TAX AND  COMMERCE  OECD

REPORT BY THE PROFESSIONAL DATA ASSESSMENT TECHNICAL ADVISORY GROUP (TAG)

December 2000

DRAFT FOR INFORMATION AND PUBLIC COMMENT*
Deadline: 30 April 2001

* Comments are invited on the proposals set out in this TAG report, particularly in the context of the Committee's own report on "Tax Administration Aspects of Electronic Commerce: Responding to the Challenges and Opportunities" (see <http://www.oecd.org/daf/fa> for a link to this report). To **comment on this TAG report,** please send an e-mail to: Mr. Jeffrey Owens, Head of Fiscal Affairs (daffa.contact@oecd.org) by 30 April 2001.

REPORT BY THE PROFESSIONAL DATA ASSESSMENT TECHNICAL ADVISORY GROUP (TAG)

TABLE OF CONTENTS

REPORT BY THE PROFESSIONAL DATA ASSESSMENT TECHNICAL ADVISORY GROUP (TAG)

I. Introduction and structure of report

1. In accordance with its specific mandate[1], on behalf of the members of the Professional Data Assessment Technical Advisory Group (PDA TAG), the Business and Government co-chairs of the TAG are pleased to submit the following report to the Chairperson of the Forum on Strategic Management Sub-group on Electronic Commerce for consideration by the members of the Sub-group.

2. This report synthesises the results of over 18 months worth of work by the representatives of both business and government who worked together on a range of issues drawn from the mandate of the PDA TAG. It concentrates on the key findings of the TAG, some of which have been condensed. These findings are set in a contextual narrative which has been designed to convey the deliberations of the representatives of the TAG with the minimum of technical language. Arising from its deliberations, the TAG has made eighteen recommendations and these are contained in Section X of the Report.

3. During the course of its eighteen month life, the TAG has either produced detailed papers on, or, achieved outputs in relation to the following:

a) Conducted an analysis of the audit risks associated with e-commerce trading highlighting, either extensions to traditional audit risks or, new risks arising.

b) A list of current or emerging standards or statements of best practice which are relevant for accessing electronic data or assessing its reliability.

c) Conducted, and reported on, a survey of private sector and public sector auditors, dealing with electronic records, seeking views on a variety of relevant issues.

d) Identified, and reported on, the desirable data elements for business and tax purposes, for use in trading, payment or transaction recording systems.

e) Catalogued existing or emerging mechanisms that could:

- Provide for authenticity and reliability of data.
- Facilitate “remote access” audits.
- Protect against or recover from, loss of encryption keys.

1. See Annex VIII for the Mandate, Composition of TAG, Workplan and Schedule of Meetings.

as well as reporting on the costs and benefits involved.

4. In order to give a full representation of the work of the TAG and to give a greater depth of technical discussion for specialised readers, this report is structured with a number of annexes which report in detail on the work carried out by the members of the TAG. Further annexes cover additional information such as the mandate, membership and workplan of the TAG.

II. Purpose, scope and methods of the PDA TAG

5. The purpose of the PDA TAG is to provide input into the OECD's work in taking forward the tax administration conditions, contained in Section V of the report, *Electronic Commerce: Taxation Framework Conditions*, which was welcomed by Ministers at an OECD Ministerial meeting in Ottawa, Canada in October 1998.

6. The role of the PDA TAG is advisory. The TAG's work is supervised by the Forum on Strategic Management which is the Committee on Fiscal Affairs (CFA) subsidiary body responsible for tax administration matters.

7. The purpose of the PDA TAG has been a subject of some debate between the members of the TAG and much confusion by people outside of the TAG. The name of the TAG - Professional Data Assessment - was intended to convey some information about the purpose, that the TAG was to report on data assessment as conducted by the professions - primarily the accounting and information technology professions.

8. The TAG was premised on the understanding that private sector external auditors had developed techniques and approaches to address audit issues in the Internet electronic commerce environment and that fiscal auditors should examine the private sector techniques for their suitability to fiscal audits to avoid conflicting expectations between fiscal auditors and other external auditors. At the first physical meeting of the TAG, private sector external auditors advised that the private sector did not yet have a "codified" approach to auditing in the Internet electronic commerce environment. The financial statement audit approaches for "dot-com" entities were primarily developed and performed on a "case-by-case" basis. The private sector external auditors were, however, very willing to explore the relevant audit and technology issues and their implications for auditing in an electronic commerce environment.

9. From this point it was possible to agree a refined purpose of the TAG; it would identify the audit risks posed by the Internet electronic commerce environment considering such matters as access to data, systems controls and the audit quality of the data and make recommendations based on the assessment of those risks and the available techniques and technology.

10. Some of the risks identified are not new. They have existed since accounting systems were first computerised. However it is worth restating these findings. Other risks are new, or have assumed different magnitudes due to some of the characteristics of Internet electronic commerce particularly the ability to more freely inter-connect systems.

11. There are also a number of important e-commerce issues, both in the general arena and specific matters relating to audit practices, which were deemed to be outside the mandate of the PDA TAG. Predominant among these is fraud: the TAG was not mandated to consider fraud issues.

12. In addition, while acknowledging the important role played by internal auditors, the area found to be of common knowledge and interest between the business and government representatives on the TAG was primarily external audit issues. These external issues were, however, confined to the data contained within an enterprise. In an audit of a business using paper based accounting systems, the auditor does not audit external infrastructure such as the postal system that delivers accounts payable and accounts receivable documents. Similarly, the members of the PDA TAG were not primarily concerned with addressing the risks associated with external infrastructure for business engaged in Internet electronic commerce. However, an auditor, in a paper-based environment may choose to rely on the date evidence contained in a post-mark so the PDA TAG representatives kept themselves informed about technologies and data outside of the enterprise where this external data may be of assistance in verifying the internal data of the enterprise.

13. Finally, the TAG was not fiscally focussed in that it did not concentrate on issues such as the deductibility or otherwise of the expenses associated with creating an Internet web site. Likewise the TAG was not concerned with issues such as the timing of revenue recognition. These issues are a matter of law, rules and interpretation in each country. What the TAG did concentrate on was ensuring that the data relating to the web site expense or revenue would be available, reliable and verifiable so that the laws, rules, standards and practices relating to such data could be adhered to and properly administered.

14. The TAG conducted its business principally through face to face meetings, some of which were joint meetings with other TAGs[2]. The TAG's own electronic discussion group (EDG) and Internet e-mail were also used extensively to further its deliberations. The establishment of teams (headed by a team leader) was successfully employed in progressing work on tasks.

III. Audit risks

15. Implicit in the general mandate of the PDA TAG is an understanding that there are risks which need to be managed by assessing data for "… authenticity, completeness, reliability and verifiability…". The specific mandate of the TAG echoes these areas of risk and charges the members of the TAG to collate and advise about relevant international audit or accounting standards and to advise on best practices to address the identified risks, particularly those that can reduce the burden on business during external audits.

16. The need to reduce the burden on business and the need to take into account the special considerations of small to medium sized businesses was an overlay to our work.

17. In analysing the risks in the Internet electronic commerce environment[3], it is important to distinguish why this environment is different. Remote selling by mail order, telephone or facsimile has been common in many countries for decades. Similarly, computerised accounting systems and electronic data interchange between businesses are not new concepts.

18. What is notable about the Internet electronic commerce environment is the convergence of these, and other, practices to create some unique characteristics.

---

2. Details of these meetings are contained in Annex VIII.

3. A more detailed analysis of the risks in the Internet electronic commerce environment is available in Annex I.

19. Mail order, facsimile and telephone order technologies are primarily concerned with the remote delivery of physical objects. Internet electronic commerce is not restricted in the same way. Mail, facsimile and telephone ordering systems operate on mature infrastructure platforms which give reasonably reliable information, for example, about the jurisdiction of the seller and or buyer and have, inbuilt audit evidence such as physical, dated post-marks or country specific telecommunication prefixes. The infrastructure platform for Internet electronic commerce is not as mature and does not offer such audit evidence as a matter of course.

20. Computerised accounting systems of the late 20th century are predominantly closed systems, operated within a business enterprise with data entry linked to physical documentation associated with a paper-based accounting system. Where computerised accounting systems are more open, with electronic linkages to external enterprises, these linkages have tended to conform to formal data structures such as UN/EDIFACT standard electronic data interchange (EDI) messages. The process of creating such standardised messages and the protocols around their use, have ensured that audit evidence is available where these systems are used. Further, their use has not been widespread and so the risks represented by any weakness in their audit evidence value was accordingly reduced.

21. Internet electronic commerce, which may change the magnitude of existing risks in an enterprise, may also present new risks. One example of a new risk is that the ability to do business in a wholly electronic environment via the Internet changes the nature of audit evidence and the reliability an auditor can place on that evidence. Another example is the increasing complexity of computer systems, including greater integration of business systems between partners. Furthermore, the increased numbers of smaller transactions in companies with B2C trading creates its own risks. The availability of counters to these risks varies according to the business model and, in the absence of any such counters, requires new or updated proportionate responses.

22. However, with the exception of the adoption of digital cash or unaccounted payment systems which may have adverse implications for reconciliation controls, audit risks are not necessarily constant for all business models and a number of variables were identified which need to be taken into consideration. The first variable was the presence or absence of internal controls. Typically, small businesses have less or weaker internal controls than large business and, broadly speaking, the risks associated with weak internal controls require more substantive testing. Another variable is the extent to which the technology itself provides assurance as to the reliability of electronic audit evidence. The other main variable was the emergence of new business models for Internet electronic commerce, which may contain different types of risk.

Findings

23. The use of electronic commerce via the Internet changes both the magnitude of existing risks in an enterprise, and also presents new risks.

24. Electronic documents from an external source may be, without additional measures, less reliable than their paper equivalents. The loss in reliability can be compensated to an extent by adequate internal controls that give audit assurance. However, some Small and Medium sized Enterprises may not have adequate internal controls and therefore the auditor cannot rely on their documentation when conducting an audit. This means that a systems approach and a substantive testing approach to the audit may be seriously compromised.

25. The emergence of new business models for e-commerce may also bring with it new risks according to the nature of the model.

26. The digital cash payment model, including unaccounted payment systems, may seriously inhibit the auditor's use of reconciliation techniques to agree sales and profit declarations.

IV. Data access

27. Prior to any assessment of data an auditor needs to have access to the data. The OECD paper, Electronic Commerce: A Discussion Paper on Taxation Issues, identified a risk that data might be stored in a jurisdiction other than that where a client was located. The specific mandate of the PDA TAG contemplated that it may be possible to remotely access data stored in a remote location.

28. There is very little practical experience with remote access of data for external audit purposes[4]. An analysis of the current technologies in relation to remote access to data, and a theoretical analysis of the benefits showed that remote access offers the client advantages in terms of time savings and greater convenience and that the auditor would also find greater convenience and potential cost savings through reduced travel and potential reduced audit time. However, allowing remote access to data reduces the ability of the auditor to conduct certain types of substantive tests, such as observation and there are concerns that it represents a security risk for the client.

29. As regards the potential security risk for the client, however, after conducting a survey, reviewing the information from a survey conducted by the Information Systems Audit and Control Association (ISACA) and reviewing existing standards it was considered that obtaining access to remotely stored data was not a key security risk, assuming the appropriate security measures were in place. However, survey sources and other research revealed concerns that remote access to data for audit purposes could compromise confidentiality.

30. Also under the heading of data access, the TAG considered the implications for auditors where businesses use encryption techniques for commercial reasons to ensure privacy, by keeping sensitive information from unintended viewers[5]. One potential impact for an auditor might arise where there is an unintentional or deliberate loss of encryption keys.

Findings

31. From published evidence, obtaining access to remotely stored data is not identified as a key security risk.

32. Remote access to data offers potential advantages to both the auditor and client. However these advantages will not be realised until the technology is much more mature.

---

4. A more detailed analysis of remote access in the Internet electronic commerce environment is available in Annex VI.

5. A more detailed analysis of key management and recovery mechanisms is contained in Annex VII.

33. There was a strong concern in the client community that allowing an auditor to access company data remotely via the web, could compromise confidentiality.

34. There is no evidence of significant widespread use of encryption of records for storage, retention or validation.

35. Current legislative record keeping requirements weighed against evidence of encryption use, would appear adequate in the short to medium term.

V. Internal control

36. As noted above, the PDA TAG had access to a wide range of material to assist it in determining risks in the Internet electronic commerce environment. One of the common themes to emerge from the collation and analysis of this material was that Internet electronic commerce systems had to have integrity, characterised as system processing which is complete, accurate, timely and verifiable.

37. It was also noted that a well-functioning Internet electronic commerce system could provide greater levels of integrity than a conventional paper-based system. The need to determine whether a particular Internet electronic commerce system was functioning well led to an analysis of systems or internal controls.

38. Testing of internal controls in a computerised accounting environment is not new. However, as noted above, the open system architecture of Internet electronic commerce presents some new challenges in that there may be reduced physical evidence (paper documents) to support electronic data entries. As a result, tests of internal control will need to be adapted to respond to the nature of Internet electronic commerce. Given that most testing of internal controls for conventional computerised accounting systems are conducted by auditors with additional information technology training and skills, we expect that testing internal controls in an Internet electronic commerce environment will require specialised skills.

39. In conjunction with an increased reliance on internal control evaluation, consideration was given as to whether technological solutions were available which would compensate for the reduced reliability associated with electronic records compared to their paper equivalents. Authenticity and reliability mechanisms such as encryption, message digests and time stamping were assessed in terms of their value for auditors and any costs associated in implementation by business[6].

Findings

40. Testing of internal controls in an Internet electronic commerce environment will require specialised training.

41. The market for technological solutions, which provide assurance as to data authenticity and integrity is immature at this time. However, time stamping was identified as giving some

6. A detailed paper on the available technologies which would support data authenticity and integrity is contained in Annex V.

assurance now. It, though, has a high cost and therefore it is used commercially only on a very limited basis for particular high value transactions.

42. In terms of authenticity and reliability of data you cannot rely on the emerging mechanisms alone. It will be necessary for auditors to hone their skills in terms of systems audit capability and to possibly adopt new audit techniques.

VI. Substantive tests

43. Where internal controls are weak, greater reliance must be placed on performing substantive testing and interpreting the results. Traditionally, smaller enterprises have had weaker internal controls than larger enterprises and there is no evidence that Internet electronic commerce will change this general tendency. In fact the trend identified by accounting firms was that they tend to make greater use of substantive tests in an Internet electronic commerce environment. By extrapolation then, external audits of smaller businesses engaged in Internet electronic commerce will tend to require more comprehensive substantive testing.

44. In conducting substantive tests, it is common for an external auditor to seek collaborating evidence to verify data contained in the records of an enterprise. This collaborating evidence may be obtained from a number of sources, including data from external sources, analysis of other internal data and inspection of physical evidence, such as inventory. One of the characteristics of Internet electronic commerce that distinguishes it from other forms of remote sales, like mail order, is the capacity to deliver an intangible or digital product. Where the inventory of an enterprise consists of digital products, which can be readily duplicated, substantive testing based on physical inspection is not possible.

45. As is mentioned above, another substantive test is to verify the data of the enterprise against external sources of data. In an Internet electronic commerce environment, the data from external sources may be electronic. The view of the PDA TAG is that external electronic data may be, without additional measures, less reliable than external physical data or documents. The convergence of an enterprise with weak internal controls and an electronic trading system that only provides external evidence in an electronic form represents an risk which was present prior to Internet electronic commerce but which has acquired new magnitude in the Internet electronic commerce environment because of the potential prevalence of this convergence. The combination of weak internal controls and less reliable external electronic data may require even more detailed substantive testing before an audit opinion can be formed. This finding is supported by the experience of accounting firms.

46. Because external electronic data may be, without additional measures, less reliable than external physical data, at any given level of internal control, more extensive substantive testing may be required where external data is electronic rather than physical.

47. Accounting firms indicated that they are making extensive use of file interrogation and data analysis software for substantive testing and also of computer assisted audit techniques. As noted above, however, substantive testing, particularly if performed on data stored on the system under examination, can be intrusive and costly to the client. In enterprises with good internal systems controls, the accounting firms are placing greater reliance on system control evaluation and less intrusive testing. Enterprises found to have weaker internal controls may be subject to more detailed substantive testing. SMEs are found to fall within this latter category with the result that businesses with the least capacity to absorb compliance costs may be subject to those costs.

48. As regards the question of minimising compliance costs when substantive testing is performed by fiscal auditors, and when audits are conducted generally, the TAG did not discuss this matter to any great degree but it was agreed that it was an area where, with co-operation from the developers of software packages used for e-commerce trading, progress in minimising such costs could possibly be made. It was also felt that this was a potential future work area for the TAG.

49. Finally, data in an Internet electronic commerce environment is more easily subject to analysis. Analysis of data in an active system can be intrusive and raises the potential risk of inadvertently corrupting actual accounting data. However, in conducting audits on computerised accounting systems, auditors would be familiar with obtaining a copy of the client data for analytical testing, in order to reduce the inconvenience to clients and to protect against corruption of the original data.

Findings

50. Audits of smaller businesses engaged in electronic commerce will tend to require more substantive testing than larger businesses with better internal controls.

51. More extensive substantive testing may be required where external data is electronic rather than physical.

52. Accounting firms indicated that they are making greater use of file interrogation and data analysis software and also of computer assisted audit techniques.

VII. Current auditing standards and guidelines

53. In addition to their own specialist knowledge, the TAG participants analysed published national and international accounting and auditing standards or guidance notes on electronic commerce[7], conducted a small survey of external and Government auditors engaged in audits of businesses carrying on Internet electronic commerce[8], approached the public accounting firms and had access to a more substantive survey conducted by the Information Systems Audit and Control Association (ISACA).

Findings

54. While there were limited numbers of standards specifically focussed on the electronic commerce environment, more standards will emerge over the next few years.

55. While audits have been conducted on electronic commerce operations, the level of experience of auditors in conducting such audits is low.

7. A detailed report on existing auditing standards and guidelines is contained in Annex II.

8. A summary of the results of the survey of auditors is contained in Annex III.

VIII. Approach to audits and auditor training and development

56. As is stated above, the level of experience which auditors have in conducting audits of Internet electronic commerce businesses is low at this point. However, the TAG considers that auditors, both private and public sector may need to re-think their audit methodology when faced with e-commerce audits. Auditors may make more extensive use of file interrogation and data analysis software and may adopt new techniques like querying electronic transactional log files. Fiscal auditors, in particular, may need to rely more heavily on a business' systems or internal controls. In order to be able to adapt to the potential changing nature of the audit, auditors will need to be re-skilled. They will also have to have sufficient knowledge to understand the e-commerce trading environment and the technological issues involved. In order to be able to perform effectively in the new environment, auditors will need appropriate additional training and development.

Findings

57. New audit techniques may have to be adopted by auditors in the absence of the traditional audit trail.

58. Auditors may have to place greater reliance on systems controls.

IX. Desirable data elements[9]

59. The vast majority of the work of the PDA TAG, covering risk and research into matters such as techniques to provide for authenticity and reliability of data was fundamental work that could be applied to any set of data in any system. However the members of the PDA TAG were conscious of dealing with Internet electronic commerce systems that support commercial transactions and the reliance, particularly of consumption tax, on transactional level data. Hence a particular practical stream of their work was to apply their expertise to the consideration of what data, from an audit perspective, would be desirable in Internet electronic commerce trading systems to assist the reliability of those systems.

60. The work on "desirable data elements" was not designed to specify minimum requirements. Rather, this work sought to summarise the generic elements of most tax systems and to cater for both direct and consumption taxes. Its purpose was to provide a specification of desirable data for a generic system.

61. In addition to providing that specification, the data elements would also appear to satisfy substantially, or fully, the vast majority of consumption tax system requirements for systems used by OECD member countries and so the data elements may be a useful addition to the knowledge-base of those parties considering simplifications to consumption tax systems.

X. Conclusions

62. Since its inception the PDA TAG has examined a wide range of issues in delivering on the terms of its mandate and workplan. However, the nature of Internet electronic commerce

9. The desirable data elements are outlined in full in Annex IV.

trading is that it is constantly evolving, with new business models and technologies pushing the boundaries of commerce out further, with consequences for the audit function as a result. In addition, at the time the TAG was conducting its work the Internet electronic commerce market was relatively immature. For these reasons, the TAG members are of the view that there are opportunities for further work in this area and they have sought to highlight a number of specific topics in this Report. Suggested future topics include:

a) Ongoing monitoring of developments in auditing standards, data assurance mechanisms and Internet e-commerce business models as well as considering the impact of these developments on the audit function.

b) Research into and, development of, future audit standards and methodologies.

c) Consideration of the implications of electronic data storage and retention as audit evidence.

d) Looking at opportunities to minimise compliance costs associated with Internet electronic commerce audits.

63. The members of the PDA TAG believe that the TAG process, with private sector external auditors and government auditors working together, is a suitable vehicle for continuing and building upon the work which is presented to you in this Report. The PDA TAG members urge the members of the FSM sub-group on e-commerce to recommend this proposal to the main Forum on Strategic Management and onwards to the Committee on Fiscal Affairs.

XI. Recommendations

64. Finally, arising from the deliberations of the PDA TAG, the following eighteen recommendations have been agreed by the TAG members:

Data access

1) There should be continued monitoring of remote access technologies by public sector and private sector auditors with a view to incorporating discussion of remote access into appropriate standards or training material.

2) In order to alleviate the concern that confidential data could be compromised, all relevant parties, including auditors and management, should be trained on best practices for e-commerce and web security, particularly regarding mechanisms to minimise the risks associated with accessing business data.

3) Businesses should be encouraged to use prudential systems for the management of encryption keys.

Internal control

4) In the context of Small and Medium sized Enterprises, tax administrations should work with software developers to encourage the incorporation of internal controls in their products for use in e-commerce trading.

5) Tax administrations should encourage the use of new assurance technologies such as time stamping on the grounds that its adoption can give greater assurance over the integrity of data when combined with other systems controls.

6) Tax administrations should also engage with software developers to encourage the adoption of time stamping technologies within their software design.

7) Tax administrations should encourage business to adopt strong authentication measures using technologies such as Public Key Infrastructure.

Substantive tests

8) In clients with good internal controls, fiscal auditors should consider placing greater reliance on the system controls and the use of less intrusive tests.

9) In clients with weak internal controls, fiscal auditors should examine the use of computer assisted audit techniques where these will give reasonable audit assurance at a reduced compliance cost to the client.

Current auditing standards and guidelines

10) Tax administrations should continue to monitor new standards from standard setting bodies, best practices from the private sector and any emerging protocols.

11) Tax administrations should provide input, as appropriate, to standard setting bodies and other relevant parties.

Approach to audits and auditor training and development

12) Public Sector and Private Sector auditors working in the electronic environment of e-commerce must be provided with the requisite training in order to understand that environment, to employ the correct computer-assisted audit tools and techniques, including web-based technologies and, to conduct systems audits.

13) Public Sector and Private Sector auditors need to be trained in data assurance mechanisms and understand what assurances these mechanisms provide in an audit context and they must also know how to audit the relevant mechanisms.

14) Consideration should be given by the OECD to conducting a further survey at some future stage to assess the level of experience of auditors in the e-commerce environment.

Desirable data elements

15) The list of desirable data elements should be provided to the appropriate fora considering Consumption Tax issues at the OECD and elsewhere, as an aid in the furtherance of their work.

16) The list of elements should be issued by the OECD in the form of an information or best practice note.

17) The list of elements should be refined and incorporated into a de facto protocol such as XML or other protocols.

18) Tax administrations should approach software developers and standards bodies with a view to ensuring that the list of elements is considered in the development of appropriate systems and standards.

ANNEX I

ELECTRONIC COMMERCE AUDIT RISKS

Introduction

1. IT auditors need to access and audit computerised accounting records produced by systems used for Internet-based electronic commerce (e-commerce) trading; in particular auditors from tax administrations need to audit these records in order to help protect the tax base of their respective countries. This is an important need within an environment that is growing, and is predicted by most commentators to continue to grow at a phenomenal rate.

2. The members of the Professional Data Assessment Technology Advisory Group (PDA TAG) have produced this analysis of the audit risks associated with e-commerce trading, noting these risks as being either extensions of existing risks from traditional business models or new risks; demonstrating how these may vary across business models; and attempting to catalogue possible audit solutions. The paper concentrates mainly on companies and individuals who comply with a requirement to register their business operation with the appropriate tax authorities; the identification by tax authorities of non-compliant e-businesses physically located within their jurisdictions and determining their liability to taxation is a fraud issue, and one which is outside the scope of the mandate of the PDA TAG. The PDA TAG recognises the latter scenario may also bring to the fore issues such as access to records which may be either encrypted or stored on an overseas server, or both.

3. When analysing the risks in e-commerce via the Internet it is necessary to examine why the environment is different from the established remote selling by mail order, fax or telephone that has been a common feature of business in many countries for decades. Also, the exchange of accounting information between computer systems via Electronic Data Interchange (EDI) is not a new concept. What is notable about e-commerce is the convergence of these and other practices to create some unique characteristics and inevitably, some new audit risks. For example, mail order, fax and telephone order technologies are primarily concerned with the remote delivery of physical goods, whereas e-commerce can incorporate the remote delivery of both physical and virtual goods (“digital goods”). Mail order, fax and telephone ordering systems operate on mature infrastructure platforms which give reasonably reliable information about such items as the jurisdiction of seller and purchaser, and have readily accessible audit evidence such as post marks and country-specific telecommunications prefixes. By contrast the infrastructure for Internet e-commerce is not as mature, and does not offer the auditor such reliable evidence as a matter of course.

Audit risks

4. External and tax administration auditors will need to obtain an understanding of the accounting and internal control systems in order to plan the audit, and develop an effective audit

approach. The auditor uses professional judgement to assess audit risk and to design audit procedures to ensure risk is reduced to an acceptably low level.

5. "Audit risk" is the risk that an auditor will give an inappropriate audit opinion in cases where the financial statements are materially misstated. The accepted view of audit risk is that it consists of three components: inherent risk, control risk and detection risk.

6. "Inherent risk" is the susceptibility of an account balance or class of transactions to a misstatement that could be material, either individually or when aggregated with misstatements in other balances or classes, assuming there were no related internal controls.

7. "Control risk" is the risk that misstatements that could occur in an account balance or class of transactions and that could be material individually or when aggregated with misstatements in other balances or classes, will not be prevented or detected on a timely basis by the internal control structure.

8. "Detection risk" is the risk that an auditor's substantive procedures will not detect a misstatement that exists in an account balance or class of transactions that could be material, individually or when aggregated with misstatements in other balances or classes.

9. E-commerce trading has an impact on all these three risk components. New e-commerce business models create new ways of doing business. These new models, closely bound up with the complexity of underlying transactions and other events, may create new risks. Integration of front end and legacy systems as well as business systems between trading partners (with an increasing dependence on internal controls in complex computer systems) may increase control risk; the provision of information from one party to another in order to process and record the transaction on that parties system may increase inherent risks; and greater numbers of smaller transactions in companies with B2C trading may increase control risks. Finally, doing business completely electronically can change the nature of audit evidence, which may increase detection risks.

10. In order to assess the audit risks the auditor needs to have sufficient knowledge to understand the e-commerce trading environment and, if required, the correct application of computer-assisted audit techniques as part of an overall audit programme

11. The ultimate objective of the IT auditor is to gain a satisfactory level of audit assurance from the system under examination. The manner in which this is achieved varies according to whether direct or indirect taxes are involved and the audit methodologies followed by individual tax administrations within their own jurisdiction. For example, some auditors may begin their examinations with the audited final accounts and scrutinise the reports produced by external auditors, drawing conclusions as to the level of internal controls exercised to inform the conduct of the audit; other auditors may take a more transaction-based approach by making use of the *audit trail* to verify the completeness, accuracy, authentication and timeliness of data; identifying the *internal controls* on data processing; and performing *compliance and substantive testing* on key controls and control weaknesses thus discovered. Common to these approaches is the need for access *to records* to perform the audit in terms of both accounting records and external audit reports; the level of access will vary according to the legal powers granted to tax administrations by their respective Governments.

12. The emergence of e-commerce trading provides a challenge for auditors who may have previously relied on audit trails based on paper with its inherent look, feel and authenticity and

are now faced with electronic trails containing data of increasing volume and complexity, which do not at first glance provide these comforts.

13. IT auditors will also have to pay particular attention to controls on security of access for systems connected to the Internet, particularly if third party access is allowed for trading purposes.

14. From the perspective of the tax administration auditor, the impact of any particular risk may vary according to whether direct or indirect taxation is involved, and in accordance with the regulatory requirements of the taxing jurisdiction. Tax administrations may also seek to increase their usage of exchange of information procedures under the terms of the double taxation convention where one party to the transaction is located in another jurisdiction.

Identified risks in e-commerce

15. Members of the PDA TAG have supplied the following examples of audit risks in Internet e-commerce trading, based on the auditing principles of completeness, accuracy, authentication and timeliness, and where possible have suggested actions that may be taken to counter these risks. It was recognised by the members at an early stage in the life of this paper that this would not be a complete catalogue of risks or counters due to the developing nature of much of e-commerce trading.

Completeness

16. An initial concern of an e-commerce audit will be to determine if transactions are being entered and recorded onto the system. As in any computer system auditors will be concerned with system information to prove completeness including the use of audit trails and log files.

17. The use of the Internet as a communications medium could increase the risk of transactions being lost or duplicated; an auditor, for business to business transactions at least, may consider it desirable to have access to the systems of both receiver and sender, possibly remotely, in order to check completeness. This particularly applies if customer or suppliers have the facility to access the system to create internal accounting documents. Examination of company records such as stock inventories may be suitable for trading in physical goods, but this check rapidly loses its effectiveness in instances of trading in digital goods or intangible services. There is no apparent relationship anymore between the costs of digital goods/services and the generated turnover. It may in any case be desirable to examine records held or maintained by third parties such as banks and credit card companies for both businesses to business and business to consumer transactions. This independent confirmation may be seriously inhibited by the adoption of the digital payment model, including unaccounted payment systems.

Accuracy

18. Auditors, in particular auditors from tax administrations, will be concerned with the correctness or other wise of any declaration in the records in relation to the location of a customer or supplier within or without a jurisdiction; and about the nature of the goods or services supplied. Such considerations are usually of interest to consumption tax auditors. A number of measures could be employed to check the accuracy of these records such as examination of address

information; credit card issuer information; reverse IP number checks, although it is recognised that the effectiveness of such checks is likely to vary.

Authentication

19. Checks on authentication are likely to centre around the transaction record and the parties to that record, *e.g.* is the electronic record genuine and has it been altered in any way; and are all parties to the transaction who they claim to be. Controls on authentication that may satisfy the auditor will include use of third party confirmations and technological solutions such as digital signatures and certificates.

Timeliness

20. The main concern with timeliness in e-commerce is to ensure that transactions are brought to account in the correct accounting period. An auditor would wish to examine system controls including any use of technologies such as timestamping. Techniques such as the use of computer assisted audit could be employed in order to attribute records to their correct accounting period and highlight any differences.

Trading relationships

21. The different types of relationships in e-commerce will contain different types of audit risks and counters to those risks. It is generally accepted that 80% of e-commerce transactions are business to business (B2B) and the remainder is business to consumer (B2C) and consumer to consumer (C2C). Businesses using EDI via the Internet are likely to have a mutual interest in obtaining audit information about the transaction. Also, their exchange of information is more likely to conform to formal data structures such as EDIFACT, and the use of these standard message formats and their associated protocols ensures that audit evidence is available when these are used.

22. The same cannot be said about B2C where a minimum exchange of information beyond payment details (usually credit card details) may be made between either party.

Business models

23. There are a number of established business models already in existence in e-commerce as shown in the following table which also identifies audit risks particular to each (based on audit concerns at seller and buyer). Tables 1 and 2 divide between physical goods and digital goods and services.

Table 1. Physical goods

Parties	Supply	Accounting	Stock inventory	Payment	Risks
Identify parties and their location	Identify what was supplied and when	How recorded in system? Should taxes be accounted for?	Reconcile goods supplied against stock records	Reconcile payments received to goods supplied	Identification & reconciliation controls should minimise risks.
Sellers will require a delivery address from their customers. Buyers will require an address for returns	Records should allow identification of goods	Third parties may be allowed access to system in order to complete transaction	Physical stock records will allow reconciliation of sales against stock	Payments may be received as digital cash or paid into online banks	E-commerce becomes essentially an ordering and payment medium: payments could be problematic.

Table 2. Digital goods/intangible services

Parties	Supply	Accounting	Stock Inventory	Payment	Risks
Identify parties and their location	Identify what was supplied and when	How recorded in system? Should taxes be accounted for?	Reconcile goods supplied against stock records	Reconcile payments received to goods supplied	Identification & reconciliation controls should minimise risks.
Sellers may require little information from customers beyond credit card details. Seller web sites may also contain little information about company. Both may claim to be located offshore.	Evidence of supply may be insufficient	Third parties may be allowed access to system in order to complete transaction May be difficult to determine exact nature of digital goods, and where buyer/seller located to determine tax liability.	No physical stock records to reconcile against	Payments may be received as digital cash or paid into online banks	Auditor cannot be sure of identity of parties; their location; what was supplied; whether tax should have been charged; what payment was received or made.

Emerging e-commerce business models

24. There are a number of new business models emerging in e-commerce trading which may pose audit risks by the very nature of their operation. PDA TAG members are of the view that in any case, until the business models become more widely used, any evaluation of risk should be performed on an individual basis. A number of examples are listed below.

Business models	**Risks**
Application service providers and application hosting	Internal controls are in the hands of a third party, which may be more difficult to get access to for audit purposes.
Data warehousing	If records are maintained off shore it may be more difficult for auditors to determine internal controls and gain access to data.
Bartering	Identifying that bartering transactions are taking place and then valuing them for tax purposes.
Online auctions	It may be difficult to identify that taxpayers have been engaged in transactions via online auctions. It is also difficult/impossible to examine the internal controls in respect of transactions conducted through online auctions as the system is run by a third party which may not even operate within the auditors jurisdiction. Auctions provide scope to suppress transactions and avoid tax.
Online shopping portals	A third party is collating order information and transmitting this to merchants to fulfil. It may be difficult to audit controls over the order taking and validations made regarding the jurisdiction of a consumer, particularly if supplies are made in digital format.
Web procurement and exchange sites	Companies collaborate to get economies of scale for procurement items. The companies specify what they want and suppliers make bids.
Enterprise resource planning	Software is configured by external consultants rather than by IT departments. The risk is lack of onsite knowledge of system.
Outsourcing	Controls may become remote from the principal. Access to programmers and documentation may be difficult for auditors.

Audit evidence

25. "Audit evidence" means the information obtained by the auditor in arriving at the conclusions on which the audit opinion is based. Audit evidence will comprise source documents and accounting records underlying the financial statements and corroborating information from other sources. Some tax administrations also require retention of records showing changes to system programs.

26. The external and tax administration auditor should obtain sufficient appropriate audit evidence to be able to draw reasonable conclusions on which to base the audit opinion**.** Audit evidence is obtained from an appropriate mix of tests of control and substantive procedures. In some circumstances, evidence may be obtained entirely from substantive procedures.

27. The reliability of audit evidence depends on:

- The nature of the audit evidence.
- The source of the audit evidence; and
- The effectiveness of the internal controls.

28. In addition, the three major categories of documentary audit evidence, which provide different degrees of reliability to the auditor, are:

a) Documentary audit evidence created and held by third parties.

b) Documentary audit evidence created by third parties and held by the entity; and

c) Documentary audit evidence created and held by the entity.

29. The documents in a traditional environment are paper based whereas the documents in an electronic commerce situation are more likely to be exclusively in an electronic format. Although documents from a source outside the audited company usually have a higher degree of credibility than internal documents, an electronic document from an external source may not be distinguished from internal documents, without additional measures to give it authenticity. The effectiveness of the internal controls determines the reliability. If the internal controls in an entity are adequate, the auditor can also qualify the external electronic documents as credible.

30. Small and medium-sized enterprises (SMEs) will form the majority of businesses in any country. Many internal controls that would be applied by large companies are not practical for SMEs. For example, in small businesses a few persons may have both operating and supervisory responsibilities and also perform accounting procedures; therefore segregation of duties may not occur or be severely limited. In circumstances where segregation of duties is limited and audit evidence of supervisory controls is lacking, the audit evidence necessary to support the auditor's opinion may have to be obtained entirely through the performance of substantive procedures or by reference to evidence held by other parties. However, in a situation where adequate internal controls are not in place the auditor may not be assured that external electronic documents are credible, and therefore cannot rely on this documentation when performing substantive tests. This means that both a systems approach and use of substantive testing may be seriously compromised.

31. The combination of a SME that sells digital goods/intangible services that are settled by an unaccounted payment system and electronic documents would mean that these businesses will become extremely difficult to audit effectively.

32. The expertise and judgement of the auditor when assessing the effect of internal controls is, of course, an important factor in establishing the credibility of the system and achieving audit assurance.

33. Tax administrations may need to consider action at an early stage to help mitigate the problems that may be encountered with SMEs initially by working with the developers of software packages marketed for use by SMEs trading in e-commerce, to encourage the placement of suitable internal controls in the data processing programs.

Additional skills required for auditors

34. Computer systems that handle e-commerce transactions may no longer produce paper audit trails, replacing them with wholly electronic versions that may contain significantly more data, one consequence being that the internal controls will become more software based. In the short term, some auditors may need to refer to computer audit specialists in order to fulfil their audit program on e-commerce systems; in the longer term, it is foreseen that auditors will need to develop a systematic approach to audit in an electronic environment, in particular by the application of computer-assisted audit techniques. The testing of system controls and data may also become more computer orientated through use of file interrogation techniques on data files and advanced sampling methods such as the application of Benford's Law[10].

10. Benford's Law is an audit technique that uses the natural distribution of digits to look for anomolies in data.

35. Auditors must also become more familiar with the underlying technologies of e-commerce and the Internet, especially where these become the basis of internal control mechanisms.

Approach to audit

36. The electronic commerce world is fast changing; financial statements will be less reliable predictors of the future and therefore the conduct of audits may have to change. Examples of suggested techniques include:

- *Continuous auditing* where software or integrated application controls on the client's system are used to keep the auditor updated online and in real-time with any exceptions or red flags occurring in the client's database. The PDA TAG is of the opinion that this may not be an appropriate technique for tax auditors in some jurisdictions.

- *Remote auditing* where the auditor enjoys remote access to a client system through a web browser.

- *Sampling in real time* when an auditor will arrange to visit a business on a pre-agreed number of occasions within a specified time period, each visit date selected at random and made without prior appointment. The auditor will then visit and perform the necessary checks and reconciliations.

- *Increased reliance on systems assurance methodologies* such as SysTrust which test system controls for reliability

- *Use of XML[11] and other emerging protocols* as a technology based approach to substantive testing. Auditors have used a technology-based approach for some time in this area, and the emergence of these protocols provides the opportunity to expand this approach and gain efficiencies.

Findings

37. The majority of audit risks in electronic commerce fall into two categories: extensions of existing risks from computerised accounting systems and additional risks from new technologies enabled through use of the Internet. The availability of counters to these risks varies according to the business model. For example, a company selling physical goods using e-commerce but only for accounting purposes and a company selling digital goods using e-commerce for both accounting purposes and as a delivery mechanism may have similar risks; however, in the first example the availability of mechanisms such as stock inventory controls would counter the risks; in the second example the wholly electronic nature of the business would provide no such counter. Therefore the greatest audit risks may be found in these providers of digital goods and services. Also, there is for the tax auditor the prospect when dealing with suppliers of digital goods and services of being unable to determine the nature of the supply and the tax jurisdiction of either buyer or seller; vital information in order to determine if any charges have been correctly applied.

38. The business models may also generate new risks. Both inherent and control risks can increase with the increased complexity of computer systems that enable integration of business systems between trading partners.

39. Common to all these models is the prospect of the digital payment model, including unaccounted payment systems that may seriously inhibit the auditor's use of reconciliation techniques to agree sales and profit declarations.

---

11. XML (Extensible Markup Language) is a flexible way to create common information formats and share both the format and the data on the World Wide Web, intranets, and elsewhere.

40. External electronic documents are, without additional measures, less reliable than their paper equivalents. The loss in reliability can be compensated to an extent by adequate internal controls that give audit assurance. In the particular case of SMEs, however, systems may not have the proper internal controls in place to qualify external documents as credible. Therefore, the auditor may not rely on the documentation when performing substantive tests. This means that both a systems approach and use of substantive testing is seriously compromised.

41. The impact of audit risks may vary for indirect and indirect taxes as well as from one tax administration to another.

42. In some instances where one party to a transaction is located in another jurisdiction, tax administrations may seek to increase their usage of exchange of information procedures under the terms of double taxation conventions.

43. Government and external auditors may seek to rely on systems assurance methodologies, such as SysTrust, which test systems reliability as well as substantive testing

44. While auditors have used a technology based approach for some time to perform substantive testing, XML and any other emerging protocols provide an opportunity to expand this approach and gain efficiencies.

Recommendations

45. Auditors working in the electronic environment of e-commerce must be able to employ the correct computer-assisted audit techniques and understand the technological issues around e-commerce trading. Insufficient knowledge in these areas is likely to contribute to increased audit risks.

46. In the context of SMEs, tax administrations should consider working with software developers to encourage the incorporation of internal controls into their products marketed for use in e-commerce trading.

47. Suitable technologies should be applied to electronic documents in order to ensure they possess at least the same level of authenticity and integrity as their paper equivalents.

ANNEX II

ELECTRONIC COMMERCE AUDIT STANDARDS AND PROTOCOLS

Task 1 – Report on Auditing Standards of Electronic Commerce

Contents

1. Outline of the task

1. In order to achieve its mandate the PDA TAG undertook research with regard to identifying current or emerging standards, or statements of best practice in determining the authenticity and reliability of electronic records. The following is Task 1 of the PDA TAG Work plan:

2. While private sector auditors can be either internal or external auditors, taxation auditors are external auditors. Given that, the TAG was created to help tax administrations address the challenges of electronic commerce, it will primarily have an external audit focus. However, external auditors must place appropriate reliance on internal audit controls and so, during the work of the TAG, participants may generate views on internal audit issues. In this context, the TAG will attempt to identify any new challenges posed by electronic data held by a taxpayer or client and created in an open Internet environment (as opposed to a closed EDI-type environment).

1) The TAG will compile a list of any current or emerging standards or statements of best practice or similar pronouncements which are relevant for

2) Accessing electronic data, books and records, authenticating them or assessing their reliability and extract the common or “best practice” elements if possible.

2. Summary of work undertaken

3. The TAG contacted the auditing standard setting bodies in several countries to determine whether or not there were standards either existing or emerging that was specific to auditing in an electronic environment. The TAG also contacted several international auditing firms to determine if the firms had specific auditing practices with regard to electronic commerce that were firm wide policy.

4. Auditing standard setting bodies were contacted in the following countries:

- Australia
- Canada
- France
- Germany
- Ireland
- Japan
- Netherlands
- New Zealand
- United Kingdom
- United States
- Hong Kong
- Malaysia
- Puerto Rico

5. In addition to the above countries, International Federation of Accountants (IFAC), Information Systems Audit and Control (ISACA) and the "Big 5" firms were contacted.

6. The reader should note that not every country responded to the request. After several attempts, the group's final correspondence asked for "negative assurance", i.e. if they did not respond otherwise, it was assumed that they did not have any specific guidance on auditing electronic commerce.

7. The reader should also note that while the TAG contacted a wide range of countries as well as organisations, there may have been some that are working in this area that were not uncovered through this task. In this regard, this paper is comprehensive but may not be all-inclusive with respect to current or emerging standards in the area of e-commerce.

8. This task was initially started in the summer of 1999, at that time there were very few organisations addressing the issues associated with auditing in an E-Business environment. During the course of this task, a few organisations have begun to address some of the issues. We expect that there will be more organisations addressing the issue subsequent to the completion of this report. In this regard, the reader should be cognisant that further guidance may have been developed after the publishing of this report.

3. Summary of countries/organisations with standards related to e-commerce

9. The following countries/organisations responded and either had specific standards on auditing e-commerce or related guidance:

- Australia: Statement AGS 1056 "Electronic Commerce: Audit Risk Assessments and Control Considerations".

- United States: AICPA currently developing a Risk Alert on Auditing E-commerce (WebTrust, SysTrust, XBRL).

- International: IFAC, ISACA

4. Australia statement AGS 1056 "Electronic commerce: audit risk assessments and control considerations"

10. The Auditing Guidance Statement (AGS 1056) has been issued by the Australian Accounting Research Foundation on behalf of CPA Australia and the Institute of Chartered

Accountants of Australia in order to provide guidance in this circumstance to address a new business environment affecting the profession as a whole.

11. The AGS 1056 is not mandatory and does not establish a new Auditing Standard. However it does provide guidance in relation to the application of existing Auditing Standards (the AUS Series).

12. AGS 1056 recognises that the use of a public network presents new aspects of risk that need to be addressed by an entity and considered by an auditor when planning an audit. In particular the increasing use of the Internet for e-commerce introduces new variables of risk, especially in relation to security. The new risks may expose the entity to systemic risks and thus may impact the auditor's assessment of audit risk. The nature and magnitude of the risks may vary with the size of the organisation.

13. The Guideline indicates the following are key audit areas affected, which the auditor should consider:

- Knowledge of the Business
- Use of an Expert
- Outsourcing Arrangements
- Risk Assessment
- Control Considerations

14. The Guideline highlights the impact e-commerce may have on the traditional business environment of the entity and suggests the auditor in the assessment of audit risk review the entity's e-commerce strategy, business model and skills of the entity's IT personnel. The auditor will have to understand the technology and /or use an expert to assist in this area.

15. The entity itself may not have the capacity to manage its e-commerce activities and may have outsourced the activity. In this case the auditor should assess the impact of the outsourcing arrangement on audit risk.

16. In assessing the risk of e-commerce to the entity, the auditor may consider the control framework in the IT strategy and the risk level to the entity's financial information security, completeness and reliability. The e-commerce business model should be reviewed to assess the adequacy of security and controls to ensure data integrity. In the new environment issues may arise in relation to the authenticity and integrity of transactions and trading partners, including the risk of transactional repudiation.

17. Control considerations are an area of potential risk in the new e-commerce environment. AGS 1056 recommends the adoption of an attitude of professional scepticism when considering the security controls used by the entity. Some issues may arise in relation to encryption risk and the authorisation and control of decryption keys, as a result of the dynamism of the environment and in relation to the need to maintain privacy over customer information. (For further information: http://www.aarf.asn.au)

5. AICPA risk alert

18. This Audit Risk Alert is under development and will be completed by 31 December 2000.

6. WebTrust

19. WebTrust is an attest level service performed on a companies' website by CPAs and CAs, or their international equivalent. It is focused primarily on protecting businesses and consumers. There are other seal programs in the marketplace that primarily focus on privacy. The rigor of these seal programs vary from seal to seal, with some being only the "sale" of the seal to others that require some form of substantiation with regard to business practices. None of the other seal programs that have been identified are based on a set of attestation level services provided by an independent auditor.

20. WebTrust has a modularized approach, so that a company may subscribe to one or several modules of WebTrust as follows:

- Privacy and Confidentiality
- Business Practices and Transaction Integrity
- Security
- Availability
- Non-Repudiation
- Customised Disclosures

21. There are two principals of WebTrust that have applicability to auditing in an e-commerce environment, specifically Business Practices and Transaction Integrity and Security. These two principals address the integrity of the data and the reliability of the data from a standpoint of security controls. The following are the definitions of each of these principals:*Business Practices and Transaction Integrity* - The enterprise discloses its business practices for electronic commerce, executes transactions in conformity with such practices, and maintains effective controls to provide reasonable assurance that electronic commerce transactions are processed completely, accurately and in conformity with its disclosed business practices.

With regard to Business Practices and Transaction Integrity, this principal is testing the integrity of the entire transaction; as part of that testing, there is a verification of the price and all other costs to the consumer including any applicable taxes. The specific criteria that deals with this includes the following:

The entity maintains controls to provide reasonable assurance that sales prices and all other costs/fees are displayed for the customer before processing the transaction

Customers have the option of printing, before an order is processed, an "order confirmation" on line for future verification with payment records (such as credit card statement) detailing all information of the order (such as item(s) ordered, sales prices, costs, sales taxes, shipping charges, and so on).

All costs, including taxes and shipping, and the currency used are displayed to the customer. Customer accepts an order, by clicking yes, before the order is processed.

All foreign exchange rates are displayed to the customer before performing a transaction involving foreign currency.

- *Security* - The enterprise discloses key security policies, complies with such security policies, and maintains effective controls to provide reasonable assurance that access to the electronic commerce system and data is restricted only to authorised individuals in conformity with its disclosed security policies.

Certain criteria under security deals in pertinent part with identification and authentication of authorised users, as follows:

The entity discloses its security practices for providing access to its electronic commerce system and data. Such disclosures should include practices for:

- Registration and authorisation of new users.
- Identification and authentication of authorised users.
- Maintaining and terminating authorised user access.

The illustrative examples outlined under this criteria include SSL and digital certificates of the consumer.

22. Supporting each one of these principals are specific criteria to determine whether the website successfully meets the principal as defined. The criteria to each one of these principals is very detailed and beyond the scope of this paper.

23. These WebTrust Modules are not yet released so we can not comment on how widely they will be employed in the commercial market place, so as to give greater assurance to tax auditors as to the integrity of the transaction and the security of the website. (For further information: http://www.aicpa.org)

7. SysTrust

24. The SysTrust service entails the public accountant providing an assurance service in which he or she evaluates and tests whether a system is reliable when measured against four essential reliability principles. A reliable system is one that is capable of operating without material error, fault, or failure during a specified period in a specified environment. The following four principles are used to evaluate whether a system is reliable:

1. *Availability:* The system is available for operation and use at times set forth in service-level statements or agreements.
2. *Security:* The system is protected against unauthorised physical and logical access.
3. *Integrity:* System processing is complete, accurate, timely, and authorised.
4. *Maintainability:* The system can be updated when required in a manner that continues to provide for system availability, security, and integrity.

25. Of the four principles outlined above, security and integrity are the most applicable to "auditing" in an e-commerce environment. The SysTrust methodology could be applied by revenue auditors on the taxpayers accounting and tax systems to determine the level of security as well as the integrity of the system. Using the SysTrust methodology, an auditor could determine the reliance that could be placed on the system by evaluating and testing the controls over the availability, security, integrity and maintainability of the system.

26. This methodology, however, moves away from substantive testing to a reliance on the systems. While most auditors are more comfortable relying on substantive testing, this becomes increasing more difficult as businesses move away from a paper environment. Transactions that once left a clear paper trail are increasing becoming automated and it is therefore, much more difficult to perform substantive testing (however, see comments below on XBRL technology). Systems that can meet the principals and criteria of SysTrust are highly reliable and auditors will be able to rely heavily on these systems. (For further information: http://www.aicpa.org)

8. Extensible business reporting language (XBRL)

27. XBRL is a standards-based method with which users can prepare, publish (in a variety of formats), exchange and analyze financial statements and the information they contain. XBRL is based on Extensible Markup Language (XML) which provides a tag for using and storing data. The power of the XML technology is that the data itself is tagged, such that virtually any application can identify "what" the data is and use it appropriately within its own application.

28. The following is an overview of XBRL:

- Freely licensed, permits the automatic exchange and reliable extraction of financial information across all software formats and technologies, including the Internet.
- Ultimately benefits all users of the financial information supply chain: public and private companies, the accounting profession, regulators, analysts, the investment community, capital markets and lenders, as well as key third parties such as software developers and data aggregators.
- Does not require a company to disclose any additional information beyond that which they normally disclose under existing accounting standards. Does not require a change to existing accounting standards.
- Improves access to financial information/speeds up access
- Reduces need to enter financial information more than one time, reducing the risk of data entry error and eliminating the need to manually key information for various formats, (printed financial statement, an HTML document for a company's Web site, an EDGAR filing document, a raw XML file or other specialised reporting formats such as credit reports and loan documents) thereby lowering a company's cost to prepare and distribute its financial statements while improving investor or analyst access to information.
- Leverages efficiencies of the Internet as today's primary source of financial information by making Web browser searches more accurate and relevant. (More than 80% of major US public companies provide some type of financial disclosure on the Internet.)
- XBRL meets the needs of today's investors and other users of financial information by providing accurate and reliable information to help them make informed financial decisions.

29. The implications of XML as it relates to auditing in an electronic environment will be significant. The data will be tagged so that it is easily transportable from one application to another. In terms of auditing this will allow an auditor to use his/her own application to test data regardless of the applications used by the taxpayer. Because each piece of data is tagged, the auditor will be able to run many queries against the data to determine the reliability and validity of the data. This type technology will allow auditors to perform more substantive testing with their own software.

30. The XML technology as it relates to financial reporting is still in its infancy stage. As this technology is further developed and becomes widely used within the business community, auditors will be able to test and manipulate financial records in a much more efficient and economical manner. (For further information: http://www.aicpa.org)

9. IFAC

31. IFAC's International Auditing Practice Committee (IAPC) has written a Discussion Paper on "Electronic Commerce and the Auditor". This paper has identified many of the risks that are either unique to e-commerce or exaggerated by e-commerce. The report concludes that at this stage it is early

to provide authoritative guidance, but that a best practices in dealing with these risks should evolve over time and these best practices should be utilised to address the risks that are associated with e-commerce. The report concludes:

32. "Electronic commerce, at its current stage of progress, raises a number of implications of potential impacts on both assessments of audit risk and audit procedures. However, in the evolution of e-com, progress will depend to a large extent on trial and error, therefore the risks might be large and outcomes unknown. At this stage auditors should be alerted as to the nature of potential risk, on a timely basis, rather than being provided with authoritative guidance giving best practice suggestions as to how to address those risks. "Best practice" solutions are likely to be more clearly identifiable within the next 12 months.

33. Therefore it is recommended that:

- Continuing developments arising from electronic commerce and its impact on the business environment should be monitored and reported to IAPC as necessary.

- An IAPS should be developed in the next 12 months to provide guidance on issues relating to electronic commerce which impact on an audit.

34. IAPC will be meeting in October 2000 to further discuss the issues of e-commerce and the auditor and is expected to issue a document outlining the E-Business risks from an audit perspective.

10. Information systems audit and control (ISACA)

35. ISACA has jointly published a document "E-commerce Security Enterprise Best Practices". As its title indicates this document has identified the best security practices employed by enterprises as they relate to e-commerce.

36. The following is a summary of the best practices that are most applicable to the issues of auditing in an e-commerce environment:

- There should be a set of security mechanisms and procedures which, taken together, constitute a security architecture for e-commerce.
- There should be measures in place to ensure the choice of the correct protocols for the application and the world, as well as the proper use and exploitation of their features and compensation for their limitations.
- There should be a mechanism in place to mediate between the public network (the Internet) and an organisation's private network.
- There should be a means to communicate across the Internet in a secure manner.
- There should be a process whereby participants in an e-commerce transaction can be uniquely and positively identified.
- There should be a mechanism by which the initiator of an e-commerce transaction can be uniquely associated with it.
- There should be an infrastructure to manage and control public key pairs and their corresponding certificates.
- There should be procedures in place to control changes to an e-commerce presence.
- E-commerce applications should maintain logs of their use, which should be monitored by responsible personnel.
- There should be features in an e-commerce application to reconstruct the activity performed by the application.
- There should be a regular program of audit and assessment of the security of e-commerce environments and applications to provide assurance that controls are present and effective.

(For further information: http://www.isaca.org)

11. Public accounting firms' best practices

37. The accounting firms at the time they were contacted did not have any firm wide policies regarding the auditing of e-commerce companies. They felt that codification of "best practices "in an e-commerce environment as something that, for the most part, is yet to come.

38. In those situations where high-volume e-commerce transactions are a very significant part of the business our transactions work tends to be more based on internal control evaluation and reliance, and on statistically-based and other analytical review procedures. Detailed transactional testing tends to become a less significant part of the audit. Auditors will need a lot more training in systems work in the future

39. Generally the firms make extensive use of file interrogation and other data analysis software for substantive testing. Usage of analytical testing is substantially higher in paperless e-commerce environments and audit software includes a "smart audit support" module that is used extensively to identify risks and design appropriate procedures. Some firms are currently updating the underlying knowledge-bases to encompass e-Business specific considerations, and believe that it will be an ongoing project. Additionally, there is a focus on the audit risk implications of stock market valuations and compensation systems that encourage dodgy revenue accounting, etc., but these are not essentially new issues. For statistical analytical, firms are using multiple regression analysis and other statistical techniques.

40. In practice, they do not yet encounter a significant number of issues introduced by e-commerce that are really new from an audit perspective. Most of what is encountered is an evolution and intensification of the issues that they have been dealing with in EDP-intensive environments for some years.

41. There will likely be a number of new audit issues that we will have to deal with as new authentication and identification techniques are adopted on a widespread basis (e.g., digital certificates), as new electronic payment systems become accepted (e.g., digital cash) and as products and services are increasingly digitised.

42. There was also a belief that new technologies (XML, for instance) and ubiquitous broadband connectivity will enable more efficient and effective audit methodologies and practices. The market will increasingly demand "continuous" reporting, and auditing techniques and technologies will evolve to deliver this based on the new connectivity. Embedded audit modules that spin off XML files, analytical tools that troll through and analyse publicly available information on the Web, and rich data sharing with clients through extranets are now all possible. But their full development and deployment lie mostly in the future.

43. The firms recognised that this area is likely to change very rapidly over the next few years, and will continue to change rapidly after that and recommend an ongoing mechanism for tax authorities to keep abreast of developments in the private sector.

12. Conclusions/recommendations

44. Due to the fact that the Internet is still in its infancy stage, the auditing techniques are currently evolving to address this new medium. However, there are technologies that have been developed and more that are currently in development that will assist auditors in auditing in the electronic world of the Internet.

45. Auditors, both government and financial statement auditors, will have to rely more heavily on a technology-based approach as paper trails diminish. A technology-based approach includes systems testing such as a SysTrust methodology which test systems reliability as well as substantive testing using a technology tool such as computerized testing of data. Auditors, whether they are using

substantive testing or testing of internal controls and systems, should leverage technology to make the audit more efficient and effective. While the electronic world poses new risks to auditors, it also presents new opportunities. Technology can be used to make the audit function more efficient and effective and it is important that auditors capitalise on these new opportunities.

46. While auditors have used a technology-based approach for some time to perform substantive testing, XML provides an opportunity to expand this approach and gain efficiencies. The strength of XML is that it is an international standard that is being adopted and incorporated in many systems. As XML technology expands and becomes more widely used, auditors should be able to leverage this technology to perform more substantive testing with their own software applications and with greater ease. The ability to perform substantive testing on an international scale with an independent application will give auditors a higher degree of certainty with regard to records they are auditing. First, they will be able to test transactions to ensure that the items were treated properly based on the "tag" of the data. Second, they will be able to perform more substantive testing then they could in a paper world because the process is automated. Third, because it is an international standard, they will be able to utilise this technology worldwide.

47. The public accounting firms indicated that they had not yet "codified" best practices. In the situations where high-volume e-commerce transactions are a very significant part of the business the transactions work tended to be based on internal control evaluation and reliance, and on statistically-based and other analytical review procedures. Detailed testing tended to become a less significant part of the audit. Further, they acknowledged that auditors will need a lot more training in systems work in the future. Additionally, the they reiterated that change is likely to occur very rapidly over the next few years, and will continue to change rapidly after that and recommend an ongoing mechanism for tax authorities to keep abreast of developments in the private sector.

48. This task was begun in the summer of 1999, at that point very few organisations had addressed either directly or indirectly the audit issues surrounding e-commerce. Over the past 18 months, several organisations have begun to address these issues, Australia Societies of CPAs, American Institute of CPAs, International Federation of Accountants, Information Systems Audit and Control and others. We expect that this trend will continue and that guidance will continually be developed and updated as the world of e-commerce, e-business and the Internet evolve. In this regard, the reader should note that this report is current as of October 2000 and other standards, guidance, etc. may have been developed after the release of this report.

49. The standards and technology dealing with auditing in an e-commerce environment are at their infancy stage. We expect that there will be much more information in terms of standards, best practices and technology that evolve over the next few years. In this regard, the TAG recommends that the standard setting bodies and various protocol consortiums be monitored over the next few years. Further, these bodies should be provided input, as appropriate, in their development of new standards and protocols.

ANNEX III

ELECTRONIC COMMERCE AUDIT SURVEY

PDA TAG workplan - purpose of task 2

1. It was agreed in the workplan of the PDA TAG that "The TAG will conduct a survey of public and private sector auditors, dealing with electronic commerce records, and report on any new opportunities, challenges, developments or practices relevant to accessibility, authenticity and reliability of data."

2. The purpose of the survey was to establish the extent to which respondents had experience of conducting audits of businesses engaged in electronic commerce and to explore the issues which had arisen as part of these audits. It was felt that such practical experiences would be very helpful in informing the work of the TAG.

Survey questionnaire and the methodology used in its circulation

3. The survey questionnaire (copy attached in Appendix I), consisting of twenty one focused questions was developed by the OECD Secretariat and certain members of the TAG. The wider TAG approved the final draft of the questionnaire.

4. Because the survey was primarily an information gathering exercise, it was agreed that as wide a circulation as possible was desirable. Relevant OECD member and non-member Governmental bodies were provided with copies of the questionnaire and national and international representative accounting bodies (including IFAC, ISACA, IIA, AICPA and ACPA) were also circulated. The diverse nature of the private sector membership of the PDA TAG facilitated a wide circulation. Lastly, the questionnaire was also posted to the OECD's electronic commerce public discussion site.

5. The questionnaire was circulated in mid-July 1999 and a period of ten weeks was provided for its completion and return (24 September 1999 was the final return date). The return of completed questionnaires was centralised with the OECD Secretariat in Paris.

Survey results - overview

6. A total of twenty two completed questionnaires were received. In addition, four written replies (where no questionnaire was completed) were also received. A breakdown of the source of the responses is attached in Appendix II.

7. It is not possible to provide statistics on the percentage sample which returned the questionnaire completed as the total number of questionnaires which issued was never quantified. However, it is understood that a wide coverage on the questionnaire was achieved. Given this coverage, the level of response received was disappointing. It was also clear that a number of the respondents had had very little exposure to the audit of e-commerce operations at the time of completing the questionnaire. Of the twenty two completed questionnaires received, only ten contained substantive replies.

Survey results - details

Questions 1 & 2 - How many audits of businesses engaged in electronic commerce have you or your organisation carried out.

8. Responses to this question were mixed, with most saying nil. One reply stated 110 audits. The average though was in single figures. A supplementary question on how many of the audits were "purely electronic" revealed that most were not purely electronic but involved an examination of some form of paper documents/records.

Question 3 - What special steps or approach would you take when auditing a business engaged in e-commerce versus a comparable one not engaged in e-commerce.

9. Although some said that there would not be a different approach to the audit of an e-commerce business as opposed to the audit of a conventional business, in the majority of replies the view was expressed that there would be a different approach. The audit would be more of a systems audit, with a greater emphasis being placed on examining the system controls. The robustness of systems integrity and security, in particular, would need to be evaluated more so than with conventional businesses.

Question 4 - Which standards do you find useful in auditing an e-commerce operation.

10. This question was principally of relevance to private sector auditors. Those who used auditing standards referred mainly to AICPA SAS 80 as well as in-house guidelines.

Questions 5, 6 & 7 - To what extent do you find that records and audit trails of e-commerce transactions are not being created, not being maintained over time or are lost because they are combined with audit trails of other transactions.

11. Most replies indicated some concerns about a loss of audit trail associated with these businesses. Sometimes an e-mail transmission constituted a record and this was not retained.

12. In some instances, records were only retained for a very short period of time. Some experienced the deletion of log files after a period of three months. Problems also arose where there was a change in technology, with a loss of records etc. which were stored on the old system.

13. Generally, businesses do not differentiate between the records of their traditional transactions and those relating to e-commerce transactions.

Questions 8 & 9 - How do you satisfy yourself that records and audit trails of e-commerce transactions have not been altered? Is your response based on reviews of system controls or substantive testing? To what extent do you find that records have been altered?

14. The tests carried out would consist primarily of an examination of system controls which includes conducting walk-through checks as well as follow-up substantive testing. Third party confirmations were also referred to.

15. There has not been much evidence of alterations to records. One reply described instances of alterations as being very occasional and never intentional.

Question 10 - To what extent do you find that records and audit trails of e-commerce transactions are being incorrectly transferred through into accounting systems?

16. Some instances of this occurring were indicated in the responses to this question. Auditors needed to carry out alternative checking to satisfy themselves on this matter.

Question 11 - To what extent do you find that records and audit trails of e-commerce transactions are inaccessible to auditors either through being stored remotely or through the effects of data security mechanisms?

17. The replies to this question reveal that concerns do exist that there will be problems with accessing the information which an auditor will want to conduct his/her business. One reply indicated that, form experience, it was a frequently occurring problem. Examples of the difficulties expected/encountered are:

- Use of third party service provider for retaining records.
- Records retained offshore.
- Use of technologies to "hide" data.
- Difficulties in tracing back to establish where in a client's system, particularly an in-house one, records are retained.

Question 12 - In your opinion, what are the minimum types of records that must be archived by the business which will allow auditors perform their function?

18. There was broad agreement in the answers to this question. The same level of detail as "bricks and mortar" businesses was required but some also felt that log files and e-mails should be retained. Basically any document, be it electronic or paper, which supports details of the business transactions. One suggestion was that CD ROM should be used to store archived records as this cannot be altered subsequently.

Question 13 - What issues and problems have you faced in practice when carrying out audits of businesses engaged in e-commerce?

19. A number of different issues were mentioned under this question:

- Lack of experience in keeping records/poor records and increased use of "home-grown" systems.
- Manual input of data to e-commerce systems increased risks of error.
- Lack of internal controls within SMEs.
- Difficulty in getting initial transaction data.
- Relevant data not being retained, *e.g.* log files.

Question 14 - What issues and problems do you anticipate arising in the future when carrying out audits of businesses engaged in e-commerce?

20. Again a wide variety of responses was received on this one:-

- The audit of digital goods.
- Need for clear guidance to taxpayers as to what they should retain
- Increased exposure to international operations with different record requirements.
- Lack of clear audit trails.
- New technologies and changing technologies.
- New techniques developing to assist the under-reporting of income and new tax avoidance schemes being created.
- Lack of technical knowledge on the part of auditors.

Question 15 - How do the problems of auditing SMEs differ from the audit of large businesses?

21. Some felt that there would be no real difference but the majority expressed the view that there would. In particular, the absence of internal controls means that the audit approach will be different. Smaller IT budget which SMEs have means less reliable systems and lack of security controls.

Question 16 - What specific approaches, solutions, methods, procedures or techniques have you developed to assist in the audit of businesses engaged in e-commerce?

22. The replies to this question divided manly into two types. One type of response indicated that the approach was still developing, while the second type of response suggested that the same procedures would be used as those followed in conventional businesses audits. Other replies included:-

- The use of real-time audits.
- Review, evaluate and test the control, integrity and security procedures incorporated in e-commerce software packages and likewise, for the value added network provider's system.

Question 17 - To what extent do the new approaches, solutions etc. that you have devised cause additional problems or concerns that would not otherwise have occurred?

23. Based on the previous question only a few replies were received on this point. Consistent comments were that auditors would need to re-skilled to have an understanding of how the system works and audit methods and approaches would need to be regularly reviewed to ensure that they did not become obsolete.

24. In addition, the reaction to the introduction of real-time audits was described as being positively received.

Question 18 - Generally, tax administrations do not use confirmation letters as part of their audit approach. Please suggest any techniques, methods etc. that tax administrations might employ that do not involve third party communications.

25. The types of alternatives suggested here were:

- Analysing the content of system log files and tracing transactions through the system.
- Examining the potential for new technologies to provide assurance about the system.
- The development of applications which could be used to interrogate systems.

Question 19 - What approaches, solutions etc. do you anticipate might help in the future when auditing businesses engaged in e-commerce?

26. A broad range of answers was supplied in response to this question. A number of respondents commented that there would have to be a greater reliance on continuous auditing. Technological developments might also assist the work of the auditor, *e.g.* digital signatures. Other examples included:-

- Greater use of IT specialists and development of auditors' IT skills.
- Significant emphasis was placed on Governments publishing data recordation requirements for e-comm businesses.
- Greater use of lifestyle checks.

Question 20 - How do the solutions, methods etc. you devised to assist in auditing SMEs engaged in electronic commerce differ from auditing the systems of larger national and international companies?

27. Some were of the view that no differences were anticipated, while others felt that there would need to be more substantive testing in the case of SMEs where controls were inadequate. The view was expressed that the SME will require greater education as to what is required because larger entities can get the advice from their auditors/accountants.

Question 21 - Do you feel that there are differences in business-to-business e-commerce compared with business-to-consumer e-commerce that would warrant different audit considerations and if so, what are the considerations?

28. The main differences were described as being transaction volume and transaction value as well as controls. B2B will have fewer transactions but larger values. It is likely that in B2B transactions the supplier will be able to agree certain contractual arrangements in advance with the customer, like encryption but this will not be possible with B2C. B2C is also likely to have a higher level of supplies of digital goods.

29. Some felt that B2B would be easier to audit than B2C while others commented that B2B had its own special problems like transfer pricing concerns. Also it is perhaps easier to identify who is doing B2C by simply looking at the internet.

30. The absence of controls in B2C meant that there was more likely to be increased work involved. Third party confirmations would be easier to carry out in the B2B space and cross-checking of records is easier also.

Conclusions and recommendations

31. At the time the survey was conducted, it is now apparent, for most of the respondents, it was the very early stages of the development of theirs, and their organisation's, knowledge of the internet and, some had little or no experience of auditing in an e-commerce environment. However, as an exercise, while it did not provide the TAG with new opportunities or practices relevant to accessibility, authenticity or reliability of data, it did serve as an important confirmation at the time that the TAG's workplan sought to address the main areas where issues were likely to emerge.

32. It should be noted that a survey which covered similar topics to the one conducted by the TAG was carried out by the Information Systems Audit and Control Association (ISACA). It is also re-assuring for the TAG that the findings in the ISACA survey are consistent with those of the TAG's survey. Appendix III provides some examples of the types of response received on two key topics. The TAG is grateful to ISACA for permission to reproduce this information.

33. The TAG recommends that, at this stage of the development of the expertise of auditors in relation to electronic commerce, there would be merit in conducting a further survey to establish at a future point what the views of auditors would be to the issues raised in the original questionnaire.

ANNEX IV

DESIRABLE DATA ELEMENTS

Task 3 - Desirable Data Elements

Contents

1. Outline of Task 3

1. The TAG will attempt to identify and report upon the desirable data elements for business and tax purposes, expected in accountable trading, payment or transaction recording systems.

2. (Covers CT letter, p15, para 31 dot 3, dot 4, dot 7 - partly and context setting work that will help us with Implementation Option 13 and 15).

3. This work examined the development of a set of desirable data elements that can be used for all transactions (B2G, B2B and B2C) in the electronic commerce environment. The elements will encompass a common set of elements for inclusion on order, delivery, invoice and payment documents that are normally generated during a transaction.

2. Summary of work undertaken

4. A detailed and wide-ranging discussion has taken place within the TAG on the issue of desirable data elements and much is contained on the EDG. Arising out of this discussion several points of focus became apparent for the TAG. These are:

- Neutrality.
- Need to be aware of leveraging invoice issues through business and not making it tax driven.
- The outcome should not be based purely on Revenue expectations.
- The outcome should be protocol independent.
- Once finalised this needs to be communicated to the Technology TAG for further dissemination.

3. Data elements

5. After much discussion the TAG agreed that expressing the desirable elements in header/detail terms would be the best outcome.

- The header would contain overall information about the transaction, and
- The detail could then handle the problem of multiple tax rates.

6. The mandatory/optional element would then come into effect if the transmission was for goods or services only as some of the elements would not necessarily apply, particularly for services.

7. The specification as proposed by the PDA TAG are at appendix 1 and contains details for Order, Delivery, Invoice and Payment transactions.

4. Desirable data elements

8. The following elements have been defined by the team working on this issue. As mentioned previously four key documents have been considered.

9. The column on the right hand side of the table below notes the origin of the information for each of the documents.

Order form			
	Order Number:	This would be a sequential number generated by the supplier. It is used for audit trail purposes	Auto
	Order Date	The date the order was received by the supplier	Auto
	Customer Name	Name of the customer	Customer
	Customer Address	Customer's address	Customer
Order detail			
	Description	This would be a description of the products, including where applicable sufficient information to determine if it is subject to taxation and the applicable tax rate.	Catalogue
	Stock Reference	As for description	Catalogue
	Quantity ordered	Number of items ordered by the customer	Customer
	Weight	weight of the items (where applicable)	Catalogue
	Unit of measure	kilograms or pounds	Supplier

Delivery note			
	Delivery note number	This would be a sequential number generated by the supplier. It is used for audit trail purposes	Auto
	Order number	See order form	Order form
	Delivery date	Date items were delivered/dispatched	Auto
	Ship to address	Address customer nominated for delivery, this can be important where the customer's address is not the delivery address.	Order form
	Carrier	Method of shipment or courier used	Supplier/
Delivery detail			
	Description	This would be a description of the products, including where applicable sufficient information to determine if it is subject to taxation and the applicable tax rate.	Order form
	Stock Reference	As for description	Order form
	Quantity delivered	Number of items delivered by the supplier. This is important if this is a different to the amount ordered by the customer	Supplier
	Weight	Weight of the items (where applicable)	Order form
	Unit of measure	Kilograms or pounds	Order form

Invoice			
	Document Title	'invoice' or 'tax invoice' or 'receipt' - will depend on local requirements	Auto
	Invoice Number	This would be a sequential number generated by the supplier. It is used for audit trail purposes	Auto
	Invoice Date	Date of the invoice	Auto
	Supplier name	Name of the supplier	Supplier
	Supplier address	Suppliers address	Supplier
	Tax identifier	TIN, or other identifier where required by law	Supplier
	Invoice Name and	Customers name and address	Order form
	Settlement discount	Discount for early payment	Supplier
	Other discount	Any other discounts	Supplier
	Total tax value	Value subject to taxation where discounts must be taken into account	Supplier
	Total value		Supplier
Invoice detail			
	Description	This would be a description of the products, including where applicable sufficient information to determine if it is subject to taxation and the applicable tax rate.	Order form
	Stock Reference	As for description	Order form
	Quantity invoiced	Number of items invoiced/delivered to the customer	Delivery note
	Tax rate	Rate of consumption or other tax applicable to the items	Supplier
	Unit cost		Supplier
	Delivery note number	From the delivery note	Delivery note
	Order number	From the order form	Order form

Payment note			
	Payment reference	This would be a sequential number generated by the supplier. It is used for audit trail purposes	Auto
	Payment date	Date that payment was received	Auto
	Invoice number	From the invoice	Invoice
	Payment amount	Total amount tendered by the customer	Supplier
	Payment method	Credit card, cheque, direct debit etc	Supplier

Other studies

10. On 23 August 1999, PriceWaterhouseCoopers released:

'Study on the requirements imposed by the Member States, for the purpose of charging taxes, for invoices produced by electronic or other means' for the European Commission DG XXI.

11. A copy of this report is available at: http://www.europa.eu.int/comm/taxation_customs/publications/reports_studies/taxation/final_report_pwc.pdf

12. This report looked at the invoice requirements for the European Union Member country VAT/CT regimes and proposed a list of required invoice elements. The report is detailed and involved the use of questionnaires directed to EU businesses seeking comments on invoices and their content in a variety of situations (EDI, E-mail and electronic invoicing).

13. As a result of this work the following list of items was considered.

- Date of issue.
- Sequential numbering.
- Identity of supplier.
- Identify of customer.
- Description of the good or services.
- Date of supply of goods or completion of service.
- Taxable amount per rate.
- VAT amount.
- VAT rate.

14. In its final recommendation, of the above elements only the VAT amount field was not proposed as a compulsory element for an invoice.

15. A comparison of the proposed desirable data elements and the PWC report's conclusions is contained in Table 1 below.

Table 1. Comparison of proposed desirable data elements and the PWC report's conclusions

Desirable Data Elements	PWC Report
Document Title	
Invoice Number	Sequential numbering
Invoice Date	Date of issue
Supplier name	Identity of supplier
Supplier address	Identity of supplier
Tax identifier	Identity of supplier
Invoice Name and Address	Identity of customer
Settlement discount	Taxable amount per rate
Other discount	Taxable amount per rate
Total tax value	
Total value	
Description	Description of goods or services
Stock Reference	Description of goods or services
Quantity invoiced	Description of goods or services
Tax rate	VAT Rate
Unit cost	
Delivery Address	
Delivery note number	
Order number	

16. One element included in the PWC study and not contained in the desirable data elements is a 'Date of supply of goods or completion of service' field.

17. Of the additional elements specified in the Desirable data elements, Total value and total tax value have not been included in the PWC report. PWC conclude that since both of these fields are 'merely the result of a purely arithmetical calculation of ... compulsory statements on the invoice…'. They need not be stated in the list of compulsory items.

18. The other additional elements (document title, unit cost, delivery note number and order number) have not been considered by the PWC report. These items are considered to add value from an audit perspective to the document, making the document more robust. Of these additional items most would be included as a 'matter of course' in business documents due to requirements of the order processing or accounting systems in use.

5. Exchange of views with Working Party No. 9 on Consumption Taxes

19. After the commencement of this task an exchange of views has taken place with the WP9 Sub-group on Electronic Commerce given the importance of the subject for the purposes of consumption taxation.

20. Looking more specifically at the information contained on invoices there were no major differences between the WP9 Sub-group's position and that of the PDA TAG.

21. The WP9 Sub-group favoured the exclusion of a number of 'non-core' elements. The PDA TAG agreed that the minimalist approach is desirable in reducing the requirements on business.

22. However, the TAG agreed that by including a limited number of additional items the need for additional country specific modules would be significantly lessened. The reduced need to use country specific modules would outweigh the cost of the additional fields.

23. The WP9 Sub-group suggested the following elements as core elements:

- The identity of the supplier (identification number or if not available name and address).
- The identity of the customer (name, address and identification number, including a country identifier).
- The date of issuance of the invoice.
- A sequential number.
- A description of the goods or services.
- Taxable amount per rate.
- Tax rate.
- Tax charged.

24. A number of non-core elements were also suggested:

- Transmission date.
- Quantity.
- Unit costs.
- Calculation of taxation.

6. Feedback from the technology TAG and further analysis

25. At a joint meeting of the PDA and Technology TAGs feedback was received from various Business participants on the issue of Desirable Data Elements. Included below are some of the comments received.

26. Strong feedback was received on the 'nature' of the document. Concerns were expressed that the document would become a requirement for electronic commerce business.

27. At no stage is it anticipated that this document will become a 'requirement'. This is a list of ***desirable data elements*** and should be seen as a guide to ***international best practice***.

28. It should also be noted that in many jurisdictions revenue or taxation law requires that invoices and other specified documents be prepared and contain a mandated minimum amount of information. The work on desirable data elements is not seeking to impose a new requirement but an attempt to find a consistent treatment for a common, existing requirement, to facilitate electronic commerce.

29. This paper has to cover a variety of situations, B2B, B2C and B2G. Feedback indicated that for B2B the elements would be satisfactory. The use of this set of elements for B2C was questioned, as one of the big issues was the willingness of consumers to provide information to suppliers.

30. It must be acknowledged that for business and revenue systems to function correctly that certain information must be provided by customers. The differing levels of information supplied by the customer in various transactions is examined in the table below.

Information	**In Person**		**Not in person**		
	Cash	Credit Card	Internet (goods)	Internet (not goods)	Mail Order
Name	X•[1]	•	•	•	•
Address	X•[1]	X•[1]	•	X•[2]	•
Description	•	•	•	•	•
Quantity	•	•	•	•	•
Credit Card number	X	•	•	•	•

[1]May be supplied for various reasons to do with delivery, warranty etc.
[2]Where an Address Verification Scheme is used an address or part thereof will need to be supplied.

31. Credit cards have been included above as they are and will continue to be for the medium term the predominant payment system in use on the Internet for B2C transactions.

32. Much of the information contained within the desirable data elements will be generated by the supplier, the customer/recipient will need to provide a small set of information.

33. As can be seen from the table above, the general list of elements could easily be used in B2C transactions as the customer/recipient is not being asked to provide information in excess of what is currently being provided in similar transactions.

7. Conclusions and recommendations

34. There is broad general agreement within the members of the TAG that the elements outlined are desirable from an audit or review point of view. No distinction has been made between B2B and B2C transactions as this would introduce unnecessary complication and complexity into the use of these elements. It should be noted that these elements are a list of desirable elements, it is recognised that certain country specific requirements may require additional information to be provided.

35. It is noted that significant work is being done in the area of harmonisation and simplification of 'invoice' issues within a number of jurisdictions. This document should be seen as an attempt to promote further discussion in this important debate.

36. In order to achieve further discussion on these issues, the work needs to be progressed and communicated to appropriate fora. Outlined below are recommendations for the furtherance of this work, it may be necessary to pursue a number of these in parallel in order to ensure that the information is communicated to the appropriate audiences.

1. The list of DDEs be provided to the appropriate fora considering Consumption Tax issues at the OECD as an aid in the furtherance of their work.
2. The OECD could provide the list of elements in the form of an information or best practice note.
3. Interested parties should be approached with a view to further progressing the work.
4. The OECD could incorporate or develop the list of elements into and appropriately defined de facto protocol such as XML or other protocols.
5. Approaches be made to the appropriate software developers and standards bodies to ensure that the list of elements is considered in the development of systems and standards.

APPENDIX (DESIRABLE DATA ELEMENTS)

Order	***Reason Required***	**Delivery**	***Reason Required***	**Invoice**	***Reason Required***	**Payment**	***Reason Required***
Order Header		**Delivery Note Header**		**Invoice Header**		**Payment Header**	
Order Number [1]	**Audit trail**	Delivery Note Number [2]	*Audit trail*	Invoice Number [3]	*Audit trail*	Payment Reference	*Audit trail*
Order Date		Order Number [1]	*Audit trail*	Invoice Date	*This is likely to be the date tax is due to revenue authority*	Payment Date	*This could be the date when tax is due to revenue authority.*
Customer Name	*Need to know who can claim input tax or who is eligible for zero rating*	Delivery Date	*This date can override the invoice date in certain circumstances as being the date when tax is due to the revenue authority*	Supplier Name	*Need to know who is liable to pay the Output Tax*	Invoice Number [3]	*Audit trail*
Customer address (could include e-mail address) [4]	*Need to know who can claim input tax or who is eligible for zero rating*	Ship to Address [4]	*Need to know why customer is eligible for zero rating, this is important where the customers address and the ship to address differ.*	Supplier Address	*Need to know who is liable to pay the Output Tax*	Payment Amount	*May be required to calculate tax due if operate for tax on a payments basis.*
		Carrier	*Helps establish audit trail of where evidence can be obtained for zero rating*	Tax Identifier	*Need to know who is liable to pay the Output Tax*	Payment Method	*Audit trail*
				Invoice Address			

Order Detail		Delivery Detail		Settlement Discount	*Required to calculate tax amount*		
Description [5]		Description [5]		Other Discount	*Required to calculate tax amount*		
Stock Reference [6]		Stock Reference [6]		Total Tax Value	*Required to verify system calculation of tax*		
Quantity Ordered [7]		Quantity delivered [7]		Total Value			
Weight [8]		Weight [8]		Invoice Detail			
Unit of measure [9]		Unit of measure [9]		Description [5]	*Helps determine product category and thus rate of tax applicable.*		
				Stock Reference [6]	*Helps determine product category and thus rate of tax applicable.*		
				Quantity Invoiced [7]	*Required to calculate tax amount.*		
				Tax Rate	*Required to calculate tax amount.*		
				Unit Cost	*Required to calculate tax amount.*		
				Delivery Note Number [2]	*Audit trail*		
				Order Number [1]	*Audit trail*		

The footnote numbers are a cross reference for common fields between the various documents.

ANNEX V

AUTHENTICITY AND RELIABILITY MECHANISMS

Contents

1. Outline of task

1. Task 4 – The TAG will catalogue existing or emerging mechanisms that can provide "authenticity" of data, including digital signatures and other uses of cryptography, report on the costs and benefits of their use and attempt to recommend the most appropriate mechanisms.

2. Task 5 – The TAG will catalogue existing or emerging mechanisms that can provide "reliability" of data, including digital notarisation and data recordation techniques etc, report on the costs and benefits of their use and attempt to recommend the most appropriate mechanisms.

3. Tasks 4 and 5 as defined above both relate to mechanisms that provide some assurance over data. They are closely aligned and have therefore been combined into one paper.

2. Introduction

4. The Oxford dictionary defines authenticate as "*establish truth or authorship or validity or genuineness of.*" In the electronic commerce context, authentication refers to the need to establish who the other party is that you are dealing with. This paper discusses the mechanisms that can be employed to give assurance over identity and thus establish the validity of transactions.

5. The Oxford dictionary defines reliable as "that may be relied on; of sound and consistent character or quality."

6. Reliability is referred to in the context of "transaction integrity" which is defined in AGS 1056[12], as relating to the completeness, accuracy and reliability of the information provided for recording and processing in the entity's financial records.

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

7. The Oxford dictionary defines integrity as “wholeness; soundness; uprightness, honesty.”

8. AGS 1056[13] goes onto explain that “audit procedures to assess the reliability of information in the financial records relating to e-com transactions are largely concerned with procedures which confirm the reliability of the systems in use for capturing such information.”

9. As the PDA TAG risks paper refers computer auditors are concerned with completeness, accuracy, authorisation and timeliness.

10. This paper discusses mechanisms that can be employed to increase auditors trust in data that has been generated in an electronic commerce context.

11. It is acknowledged that much of the information for this report has been supplied by the Technology TAG.

3. Existing and emerging mechanisms

12. The following mechanisms are discussed:

- Digital certificates and digital signatures.
- Message digests.
- Encryption.
- Time stamping.
- Notarisation.

Digital certificates and digital signatures

13. The Technology TAG reports that “there is general agreement that digital certificates and digital signatures show the most promise for identification of parties in the future. Digital certificates (also known as electronic credentials or digital IDs) are digital documents attesting to the binding of a public key to an individual or entity. They allow verification of the claim that a given public key does in fact belong to a given individual or entity.”

14. Digital signatures work 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 used to decipher it. The private key needs to be protected to preserve its value. The private key can be stored in various ways. For example, it can be stored on the user’s hard disk, on removable media (such as a floppy disk), or on a smart card or other “smart device.” These digital signatures are usually used with digital certificates to authenticate the attestation in a certificate.

15. The following is a step-by-step explanation of the digital signature process:

Alice applying a digital signature to a file:

1. Alice applies the file to a hashing algorithm such as SHA-1. The resulting output we will call the original hash.

13. Australian Accounting Research Foundation (2000), *Electronic Commerce: Audit Risk Assessments and Control Considerations*, Auditing Guidance Statement 1056, August, paragraph 46.

2. Alice then uses public key encryption to protect or sign the original hash result. She does this by applying her own private key and the original hash result to a public key algorithm such as RSA. The result of this is an encrypted or signed hash. This result is the actual digital signature for this particular file.
3. To complete the process, Alice attaches the original file to the digital signature and also attaches a copy of her public key, so that her signature can be verified.

For Bob to verify the receipt of a file from Alice, to ensure it is from Alice and that it has not been tampered with:

1. Bob generates a "fresh hash" of the message. He does this by applying the data to the same function that Alice used.
2. Next Bob will use Alice's public key and the proper public key algorithm to decrypt the "original hash" result.
3. Finally Bob will compare the fresh hash to the original hash. If they are the same, Bob can be assured that the data has not been altered, and that it was indeed Alice who signed the message.

16. This process provides proof of integrity and authentication. It supports non-repudiation since only Alice knows her private key and Bob was able to decrypt the message with Alice's public key.

17. Digital certificates are issued and managed by Certificate Authorities. A Certificate Authority (CA) is a trusted third-party organization or company that guarantees that the individuals or organizations granted these unique certificates are, in fact, who they claim to be. CAs can be governments, or private organizations that may or may not be regulated by government. CA functions are no longer necessarily unified; models relating to authentication have begun to evolve dramatically. Previously, all authentication service aspects of the transaction were conducted by one party - the CA - for digital signatures. Since then, the functions related to authentication and the types of parties involved and roles they may play have changed dramatically (registration, operation, device creation).

18. **Client or server side certificates:** Digital certificates are used today on commerce servers. These server IDs allow web sites to identify themselves to users and to encrypt transactions with their visitors. A CA (*e.g.* Verisign, Entrust) issues such certificates for a particular Internet host name (*e.g.* OECD.org). This kind of digital certificate helps the host server's users know that they are communicating with a particular host and not an imposter.

19. Digital certificates are also used to implement Secure Sockets Layer (SSL), which is the most common form of providing a secure channel between a web browser and the host. When a server uses an SSL ID, all browsers know that they are dealing with a legitimate source. Information passing between the browser and the host is encrypted after a certificate sent from the host to the browser is authenticated. Many have come to consider browser-based authentication (browsers have the capacity to hold digital signatures and support two-way authentication.) to be the largest deployable, scaleable authentication mechanism for low value transactions.

20. Server certificates are used for B2C transactions where most consumers do not have a digital certificate. Only the originating server is authenticated. This tries to assure the consumer that the business is authentic. There are very few consumers who have a certificate enabled on their browser for a reciprocal check and very few (if any) businesses that require such a check to transact business. This means that businesses will not have the same confidence as to who they are dealing with. There seems to be a business rationale that fraud remains a lower percentage of business and an acceptable risk when weighed against increasing complexity to the consumer. With competition only one click away, the increased complexity or set up/infrastructure requirements drives potential consumers away from a site to the competition. Whether

some businesses are happy to continue with a minimalist approach to information gathering remains to be seen, given the apparent prevalence of credit card fraud associated with Internet transactions.

21. The technology may evolve in the future, so as not to further complicate B2C transactions, providing a viable reciprocal check on a consumer which should help improve the integrity of B2C transactions.

22. On the other hand, client certificates are currently used for B2B transactions which together with SSL provide end to end encryption, ensuring authentication, message privacy and integrity. By exchanging digital certificates and using SSL, clients and servers can verify each other so that each knows who they are dealing with, the contents of the communications are protected from being altered on route and those involved can have confidence that what is received is what was sent.

23. In order to audit the use of digital certificates, an auditor needs to review:

- How the certificate is assigned and maintained to ensure security provisions are sufficient to prevent unauthorised changes to the CA server.
- The placement of the LDAP[14] directory and the CA servers to ensure that they cannot be penetrated by anyone. All data must be encrypted.
- The delivery procedure of the keys and download procedures of the client software if appropriate.
- The procedures for certificate recovery.
- That certificates are assigned under a trusted environment.
- And undertake substantive testing such as, for the SSL server certificate, sign on to the web site and check if the messages are encrypted during that session, - and for the client certificate, ask the client to issue a certificate, test the certificate replacement procedures and how they replace the certificate, recover the key etc. Also try to access the LDAP directory to see whether you can access any information in clear text. Also attempt to access the CA server without the proper key privileges.
- Whether the CA server and LDAP master server are locked in a secured location.
- Whether the shadow LDAP server is located in the DMZ[15] with firewall protection.

Message digests

24. A message digest is a string of digits and is created by applying a one way hash function to a block of data. If the block of data is changed then the message digest will not represent the block of data any more, so it is impossible to change a block of data and for it to then tie back to the message digest. Therefore it may be possible to detect the alteration of original electronic documents.

---

14. Lightweight Directory Access Protocol - an Internet standard defining the protocol for accessing online directory services defined as X.500 over the TCP/IP protocol suite. This server contains the certificates, public keys and certificate revocation list. Information in this directory is not confidential and is accessible by anyone. When signing onto the web site, the user's certificate will be checked against the information in the LDAP directory before access to the web site is permitted. If the certificate does not check out or is on the revocation list, access will be denied. The LDAP also contains the public key for encryption.

15. De-Militarised Zone – the area of a network residing between an external firewall and an internal firewall. Most companies'external web servers are installed in the DMZ where as private Internet servers are installed behind the internal firewall. The external firewall implements security policy that is designed to keep all unwanted external traffic from entering the corporate network. It also may apply security policy to outbound traffic. The internal firewall plays a more complex and active role in deciphering which traffic can go within the network.

25. However, message digest's use lies generally within encryption techniques and in specialised algorithms that involve the exchange of information giving assurance over what was sent has been received intact at the other end. To this end, no assurance can be given from the current use of message digests used in association with data transmission as to what happens with the data after receipt.

26. The common use of this technology is for the assurance that data transmissions are complete and unaltered and within encryption techniques, see Encryption below. It does not provide creation time/date assurance for the block of text. Message digest information generated in conjunction with data transmission is not stored. From an auditing perspective use of this technology would give assurance that the business has a level of control in place for the exchange of information. Apart from identifying that this control is in place the auditor cannot check the technology as such for individual transactions received in the past. Therefore use of this technology has limited value from an audit perspective.

Encryption

27. The Technology TAG has advised the following.

28. Encryption is the translation of data into a secret code. The object of encryption is to control access to data in circumstances where physical access can't be controlled.

29. To read an encrypted file, you have to have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text and encrypted data is referred to as cipher text. There are two main types of encryption, symmetric and asymmetric encryption.

30. Symmetric encryption is a cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation. It has a number of shortfalls, which have led to the development of asymmetric encryption, which provides a higher level of security.

31. Asymmetric or public key encryption uses two keys, a public key known to everyone and a private or secret key known only to the recipient of the message. The sender uses the recipient's public key to encrypt the message and the recipient uses their private key to decrypt the message. It is virtually impossible to deduce the private key if you know the public key.

32. Public key infrastructure (PKI) systems, such as VeriSign and Entrust are becoming popular for transmitting information via the Internet. They are extremely secure and relatively simple to use after initial set-up. The only difficulty with public-key systems is that you need to know he recipient's public key to encrypt a message for him or her.

33. The following is a step-by-step guide to the basic encryption process:

Assume Alice has a file that she wants to encrypt for Bob:

1. Alice using her client application selects the file to be encrypted and indicates that Bob should be a recipient. Bob's encryption public key is retrieved from the LDAP directory that holds all public keys.
2. Alice generates a one-time use symmetric key, which is then used to encrypt the file. Now the problem is how to share the symmetric key with Bob in a way that ensures only he has access to it in order to decrypt the file.
3. The solution is to encrypt the symmetric key with the Bob's public key. Now only Bob will be able to decrypt the encrypted symmetric key.
4. The output file is written. It includes the cipher text, which represents the original file as well as the encrypted symmetric key.

Decryption process:

1. Bob's client application determines that he is the intended recipient.
2. Bob uses his decryption private key to decrypt his copy of the symmetric key that was created during the encryption operation.
3. Now that the symmetric key has been decrypted, it may be used to decrypt the cypher text.
4. The output file is written. All protection has been removed at this point and the file is written in it's original form.

34. Use of this technology in transmission would provide confidentiality of data and ensure that communication was only successful between two intended parties.

35. Encryption is also used in some instances to provide a level of security over stored data.

36. In current usage encryption by itself does not allow for time creation and subsequent alteration detection. From an audit perspective, transmission integrity is assured. More importantly, if its use is connected to data storage and other internal controls are in place, (*e.g*. separation of duties, restriction of access to segments of the information system and proper encryption key management) auditors may be able to place greater reliance on the financial information. However, we do not believe that any significant storage of records in encrypted format is currently occurring.

Time stamping

37. Time stamping means that each document is, at the time of it's creation (more specifically presentation to the 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 are unchanged.

38. The following has been provided by the Technology TAG:

39. Over time several different techniques for time stamping[16] have emerged, many of which incorporate 'message digesting' and 'encryption' techniques into the process to strengthen the process and overcome some of the shortfalls of encryption. For example [17]:

In order to time-stamp a message M, a user U first computes the ***message digest*** *X=H(M), where H is a cryptographic hash function. The message digest X has the following properties:*

- *It is a relatively* ***short fixed size bit-string****, typically 128 or 160 bits. This reduces the communication cost.*
- *It is computationally* ***infeasible****, given only the message digest,* ***to recover the original message****. This prevents the leakage of confidential information during time stamping. Even the TSA is not supposed to know the content of M.*
- *Even if one has both the message M and the message digest X, it is* ***infeasible to find*** *another message M' with* ***identical message digest****. This prevents the user from modifying the content of M after time stamping.*

16. Further information on the various time stamping techniques may be sourced from http://moomin.ee/'helger/crypto/link/timestamping/

17. Sourced from www.cyber.ee/research/projects.html.

Next, the user sends the message digest X to the TSA.

*The TSA creates the **time-stamp for X**, i.e. a signed message* $S = signed_{tsa}\{X,t,n,L_n\}$*, where t is the current time, n is the sequence number and* L_n *is the linking information. The **linking information** is formed from X, n and the previous time-stamps using the cryptographic hash function H:*

- $L_n = H(X,n,L_{n-1},L_m)$,

where m is the sequence number of a suitably chosen older time-stamp. This linking scheme guarantees the following properties:

- *The TSA **cannot manipulate** the temporal order of issued time-stamps without breaking the cryptographic hash function.*
- *The mathematical relationship between* L_n *and* L_{n-1} *ensures that the n-th time-stamp **was indeed issued** after the (n-1)-st one.*
- *The good choice of the sequence number m (depending on n) provides efficient method for between the time-stamps* issued.

*In order to **compare two time-stamps**, one has to compose a chain of intermediate time-stamps linked together mathematically via the hash function. So one obtains the **linking chain**.*

40. Many of the time stamping methods offered by various TSA's combine encryption techniques within their time stamping service to overcome many of the potential integrity problems associated with electronic documents. For example, where the TSA's service takes a 'fingerprint'[18] of the electronic document and certifies the time and date. This may overcome such associated problems by attesting that the contents, including any identifying information of the electronic document have not been altered since they were time and date stamped. While it does not overcome the shortfall of distinguishing between the 'original' and a 'copy', it does however, verify that the 'contents' of the document has not been altered since it was time stamped. Thus the integrity of the document remains intact.

41. Commercially, time stamping by third parties is only likely to be adopted for specific high value transactions and not for general commerce because it is relatively expensive for every time use. It is possible that in the future the software design of commercial and in-house accounting systems may incorporate the underlying time stamping technologies used by many of the independent time stamping authorities. This will enable the automatic time stamping of data on creation and alteration.

42. From an audit perspective the use of time stamping by a third party provides assurance over the integrity of the contents of a document since it was time stamped. Therefore it will be important to establish at what point in the system time stamping is deployed. To check whether a particular time stamped document has been changed the auditor can electronically resubmit the document to the time stamping authority who will confirm whether the document has been changed or not. If the time stamping authority verifies the document as not being altered, the auditor can have confidence in saying that the document existed in this form at this particular time. To be confident that the document, for example, an invoice, reflects a transaction which actually took place the auditor would need to go to supporting documentation (i.e. credit card slips, delivery documents etc).

---

18. *Fingerprint* is a unique number calculated from the contents of your electronic document. If the file's contents were to be changed at a future time, even by one character, a different number would be returned thus detecting the alteration.

Notarisation

43. The Technology TAG advise that according to the ISO, notarisation is the registration of data with a trusted third party that allows the later assurance of the accuracy of its characteristics such as content, origin, time and delivery[19].

44. 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 (they don't usually see the contents of the data) which implicitly acknowledges that the message was received by them at a particular time. Therefore the document must have been in existence at that time and could not be created later and backdated.

45. There is little differentiation between how modern notarisation occurs and that described above in the section on time stamping.

General comment on mechanisms

46. As mentioned under time stamping, it is combining the above mechanisms that strengthens the integrity of data being transmitted between parties and give some assurance over document integrity.

47. From an auditing perspective, these mechanisms provide:

- A greater level of assurance that what has been sent between two parties was received.
- The third party time stamping provides assurance that the document was in existence in a particular form at a particular point in time. This combined with message digest functionality should also show that the document has not been tampered with since the time stamp authority stamped it.

48. The above mechanisms represent only a small part of the puzzle. The auditor needs to examine the reliability of the system as a whole to ensure integrity of transactions. Other controls that should be in place to give greater assurance of completeness, accuracy, authorisation and timeliness within a system and thereby increase the reliability of data are:

- Controls over access to data – designed to ensure that only the right personnel can process the data.
- Data capture controls – to ensure that the right data gets into the system.
- Processing controls – to ensure that the data remains correct throughout processing.
- Controls over standing data – to ensure that any criteria used to process the data are correct.
- Controls over output – designed to ensure that system output is in the correct format. Also that any required action is undertaken by the recipient of the output.

49. It is the consideration of the system as a whole by the auditor that will indicate the degree of reliability that can be assigned to the data generated by the system.

---

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

Costs and benefits

Mechanism	Costs	Benefits
Digital Certificates/Signatures	Expensive – Requires adoption by consumers in order to assist identifying jurisdiction. However, in some countries Government absorbed the costs *e.g.* ATO rollout of free certificates to business.	This is a very reliable way of transacting over the Internet and tends to be commercially driven for particular types of transaction that involve greater risk from a commercial perspective.
Message Digests	Where message digesting is used it is an integral part of the system and as such can't be costed separately.	Gives assurance that what was sent was actually received and hasn't been tampered with.
Encryption	As above.	Provides some assurance that an encrypted document is likely to be the same when decrypted as it was just before it was encrypted.
Time Stamping and Notarisation	Costs depend on a number of factors such as, volume and type of process. Cost of time stamping ranges from a flat fee of USD $0.50 per file[20] to others who scale their fees ranging from USD $1.00 per file up to 5,000 files to USD $0.13 per file for in excess of 1.5 million files[21]. Sometimes there is a fee for each time you require a file validated, these range up to USD $0.05 per validation.	Provides assurance that a document was in existence prior to a certain date and time.

4. Findings and recommendations

50. Our study has found that the market is immature at this time. However. third party time stamping was identified as a component of the above mechanisms that can give some assurance over integrity. From a commercial perspective, this technology is expensive and therefore is only likely to used on a very limited basis for particular high value transactions. Therefore in reality the above mechanisms are likely to be of limited use to the auditor as third party time stamping is unlikely to be that prevalent in general business.

51. For revenue authorities to require business to adopt current time stamping mechanisms would place additional burden on taxpayers and would demand a higher standard of integrity be applied to electronic transactions compared to traditional transactions. However, revenue authorities could encourage the use of time stamping on the grounds that its adoption can give greater assurance over the integrity of data when combined with other systems controls. Revenue authorities could also engage with software developers to encourage the adoption of time stamping technologies within their software design.

52. Electronic documents, especially from a source outside the audited entity, are used in performing substantive tests by private sector and tax administration auditors. This type of testing must give the auditor assurance on his opinion. In the case of SMEs an auditor may have to rely entirely on the performance of substantive procedures. The study on risks in electronic commerce states that electronic documents, without additional measures, are less credible than their paper equivalents because of a lack of authenticity and integrity characteristics. These entities will become extremely difficult to audit effectively.

20. See firstuse.com for details.

21. See surety.com for pricing structure.

53. In line with the neutrality principle the authenticity and integrity aspects of electronic documents should be at the same level as their paper equivalents. Techniques such as digital signatures can provide the necessary assurance that the electronic document is from a source outside the company and is not tampered with. The sender of the electronic document cannot deny that he or she was indeed the sender of this document (non-repudiation). When these techniques are used the private sector and tax administration auditors will be able to perform substantive tests again and will therefore be able to express an opinion on the financial statements of an entity. Therefore business should be encouraged to adopt strong authentication measures.

54. In general, there will be a (considerable) timelag between the closing of the financial statements and the actual auditing of those financial statements, especially in the case of a tax audit. In order to be able to

55. test the authenticity and integrity of electronic documents with a source outside the entity, a condition will be that the complete message, including message digest and digital signature is retained for the legislative term. Also, the auditor must be able to check the public key of the sender of the message which means that these keys should be available for auditors, even years after issuing.

56. It should be noted that examination of the mechanisms discussed in this paper will not by themselves provide complete assurance over integrity of data but as part of a set of systems controls will increase the level of reliability that can be placed on data.

57. To gain assurance over the reliability of data auditors will have to place greater reliance on:

- Systems controls, which means there will be an increased requirement for auditors to be skilled in carrying out systems audits.
- Management systems.
- Third party information/verification.

58. In addition, new audit techniques may have to be adopted in the absence of hard copy information, such as:

- How to query electronic transactional log files derived from accounting systems or servers.
- Analysing patterns within data, for example using digital analysis techniques such as Benford's Law.

59. In conclusion the answers to the question of reliability of data do not lie entirely in the adoption of new technologies but will require auditors to hone their skills in terms of systems audit capability and to possibly adopt new audit techniques.. It will be important for auditors to also be trained in what the mechanisms discussed in this paper are, how to audit them and to understand what assurances these mechanisms provide in an audit context.

60. For the future, further work should be done in considering the impact and usefulness of developing technologies in relation to storage and retention of data including information that facilitates authentication.

61. As the market is currently immature, continued monitoring should be undertaken of emerging mechanisms and these should be evaluated from an audit perspective.

62. In terms of the issue of authentication of a customer's jurisdiction, it is acknowledged that other OECD E-Commerce groups are examining this issue. However, we recommend that their recommendations be reviewed as to their auditability.

ANNEX VI

REMOTE ACCESS IN THE ELECTRONIC COMMERCE ENVIRONMENT

Contents

1. Outline of task 6

1. Task 6 - The TAG will catalogue existing or emerging information technologies (IT) for "remote access", report on the costs and benefits of their use and attempt to recommend the most appropriate mechanisms.

2. Introduction

2. The purpose of identifying mechanisms that can be used for digital delivery of information from the taxpayers' systems is to promote speedy and timely access of audit data. Many organisations are using the Internet to bring a global edge to a provincial business. They are much less constrained by national boundaries. The most common Internet services used are World Wide Web, e-mail, File Transfer Protocol (FTP) and Telnet. Businesses are using Internet services to access company information from remote sites or communicate between business partners.

3. The goal of this task is to identify technologies that will assist auditors in conducting their audits in light of the way that businesses are storing and accessing their financial information. Specifically, as businesses increasingly store their financial records at remote locations, auditors will have to change the way they access taxpayer records. Traditionally, auditors will conduct their audits on a taxpayer's premises, this becomes more difficult as records are stored remotely and potentially in many places. The intention is to identify technologies that will enable auditors to conduct audits from remote locations, giving them the same access to records that they have traditionally had. The intention of pursuing remote access audit capabilities is to help audits be performed in a more effective and efficient manner. Obviously, each country's laws with regard to obtaining business records would apply equally in a remote electronic access environment as they do in the physical paper environment.

3. Existing or emerging information technologies

4. As stated in the Introduction, the most commonly used Internet services to obtain data from remote sites are the Web, e-mail, FTP and Telnet. The following is a brief description for each service.

The world wide web service

5. The World Wide Web is the multimedia part of the Internet. It is one of the many systems used on the Internet to find and transfer information. It has become one of the fastest growing segments of the Internet service for business use. The World Wide Web is also called the Web, WWW, and W3. For the purpose of this paper, we will use the term "Web".

6. The Web is made up of documents on computers throughout the world. A Web document is called a "page." These documents are developed based on a standard set of rules called the HyperText Transfer Protocol (HTTP). Software used by computers to hold Web documents is called Web servers. The client program used to access the Web documents is called a Web browser. The Web servers communicate via the Internet with the Web browsers. Individuals use Web browsers, which are installed on their own computers to find and view Web pages and other documents linked to them. When a browser retrieves a Web document from a Web server, it interprets instructions in the HyperText Markup Language (HTML) within the document and displays the document based on the HTML instructions. Each Web page has an assigned unique Internet address. They are written in a standardized Uniform Resource Locator (URL) format. Browser may be directed, or pointed to a particular Web page by typing in the page's URL.

7. In addition to documents created using HTML, the Web browser can also interpret Web documents developed following the meta language of the Standard Generalized Markup language (SGML) such as Web documents created using Extensible Markup Language (XML), Extensible Hypertext Markup Language (XHTML), Extensible Business Report Language (XBRL) and others. Most Web browsers can display information and retrieve files from servers on other Internet systems in addition to the World Wide Web. These include FTP and Telnet.

Internet System	URL prefix
World Wide Web	http://
FTP	ftp://
Telnet	telnet://

8. Currently, the Web is primarily used as "public space". Organizations provide information, advertise, and sell products, etc. to the public. The Web is increasingly being used as "private space". Organizations are setting up private workspaces on the Web to allow employees, business partners and other parties to accesses "private" workspaces where they can share information collaborate on projects, etc. It is the "private work spaces" that provides the most promise for remote audits. For example, an organization can set up a private space, which is accessible only by the tax authority. In this space the organization can provide the records which were requested by the taxing authority.

9. Although there are various technologies that make this arrangement very secure, there are many taxpayers and taxing authorities that do not feel comfortable with this type of arrangement. The primary fear is that an unauthorized individual can access the information. While this is clearly a risk, the "perceived" risk is probably greater than the "actual" risk.

The e-mail service

10. As stated before, e-mail is the most popular of the Internet services. It is the key Internet resource for most people. E-mail is commonly used for:

- Sending single or multiple messages to individuals.
- Sending single or multiple messages to several individuals or to groups of associated users.

- Sending text files.
- Sending binary items such as a spreadsheet data file or graphics.
- Distributing electronic newsletters.
- Broadcasting notices.
- Supporting business functions.

11. To use e-mail, one must establish an account with an Internet access service provider (ISP) or with a company or organization that has an e-mail account or mailbox. E-mail travels well beyond the Internet backbone, to and from many associated nets and commercial services such as America Online (AOL), MCImail, Microsoft Network (Hotmail), SprintMail, Yahoo, and ATTmail (Worldnet), etc. Most sites have an e-mail postmaster or a staff member who maintains the e-mail functions for the organization. The user, platform or system depending on the particular mail services can differentiate E-mail message management. One may read mail on line, or download the mail at once for reading and management on a personal computer. Businesses often use e-mail to send formatted spreadsheets, graphs, and word processing files. These files will be in binary format and use the MIME (Multipurpose Internet Mail Extension) protocol. Sometimes, businesses may wish to send images, sounds and animated files, they must use UUENCODE to encode a binary file and send it through regular e-mail. The sender encodes the file, inserts it in an e-mail message, and sends it. The recipient retrieves the message as usual, then extracts and decodes the file. E-mail forms an important support and enhancement for other Internet functions. While using a mail program will be the usual method for managing the mail messages, it is possible to include a "mailto" link in the Web page to permit page visitors to send a response to the appropriate contact's mailbox address while they are using the pages. An individual can also send and receive mail using a browser by specifying the mailbox address.

12. E-mail is probably the most straightforward technology as it relates to auditors conducting audits remotely. Traditionally, auditors request various financial records from taxpayers, which were generally provided on paper at the taxpayers' place of business. E-mail enables taxpayers to send these records electronically to the taxing authority, so that the audit can take place wherever the auditor is located. This technology will enable tax authorities to reduce the costs of travel to the extent that audits can be conducted off-site.

The FTP service

13. The FTP system will transfer both ASCII and binary files of almost any size and type such as data files from spreadsheets, CAD, word processors, databases, photo images and desktop publishing, as well as software and plain text files. The FTP system for file transfer is very powerful, but is somewhat difficult to use. There are four basic methods for getting these files. They are:

- Using a GUI Web browser.
- Using a text-based Web browser.
- Using command-line FTP with a shell account.
- Via e-mail.

14. Many of the files at FTP sites have been compressed in order to save storage space and increase the speed of the file transfers. Compression programs are also used because they can store a group of files (including dissimilar types) inside one file. Thus, a program, its supporting files, data files and documentation files can all be stored and moved together as a single file. It was probably one of the first services of the Internet and was widely used as the preferred method to transfer files prior to the browser and e-mail. The FTP system for file transfer is very powerful, but is somewhat difficult to use.

15. This technology will assist in remote audits because they allow large amounts of data to be transferred at an increased speed and save space when the data is stored. This will be very important in audits of large companies or companies that have a lot of transactions.

The telnet service

16. The Telnet service allows one to command the browser software or the Internet access service provider's computer, to connect to another computer on the Internet. One can operate that remote computer as if the individual is physically at the computer. With the Telnet system, one can use the Bulletin Board Systems (BBSs) databases, search tools, services and files otherwise not available on the host computer. The use of a Telnet site to maintain a business presence on the Internet has declined with the rapid rise in the use of the Web and security issues. Because of the decline in its use, this technology does not provide great promise for conducting remote audits.

4. Findings

17. Accessing remotely stored data using the Web technologies is not identified as a key risk since security services are available to safeguard the Web environment. However, there is a strong concern in business and government that by allowing the auditor to access company data via the Web confidentiality could be compromised.

18. The Web is built on the Internet and makes use of many of the mechanisms the Internet provides. Since the Internet was meant to be a very open and flexible medium, potentially the entire Internet community can peer through the Web content. While most visitors are content to window shop, a few will try to peek at things that are not intended for access by the public. Most clients are not familiar with the available security services that can be implemented to safeguard the data made available to site visitors and they have expressed a concern about allowing the auditor to access confidential and proprietary information from the Web server via the Internet. Specifically, they are concerned with the surround site security, data integrity, authentication and the broad implications of secure transactions. They are also concerned that the auditor may gain access to the internal networks and access information other then those authorized.

19. The following are security services that are available to safeguard the Web environment and should not be a key risk if the security measures are implemented appropriately. These include the use of:

- Certificates, digital signatures, dynamic one time password token, smart card, IP addresses and public key cryptography for strong authentication.
- Access address restrictions, firewall filtering, and the creation of roles and views by the relational databases for Web access controls.
- Encryption and digital certificates to protect against the disclosure or revelation of confidential information to people who are not authorized to have that information.
- Object-oriented technology and objects to encapsulate and protect data against changes and ensure data integrity.
- Digital signature to verify the sender's identity to verify the authenticity of the message and support non-repudiation.

20. There is also a concern that the data may not be complete and reliable. In reality, this concern predates the Web and the Internet. However, it should be noted that the inability of the auditor to perform on site observations exacerbates this concern. Most organizations are using back-end integrated databases where organizational databases are tied together through Web servers to make the data accessible in real

time and live from the databases to the Web browser. Consequently, only the Web server can make a query to the databases. In reality, the data that is provided from the Web server could be more reliable and complete compared to creating a separate flat file for the auditor. Also, using object-oriented technology, most data is encapsulated in objects to prevent alteration or change to the data.

21. Another concern is that when performing remote access audits, an auditor may not be able to perform many of the physical observations to confirm adherence to company policies, standards and procedures. Further, the opportunity for the auditor to detect control risks from observation would not be possible. However, many clients are using Enterprise Resource Planning (ERP) systems for e-commerce and many of the ERP systems maintain a comprehensive audit trail. An auditor could, to a certain extent, rely on the controls and audit trails that are being maintained by these systems. While ERP systems mitigate the loss of the auditor's observation, they do not replace it.

22. The Web technologies enable an auditor to obtain data that are physically stored at remote sites in a timely and more efficient manner.

23. The Internet services and net centric technologies have enabled the client to collect and prepare all the requested information from all locations immediately and simultaneously. In today's global business environment, company records may reside in different databases and/or tables, or even on different computers. There are minimal efforts on the client's part to make the information available for the audit. They only require creating a link to the appropriate database(s) that contain the required information and convert the file information to a basic markup language file such as HTML, XML, XBRL, XHTML, etc., and place the Web document on the Web server. Also, traditionally, the auditor must physically travel to the client's site to conduct audit reviews. If the client's operation is global, the auditor may be required to travel to the varied remote locations to collect the necessary data in support of the audit plan. Remote access for audit not only save travel time and costs, it could also reduce the audit time required to complete the audit, and thus free the auditor to assume other audit assignments and obligations. Based on the foregoing, there would appear to be benefits for both the client and the auditor associated with remote access audits, provided the concerns outlined above are also addressed

24. Auditors must be trained in this new Web technology environment so that he or she can conduct audits in a more efficient and effective manner. Besides HTML, most auditors are not familiar with the use of the standard generalized markup languages such as XML, XHTML, and XBRL and the Web technology environment. In order for them to conduct audits efficiently and effectively in this new environment there will be training requirements involved in using the markup languages and costs associated with this training.

5. Recommendations

25. Continue monitoring of remote access technologies by government and external auditors with a view to incorporating remote access into audit functions as appropriate, to make the audit process more efficient and effective.

26. It is clear that remote access using the Web technologies is the preferential trend for conducting business. However web technology is still evolving, and international standards for the Web are still emerging. Once these standards are formalized, they can be incorporated into audit functions as appropriate. However, while these international standards will become more concrete, they will never stop evolving. Therefore, auditors will have to continue to adapt their processes as this evolution occurs.

27. In order to allay any concerns that may exist, Business and Government auditors should be educated on the best practices for e-commerce and Web security.

28. There are a number of "best practices" documents published for e-commerce and Web security. Business and Government auditors should be made familiar with these, and any new, best practices.

ANNEX VII

ENCRYPTION KEY MANAGEMENT AND RECOVERY MECHANISMS

Task 7 - Encryption key management and recovery mechanisms

Contents

1. Outline of task 7

1. The TAG will catalogue existing or emerging mechanisms to protect against or recover from loss of encryption keys, report on the costs and benefits of their use and attempt to recommend the most appropriate mechanisms.

(Covers Implementation Option 16 when combined with work item 2, above)

2. Introduction

2. The purpose of encryption is to ensure privacy by keeping sensitive information hidden from unintended viewers. The Technical Advisory Group (TAG) recognises that there are commercial reasons for the use of encryption by businesses and it satisfies a genuine need for ensuring privacy.

3. Some of the commercial reasons for using encryption are:

- Commercial confidentiality.
- Security.
- Privacy, and
- Authentication.

4. One of the issues with the use of encryption is the inability of the user to decrypt information due to the unintended or deliberate loss or destruction of the required keys. Several country specific approaches already exist that attempt to overcome issues that may be faced with the use of encryption. Where these specific remedies are not available other mechanisms need to be encouraged or be in place, so that information is still accessible.

5. The TAG has been tasked with cataloguing existing or emerging mechanisms to prevent or recover from the loss or destruction of encryption keys.

6. Encryption has many and varied uses, it can be used to:

- Encrypt messages while being sent over the Internet.
- To secure commercially sensitive information in transit or while being stored.
- To protect financial information (credit card details) while being sent to an online merchant.
- To authenticate or verify the identity of a person.
- To provide a facility to ensure that documents have not been altered (message digests).

7. Comment sought from the Technology TAG on the existing use of encryption and trends. What is encryption being used for storage or protection in transmission.

8. The most common encryption methods use key-based algorithms. The two main types of key-based algorithms are symmetric (or secret-key algorithms) and asymmetric (or public-key algorithms) systems.

9. In most secret-key algorithms, the encryption key and the decryption key 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.

10. Unlike secret-key algorithms, public-key algorithms are designed in such a way that the encryption key and the decryption key are different. The decryption key (also known as the private key) is only known by the message receiver, whereas the encryption key (also known as the public key) is publicly available to anyone. It is extremely difficult to calculate the private key from the public key.

11. The advantage of public-key algorithms is increased security and convenience. Private keys never need to be transmitted or revealed to anyone. Whereas secret-key algorithms require the secret key to be transmitted allowing for possible interception. However, a disadvantage of public-key algorithms is that many secret-key algorithms are significantly faster.

12. Both types of encryption have a place in securing messages.

> "In most practical implementations, public key mechanisms are used to encrypt keys and not messages."
>
> "Consequently, a mixture of mechanisms is usually used: Symmetric mechanisms to encrypt/decrypt the message using a session key which is exchanged using public key mechanisms."[22]

13. Comment sought from the Technology TAG - what is the most common type of encryption in use, symmetric or asymmetric?

22. Hilton, J. and Mansfield, N., (1997) *An Introduction to the Use of Encryption to Provide Confidence in Global Commerce*, January.

3. Overview of robustness

What key size should be used?

14. Generally speaking, the larger the key size (number of bits) an encryption system has the more secure it will be. For example, a system with only a 3 bit key would have 8 possible key combinations, whereas, one with a 56 bit key would have 7.2e+16 possible key combinations. Therefore, for an encryption system to be secure, there have to be enough possible keys to make it *practically* impossible for someone to try every possible key until they find the right one that works. Table 1 highlights the number of possible key combinations for various key sizes. It can be seen that a 128 bit key size is far more secure than any of the smaller key sizes due to the immense number of key combinations to be tested.

Table 1. Possible combinations for larger binary locks

Symmetric key size (bits)	*Number of possible combinations*	
40	1 099 511 627 776	1.0e+12
56	72 057 594 037 927 936	7.2e+16
64	18 446 744 073 709 551 616	1.8e+19
128	340 282 366 920 938 463 374 607 431 768 211 456	3.4e+35

15. Several projects have been conducted in an attempt to crack some of the more secure systems. An Internet organisation (www.distributed.net) has formed an immense, globally distributed computer that solves large-scale problems and provides an accessible pool of computational power to projects that need it. Distributed.net's computing power is equivalent to that of more than 160,000 PII 266 Mhz computers working 24 hours a day, 7 days a week, 365 days a year. In 1997 distributed.net cracked the 56 bit encryption system RC5 (RC5-56)[23]. It became apparent that RC5-56 was not as secure as previously thought.

16. One of distribute.net's current projects is an attempt at cracking the RC5-64[24] bit encryption system. Table 2 shows the current progress of the project as of 12 July 2000.

Table 2: Aggregate Statistics of the RC5-64 Project.

Total Blocks to Search:	68 719 476 736
Total Blocks Tested:	19 061 159 214
Keyspace Checked:	27.738%
Total Keys Tested:	5 116 690 965 498 691 584
Time Working on Project:	992 days
Overall Rate:	59 698 549 Kkeys/sec
Number of Participants Since Commencement:	259 013

17. As can be seen in Table 2, the project has been running for approximately three years and only 27.738% of the keyspace has been checked. Distribute.net claim that at the current testing rate, the keyspace will be exhausted in 1 039 days. Therefore, an overall time frame of approximately six years has been determined. Considering that a globally distributed supercomputer has been used and that the number

23. An encryption system developed by RSA Security http://www.rsasecurity.com

24. Ibid.

of participants has exceeded 250 000, it is evident that RC5 is currently considered secure. To provide a comparison, distribute.net were able to crack 3DES[25] in less than 24 hours.

Cost

18. The cost associated with cracking a robust encryption system is difficult to determine at this time, but would most likely be very expensive as indicated by the computer power and manpower required by distibuted.net in their cracking project work.

19. http://rsasecurity.com/rsalabs/bulletins/bulletin13.html contains a technical analysis of cost-based key size equivalencies. Note: due to the manner in which this paper was written it is difficult to extrapolate the relevant information. The web page www.interhack.net/projects/deschall/what.html also has a very small amount of information on cost.

20. Need further feedback from the technology tag on this issue.

4. Existing and emerging mechanisms

- Protection against loss.
- Recovery from loss.

What is the life cycle of a key?

21. All keys have a particular period for which they are authorised to be used. The life cycle of a key typically includes the following phases:

1. Key generation and registration

22. An essential requirement of key generation is that a sufficiently unpredictable random number source is involved. It is recommended that a hardware random noise source be used. Key registration involves linking a generated key with its particular use. For example, a key to be used in authenticating a digital signature needs to be associated with or bound to the identity to which the signature will be attributed. This binding must be securely registered with some authority.

2. Key distribution

23. With a symmetric encryption system, the two parties who require protected communications must have a copy of a single key, which is kept secret from all other parties. With a public-key encryption system, only one party must have a copy of a single key (in this case the private key) which is kept secret from all other parties. When distributing a public key, confidentiality is not required. However, it is essential that the integrity of the public key be maintained.

25. Ibid.

3. Key backup/recovery and/or key escrow

24. Key backup/recovery refers to the ability to recover a copy of a secret or private key should it be lost or otherwise unobtainable. In particular, if a message is encrypted and requires a particular key to decrypt it, loss of the key may mean loss of the message. The idea behind 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.

4. Key replacement or key update

25. Key replacement/update involves re-executing a key distribution process when a key expires.

5. Key revocation

26. Key revocation may be necessary in exceptional circumstances. Reasons for key revocation include:

- Decommissioning of a system with which a key was associated.
- Suspicion that a particular key may have been compromised; and,
- Changes in the purpose for which the key was being used (for example, increased security classification).

6. Key destruction and/or archival

27. Key destruction involves destroying all copies of keys after their active use terminates. Archival of a key is sought if a copy of a key might be required in the future.

5. Conclusions

Key management (from a users perspective rather than an issuers)

28. Key management issues have been mentioned in relation to the issuer or certifying authority to ensure that the security of the keys and the underlying system is not compromised.

29. Key management issues from the user of the encryption system are also important.

> "…. management establishes appropriate controls in respect of the use of encryption-based security measures to ensure access to information."[26]

26. Australian Accounting Research Foundation (2000), *Electronic Commerce: Audit Risk Assessments and Control Considerations* - AGS1056, August.

30. Consideration must be given to the use of appropriate key management handling, use and storage practices. This would include:

- 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 (is it necessary to store documents in encrypted form after receipt.)
  - Authorisation procedures.
- Appropriate internal key management as for the certifying authority.

Key recovery/key escrow/trusted third party

31. Key recovery and key escrow systems offer similar outcomes but are based on different models. These concepts have been adequately described in paragraph 4 above.

32. There are numerous advantages and disadvantages resulting from the adoption and use of these systems. Some of these have been documented below:

Advantages:

- Encryption/decryption keys are recoverable.
- With internal escrow/recovery an organisation has control over their data.
- No need to store and retain numerous numbers of old or expired keys.
- Emergency key recovery is possible and quick.
- Internal key escrow/recovery allows increased trust in the reliability of the system.

Disadvantages:

- No security if external escrow agency is compromised.
- External escrow may be open to abuse.
- Trust of the third party agency.
- How is control to the keys determined or allowed.

33. Whilst some governments have sought to mandate the use of particular key recovery systems, ultimately business needs will drive the adoption of particular systems. The TAG is of the opinion that currently the use of encryption is not widespread. That is not to say that this situation will remain static. Given the possibility that business does not adopt measures as described above Auditors need to be in a position to ensure that information is not lost and other approaches need to be considered.

Other approaches

34. There are many pluses and minuses for using the above systems, from both a Government and Business perspective. It will be difficult to get agreement between these parties on the most appropriate system or technology to use.

35. At present revenue auditors have reported no significant use of encryption in the storage of taxpayer records. In light of this and the legislative rules around record keeping, the current rules are considered to be sufficient in the medium term.

36. Given developments in technology and user knowledge consideration must be given to the use of alternate methods to recovery from instances where encrypted records are encountered.

37. A number of approaches not based on technology have been suggested or are currently in existence and are discussed generally below.

In all these instances it is assumed that encrypted records have been encountered by an auditor and that the decryption key has been lost (inadvertnetly or deliberately).

- Where records have been encrypted, there is a legislative requirement that these records be readily convertible to the countries language(s) of choice.
- Where records have been encrypted, records must be supplied decrypted in either plain text (or other agreed format) or in a format specified by regulation or legislation.

6. Findings and recommendations

Findings

38. No significant widespread use of encryption of records for storage, retention or validation.

39. Current legislative record keeping regimes, weighed against evidence of encryption use, would appear adequate in the short to medium term.

Recommendations

40. Businesses should be encouraged to use prudential systems for the management of encryption keys.

41. Future developments in the area of encryption and encryption management need to be monitored.

APPENDIX (ENCRYPTION KEY MANAGEMENT AND RECOVERY MECHANISMS)

Secret-key (Symmetric) encryption systems

There are a variety of secret-key algorithms available. The following is a list of the more common secret-key systems used and a brief description of each.

DES (Data Encryption Standard)

DES is a block cipher algorithm (i.e., an algorithm that operates on the plaintext in groups of bits. The group of bits are termed 'blocks'). DES encrypts a block of 64 bits at a time using a 56 bit key. According to RSA Laboratories, DES is at least 100 times faster than the most commonly used public key algorithm - RSA (see page 2 for a description of RSA). However, DES is relatively easy to break with special hardware. DES is considered unsafe for top-secret data, but is sufficient for individual everyday use. A variant of DES, Triple DES (3DES) is based on using DES three times (normally in an encrypt-decrypt-encrypt sequence with three different, unrelated keys). 3DES is considered a safer alternative to DES.

Blowfish

Blowfish is a block cipher algorithm with 64 bit block size and variable length keys (up to 448 bits). The cipher was developed specifically for 32 bit machines and is significantly faster than DES. Blowfish has been well accepted in a number of applications. Certain weak keys and an attack against different versions have been found. However, Blowfish is still considered secure.

IDEA (International Data Encryption Algorithm)

IDEA is considered one of the best and most secure algorithms available today. It uses a 128 bit key to encrypt 64 bit blocks, and the same algorithm is used for encryption and decryption. IDEA is similar in speed to that of DES, be it a little slower. No practical attacks have been published. It is generally considered secure. Triple IDEA (similar to 3DES) has been developed and is considered an even safer alternative having a 256 bit key length.

Skipjack

The details of Skipjack are classified. Due to this, government-authorised chip manufacturers can only implement it in hardware (not software). Skipjack is known to have an 80 bit key to encrypt 64 bit blocks of data, and 32 steps or rounds of processing to scramble the data. Skipjack is considered to be secure, however, due to its classified status, it has not undergone heavy scrutiny.

SAFER (Secure and Fast Encryption Routine)

SAFER is a block cipher algorithm with a 64 bit block size. Two versions of SAFER have been developed, one for 64 bit keys and the other for 128 bit keys. It has a variable number of rounds of processing with a minimum of 6 and a maximum of 10 rounds. SAFER is considered to provide secure encryption with fast software implementation even on 8 bit processors.

RC2 and RC4

RC2 and RC4 are ciphers designed by RSA Data Security, Inc. 'RC' stands for 'Ron's Code' or 'Rivest's Cipher'. RC2 is a block cipher with a block size of 64 bits and is almost three times faster than DES. RC4 is a very fast 'stream' cipher algorithm (i.e., an algorithm that operates on the plain text a single bit at a time).

RC5 and RC6

RC5 is a fast block cipher with a variable block size, a variable key size, and a variable number of rounds. The block size can be 32, 64 or 128 bits in length. The key can range from 0 bits to 2048 bits in size. The number of rounds can range from 0 to 255. This variability makes the algorithm secure and efficient. RC6 is based on RC5 and so too retains the same variability. The main goal of RC6 was to meet the requirements of the Advanced Encryption Standard (AES) which will replace DES as the federal standard.

Public-Key (Asymmetric) encryption systems

There are a variety of public-key algorithms available. The following is a list of the more common public-key encryption systems used and a brief description of each.

RSA (Rivest-Shamir-Adelman)

RSA is the most commonly used public key algorithm. It can be used both for encryption and for signing. It is generally considered to be secure when sufficiently long keys are used (512 bits is insecure, 768 bits is moderately secure, 1024 bits are probably secure enough for most purposes, and 2048 bit keys are likely to remain secure for decades). The security of RSA relies on the difficulty of factoring large integers. Dramatic advances in factoring large integers would make RSA vulnerable. RSA is currently the most important public-key algorithm.

Diffie-Hellman

Diffie-Hellman is a commonly used public-key algorithm for key exchange. It allows two users to exchange a secret key over an insecure medium. It is generally considered to be secure when sufficiently long keys and proper generators are used (it should be larger than 512 bits, preferably 1024 bits). Diffie-Hellman depends on the discrete logarithm problem for its security (put simply, the discrete logarithm problem is an example of a mathematical problem which is extremely difficult to resolve).

The ElGamal system

The ElGamal system is a public-key system based on the discrete logarithm problem. It consists of both encryption and signature algorithms. The encryption algorithm is similar in nature to Diffie-Hellman. ElGamal and RSA have similar security for equivalent key lengths. The main disadvantage of ElGamal is the need for randomness, and its slower speed.

Elliptic Curves

Elliptic curve public key systems are an emerging field. They have been slow to execute, but have become feasible with modern computers. Elliptic curve systems are analogs of public-key systems such as RSA and ElGamal, in which modular arithmetic is replaced by the elliptic curve operation.

The elliptic curve analogs do not seem to offer any significant advantage over RSA, as the underlying problem is the same and the key sizes are similar for equivalent levels of security. Two of their alleged advantages; resistance to "low-exponent" attacks, and to signature forgery against a chosen message attack; have recently been shown not to hold. They are considered to be fairly secure, but haven't yet undergone the same scrutiny as RSA.

DSA (Digital Signature Algorithm)

DSA is based on the discrete logarithm problem and is used for authentication only. The algorithm is generally considered secure when the key size is large. DSA has been criticised since its release. Such criticism includes a lack of key exchange capability; not enough vigorous scrutiny to be confident of its strength; and verification of signatures are too slow.

LUC

LUC is a public-key system that uses Lucas sequences (based on factoring two large primes) instead of exponentiation. LUC implements the analogs of ElGamal, Diffie-Hellman, and RSA over Lucas sequences. Many of the supposed security advantages of LUC over systems based on modular exponentiation are either not present, or not as substantial as claimed.

McEliece system

The McEliece system is a public-key encryption algorithm based on algebraic coding theory. The system uses a class of error-correcting codes, known as the Goppa codes, for which fast decoding algorithms exist. The basic idea is to construct a Goppa code as the private key and disguise it as a general linear code, which is the public key. The general linear code cannot be easily decoded unless the corresponding private matrix is known. However, there is a number of drawbacks such as large public-key sizes and substantial expansion of data.

Knapsack systems

The knapsack system is based on the subset sum problem in combinatorics (again, put simply the subset sum problem is a problem which is difficult to solve and is therefore used as a base in an encryption system in an attempt to make it secure). Certain cases of the problem are relatively easy to solve making the knapsack system vulnerable to attacks.

REFERENCES

RSA Security - Bulletin 13 - April 2000
'A cost-based security analysis of symmetric and asymmetric key lengths'
rsasecurity.com/rsalabs/bulletins/bulletin13.html

Dorothy E Denning
A taxonomy for key recovery encryption systems
Descriptions of key escrow systems
www.cs.gerorgetown.edu/~denning/crypto/taxonomy.htm

Matthew Curtin and Justin Dolske
A brute force search of DES keyspace
www.interhack.net/pubs/des-key-crack.htm

Matthew Curtin
What DESCHALL means
www.interhack.net/projects/deschall/what.htm

Brian Gladman
Key recovery - meeting the needs of users or key escrow in disguise?

ANNEX VIII

MANDATE, COMPOSITION OF TAG, WORKPLAN AND SCHEDULE OF MEETINGS

The specific mandate of the Professional Data Assessment TAG

Purpose

The purpose of the Professional Data Assessment Technical Advisory Group (PDA TAG) is to provide input into the OECD's work in taking forward the tax administration conditions, contained in Section V of the report, *Electronic Commerce: Taxation Framework Conditions* (the Taxation Framework Report), which was welcomed by Ministers meeting in Ottawa in October 1998. The tax administration conditions are:

- 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.
- Countries should ensure that appropriate systems are in place to control (audit/verify) and collect taxes.
- International mechanisms for assistance in the collection of tax should be developed.

Section VI of the taxation framework report indicates that Revenue authorities will work through the OECD and in consultation with business to identify concrete substantive steps that can help implement and extend the taxation framework conditions. Revenue authorities were also to consider the feasibility and practicality of those steps, including:

- Developing internationally compatible information requirements, such as acceptance of electronic records, format of records, access to third party information and other access arrangements and periods of retention and tax collection arrangements.

General

- To advise about any relevant international standards or statements of best practice or similar pronouncements which are relevant for accessing electronic data, books and records, authenticating them or assessing their reliability.

Authenticity

- To advise on ways and means of using existing and developing technology, or adapting technology, to authenticate electronic data, books and records relevant to tax, including receipts, invoices and other source documentation maintained by a business.
- To advise on developments and practices that may affect the authentication of electronic data, books and records and to examine methods used by private sector professionals to address these developments and practices.

Reliability

- To advise on how private sector professional auditors satisfy themselves about the reliability, completeness and accuracy of electronic data, books and records.
- To advise on how existing and developing technology can be used or developed to ensure that electronic data, books and records are at least as complete and reliable as their physical equivalents.

Accessibility

- To advise on how, in accordance with domestic law and practice on access to records, existing and developing technologies can be used or developed to remotely access electronic data, books and records of a business which are relevant to tax.
- To advise on how existing and developing technology, software and electronic tools can be used to provide more convenient access to data, books and records held by a business which are relevant to tax.

Best practices

- To advise on specific techniques, software, electronic tools and best practices developed by private sector professionals relating to the gathering and verification of the electronic data, books and records of a business which are relevant to tax
- To advise on best practice considerations by private sector professionals to reduce the burden on businesses during external audits of electronic data, books and records of a business.

PDA TAG Workplan

Notes

Teams

As there is so much material to be covered within the two-year life span of the TAG, the Secretariat suggests that it could be taken forward by teams. This would allow task 1 and task 3, (discussed below) for example, to be taken forward at the same time.

The work of the teams would be posted to the EDG so that every participant in the TAG can see developments on each task, and post comments if they wish. Teams will be chosen near the commencement date of each task based on the availability and interest of participants. Teams will be composed of private sector and public sector participants. A person may (will) be a member of multiple teams during the life of the TAG.

Workplan ideas

Preamble

While private sector auditors can be either internal or external auditors, taxation auditors are external auditors. Given that the TAG was created to help tax administrations address the challenges of electronic commerce, it will primarily have an external audit focus. However, external auditors must place appropriate reliance on internal audit controls and so, during the work of the TAG, participants may generate views on internal audit issues. In this context, the TAG will attempt to identify any new challenges posed by electronic data held by a taxpayer or client and created in an open Internet environment (as opposed to a closed EDI-type environment).

Tasks

1. The TAG will compile a list of any current or emerging standards or statements of best practice or similar pronouncements which are relevant for accessing electronic data, books and records, authenticating them or assessing their reliability and extract the common or "best practice" elements if possible.

(Covers point 1 of the Mandate)

Commence: Immediate
Compile list: 3 September 1999
Finalise: 1 October 1999
Report: November 1999.
Note: Ongoing revision may be required for emerging standards
Team: Team 1

2. ***The TAG will conduct a survey of public sector and private sector auditors, dealing with electronic commerce records, and report on any new opportunities, challenges, developments or practices relevant to the accessibility, authenticity and reliability of data.***

(Covers point 2 - dot 2, point 3 - dot 1, point 4 - dot 2 of the Mandate and Implementation Option 16 - partly)

Commence: Immediate
Survey out: 23 July 1999
- dissemination to government auditors via FSM, WP8, WP9
- dissemination to business via business members, itaudit.org, others(?)
- dissemination to public via public EDG

Return: 24 September 1999 - Discussion at possible PDA TAG in early October 1999
Finalise: 19 November
Report: November 1999.
Team: Team 2

3. ***The TAG will attempt to identify and report upon the desirable data elements for business and tax purposes, expected in accountable trading, payment or transaction recording systems.***

(Covers CT letter, p15, para 31 dot 3, dot 4, dot 7 - partly and context setting work that will help us with Implementation Option 13 and 15)

Commence: Immediate
Draft: 24 September 1999 - Discussion at possible PDA TAG in early October
Finalise: 3 November 1999
Report: November 1999
Team: Team 3

4. ***The TAG will catalogue existing or emerging mechanisms that can provide "authenticity" of data, including digital signatures and other uses of cryptography, report on the costs and benefits of their use and attempt to recommend the most appropriate mechanisms.***

(Covers point 2, dot 1 of the Mandate)

Commence: December 1999
Catalogue: 28 January 2000 - Report to FSM sub-group, February 2000
Finalise: 31 March 2000
Report: May 2000
Team: Team 4

5. ***The TAG will catalogue existing or emerging mechanisms that can provide "reliability" of data, including digital notarisation and data recordation techniques etc, report on the costs and benefits of their use and attempt to recommend the most appropriate mechanisms.***

(Covers point 3 - dot 2 of the Mandate)

Commence: December 1999
Catalogue: 28 January 2000
Finalise: 31 March 2000
Report: May 2000

Team: Team 5

6. ***The TAG will catalogue existing or emerging mechanisms for "remote access", report on the costs and benefits of their use and attempt to recommend the most appropriate mechanisms.***

(Covers point 4 - dot 1 - partly and point 4 - dot 2 of the Mandate and CT letter, p3, Q3 - partly)

Commence: April 2000
Catalogue: 26 May 2000
Finalise: 28 July 2000
Report: December 2000
Team: Team 6

7. ***The TAG will catalogue existing or emerging mechanisms to protect against or recover from loss of encryption keys, report on the costs and benefits of their use and attempt to recommend the most appropriate mechanisms.***

(Covers Implementation Option 16 when combined with work item 2, above)

Commence: April 2000
Catalogue: 26 May 2000
Finalise: 11 August 2000
Report: December 2000
Team: Team 7

8. ***Taking into account work undertaken in tasks 1 through 7 and any other relevant research, the TAG will develop, if possible, proposals for consideration by the TAG's supervising body on "authenticity", "reliability", "remote access", "key protection" and "electronic payment systems" etc. The Committee on Fiscal Affairs, based on advice from the TAGs supervising body, may use these proposals in publications or in submissions to appropriate "standards bodies" or both, to try to influence the development of "standards" in a mutually acceptable manner.***

(Covers point 5 - dot 1 of the Mandate and Implementation Option 14)

Commence: Immediate
Interim: Preliminary views offered as required to standards bodies or others
Draft: 11 August 2000
Finalise: 1 December 2000
Report: December 2000
Team: Team 8

9. ***The TAG will develop a position paper(s) about ways to reduce the burden on a client during audits, within acceptable risk parameters, based on use of the existing or emerging mechanisms and best practices. This should address differences between expectations for large and small businesses, for example.***

(Covers point 5 - dot 2 of the Mandate)

Commence: July 2000
Draft: 25 August 2000
Finalise: 27 October 2000
Report: December 2000
Team: Team 9

Composition of the TAG

The following people participated in the activities of the TAG and attended one or more of its meetings.

Full Name	Company/Organisation
Mr. Akira MATSUO (Business Co-Chair of the TAG)	Chuo Aoyama Audit Corporation, Japan
Mr. Declan RIGNEY (Government Co-Chair of the TAG)	Office of the Revenue Commissioners, Ireland
Government representatives	
Mr. Michael HARDY	Australian Tax Office
Mr. John MEYER	Australian Tax Office
Mr. Pierre PERON	CCRA, Canada
Ms. Nadine DELAUR	Ministère des finances, France
Mr. Antoine GLAIZE	Ministère des finances, France
Mr. Hervé GOUZIEN	Direction générale des impôts, France
Mr. Rob VLAAR	EDP, the Netherlands
Ms. Karen McGEOUGH	Inland Revenue Corporates, New Zealand
Mr. Domingo CARBAJO VASCO	Ministerio de Hacienda, Spain
Mr. Fred WALL	HM Customs & Excise, United Kingdom
Mr. Stewart WESTON-LEWIS	Inland Revenue, United Kingdom
Mr. Elvin HEDGPETH	Internal Revenue Service, United States
Mr. Mike RICKUS	Internal Revenue Service, United States
Mr. Richard WEAKLAND	Internal Revenue Service, United States
Mr. Joseph WEST	Internal Revenue Service, United States
Business representatives	
Mr. Joe FEUER	BIAC
Mr. Robin MATHIESON	International Federation of Accountants (IFAC)
Ms. Anne MOLYNEUX	CPA Australia
Ms. Valerie RAINEY	AICPA, United States
Mr. Richard REGAL	International Federation of Accountants (IFAC)
Mr. Trevor STEWART	Deloitte & Touche, United States
Mr. Bill STROMSEN	AICPA
Mr. Brad THIESSEN	ACL Services Ltd
Ms. Lily SHUE	ISACA, United States
Mr. Marc VAEL	Arthur Andersen, Belgium

Schedule of meetings held

1st meeting	Washington	20-21 April 1999
2nd meeting	Stanford University, California (joint meeting with TECH and CTTAGs)	1-2 June 1999
3rd meeting	Dublin	2-3 November 1999
4th meeting	New York (joint meeting with TECH TAG)	31 July-1 August 2000
5th meeting	Paris	25-27 September 2000