost of establishing the domain name. Any measures adopted would need to be targeted and proportional to the risks posed so that the compliance burden placed on registries and domain name holders is the minimum necessary to reduce the risk to acceptable levels. No validation mechanism would ensure that WHOIS data is accurate at all times – a balance is needed.

Verification of :	**Validates…**	**Strength…**	**Cost per registration…**	**Feasibility…**
Contact e-mail	Address exists	Low	Automated – low cents.	Possible now – performed by some registrars
Contact postal address	Address exists	Medium – High	Automated – low to medium dollars (registered mail).	Possible now
Contact phone number	Number exists Number-name	Low Medium – High	Automated against database – low cents. Manual call back - medium dollars ($20 - $100).	Possible now

The ccTLD WHOIS data

26. While the majority of business registrations have been on the .com gTLD, significant and growing numbers are found on country code TLDs. The accuracy and availability of WHOIS information can vary widely between ccTLD registries. Some ccTLD registries ('restricted registries') will not allow a business to register unless it has evidence that it is registered with the relevant jurisdictions authorities. (See .it and .fr examples in Annex 1.) Others (open registries) operate a competitive fee for listing service, open to all. A small minority openly play on the fact that they either will not collect nor make available WHOIS data.

27. Some efforts by ICANN[15] have been made to check that Governments are satisfied with 'their' ccTLD registries. A few Governments have taken an active step in the regulation and management of 'their' jurisdiction's ccTLDs. Others have not. Some do not appear to be aware of the potential significance of the domain name space represented by their country code. It should be noted that some ccTLDs [for

---

15 See: http://www.icann.org/cctlds/draft-letter-to-govts-12nov00.htm

example .md (Moldavia) for doctors, .tv (Tuvalu) for media etc] are more popular to external businesses than others.

28. Despite the wide variety of approaches to ccTLD regulation and management it is clear that a consistent set of WHOIS requirements applying to gTLD and ccTLDs would engender better integrity in the system from a regulatory viewpoint. This in turn would assist revenue authorities to adequately identify commercial activities being carried out by their residents who enjoy the benefits of publicly provided infrastructure and services.

Privacy

29. Support for the concept of anonymous domain name registration has been put forward in some forums[16]. It is recognised that legitimate individual privacy concerns need to be taken into account in the formulation of policy in relation to the global availability of WHOIS data from either gTLD or ccTLD registries in a way that accords with the principles expressed in guidelines on the issue[17]. In regard to this a clear distinction can be made between the privacy concerns of an individual acting for commercial reasons in registering a domain name (*i.e.* a natural person seeking to undertake business activities on the Internet) and a person establishing a domain for non-commercial reasons.

30. In this analysis it is paramount to realise that businesses establish domains on the Internet for the express purpose of being globally accessible to customers. Businesses hold themselves out to the world to conduct business and for direct taxation systems to work such businesses cannot be anonymous. This is also true for indirect tax systems that use the business as a tax or information collection point. There is a strong synergy between consumer protection requirements regarding adequate business identification and the needs of revenue authorities and other regulatory agencies in this regard.

31. In order to ensure that the global availability of business identification information does not conflict with relevant privacy instruments[18], it may be necessary for gTLD and ccTLD registries to include explicit waivers in their contracts with the registering business. These waivers would allow for the global availability of identifying WHOIS data on business registrations.

32. Revenue authorities should seek to ensure that legislation, such as privacy/data protection instruments, does not compromise the imposition, collection or recovery of taxes by creating avoidance or evasion opportunities.

Conclusion

33. Ultimately, without steps to protect the viability and integrity of the taxation systems in an Internet environment Governments may find it difficult to take forward the liberalisation of cross-border trade. It is therefore critical that Governments, Businesses and other interested parties work together to provide acceptable guidance to make the emerging global electronic commerce market workable for all.

---

16 See http://www.epic.org/privacy/internet/ICANN_privacy.html for example.

17 See for example OECD *Guidelines governing the protection of privacy and transborder flows of personal data* http://www1.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.

18 See for example http://europa.eu.int/comm/internal_market/en/dataprot/inter/index.htm.

Guidance

1. Revenue authorities *are encouraged to* derive and promulgate a common position on the issue of Business Identification in an electronic commerce environment.

2. Revenue authorities *are encouraged to* work with relevant government regulatory agencies, business associations and other organisations to ensure that businesses engaged in eCommerce provide, and accurately maintain, the following contact information on their web site:

- The business's legal name and the jurisdiction in which it is registered together with any applicable business and tax registration numbers.
- The trading name under which it conducts business.
- The principal physical addresses of the business, including jurisdiction, sufficient to ensure the Revenue authority can locate the business offline.
- An online method of contact such as e-mail.
- The name of a point of contact within the business, and
- The telephone number of that point of contact.

3. Revenue authorities *are encouraged to* work with relevant government regulatory agencies, business associations and other organisations to ensure businesses engaged in eCommerce provide and maintain complete and accurate information to the Internet registrar with which they register.

4. Revenue authorities *are encouraged to* work with relevant government regulatory agencies, business associations and other organisations to ensure that country code Top Level Domain registries for their geographic jurisdictions abide by relevant national legislation and, to the extent they exist, internationally recognised requirements in respect to the collection, verification and global availability of WHOIS data for business registrations.

5. Revenue authorities *are encouraged to* work with relevant government regulatory agencies, business associations and other organisations to periodically consider whether regular pre or post verification of WHOIS data by registrars and registries is warranted in certain circumstances.

6. Revenue authorities *should* closely monitor developments in business identification.

History

April 2001: The FSM Electronic Commerce Sub-group forms a team to analyse the issue of business identification further.

March 2002: 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

Privacy

- **Guidelines governing the protection of privacy and transborder flows of personal data**

OECD Council recommendation adopted 23 September 1980

- **Guidelines concerning computerized personal data files**

United Nations General Assembly adopted 14 December 1990

- **Convention for the protection of individuals with regard to automatic processing of personal data**

Council of Europe directive adopted 24 October 1995

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

ANNEX 1: EXAMPLE OF CCTLD BUSINESS DOMAIN NAME REQUIREMENTS.

From the Italian Registration Authority (www.nic.it) Document at http://www.nic.it/RA/en/lar/lar-socditte1.txt
Emphasis added to relevant points.

To the Italian Registration Authority (RA)
Institute for Telematic Applications of CNR
Via Giuseppe Moruzzi,
56124 Pisa

Object: request for the registration of the domain name.....

Here, the undersigned..... entitled, for the present agreement, to represent the company /firm (indicate the business name, and the name and surname of the legal representative, if different from the entitled person) ....., registered at the Chamber of Commerce and/or at the Enterprises Registry of ..... with number .....on (day/month/year).....…, VAT number ....., whose head office is located in ....., asks for the registration of the above mentioned domain name according to the precise techniques that are included within the technical registration form forwarded (via E-mail) to the Registration Authority by the provider/maintainer ..... (indicate the exact "abbreviation" of the provider/maintainer which will forward the technical registration form to the RA). ***Furthermore, he/she undertakes the responsibilities coming from the use and management of the domain name and pledges him/herself to inform immediately the RA of any future changes related to:***

- ***change of the business name;***
- ***change of provider/maintainer;***
- ***change of admin-c;***
- ***termination of the domain name use;***

Particularly, here the undersigned declares under his/her responsibility that he/she:

- is aware and accepts that the assignment of a domain name and its registration are subject to the Naming Rules and the Registration Technical Procedures as established by the Italian Naming Authority;
- is aware of and accepts the rules for a "good use" of the Internet resources as established in the "Netiquette" document, published on the web site of the NA, as well as commits him/herself to respect them;
- is aware of and accepts the procedure concerning the dispute resolution as established in article 14 of the Naming Rules;
- has the title to use the requested domain name and/or the juridical disposability of the requested domain names, and therefore, if registering the requested domain name, is not prejudicial to someone else rights;
- entitles the RA to insert the registration data of the domain in the public database (Register of Assigned Names) of the RA and RIPE-NCC;
- ***guarantees the accessibility via E-mail of all the people indicated in the "postmaster" tag of the domain registration form, given that the RA will insert them into the mailing list of the Italian postmasters***;
- relieves the RA of any responsibility coming from the assignment and use of the domain name that the requesting organisation will carry out;
- ***is aware that, in the instance of false or erroneous declaration in the context of the present request, the Italian Registration Authority will ensure the immediate cancellation of the domain name, unless more extended legal action is in progress***;
- is aware of the Italian Codes rules regarding the right of having a name and the individual people right of protecting their names;
- accepts the Italian jurisdiction and the laws of the Italian legal system;
- is aware and accepts that the Court of Rome is the place of jurisdiction for any dispute that comes or is related to the commitments undertaken with the present letter.

Name and surname
Legible signature

Regarding the French Registration Authority http://www.nic.fr.

Domain name registration requirements for .fr

A domain name within the **".fr"** ccTLD can be attributed to any body officially registered in France (entities with a legal existence in France, trademarks registered with INPI or OMPI) or to any natural person living in France or of French nationality. Requesting bodies **must** apply to Registrar that has a membership agreement with the **AFNIC**[19].

Registrars ensure that their clients respect the **Naming Charter** (further information is available at www.nic.fr/english/register/charter-fr.html) and relay the successive updates of the charter to their clients. Registrars take responsibility for certifying that all information supplied to the AFNIC is accurate, in particular checking the validity of the supporting documentation and information required. (A pre-registration validity check.)

The following supporting documents are required

- For a company or a legal entity with a **SIREN/SIRET number** (trade register number), on receipt of a **K bis extract** or an identifying entry in the **INSEE** directory;
- For a body holding a registered trademark: a definitive **registration certificate** from the INPI, or OMPI;
- For any organisation not identified with the INSEE, set up by law or decree, or listed with a professional association: on receipt of **law** or decree AND copy of local government or *préfecture* registration document;
- For association **".asso.fr"**: on receipt of a copy of the **Official Journal** announcement or certificate of declaration from the préfecture AND copy of **INSEE identification**;
- For natural person residing in France **".name.fr"**, on receipt of approved copy of national **identity card** AND a document less than three months old proving the **address**;
- For natural person of French nationality residing abroad, on receipt of approved copy of national **identity card** AND a document less than three months old proving the address in the country of residence.

Further information is available on the website of the AFNIC at : www.nic.fr.

It should be noted, however, that since the 20 September 2001, the AFNIC check the accuracy of the information on-line via INFOGREFFE and INPI databases so supporting documents are no longer required to be sent to AFNIC to register a .fr domain names.

[19] The AFNIC (French Network Information Centre) is a non-profit organisation. It was created in December 1997 by the **INRIA** (French National Institute for Research in Computer Science and Control) and the Ministries of Telecommunications, Industry and Research.

Centre for Tax Policy and Administration

Tax guidance series

Tax Administration Guidance – Transaction Information

Transaction Information 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.

TRANSACTION INFORMATION GUIDANCE

Introduction

1. To facilitate the growth of electronic commerce the OECD's Forum on Tax Administration has been developing guidance papers[1] to assist revenue authorities and business in creating more consistent practices across borders. The purpose of this paper is to encourage appropriate standards for transaction information for businesses offering services or products via the Internet. The desirable data elements contained in this guidance paper will be promulgated to interested groups such as, for example, the OASIS Universal Business Language (UBL) Technical Committee [http://www.oasis-open.org/committees/ubl] and the XML Common Business Library Working Group http://www.xcbl.org/about.html. Where practical the guidance will utilise the extensive work already performed by such groups in mapping out data requirements for business transactions in an e-commerce environment. While written for the emerging electronic commerce environment it applies equally to traditional business transactions using electronic systems.

Background

2. 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.

3. 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]

4. 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.

5. From the revenue authority viewpoint, expectations about the adequacy and accuracy of transaction information on the Internet, were explicitly expressed in the Ottawa Taxation Framework conditions.

"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]

6. The Taxation Framework Conditions also recognised that there are ongoing developments in areas such as Internet governance where revenue authorities both individually and through international fora, such as the OECD, may need to play a role if they are to succeed in implementing the tax principles.

7. 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:

Implementation Option 15

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.

---

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

through the OECD, at an early stage to enhance a constructive dialogue designed to find mutually acceptable solutions.

8. Since 1999 the OECD has been working with revenue authority delegates and business 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).

9. More detailed on work 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).

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

Objectives

11. There are a number of overlapping objectives associated with the production of this guidance:

- To simplify and have greater consistency between revenue authority requirements - where this is practical;
- To reduce compliance burdens for businesses and administrative costs for revenue authorities;
- To provide a guide for international best practice;
- To help both internal and external auditors in testing the effectiveness of internal controls;
- To provide systems and software developers with the key data elements that if provided by their systems will help facilitate compliant systems;
- To enhance understanding by revenue authorities and businesses of the issues associated with transaction information in an electronic commerce environment; and
- To assist revenue authorities verify tax declarations.

Scope

12. While a tax guidance paper on transaction information will naturally appear to focus on tax requirements associated with a transaction, such as consumption taxes and sales and use taxes, this guidance paper is also applicable to taxes that make use of aggregated transaction information, such as income taxes. The paper is written from an audit perspective, that is to ensure that an appropriate amount

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

of information exists in the transaction so as to enable verification of the tax results arising from the transaction or aggregated series of transactions. While written for the emerging electronic commerce (e-commerce) environment, it applies equally to traditional business transactions using electronic systems.

Issues

A common need for reliable transaction information - Business needs

13. Private enterprise needs reliable information in order to manage a business so that it operates in an effective and cost efficient manner. These management information needs within a business are generally fairly consistent across an organisation, even when it spans multiple jurisdictions, so as to minimise information costs while maximising reporting comparability. It should be noted that transaction information needs may vary between jurisdictions for the purposes of satisfying other stakeholders and that to the extent that these information requirements can be made more consistent, the overall system's compliance costs are likely to be reduced.

14. The policies and practices that are designed to provide management with reasonable assurance that their goals have been met are known as the internal control procedures. The internal control procedures aim to ensure the orderly and efficient conduct of business including:

- Adherence to management policies,
- The safeguarding of assets,
- Prevention and detection of fraud and error,
- Tthe accuracy and completeness of the accounting records, and
- The timely preparation of reliable financial information.

The internal control procedures[7] are also designed to ensure that business can comply with the various legislative requirements of the jurisdictions in which it operates.

15. Management balances the costs of internal control against the benefits expected. Many internal controls, which would be relevant to large businesses, may not be practical or cost-effective in small and medium sized enterprises (SMEs[8]). These SMEs may lack effective segregation of duties and this internal control weakness is often compensated for by stronger formal and informal supervisory controls by the owner/manager.

16. Information from both internal and external sources is used to control processes in businesses. In a traditional environment, paper documents are often used to distribute control information whereas in an e-commerce environment this information is generally exchanged in an electronic format.

---

7 The COSO report states "Internal control is a **process** (bold emphasis added), effected by an entity's board of directors, management and other personnel, destined to provide reasonable assurance regarding the achievement of objectives in the following categories:
- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with laws and regulations."

8 It should be noted that the criteria to classify an enterprise as a small or medium sized business may differ from jurisdiction to jurisdiction.

17. Regardless of their form, internal controls and documentation must be adequate to provide reasonable assurance that assets are safeguarded and transactions are properly authorised and correctly recorded in the accounting records. This recording or documentation of transaction information must be:

- Complete (all transactions are recorded with no duplications or omissions),
- Accurate (the right accounts are correctly debited or credited with the right amount), and
- Timely ('cut-off' - transactions must be recorded in the relevant time period).

18. Transaction information documentation, or its electronic equivalent, is usually consecutively numbered to facilitate a completeness control over documents (so that all transactions can be accounted for) and as means to trace documents if they are needed at a later date. Documents are often designed for multiple purposes so as to minimise the number of different forms.

19. The transaction information recorded on the documents must be sufficient to carry out adequate internal control. The documents, and the specific transaction information data on the documents, will naturally vary depending on the type of business and from business to business within an industry. Just as there is no standard internal control system, there is no unique set of control information. That said, there is often a high degree of commonality of the data elements required for internal control purposes between businesses.

20. Annex 1 gives an example of a generic sale and purchase process and the documents that are used to control these transactions. The four main control documents in a sales/purchase cycle are identified as:

- Customer order,
- Delivery note,
- Invoice, and
- Payment advice.

21. It should be noted that in many retail businesses, where the product is both on-hand and the order, delivery and payment processes effectively take place at the same point in time, the invoice/receipt is often the primary document generated. It should also be recognised that the processing of transaction data can be outsourced to third parties or to the customer (referred to as self-billing).

22. Many internal control procedures are preventive (*i.e.* they exist to prevent an error in the making – *e.g.* authentication and approval processes at the time of the transaction). Other internal control processes are detective and corrective (*i.e.* they exist to detect and reverse an error that has been processed through to the accounts – *e.g.* via a regular review of the accounts, regular reconciliation to control accounts and the like). The proof that these internal control processes have occurred may be obtained from the use of transaction data. In a paper environment this might be via the approving staff member's initials, in an electronic environment via some authentication mechanism. The very nature of an electronic environment changes the way of undertaking tests of internal control procedures.

23. Ideally the transaction information data elements exchanged in electronic form will be sufficient to perform an effectively similar level of internal and taxation control as those in a paper-based environment at the time of the transaction. However the associated audit trail[9] may initially be less visible. The traditional approach of physically viewing the document with its transaction details and control

[9] The audit trail is the ability to trace accounting entries back to their initiation (source documents) and the reverse.

information is no longer viable and more substantive testing of electronically held transaction information often needs to occur via the use of computer assisted auditing techniques. Such techniques can often be more effective and efficient than traditional paper based approaches. The use of other electronic processes such as the production of a standard audit file may increase savings for both businesses and tax administrations (see paragraph 51).

24. The invoice is an internal control document common to all industries and specifies the goods that are delivered/received or services rendered/received. The invoice normally consists of all the data elements necessary to allow for proper accounting treatment and to facilitate taxation control. However it should be noted that a formal invoice is not required in all jurisdictions, circumstances or in all trading environments, *e.g.* retailing and B2C e-commerce transactions. From an internal control point of view the existence of an invoice is not by itself sufficient evidence of the transaction and it is usually matched with other tests or data to confirm the validity of the transaction. (Refer to Annex 1 for other documents that may evidence the transaction.)

Other stakeholder requiring reliable information –The use of audit processes for verification

25. Other stakeholders requiring reliable information include shareholders, banks, suppliers, customers, regulatory authorities and tax administrations. On the basis of the financial documents and statements, potential and existing business shareholders decide whether to invest equity in business and banks decide whether to provide loans or other financial means. Suppliers and customers decide whether to undertake transactions. For the businesses that have a tax liability in their jurisdiction, tax authorities also have to verify and collect the right amount of tax at the right time and the financial documents and statements of the business usually form the basis of their tax declarations.

26. These other stakeholders can need assurance that the financial documents and statements of the business reflect economic and legal reality. Auditability of the financial statements and supporting records and systems, is a prerequisite for this assurance. The statutory audits performed by private auditors for public companies, and many private ones, normally provide the needed assurance to the stakeholders. From a Government perspective, tax auditors verify the reliability of the information in tax declarations.

27. In order to plan the audit[10] and develop an effective audit approach[11], private auditors obtain a detailed understanding of the accounting and internal control system of the business. The private auditor then makes a preliminary assessment of risks that are involved in the internal control structure of the business and where substantive testing of transaction information and significant account balances will be needed. Compliance tests are performed to obtain audit evidence about the effectiveness of the accounting and internal control system and the operation of these internal controls over time. Substantive test procedures for significant account balances and classes of transactions are also performed as part of the financial statement assurance process.

28. Depending on the audit methodology followed by individual tax administrations, and whether direct or indirect taxes are involved, tax auditors may build on the work of the private auditors or may perform their own compliance and substantive testing.

---

10 See International Federation of Accountants (IFAC) International Standards on Auditing (ISA) 300 (planning) and ISA 310 (Knowledge of the business) available from www.ifac.org.

11 See IFAC ISA 400 (Risk assessment and internal control) and ISA 401 (Auditing in a computer information systems environment). Also relevant is International Auditing Practice Statement (IAPS) 1005 (The special considerations in the audit of small entities), IAPS 1008 (Risk assessment and Internal control – CIS characteristics and considerations), and IAPS 1009 (Computer assisted audit techniques).

29. As is noted in the International Standards on Auditing "Audit Evidence" (ISA 500) issued by the International Federation of Accountants[12], auditors need to collect sufficient appropriate audit evidence to persuasively support their opinion. This audit evidence can be obtained by techniques such as inspection, observation, inquiry and confirmation, computation and analytical review procedures.

30. Inspection consists of examining the records, documents and tangible assets. The reliability of documents depends on the nature and source as well as the effectiveness of internal controls. In general three categories of documents, with a decreasing level of credibility, are distinguished:

- Documentary audit evidence created and held by third parties;
- Documentary audit evidence created by third parties and held by the business; and
- Documentary audit evidence created and held by the business.

31. In an environment where some or all of the business records are computerised, this inspection (or a substantial part of it) may be performed by the use of computer assisted audit techniques. Such techniques can increase both the coverage and reliability of the inspection while reducing the cost and impact on the business being inspected.

32. The invoice has a specific function with respect to indirect taxes. The invoice contains the data elements necessary to calculate the amount of tax (VAT/GST/S&UT) that has to be declared to the tax authorities. In most consumption tax systems the recipient of the goods or services can claim an input tax credit (or in some systems a deduction) for the amount of tax paid to the seller if the recipient is a business. The invoice is used as the primary documentary audit evidence with respect to such tax credits (or deductions).

33. As has been noted, traditional paper documents are increasingly being replaced by information held in electronic form. In order to be able to rely upon the internal controls of the business the transaction information data elements that are exchanged in electronic form between businesses need to be sufficient to perform the same level of control as in a paper based environment. Furthermore, the authenticity and integrity of exchanged and stored electronic information needs to offer at least the same reliability to their paper equivalents if they are to serve as appropriate audit evidence for both private and tax auditors.

34. By far the greatest numbers of business enterprises are small to medium in size and complexity. Such businesses may have minimal levels of internal control that can be relied upon. For example the small number of staff may mean there is inadequate segregation of duties. For such businesses, audits have to be carried out by substantive testing procedures and third party confirmation approaches in most cases. Moreover few small businesses are privately audited and hence any tax audits that occur often need to use substantive testing of transaction information as a means for forming a view as to the accuracy of the accounting records. In a situation where adequate internal controls are not in place, both private and tax auditors may not be assured that electronic documents are credible, and therefore cannot simply rely on this documentation when performing substantive tests. This means that both a systems approach and use of substantive testing may be compromised and therefore auditability of the financial statements may not be ensured unless recourse is made to external or third party records.

The need for authenticity and integrity

35. In keeping with the neutrality principle, tax authorities need to maintain their access to reliable and verifiable information to administer their tax systems. The authenticity and integrity of important third

[12] See ISA 500 (Audit Evidence). Also relevant is the IFAC International Auditing Practice Statement: IAPS 1013 (Electronic Commerce-Effect on the Audit of Financial Statements).

party documentation like invoices and bank statements should be effectively at the same level as their paper equivalents[13].

36. External electronic documents are sometimes perceived as less reliable than their paper equivalents. However the perceived loss in reliability can be compensated by the use of techniques that provide the necessary level of assurance of the authenticity and integrity of electronic documents. Within the EU, for example, the EU Invoicing Directive[14] obliges EU Member States to accept invoices sent by electronic means provided that the authenticity of the origin and integrity of the contents are guaranteed by means of:

- An advanced electronic signature[15]. Member States may however ask for the advanced electronic signature to be based on a qualified certificate[16] and created by a secure-signature-creation device[17]; or

- Electronic data interchange (EDI)[18] when the agreement relating to the exchange provides for the use of procedures guaranteeing the authenticity of the origin and integrity of the data. (However a Member State may also require an additional summary paper document.).

37. Electronic documents, such as invoices, may also be guaranteed by other means subject to acceptance by jurisdictions. For example, other documents generated in the sale process (see Annex 1) could be used to support and guarantee the authenticity of the origin and integrity of the invoice if the business can demonstrate an appropriate high level of integrity in their electronic and other internal control systems over time. The use of these types of techniques can enable both private and tax auditors to obtain a similar level of assurance with respect to the reliability of invoices and, in the end, financial statements as in a traditional paper environment.

---

13 See final report PDA TAG para 53 page 56. http://www.oecd.org/pdf/M000015000/M00015523.pdf

14 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

15 An advanced electronic signature is an electronic signature that meets all of the four following requirements:

The signature is uniquely linked to the signatory.

The signature is capable of identifying the signatory.

The signature is created using means that the signatory can maintain under his sole control.

The signature is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable 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.

16 I.e. an electronic certificate that links data for verification to an electronic signature (such as codes or public cryptographic keys) to a person and confirms the identity of that person. In order to be regarded as qualified this certificate has to meet a number of minimum requirements with regard to content and has to be issued by a certification-service provider (who, himself, also has to meet certain strict requirements)

17 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.

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

38. A survey among OECD members has shown that some jurisdictions[19] have already introduced specific requirements with respect to the techniques of assuring the authenticity and integrity of electronic documents. A review of these requirements indicates that different approaches have been adopted by some countries.

39. 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 countries there is a lack of electronic certificates meeting a sufficient level of integrity. In some countries the tax administration, or another Government authority, has acted as the issuer of high integrity digital certificates.

40. In order to avoid potential problems caused by the differing approaches by countries, there is a need for the development of more consistent cross-border standards for electronic signatures, possibly based on electronic certificates, and for simple procedures to enable the cross-jurisdictional recognition of electronic certificates. If this does not occur the current inconsistencies of approach between countries may slow the adoption of electronic invoicing on cross-border transactions.

41. Another factor affecting the deployment of electronic invoicing is that many businesses are themselves not in a position to accept invoices assured by electronic signatures. Therefore jurisdictions should not necessarily restrict themselves to the use of electronic signatures, possibly based upon electronic certificates, as the only sufficient guarantee for authenticity and integrity with respect to electronic documents (such as invoices – see paragraphs 36 and 37).

Costs of compliance and administration

42. Governments and their tax administrations generally seek to administer the tax system in a manner that minimises the long term overall operating costs: business compliance costs, revenue authority administration costs, and other costs to society. This means having to strike a balance between those costs borne by business in complying with tax regulations and those costs borne by the revenue authority in running the system. The two types of tax system operating costs are inextricably linked but not necessarily inversely - where one rises while the other falls.

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

44. 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*

[19] For example, Switzerland and members of the EU

risks[20]*. 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 include education, service, marketing, profiling risk, auditing, general anti-avoidance efforts, prosecution and proposals for legislative change."*

45. To enable voluntary compliance, from the perspective of transaction information flows, business compliance costs are minimised to the extent it is possible for tax requirements to take advantage of pre-existing business processes. Revenue authority administrative costs are minimised when this is done in a way that is compatible with their overall management of the tax system, including its auditability.

46. With large businesses this is often possible as their internal control systems and procedures are generally reasonably robust and auditors, acting on the behalf of shareholders, usually audit the business. Small to medium businesses can sometimes have relatively significant compliance costs and difficulties in understanding and complying with tax requirements. The ability of small business to create, record and maintain adequate transaction information data as an integral part of their normal business operations appears to have been somewhat limited.

47. The ongoing development of accounting software packages aimed at small businesses has ameliorated this issue to some extent, although the issue of data integrity due to inappropriate segregation of duties remains an enduring concern. It should be noted that to the extent that the creation, recording, maintenance and exportation of adequate transaction information requirements can be integrated into business software packages, the costs of compliance and of administering the system are likely to be reduced.

48. The development of e-commerce has allowed many SMEs to engage in trade across borders where previously this was not practical. To the extent that jurisdictional legal and regulatory systems vary significantly, these SMEs may have difficulty in complying and may have increased compliance costs, while administrations may suffer increased administrative costs in trying to enable or enforce such compliance. Increased consistency, where this is practical, between jurisdictions in their legal and regulatory requirements is one mechanism for reducing both compliance and administrative costs. To the extent that transaction information requirements and their format and mode of storage can be more consistently agreed between jurisdictions the costs of compliance and of administering the system are likely to be reduced.

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

50. Some revenue authorities, external audit bodies, and accounting package software developers are participating in the development and use of standard audit file approaches to reduce audit time. A Standard Audit File, as its name suggests, is a data file containing transaction elements that both a private and a tax auditor need to substantively test data using specialised audit software.

51. Standardisation of the data elements and their formats allows the same audit software routines to be used with many businesses and can provide benefits for both businesses and auditors (see paragraph 23.). It

[20] See GAP003 Risk Management and GAP004 Compliance Measurement

should however be recognised that the audit file approach does not obviate 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, *e.g.* retail or hotel booking systems.

The need for additional data requirements

52. It should be recognised that most of the transaction information data elements are already in place in most businesses as part of their existing accounting systems and processes, either for internal control reasons or to comply with domestic legal requirements. The approach of this guidance paper is therefore a minimalist one that aims to provide a pragmatic balance between the costs and burdens placed on business and the need for revenue authorities to establish that the correct tax has been declared. Additional data to that required for normal business practices should only be required where it is essential for good governance of tax systems.

53. Any additional data requirements would also need to comply with the neutrality principle. Neutrality is one of the fundamental principles for the taxation of e-commerce endorsed by the OECD at the 1998 Ottawa Ministerial conference. In the context of guidance on transaction information, neutrality is taken to mean the following:

- Guidelines on transaction information should be technologically neutral and should not inhibit the development of new and emerging technologies.
- There should be no effective additional burden placed on transaction information provided electronically to that provided on traditional paper documents, recognising that there may be different data elements necessary in an electronic environment to maintain the same overall level of integrity and auditability in the system[21].
- Information requirements should be the same for all businesses irrespective of trading sector or location. This does not prevent certain types of transactions that entail higher risk, such as those that may involve transfer pricing[22], from having appropriate and commensurate increases in documentation requirements.

Conclusions

54. A survey among OECD countries with respect to required data elements on invoices showed that certain data elements are required in most jurisdictions while others are country specific. On the basis of

---

21 For example: transactions involving the sale of digital products may require additional verification indicia. For Consumption tax purposes the customers identity and location are important in the taxing decision. There is an incentive for the customer to claim they are in an exemption category and / or that they are outside the taxing jurisdiction. These aspects are currently being analysed and recommendations on indicia should be complete by June 2003. At this stage it seems likely that the Customers IP number should be retained as part of the transaction set, given that high integrity electronic certificates are not commonly used in many jurisdictions.

22 For example a number of countries require the creation of contemporaneous transfer pricing documentation for cross jurisdictional related party or intra-party dealings. Transactions with tax havens may also lead to additional documentation requirements.

the survey, an initial list of data elements[23] has been made (see Annex 2) and definitions for each element given (see Annex 3).

55. This list of transaction data elements has been distilled down to the core transaction information set detailed in Annex 2. It is proposed that this list of data elements be promulgated to interested groups and that revenue authorities encourage their use as an acceptable basis for broadly meeting jurisdictional tax transaction information requirements on a global basis in an electronic commerce environment.

56. As with paper based systems, electronically transmitted transaction data that are required for tax purposes will in most cases require appropriate controls to prove their authenticity and integrity. These controls may be technological, *e.g.* electronic signatures, or they may be based on other approaches that may be agreed by tax authorities.

57. It is accepted that electronic documents can provide both tax and business auditors with the possibilities to achieve more efficient audit procedures. When coupled with the use of a standard audit file with transaction data elements that are agreed and accepted by all parties it provides the opportunity for businesses to reduce compliance costs and for tax and business auditors to gain greater efficiency in audit coverage and productivity.

58. The guidance in this paper aims to provide support for a win-win situation in which tax administrations can realise the increased efficiency and effectiveness of computer based auditing of electronic transaction information, and businesses benefit from lower costs of complying with differing transaction information requirements.

59. Ultimately, without steps to protect the viability and integrity of the taxation systems in an Internet environment, Governments may find it difficult to take forward the liberalisation of cross-border trade. Equally, for cross border e-commerce to achieve its potential, businesses require more consistent approaches between Governments. It is therefore critical that Governments, businesses and other interested parties work together to provide acceptable guidance to make the emerging global e-commerce market workable for all.

[23] These transaction data elements have been compared to those required by the EU invoicing directive, the data elements that were identified by the Professional Data Assessment TAG, a study by PricewaterhouseCoopers on behalf of the European Commission and the Working Party 9 report.

Guidance

1. **Revenue authorities *are encouraged to* work with relevant government regulatory agencies, business associations and other organizations, such as developers of accounting software and private auditors, to promulgate the common position, set out in annex 2 of this guidance paper, as a basis for:**

   - Ensuring that businesses engaged in e-commerce create, record and maintain appropriate transaction information,
   - Developing specifications for a standard audit file that meets the requirements of all parties

   in an electronic commerce environment[24].

2. **Revenue authorities *are encouraged to* work with relevant government regulatory agencies, business associations and other organizations, such as developers of accounting software and private auditors, to develop 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.**

3. **Revenue authorities should closely monitor developments in exchanging transaction information.**

[24] Including where records are created, recorded and/or maintained electronically.

History

April 2001: The FSM Electronic Commerce Sub-group forms a team to analyse the issue of transaction information further.

October 2002: 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

Privacy

- **Guidelines governing the protection of privacy and transborder flows of personal data**

OECD Council recommendation adopted 23 September 1980

- **Guidelines concerning computerized personal data files**

United Nations General Assembly adopted 14 December 1990

- **Convention for the protection of individuals with regard to automatic processing of personal data**

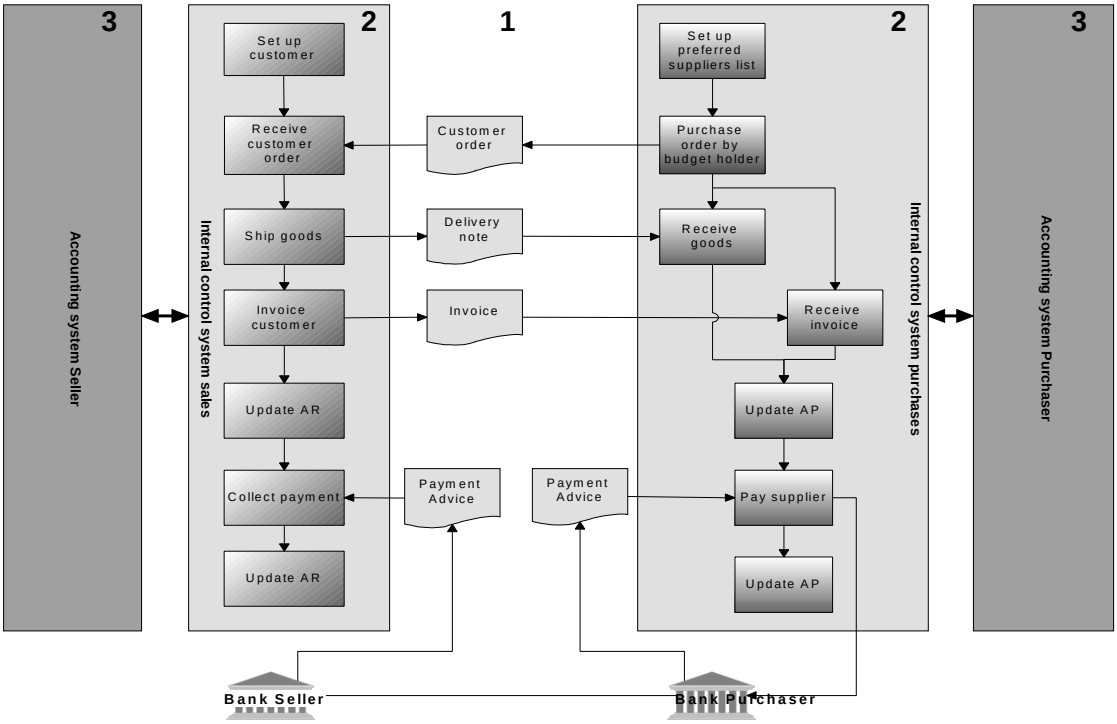
Council of Europe directive adopted 24 October 1995

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

ANNEX 1- EXAMPLE OF A GENERIC SALES AND PURCHASING SYSTEM FOR GOODS. HIGH LEVEL.

A purchaser and seller have to exchange information to accomplish a commercial transaction. In a traditional environment paper documents are often used to distribute this information whereas in an e-commerce environment this information is generally exchanged in an electronic format. The transaction information recorded on the documents must be sufficient to carry out adequate internal control. The documents, and the specific transaction information data on the documents, will naturally vary depending on the type of business and from business to business within an industry. Just as there is no standard internal control system, there is no unique set of control information. That said, there is often a high degree of commonality of the documents required for internal control purposes between businesses as shown in this figure.



There are three types of information that can be distinguished in a generic sale and purchasing system in relation to a transaction:

1. *The transmission information*. This is the information that is needed to exchange the actual transaction messages between the parties. In a traditional situation the messages are printed on paper and packed in a paper envelope. The messages are delivered by postal services or courier. In an e-commerce situation the actual messages are in electronic format and are generally sent via a network. Depending

on the network, specific network related ‘envelopes’ (packets) are used to transmit the messages between the parties. In order to guarantee the integrity and authenticity of the transmitted messages over the networks different techniques like electronic signatures can be used.

2. *The actual message*. In a generic sales and purchase transaction four types of documents are typically exchanged: customer order, delivery note, invoice and payment advice. These documents need to contain the data elements necessary for internal control purposes of both the seller and purchaser.

3. *The accounting system information*. This is the internally generated information that is recorded in the accounting system with respect to the transaction such as the general ledger code, cost centre account code and accounting period. The accounting system has to provide and maintain the audit trail for the transactions.

ANNEX 2 - COMMON TRANSACTION DATA ELEMENTS

As noted in Annex 1 there are three types of information in relation to a typical sale and purchase transaction:

1. Transmission information;
2. Actual message (source document) and
3. Accounting system information.

This annex describes the data elements for these three types of information.

Annex 1 described the four different source documents that can be distinguished in a typical sale and purchase transaction. The data elements that are commonly used on each separate document have been marked in separate columns. It should be noted that some of the marked data elements in the source documents listed may not be exchanged in some modern EDI and web enabled systems where the parties have an established trading relationship.

The data elements as described in this annex are identified as international best practice. However it should be noted that depending on the type of transaction and the jurisdictions involved other additional data elements may be required by law – particularly for invoices.

For example, the EU requires, besides the data elements as described in the invoice column, specific data elements in case of:

- intra-Community deliveries,
- margin scheme transactions, and
- the delivery of new vehicles.

This list of data elements is therefore not restrictive, but should be seen as the common denominator for international trade. The list may be used by messaging standards groups and software developers as the minimum set of data elements for electronic orders, delivery notes, invoices and payment advices.

The identified documents, or the data elements necessary to recreate them, have to be retained and maintained in accordance with the requirements as described in the TAG003 Record Keeping Guideline and any relevant laws.

It should be noted that in case of electronic documents the complete message, including transmission information, should be retained.

The list of data elements may also be used as a basis to describe a standard audit file as discussed in paragraph 50 and 51. Duplication of data elements should be avoided in the development of a standard audit file. It would only be necessary to hold one occurrence in the audit file if the same data is held in more than one of the four source documents listed.

Common transaction data elements - *Continued…*

Item No.	1. Transmission data elements	Document			
		Order	**Delivery Note**	**Invoice**	**Payment Advice**
1	IP Address of customer (if any – only the download IP address)				
2	Electronic signatures (if any)				
3	Electronic certificate (if any)				
4	Transmission date				
	2. Source document data elements				
5	Document name (e.g. Tax invoice, credit/debit note)			✓	
6	Document issue date	✓	✓	✓	✓
7	Document number (unique or sequential identifier)	✓	✓	✓	✓
8	Tax identification number of supplier			✓	
9	Supplier name and address	✓	✓	✓	✓
10	Tax identification number of customer			✓	
11	Customer name and address	✓	✓	✓	✓
12	Delivery Address (if different from customer address)		✓		
13	Description of goods and services	✓		✓	
14	Quantity of goods and services ordered or supplied	✓	✓	✓	
15	Date of supply of goods or completion of services		✓	✓	
16	Unit price for the unit/group of units			✓	
17	Tax Rate for unit/group of unit			✓	
18	Sub-total of price and tax for the unit or group of units			✓	
19	Total tax amount payable			✓	
20	Total sales value excluding tax			✓	
21	Total amount including tax			✓	
22	Tax exemption or reduction reason or rationale			✓	
23	Credit note reference (where applicable) to original invoice			✓	
24	Credit note reason or rationale			✓	
25	Settlement/Other Discount			✓	✓
26	Settlement amount				✓
27	Date settled				✓
28	Currency ($US, Euros, etc)	✓		✓	✓
29	Payment Mechanism				✓
	3. Accounting system information				
30	Tax Entity				
31	Accounting Period				
32	Posting status				
33	General Ledger and Cost Centre Account Codes				

General Notes:

1. The list above doesn't differentiate between header and item level detail.
2. Some data elements will not be required for non-significant transactions.
3. The above list includes some items that are country/region specific.

ANNEX 3 - DEFINITION OF EACH DATA ELEMENT

Item No.	Common Transaction Data Elements	**Definition** (Note: Not all elements will be applicable to every transaction or every jurisdiction)
	Transmission data elements	
1.	IP Address of customer	Internet Protocol number of customer when originating the transaction via the Internet
2.	Electronic signature (if any)	An electronic signature means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication[25].
3.	Electronic certificate (if any)	An (electronic) certificate is an electronic attestation, which links signature-verification-data (such as codes or public cryptographic keys) to a person and confirms the identity of that person[26].
4.	Transmission date	The date of the transmission over the network.
	Source document data elements	
5.	Document name (Tax invoice, credit/debit note)	The name of the document according to the requirements of the country where the issuing business is established.
6.	Document issue date	The date on which the document is issued/generated in the country where the issuing business is established.
7.	Document number	A unique number, which may be based on one or more series, which identifies the document.
8.	Tax identification number of supplier	The unique number (if any) allocated to the supplier by the tax administration.
9.	Supplier name and address	The name, full address, postal code, city and country of the supplier.
10.	Tax identification number of customer	The unique number (if any) allocated to the customer by the tax administration.
11.	Customer name and address	The name, full address, postal code, city and country of the recipient.
12.	Delivery Address	The address to which the delivery has been made.
13.	Description of goods and services	A description of the goods ordered, supplied or the services rendered. The description in plain text may be replaced by codes.
14.	Quantity of goods and services supplied	The quantity of the goods supplied or the extent of the services rendered.
15.	Date of supply of goods or completion of services	The date on which the supply of goods or of services was made or completed or the date on the payment on account was made, insofar as that date can be determined and differs from the date of issue of the document.
16.	Unit price for the unit/group of units	The unit/group of unit's price exclusive of tax and any discounts or rebates if they are not included in the unit/group of unit's price.

[25] Reference is made to article 2 (1) of the European Parliament and Council Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures.

[26] Reference is made to article 2 (9) of the European Parliament and Council Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures.

Item No.	Common Transaction Data Elements	**Definition** (Note: Not all elements will be applicable to every transaction or every jurisdiction)
	Source document data elements – *continued…*	
17.	Tax Rate for unit/group of unit	The tax rate applied for the unit/group of units
18.	Sub-total of price and tax for the unit or group of units	Sub-total of price and tax for the unit or group of units. The sub-total should be in the currency of the document.
19.	Total tax amount payable	The total tax amount payable in the currency of the document ($US, Euros, etc).
20.	Total sales value excluding tax	The total sales value excluding tax in the currency of the document.
21.	Total amount including tax	The total of the total of the sales value and the total tax amount payable in the currency of the document.
22.	Tax exemption or reduction reason or rationale	A clear description of the reason or rationale for any tax exemption or reduction granted.
23.	Credit note reference (where applicable) to original invoice	A clear reference or link to the number which uniquely identifies the original document.
24.	Credit note reason or rationale	A clear description of the reason or rationale for issuing a credit note.
25.	Settlement /Other Discount	A description of any settlement or other discount that can be effected when the payment is made.
26.	Settlement amount	The amount that has been settled and the currency of the amount.
27.	Date settled	The date on which the amount was settled.
28.	Currency	The currency of the amounts laid down in the document. ($US, Euros, etc)
29.	Payment mechanism	Whether settlement is made by cash or by some other payment mechanism.
	Accounting system information	
30.	Tax Entity	Company/Division/Branch reference
31.	Accounting Period	Business accounting period in which transaction posted to accounts
32.	Posting Status	Indicator that confirms transaction posted to accounts
33.	General Ledger and Cost Centre Account Codes	Codes used by the business to indicate category and ownership of transaction

General Notes:

1. The list above doesn't differentiate between header and item level detail.
2. Some data elements will not be required for non-significant transactions.
3. The above list includes some items that are country/region specific.

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.

60. 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.

61. 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.

62. 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.

63. 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

64. 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

65. 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

66. 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.

67. 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.

68. 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

69. 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

70. 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.

71. 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.

72. 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.

73. 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.

74. 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.

75. 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.

76. 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.

Centre for Tax Policy and Administration

Tax guidance series

Tax Administration Guidance – Electronic Payment Systems

Electronic Payment Systems – Accountability 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. The purpose of this paper is to encourage an appropriate level of accountability in electronic payment systems in a manner consistent with historical precedent so that taxpayers can continue to rely on data from these systems to substantiate their tax position. Revenue authorities also often use these systems to verify the taxes and charges due to Governments by a business. The inclusion of an appropriate level of accountability in electronic payment systems can reduce the need for costly 'after-market' adjustments to the systems of taxpayers including businesses, customers and payment system providers.

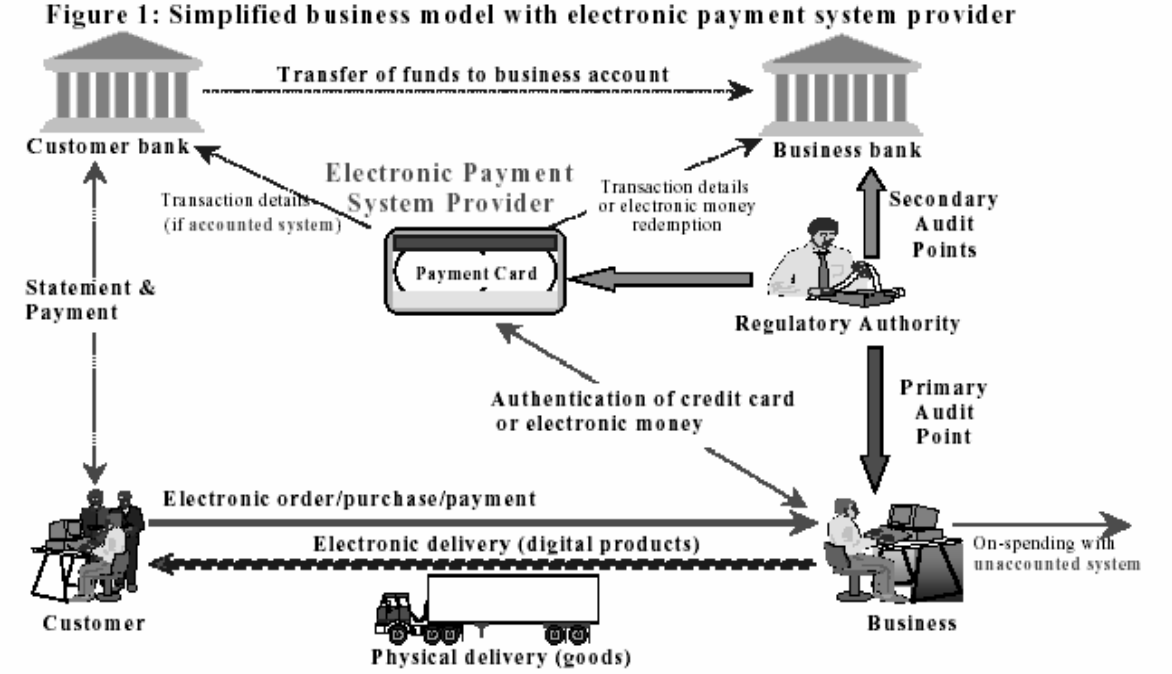
2. Accounted payment systems, based on double-entry record keeping principles, have provided both taxpayers and revenue authorities with a critical source of information to verify the accuracy of taxation liabilities for hundreds of years. With the development of electronic payment systems the need to verify taxation information has not diminished. As cross border electronic commerce becomes part of mainstream economic activity taxpayers and revenue authorities will have a continuing requirement to reliably access payment system information.

3. Many types of electronic payment systems have been proposed. Most however have fallen by the wayside and SSL enabled credit card transactions remains the major form of consumer payment mechanism over the Internet. While e-cash systems have proved largely unsuccessful and electronic payment systems based around credit and debit cards and EFT are the dominant mode for transfers of consumer value at present, new payment approaches continue to evolve and be proposed. (See: http://ntrg.cs.tcd.ie/mepeirce/project.html.)

4. In most instances the information recorded in electronic payment systems, although sometimes held outside a jurisdiction, generally provides an adequate and detailed audit trail. Indeed in many cases a transaction utilising an electronic payment system provides a better audit trail than a corresponding transaction involving physical cash.

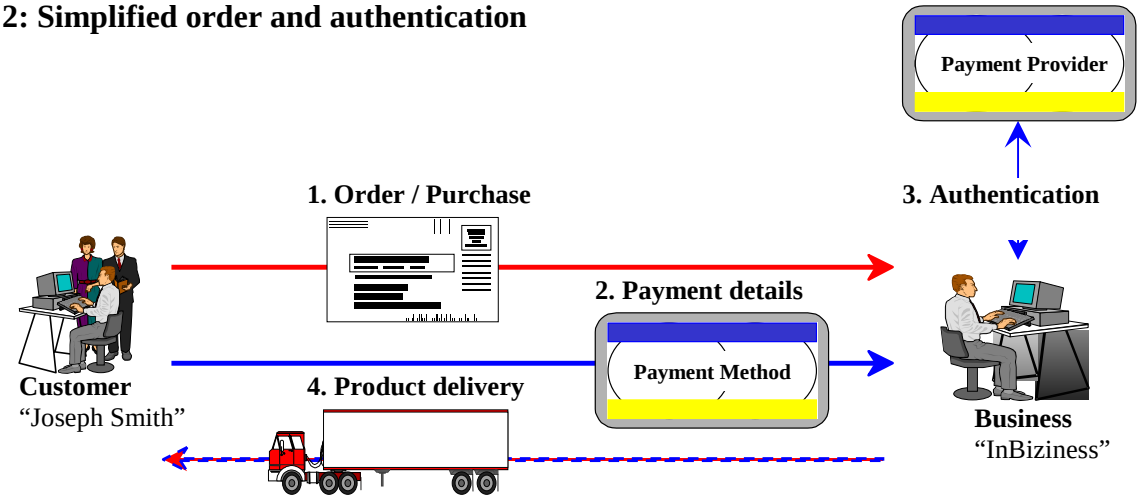
5. The following simplified business model, figure 1, can be used to illustrate the issues involved:

Figure 1: Simplified business model with electronic payment system provider



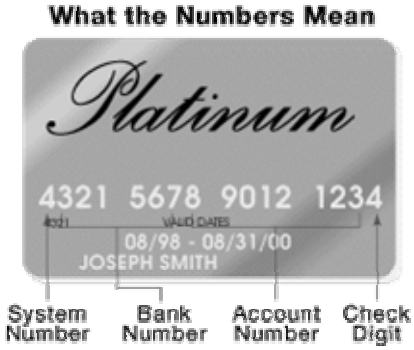
6. In this simplified model the Customer orders or purchases a product from the Business. The Business then authenticates the validity of the Customer's electronic payment. This authentication could range from a mere check of the validity of the 'form' of a credit card number through to an online real-time check of account details to the electronic payment system provider. The nature of this authentication check will generally vary according to the level of risk involved. Figure 2 shows the four basic steps involved.

Figure 2: Simplified order and authentication



7. The information about the transaction, held by the various parties involved, will vary according to the type of payment system used and its level of ***accountability***. A payment system that, in addition to the component amounts of the transaction, identifies both parties to the transaction is referred to in this paper as a '***fully accounted***' payment system. A payment system that identifies only the business undertaking the transaction is known in this paper as a '***semi-accounted***' payment system.

8. With a ***fully accounted*** system, such as payment by credit card, the Customer provides a card number to the Business as part of the order/purchasing process. The Business passes this information, together with their merchant ID and the amount of the transaction to the payment system provider. The credit card number contains enough information to enable the identification of the payment provider system (see diagram below *e.g.* System No. 4=Visa, 5=MasterCard, 37=AmEx *etc*), the Customer's bank and their account. The transaction information is passed to the Business's bank and the electronic payment system provider enabling the Customer's bank to transfer the value of the transaction to the Business's bank and debit the Customer's account. The Customer is sent a statement with the transaction details, amongst others, on a periodic basis, generally monthly. All such transactions received create third party audit trails with both the Business's and Customer's banks as well as the electronic payment provider and gives some assurance that such sales are recorded and will be reported by the Business. (Picture from http://www.howstuffworks.com/credit-card1.htm – see http://www.iso.ch/cate/3524015.html for relevant ISO standard details for card systems.)



9. With ***semi-accounted*** payment systems, such as Mondex (www.modex.com) the customer is not readily identifiable to the electronic payment provider or the Business. Instead information representing electronic money (digital tokens that the customer has previously purchased and stored on their smartcard or computer) is passed to the Business's system and the Business then authenticates and redeems (banks) these tokens via the payment provider. The customer in such a system can be anonymous while assurance is provided that all such sales are recorded and reported by the Business.

10. With an ***unaccounted*** payment system, such as eCash (www.eCash.com) neither the Customer nor the Business is necessarily identifiable to the payment system provider. The Business receiving the tokens representing electronic money can on-spend these without redeeming them through the payment system provider, leaving no third party audit trail. These payment systems are thus designed or configured so that significant transactions can be carried out with ***full anonymity*** of both parties. As both the Customer and the Business can remain anonymous this payment mechanism is most analogous to physical money – but at the same time its unique advantages over physical cash raise special concerns for law enforcement agencies and revenue authorities.

11. The following simplistic representation of payment system provider accounts may assist in highlighting the differences in accountability of the systems:

Fully Accounted Payment System Provider Record

Customer	Merchant
01/01: Joseph Smith: $100	01/01: InBizness: $100

In a fully accounted system, the payment system provider can identify both parties to the transaction.

Semi-accounted Payment System Provider Record

Customer	Merchant
09/12: purchase tokens: $100	
01/01: redeemed tokens: $100	01/01: InBizness: $100

In a semi-accounted system, the payment system provider can identify only the merchant involved in the transaction when the tokens are redeemed. The customer can purchase tokens anonymously using physical cash. The merchant cannot on-spend tokens.

Unaccounted Payment System Provider Record

Customer	Merchant
09/12: purchase tokens: $100	
	Merchant X 01/01: redeemed tokens: $100

In an unaccounted system, the payment system provider can identify only the merchant redeeming the tokens. The customer can purchase tokens anonymously using physical cash. The merchant can on-spend tokens anonymously.

Issues

12. ***Unaccounted*** electronic payment systems raise special concerns for revenue authorities because unlike physical cash such electronic payment systems allow for instantaneous transfers of significant value ***across***

jurisdictions in a manner that is undetectable for regulatory agencies. It is almost certain that unaccounted payment systems would facilitate money laundering. The risk that the perennial issue of the untaxed domestic cash economy becoming a global problem is a serious concern for revenue authorities and law enforcement agencies. In such a scenario even the secondary economic benefits of subsequent taxable transactions within the jurisdiction, arising from the spending of untaxed proceeds, is lost.

13. Legitimate ***personal privacy*** concerns are a major issue that need to be factored into electronic payment system design for the systems to be viable. Many jurisdictions have privacy legislation regarding this aspect that need to be taken into account and appropriate ***security*** and/or ***personal anonymity*** may need to be incorporated into the design of such systems to address this issue. Governments need to ensure that the mechanisms for maintaining personal privacy do not lead to a situation where taxes are unable to be calculated and collected on either the business (income taxes) or the consumer (consumption taxes).

14. It is noted that a clear distinction can be made between ***personal anonymity*** (where a private individual consumer is not identifiable) and ***business anonymity*** (where the business is not identifiable). Businesses hold themselves out to the world to conduct business and for direct taxation systems to work businesses cannot be anonymous. This is also true for indirect tax systems that use the business as a tax or information collection point. There is a strong synergy between ***consumer protection*** requirements regarding adequate business identification and the needs of revenue authorities in this regard.

15. Where the consumer is taxable and the business acts as the collection point for the tax, building it into the transaction, information on the ***consumer*** will generally only required to the extent necessary to identify the jurisdiction of the consumer for indirect tax purposes - ***where*** rather than ***who***. If the consumer seeks an exemption from, or credit of, taxation then more detailed information may be required so that the exemption could be given or the tax credit granted. If consumer self-assessment is adopted as the mechanism for the collection of consumption taxes by a jurisdiction then for verification purposes enough information to identify the Consumer (name, address, *etc.*) may be necessary.

16. Another set of issues concern the underlying cost of the transaction, an item that is significantly affected by the authentication procedures undertaken. ***Micro-payment*** systems (http://www.w3.org/ECommerce/Micropayments) are designed to operate on a pay-per-click basis as a means of generating sales revenue from digital products, such as photographs and text, where the costs associated with processing a credit card transaction would render the transaction otherwise unprofitable. An issue with unaccounted micro-payment systems is whether the Customer 'load' can be limited to a small amount per time period (*e.g.* <$100 per week). While micro-payment systems are designed for transactions of a few cents, without ***load limits*** the potential is there for significant transactions (or thousands of transactions adding up to a significant amount) to be undertaken. It should be noted that some micro-payment systems operate in a quasi-subscription mode with periodic Customer billing and are fully accounted.

17. A final issue for consideration is the reliance many taxpayers place on payment system provider records as a basis for completing and reconciling their own accounts. Electronic payment systems that do not provide such records could lead to a correspondingly lower level of adequate and accurate account keeping by taxpayers.

Proposal

18. Revenue authority and other law enforcement agency concerns regarding electronic payment systems would be greatly alleviated if such payment systems included an appropriate minimum level of accountability while at the same time meeting legitimate consumer needs for security and privacy.

19. To meet the expectations and needs of Government revenue authorities, the minimum standard of accountability appropriate for electronic payment systems is where the business undertaking the transaction is identifiable, the consumers jurisdiction (Country/State or Province) for taxation purposes is ascertained as well as the amount of the transaction. This equates to the information held in ***semi-accounted*** payment systems.

20. Concerns regarding ***unaccounted*** payment systems would be mitigated to some degree if such systems had ***load limits*** incorporated into their design so that significant transactions could not be carried out.

Guidance

1. **Revenue authorities *should* derive and promulgate a common position on the issue of electronic payment system accountability.**

2. **Revenue authorities *are encouraged to* raise the issue of electronic payment system accountability with relevant Government regulatory agencies.**

3. **Revenue authorities *may consider* suggesting to relevant government regulatory agencies that electronic payment systems should be at least semi-accounted in nature and/or that load limits for unaccounted systems should be adopted.**

4. **Revenue authorities *may consider* suggesting to electronic payment system developer's or other relevant parties that such payment systems should be at least semi-accounted in nature and/or that load limits for unaccounted systems should be adopted.**

5. **Revenue authorities *should* closely monitor developments in new electronic payment systems.**

History

1998: At the Ottawa "Electronic Commerce: A Borderless World" conference in October 1998 revenue authority concerns, about the adequacy and accuracy of business identification on the Internet, were explicitly expressed in the Ottawa Taxation Framework conditions:

"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."

From: Taxation Framework Conditions, Box 3 – Elements of a Taxation Framework,
http://www.oecd.org/daf/fa/E_COM/framewke.pdf

In an accompanying discussion paper released at the Ottawa conference these matters were developed further into implementation options for the taxation framework. Two of these implementation options foreshadow aspects of this paper on electronic payment system accountability. These are:

"Implementation Option 13

Revenue authorities should express their views to the appropriate bodies to ensure that features of electronic payment systems do not exacerbate the challenges associated with the cash economy

a) In conventional commerce, cash does not provide a very good audit trail and cash transactions are thought to account for a significant amount of the transactions that are untaxed in an economy. The tax not collected from the conventional "cash economy" is an enduring concern for Revenue authorities.

b) In the context of electronic commerce, cash-like electronic payment systems or unaccounted electronic payment systems, represent the same types of concerns as physical cash does in conventional commerce. However, unaccounted electronic payment systems raise additional concerns in that they can be used to conduct transactions over large distances, unlike physical cash, and they do not have the bulk of large quantities of physical cash, making the value easier to conceal.

c) While Revenue authorities do not have jurisdiction over the banking, finance and payment system sectors of the economy, they should express their views to the appropriate bodies to ensure that features of electronic payment systems do not exacerbate the challenges associated with the cash economy. For example, Revenue authorities might press the appropriate bodies to ensure that electronic payment system providers operate their systems in a way that enables the flows of funds to be properly accounted according to prevailing legislation. In addition, Revenue authorities may seek limits on the values attached to unaccounted electronic payment systems.

Nonetheless, while Revenue authorities have identified challenges to the reliability and verifiability of information, they also recognise that the electronic commerce environment offers the prospect of increased use of computerised accounting systems and the completeness, reliability and integrity of records associated with many of these systems.

…

Implementation Option 15

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."

From: *Electronic Commerce: A Discussion Paper on Taxation Issues,*
http://www.oecd.org/daf/fa/E_COM/discusse.pdf

April 2001: The FSM Electronic Commerce Sub-group forms a team to analyse the issue of electronic payment system accountability further. The team (*France, Denmark, Germany, Italy, Canada and the EC*) was asked to:

- Identify revenue authority Electronic Payment System requirements, including minimum levels of accountability, load limits etc
- Identify mechanisms and practices that could satisfy these requirements
- Formulate these requirements and practices into a guideline
- Identify parties to whom this guidelines should be promulgated (Including software developers, ISO, *etc.*)

September 2001: The FSM Electronic Commerce Sub-group accepts the draft subject to the inclusion of the additional guidance point:
"5. Revenue authorities *should* closely monitor developments in new electronic payment systems."

March 2002: 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

Privacy

- **Guidelines governing the protection of privacy and transborder flows of personal data**

OECD Council recommendation adopted 23 September 1980

- **Guidelines concerning computerized personal data files**

United Nations General Assembly adopted 14 December 1990

- **Convention for the protection of individuals with regard to automatic processing of personal data**
Council of Europe directive adopted 24 October 1995

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