IFAC

Information

Technology

Committee

March 2002

E-Business and the Accountant

Issued by the International Federation of Accountants

E-BUSINESS AND THE ACCOUNTANT

The mission of the International Federation of Accountants (IFAC) is the worldwide development and enhancement of an accountancy profession with harmonized standards, able to provide services of consistently high quality in the public interest.

This paper has been prepared by the Information Technology Committee of IFAC to promote awareness among all accountants of the increasing impact of e-business on the work of accountants and key issues which need to be addressed. The paper explores the role of accounting professionals in the world of electronic business and the influence of technological advancements on the functions of accounting and financial reporting.

It is not intended to update this paper. However, IFAC welcomes any comments you may have. Comments should be sent to:

Technical Director
International Federation of Accountants
535 Fifth Avenue, 26th Floor
New York, New York 10017-3610 USA
Fax: +1 212-286-9570
edcomments@ifac.org

Copies of this paper may be downloaded free of charge from the IFAC website at http://www.ifac.org.

ISBN: 1-887464-79-4

E-BUSINESS AND THE ACCOUNTANT: RISK MANAGEMENT FOR ACCOUNTING SYSTEMS IN AN E-BUSINESS ENVIRONMENT

Preface

The Internet has affected all aspects of the business world. Even enterprises not directly conducting e-business are continually influenced by information and communication opportunities available through the Internet. The speed and convenience of the new technologies have not only provided unique new business opportunities, but also certain inherent risks. Our growing dependence on information technology and the continuing expansion of Internet use have brought those underlying risks to the forefront.

From a managerial perspective, recognition of the risks related to e-business is crucial. In particular, those responsible for the health of any organization must consider the impact of potential IT failures on the basic processes of the business, including accounting and financial reporting.

The Information Technology Committee of the International Federation of Accountants has produced this document to highlight some of the risk management implications of e-business. Because this new environment touches all businesses, this topic is relevant to financial managers, chief executives and all others involved in promoting and maintaining the viability of any enterprise.

IFAC's Information Technology Committee would like to thank the IDW Fachausschuss für Informationstechnologie [IDW Technical Committee for Information Technology] (FAIT) and, in particular, its chair, Klaus Heese, its technical advisor, Horst Kreisel and Wolfgang Böhm of the IDW. Furthermore, it would like to thank the IFAC IT Committee's chair, Everett C. Johnson Jr., and the members of its E-Business working party: Aidan Collins, John M. Court, Klaus Heese, Horst Kreisel and Robert G. Parker.

E-BUSINESS AND THE ACCOUNTANT: RISK MANAGEMENT FOR ACCOUNTING SYSTEMS IN AN E-BUSINESS ENVIRONMENT

CONTENTS

1. Introduction

This document presents certain risk management aspects of e-business relevant to accounting and financial reporting from a managerial perspective. Although it includes a short description of the major risks and opportunities associated with e-business, it focuses particularly on the management of IT risks in relation to accounting information. Furthermore, this document envisages a useful framework of concepts with which accountants and others can analyze e-business from an accounting point of view. Based on this framework of concepts, the document provides guidance to accountants on principles and criteria for accounting systems in an e-business environment.

E-business affects all enterprises — including those not actively pursuing e-business — because virtually all customers, competitors and suppliers are likely to be involved in e-business in some way, and their involvement will have an impact on the marketplace, both locally and globally. E-business will generate new opportunities and risks. There will be new opportunities in terms of suppliers, customers, geographic reach, electronic marketing and vertical marketplace growth through alliances. The risks will arise in relation to technology, software, customer base, customer and transaction authentication, electronic and digital signatures, electronic documents law, product approval and product liability, and personal information privacy, etc.

E-business significantly changes the way business is conducted. In particular, e-business requires changes in organizational structures, business partnerships and alliances, delivery mechanisms and methods, and the legislation and regulations under which businesses operate. E-business also introduces new risks that enterprises may need to address by implementing a technology infrastructure and controls to mitigate those risks. Furthermore, e-business alters the roles and responsibilities of employees and different levels of management, therefore affecting personnel requirements. Moreover, e-business affects not only business conduct, but also the character of business itself.

These fundamental changes will also have a significant impact on accounting systems, changing business processes and the evidence available to support business transactions which, in turn, will lead to changes in the accounting records maintained and accounting procedures followed. Consequently, accountants and auditors will face new challenges and may need to apply new techniques, such as the development of accounting systems based on business processes, to ensure that transactions are appropriately recorded, are in compliance with local and international legislation and regulations, and meet current and evolving accounting standards and guidance.

2. E-Business Risks and Opportunities

2.1. E-Business Opportunities

E-business through the Internet offers significant opportunities. Because these opportunities are similarly available to the competition, they also represent concomitant risks. Examples of such opportunities (and concomitant risks) include:

- **Competition:** Through the creation of a website, a business can compete locally in traditional industries, as well as regionally, nationally and globally. The Internet permits an entity to effectively target niche markets or areas of specialty and to service broad markets in a cost-effective manner. The Internet also permits both economies of scale (to become a high-volume global supplier with low costs) and economies of scope (through product specialization).

Even businesses that decide not to actively participate in e-business will still be affected, because customers may embrace e-business and seek new sources of supply through the Internet, or suppliers may demand e-business capabilities and deal only with e-enabled enterprises.

- **Marketing**: With the exception of certain national and international retailers and suppliers, traditional marketing has been concentrated locally or regionally. And, until recently, marketing efforts have been focused on traditional media, such as television and newspapers for consumer products and trade magazines or trade shows for industrial products. Through the Internet, marketing can be targeted to selected customers based on customer registration information, past purchase history or other criteria.

  Through the Internet, e-business can offer new and innovative marketing alternatives, such as:

  Streaming video to demonstrate products or services;

  Detailed catalogues and user manuals to identify products, subcomponents and parts — such as pictures, part numbers and prices — to alleviate tedious manual searches for specific items; and

  Cross-selling of products and services — e.g., when a tap is purchased through the Internet, the provision of detailed installation instructions and a list of other products required (washers, Teflon tape, valve sealing and tools, such as pipe wrenches, etc.).

- **Cost Reduction**: E-business facilitates implementation of new business models, including supply chains, service and support arrangements and the creation of cost-effective alliances. It also offers profit-enhancing changes through cost reduction, such as:

  Virtual warehousing. On receipt of a customer order, the vendor orders the goods from the manufacturer and has them shipped directly to the customer. The vendor can carry less or no inventory and, thereby, reduce warehouse, insurance and financing costs for inventory while being able to offer a greater selection of products.

  Vertical integration. On receipt of an order, by means of website connections, the vendor automatically arranges shipping, delivery, installation and after-sales service through an expanded geographically based network of alliance partners. All members of the alliance benefit from membership and all participate in the "one-stop-shopping" convenience of the alliance partner integration available through the web.

  Electronic delivery of goods and services. Certain goods, such as greeting cards, music, textual materials, architectural drawings and computer software may be delivered electronically to customers globally, which reduces delivery and insurance costs and increases the timeliness of delivery.

  Automated order processing. Customers and suppliers can execute electronic transactions efficiently based on Internet standards similar to the EDI standards and even access or update each other's data files to allow inquiries on the status of orders, including links with shippers and customs brokers, etc.

Classic business approaches generally do not fit well with the new e-business models described in the third section of this paper. These new models are increasingly centered on the customer or consumer. For example, many customers now expect goods and services to be delivered 24 hours a day from anywhere in the world. The ability to meet customers, discuss their needs with them, demonstrate products and perform other activities that traditional businesses use to differentiate their services may no longer be available to the same degree.

2.2. E-Business IT Risks

Since e-business invariably involves the use of the Internet through IT, the most important risks associated with e-business are IT risks. It should be recognized, however, that IT risks are inextricably related to the risks associated with the opportunities mentioned. The following IT risks can be distinguished: IT infrastructure, IT application and IT business process risks.

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

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

IT application risks result from:

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

IT business process risks arise where analyses of security and information processing do not extend to entire business processes, but merely to some parts of them. Such risks may arise from: lack of data flow transparency, inadequate integration of systems or deficient reconciliation and control procedures in interfaces between subprocesses arising from the exchange of data between two subsystems within business processes. In this situation, there is a risk that IT controls, such as access rights or data back-up procedures, will be effective only for the subprocesses, but not for the aggregated processes.

Typical IT business process risks in an e-business environment include:

- Transaction data are not transmitted efficiently, completely or accurately from the e-business subsystem to the accounting application;
- Safeguards protect only a certain subsystem from unauthorized or unapproved transactions and, thereby, allow transaction data to be modified by one of the downstream IT subsystems;
- Improper or inadequate access control mechanisms may make it difficult or impossible to effectively manage access controls for all IT subsystems integrated into the e-business process;
- Access protection that responds to a single IT application integrated into the business process could be bypassed deliberately by manipulating the upstream or downstream IT subsystems;

- Back-up measures are effective for only the e-business subsystem and, hence, for the subprocess, but not for the entire IT business process; and
- The design and implementation of interfaces between the e-business subsystem and downstream IT subsystems may not be appropriate.

2.3. E-Business Legal Risks

Management is responsible for ensuring that e-business operations are conducted in compliance with applicable laws and regulations. Enterprises should be aware that, despite the best efforts of international rule-making bodies, applicable laws and regulations will vary across national boundaries. Nevertheless, enterprises operating in global markets are often not up to date on legal issues and governmental oversight in multiple jurisdictions. Without understanding the regulations and the law applied in different jurisdictions, enterprises may be subject to fines and adverse judgments and may incur other costs, such as legal fees, to defend themselves should they inadvertently breach such laws. Some of the relevant legal issues include:

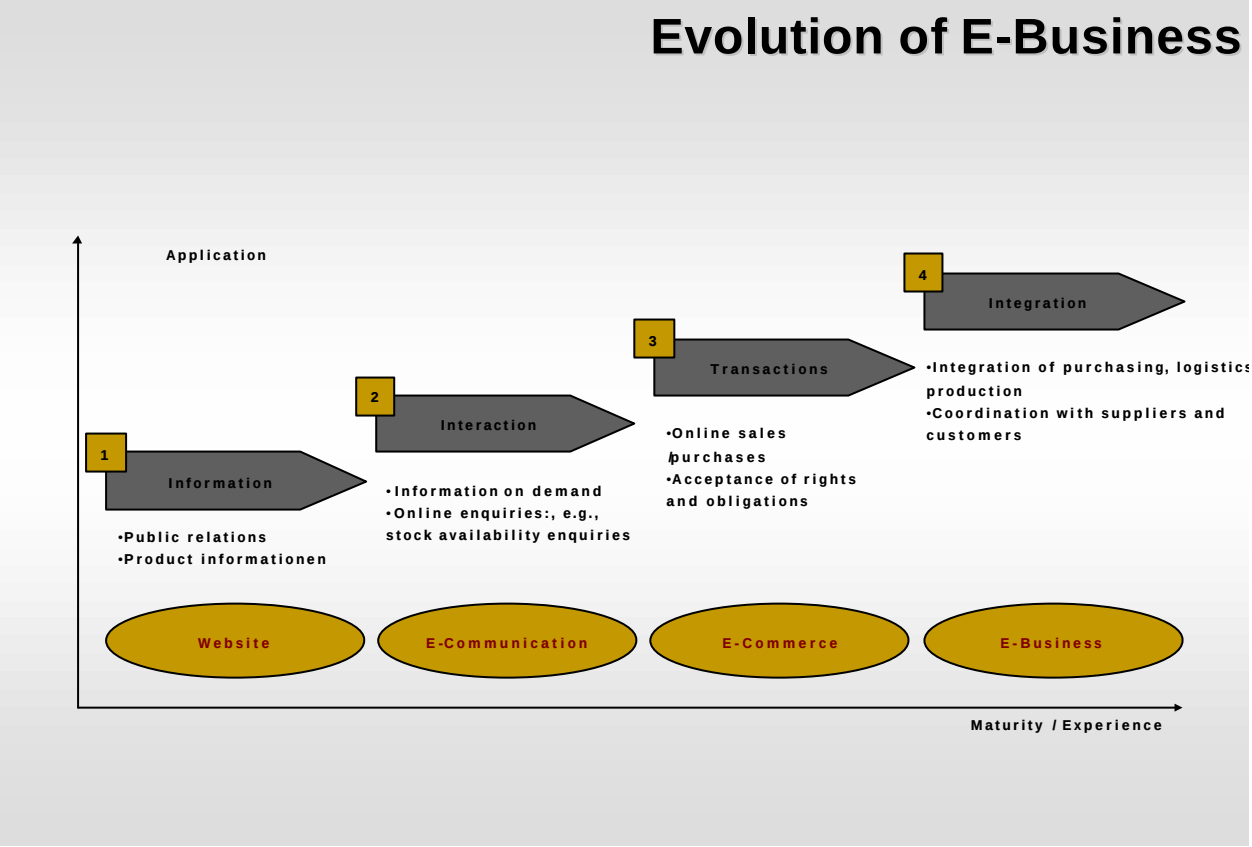
- Protection of intellectual property, including patent, copyright and trademark laws;
- Enforceability of contracts with Internet service providers; and
- Ownership of software by a software vendor or the right of a software vendor to sell software licenses.

Commercial legal risks also arise in connection with contract law and the purchase and sale of goods and services through the Internet across national boundaries. In particular, there may be problems in determining the appropriate jurisdiction for legal actions with respect to cross-border Internet transactions. Furthermore, where the applicable jurisdiction for the transaction is unclear, the requirements for entering into a contract may also be unclear, for these may vary in certain respects among jurisdictions. Therefore, in some situations, the question may arise as to whether there is a legally binding contract.

In addition, it should be noted that certain commercial activities that are not regulated in one jurisdiction might be regulated in another. Management is responsible for ensuring that regulated activities are performed in compliance with the laws in jurisdictions where those activities are conducted.

Furthermore, risks in relation to tax law compliance may also arise from e-business activities. In particular, it is often unclear in which jurisdiction taxes for cross-border transactions are payable (i.e., income or corporate tax and sales tax). A related issue is the documentation requirements for order processing and invoices to comply with tax legislation.

Management is also responsible for ensuring the privacy of personal information obtained as part of the enterprise's e-business activities. To help ensure privacy of personal information, management can establish controls to limit the risk of breaches of web security.



3. E-Business Systems and the Use of E-Business Systems in Enterprises

The use of the term *e-commerce* has already been superseded by the term *e-business*. E-commerce can be described as the procurement and distribution of goods and services over the Internet using digital technology. The more encompassing term e-business can be defined as including all activities carried on by a business via the Internet. This definition for e-business extends beyond the definition of e-commerce by encompassing a digital approach to the whole enterprise, including other parts of the IT system and other non-transactional activities, such as recruiting employees via the Internet. Because the mere definition of e-business does not fully convey the complexity of e-business reality, it may be useful to explain e-business in terms of the phases of an evolutionary process.

The first evolutionary phase in the development of e-business is the utilization of the Internet for information purposes. Websites used for browsing — like a shop window — might contain a catalogue (or parts of a catalogue). Information is conveyed in only one direction, which means that the Internet user can read the data only on the website, but cannot interact with the site other than to move from page to page.

The next phase enables the user to interact with the website. Customers can use a search engine to navigate, check the availability of goods or services or use other online information services, including

information on demand. In this phase, information is exchanged in both directions, since the website both captures and displays data.

An application reaches the e-commerce phase where a website's functions allow the procurement of goods and services that lead to the conclusion of financial transactions. Customers place orders for goods and services and pay by credit card.

The next phase of the evolutionary process is the complete integration of the e-business system within an enterprise's business processes. The Internet-based purchase of goods and services leads to interactions with other parts of the enterprise's IT system. For example, a purchase order initiated by the e-business system may automatically prompt the movement of goods from the warehouse system to the delivery department and lead to data being recorded in the management information system, including the accounting system, and to transactions with suppliers. Hence, the e-business system becomes an integral part of the enterprise's IT system. This is particularly true where sales are made globally and support is required in various geographical locations.

Such integration can be expanded to include direct links to shippers, installers and other related service providers with which the business has established contractual relations, and involves process integration with selected customers and suppliers to design and deliver products. This subsequent phase has been termed "collaborative-business" (c-business), but conceptually is still a part of the integration phase. Another advance is mobile business (m-business), which may involve additional strategic opportunities and the concomitant control and security issues because of the wireless elements.

Business models such as B2C and B2B have been widely referred to in the business media. Several new models have emerged; a summary of the current models is:

	Government	**Business**	**Consumer**	**Employee**
Government	G2G	G2B	G2C	G2E
Business	B2G	B2B	B2C	B2E
Consumer	C2G	C2B	C2C	X

The key models can be described as follows:

- B2C (Business to Consumer) — typically a retailer selling directly to the consumer; at present, this is the sector that has shown the fastest growth (lately B2B has shown the most growth potential — the B2C growth rate now appears to be decelerating).
- B2B (Business to Business) — typically a business selling up, down or across the supply chain, involving business partners or business consortia.
- B2E (Business to Employee) — typically a system enabling intercompany (intragroup) e-mails over the Internet to be directed to the correct department.

Examples for two of the other models would be:

- B2G — Electronic submission of corporate tax returns.
- C2G — Electronic submission of individual income tax returns.

E-business requires modern IT, which in turn necessitates an integrated consideration of the organization of business processes and IT implemented for this purpose. Hence, it is useful to analyze and describe

the IT system from the perspective of the business processes using IT (IT business processes). An IT system includes the following basic elements:

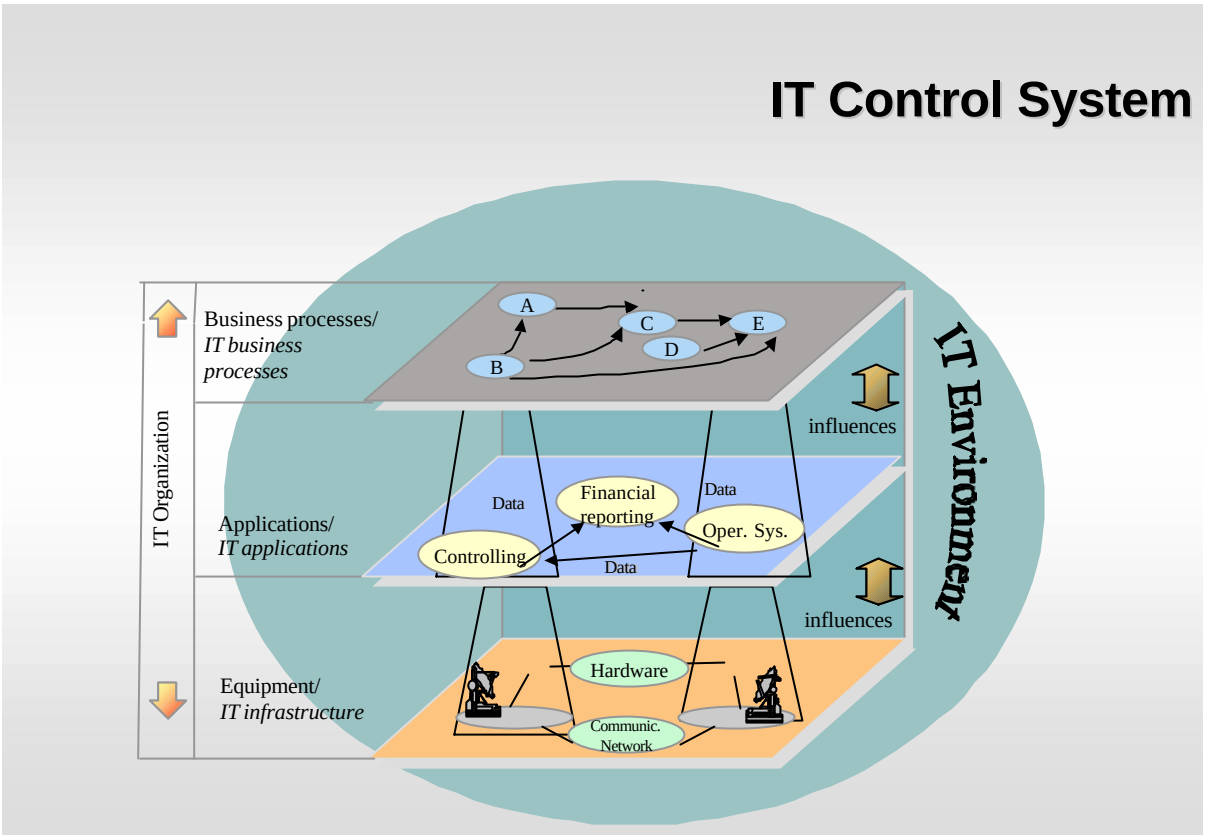
- IT business processes;
- IT applications; and
- IT infrastructure.

The IT control system controls how these elements operate together to achieve their objectives while reducing risk to a tolerable level.

An IT control system is part of the internal control system, which encompasses the internal management system and the internal monitoring system. The internal management system consists of policies and procedures for directing the enterprise's activities. The internal monitoring system monitors compliance with these policies and procedures.

An IT control system encompasses the principles, measures (arrangements) and procedures used to manage the risks resulting from the use of IT (IT risks). Hence, the IT control system includes policies to manage the use of IT in the enterprise (internal IT management system) and policies to monitor compliance with these policies (internal IT monitoring system).

IT controls form part of the internal IT monitoring system. An internal monitoring system includes both process-integrated and process-independent monitoring controls. Process-integrated controls are directly integrated into the design of particular business processes. An example of a process-integrated control would be an access control. In addition, IT controls include general controls that are independent of IT applications and that have an impact on the entire IT system (e.g., software development controls or change management controls). Process-independent controls would include internal audit and high-level controls.



The IT organization defines the responsibilities and competencies connected with the use of IT in an enterprise. On the one hand, it comprises arrangements for the development, implementation and modification of IT applications and, on the other hand, arrangements for managing the use of IT applications. IT applications can be used to manage an enterprise's business processes.

The IT environment is shaped by management's and employees' basic attitudes, problem awareness and behavior with regard to the use of IT.

For the purposes of this document, IT-aided business processes are defined as operationally or technically related activities of an enterprise in which IT is used. A feature of IT-based business processes that is relevant to accounting is the automatic transmission of information and data on operating activities (e.g., IT-aided warehouse management) directly into the accounting system through the use of integrated software solutions.

IT applications include both internally developed software and software purchased from third parties (customized or standard software) used in IT-aided business processes. IT applications software can be used either independently, when connected via interfaces, or in an integrated IT system.

The IT infrastructure reflects all of the technical resources necessary for the operation of the IT system. These technical resources consist of the fixtures and fittings of a computer center or computer room, the hardware, the operating system software, the communication installations required for internal and external networks and technical solutions for the operation and support of IT.

4. E-Business Accounting Principles and Criteria

Management is responsible for the attainment of the enterprise's objectives in accordance with the business strategy it has defined. If an e-business system is used for this purpose, it is important that management makes appropriate arrangements to manage the ensuing risks. An enterprise's e-business strategy as an integral part of the IT strategy ordinarily includes consideration of all aspects of business risks, including IT risks.

Consequently, management assesses IT risks with respect to information reliability. Information reliability depends on IT system reliability and IT system reliability depends on IT controls.

It is important that management implements IT controls that operate effectively to help ensure that an IT system performs reliably. Information generated by an IT system will be reliable where that system is capable of operating without material error, fault or failure during a specified period. This also applies to accounting information. The following principles may be used to evaluate whether processed accounting information is reliable:

- Principles for accounting information security; and
- Principles for appropriate accounting information processing.

4.1. Principles for Reliable Accounting Information

4.1.1. Principles for accounting information security

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

Management is responsible for meeting the prerequisites for accounting information security. To this end, it is necessary to develop, implement and maintain an appropriate security concept to ensure the required degree of information security.

A security concept comprises management's assessment of the security risks resulting from the use of IT and, derived from this, the technological and organizational measures needed to help ensure an adequate platform for IT applications and the appropriate and secure execution of IT-aided business processes.

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

- Integrity. This requirement is fulfilled for an IT system when data and information are complete and accurate, systems are complete and appropriate and all of these are protected against unauthorized modification and manipulation. Appropriate testing and release procedures are typical means by which the integrity of data, information and systems can be ensured. Technical measures to achieve this include firewalls and virus scanners. The reliability of IT-aided accounting processes is improved when the IT infrastructure and the data, information and IT applications are used in a specified configuration and only authorized modifications are permitted.

- Availability. Under this requirement, the enterprise ensures the constant availability of the hardware, software, data and information to maintain business operations and that the hardware, software, data, information and the requisite IT organization can be made operable within a reasonable period of time (e.g., after an emergency interruption). It is important, therefore, to establish appropriate back-up procedures for emergencies. In addition, the ability to convert digitally maintained books and records into human-readable format within a reasonable period of time is essential.
- Confidentiality. This requirement means that data obtained from third parties not be transmitted or disclosed without authorization. Organizational and technical measures, such as encryption technologies, include instructions to restrict the transmission of personal data to third parties, transmit encrypted data to authorized third parties, identify and verify the recipient of data and to delete stored personal data after a certain length of time.
- Authenticity. This requirement relates to the traceability of a business transaction to the individual who initiated it. This can be done by, for example, using an authorization procedure. When data or information are exchanged electronically, it is important that the other party be identified or identifiable – e.g., by using digital signature procedures. It may be convenient to use shared external or independent facilities (e.g., trust centers) for this purpose.
- Authorization. This requirement means that only certain persons, appointed in advance (so-called authorized persons), may access certain data, information and systems (e.g., password protection) and that only authorized persons can use the rights defined for this system. This includes reading, creating, modifying and deleting data or information or the administration of an IT system. Useful methods to achieve this are physical and logical security procedures. Organizational arrangements and technical systems for access protection are essential to segregate incompatible duties. Biometric systems will become more common in future to supplement ID cards and passwords.
- Non-repudiation. This requirement is defined as the ability of IT-aided procedures to bring about desired legal consequences with binding effect. It should be difficult for the person initiating the transaction to deny its validity on the grounds that the transaction was unintended or unauthorized. The use of public key systems can help prevent repudiation.[1]

The preceding security requirements also help serve to meet the need for the privacy of information. In an e-business environment, securing privacy of information has become a necessity. Unfortunately, there is no generally accepted definition of privacy. At a most basic level, privacy of information is tied to the ownership of information (e.g., information about products and business strategies belong to the enterprise, whereas individuals have ownership of information that they provide about themselves). Even though privacy and confidentiality are highly related, confidentiality does not automatically assure that privacy is not being abused or violated. If the use or sale of sensitive private information is not appropriate for a specific e-business model, privacy problems will still surface despite a secure IT system.

Since there are no universally accepted definitions as to what constitutes the ownership and privacy of information, it is important to develop and publish a privacy policy as an essential part of security policy. This privacy policy establishes the agreement between the information provider and the information recipient as to the use of the information exchanged. It may be expedient, therefore, to publish a description of the privacy policy in management's privacy statement on the website.

---

1 The primary advantage of public key cryptography is that private keys never need to be transmitted. A sender cannot repudiate a message by claiming the key was compromised during transmission by the other party. Users have sole responsibility for protecting their private keys.

The European Union's Directive 95/46 is relevant to privacy issues, but the principles of the EU Directive have not yet been enacted in Europe. In April 2000, Canada passed the Personal Information Protection and Electronic Documents Act, which incorporates many Directive concepts. Under the safe harbor principles of the European Union, enterprises should inform individuals as to why they are collecting private information about them.

Consequently, it is important that management assess the legal requirements in countries where their customers, suppliers or service providers are located to determine the degree of privacy that the law requires. Under the EU safe harbor principles, management is responsible for ensuring that the privacy of data used to accomplish a transaction is not compromised somewhere in the supply chain or order fulfillment process.

4.1.2. Principles for appropriate accounting information processing

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

The reliability of accounting information relating to the entire e-business process is increased if the accounting system satisfies both accounting information security principles and the principles for appropriate accounting information processing.

The principles for appropriate accounting information processing are fulfilled where the e-business system and the entire IT system safeguards comply with the following general criteria for the input, processing, output and storage of information and data about e-business transactions:

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

The *completeness* criterion refers to the extent and scope of processed e-business transactions, i.e., the recipient of transactions determines that all transactions are input completely into the e-business system. Each transaction should be individually identifiable and recorded separately. The completeness of the recorded entries should be demonstrably preserved throughout processing and for the duration of the retention period.

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

Under the *timeliness* criterion, e-business transactions should be recorded on a timely basis, i.e., as soon as possible after the transaction has occurred. When some time elapses between the occurrence of a

transaction and its recording, further appropriate action may become necessary to determine completeness and accuracy of the entry recorded.

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

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

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

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

- That all transaction details have been entered by the customer;
- The authenticity of the customer;
- The availability of the products or services to be supplied;
- The reasonableness of the order, for example, to identify an unusually large quantity resulting from an input error, or to identify erroneous duplicate orders;
- The pricing structure applied, including delivery costs, where appropriate;
- The method of payment or credit worthiness of the customer; and
- The non-repudiability of the transaction in that its author cannot later deny having entered into it.

In an e-business process, it is often not possible to provide evidence of transactions by way of conventional vouchers — nor should it be. Despite this fact, transactions should continue to be supported by appropriate documentary evidence (i.e., the source document entry function).

4.2. The Criteria for a Functioning Accounting System

4.2.1. Source document entry function

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

source document entry function provides evidence for an enterprise's management accounting and financial reporting.

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

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

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

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

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

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

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

4.2.2. Journal function

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

In a journal function, entries are stored in an analyzable form (itemized) in the e-business applications upstream of the accounting system and by transferring aggregate entries. In addition to process

documentation, a control and reconciliation system may be used to demonstrate that the entries stored in non-accounting applications are identical to those in the general ledger and subledgers.

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

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

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

4.2.3. Ledger function

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

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

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

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

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

4.3. Documentation

A prerequisite for the transparency of the e-business and IT system is adequate procedural documentation that contains a description of all of the system elements needed to understand the e-business process. An expert third party is able to assess the appropriateness of complex procedures only

if he or she has access to informative documentation to supplement input data and processing results. It is important that documentation created to understand an e-business process be adequately maintained so that the appropriateness of the processing of the accounting information can be assessed.

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

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

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

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

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

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

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

4.4. Retention Requirements for E-Business Transactions

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

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

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

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

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

The related technical and organizational requirements include:

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

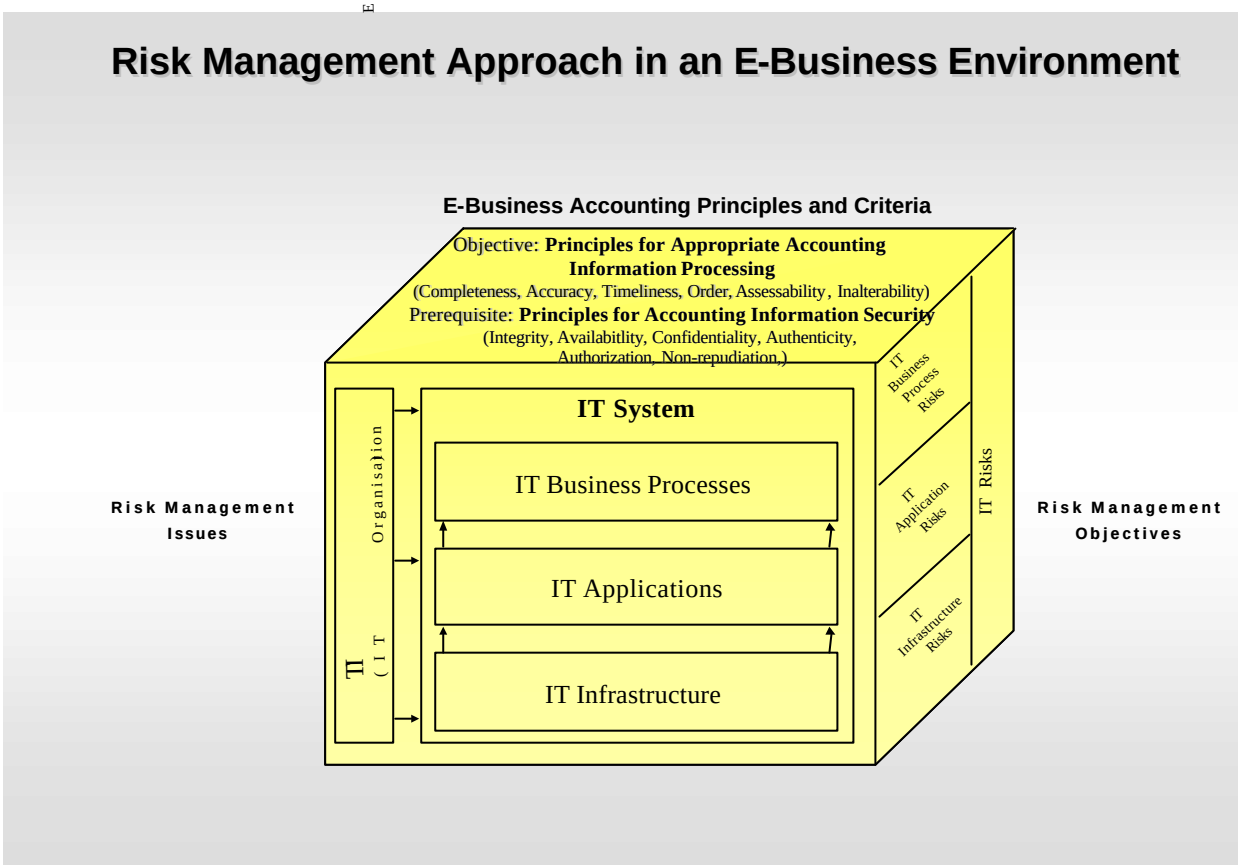
5. Conclusion

Management sets the enterprise's e-business objectives to help meet the overall business objectives. To attain the enterprise's e-business objectives and manage the risks and opportunities identified, management brings its IT strategy in line with its e-business strategy and establishes an appropriate IT control system. The IT strategy also depends on the complexity and diversification of the enterprise's e-

business activities and organizational structure and would include an evaluation of IT risks resulting from e-business activities that may affect the accounting system and the financial statements.

IT risks may also endanger the continuing existence of enterprises (the going concern problem) whose business activities are highly dependent on IT. Such risks should be identified, analyzed and assessed by the risk management system.

The risk-driven approach to managing IT risks in an e-business environment can be depicted as follows:



IT business processes, applications and infrastructure can be regarded as an integral part of the IT system. Consequently, IT business processes may directly affect the accounting system and, hence, the reliability of any information or data that it produces. This means it is important that information security and processing requirements be considered when designing IT business processes. These considerations naturally lead to an IT business process-driven perspective of IT risk management.

Appendix 1: Glossary of Terms

This glossary provides common definitions of some of the terms in this document and in contacts with clients or e-business vendors. Some of the definitions have been simplified for conciseness and ease of understanding.

Affiliate Programs	cooperative arrangements that involve providing a link to another web site in exchange for a commission on purchases made by users following that link to the other web site.
Application Service Provider (ASP)	an organization that provides software applications over the Internet. A common example is an Internet Service provider (ISP).
ADSL	see Asymmetric Digital Subscriber Line.
ASP	see Application Service Provider.
Asymmetric Digital Subscriber(ADSL)	a dedicated connection to the Internet that is suitable for individual and small business use. It is quicker for downloads than for uploads.
Auto-Responder	a feature of some e-mail programs that can be set to provide an automatic response to incoming messages. It is frequently used by business to acknowledge the receipt of a customer's messages and to provide a timeframe for the response. It is also used by individual employees to send a response to messages when they are out of the office.
Backbone	a top-level, high-speed connection to the Internet that serves as a major access point for ISPs and major users of the Internet (e.g., large business).
Bandwidth	the amount of information that can be carried through a communication system in a set time.
Bookmarks/Favorites	a list of web pages visited and to which one will likely return that are created by Internet browsers such as Netscape and Internet Explorer. These bookmarks are direct links to the web page.
Cookie	a small text file that is put on users' hard drives when they visit a web page so that other web pages can remember certain information about the user.

Digital Signature	a code that can be attached to a transmission (e.g., e-mail message, order request, etc.) that authenticates the sender.
Domain Name	a name designated to represent a location on the Internet such as the address for a web site.
Domain Name Server (DNS)	a server that associates a number (IP Address) with a text-based domain name.
DNS	see Domain Name System.
E-Business	including all activities carried on by a business via the Internet.
E-Commerce	the procurement and distribution of goods and services over the Internet using digital technology.
E-Marketplace	an online marketplace where buyers and sellers can exchange goods and services. Normally relates to business-to-business transactions.
Encryption	the encoding of a message or electronic transmission to prevent unauthorized access.
Favorites	see Bookmarks.
FAQ	see Frequently Asked Questions.
Firewall	hardware and software used to prevent unauthorized access to a computer or network.
Frequently Asked Questions (FAQ)	a list of answers to commonly asked questions, especially on a web site.
GIF	see Graphics Interchange Format.
Graphical User Interface (GUI)	a graphical tool that allows users to access the features and functionalities of a software application. On the web, it refers to the parts of the web site the users actually see, and would not include the back end software such as the database and programs that power the site.
Graphics Interchange Format (GIF)	one of the two common formats for graphics on the web (the other being JPEG).
Permission Marketing	involves persuading customers to physically request that marketing information be sent to them (sometimes called opt-in marketing).

POP (Post Office Protocol or Point Of Presence)	Post Office Protocol refers to the way that e-mail software gets mail from a mail server. Point of Presence usually refers to the locations where a dial-up connection to a mail server is available.
Portal	a web site used as a primary starting point to get to other web sites. It often refers to search directories like Yahoo and Search Engines like Google.
Search Directory	a human-compiled directory of information on the web sorted under meaningful categories (e.g., Yahoo, About, open directory).
Search Engine	a computer program that automatically seeks out websites, creates an index of these sites and then allows you to search the index (e.g., Altavista, Alltheweb, Hotbot).
Secure Sockets Layer (SSL)	a way to encrypt data that is transmitted over the Internet (commonly used in B2C e-business).
Service Level Agreement (SLA)	an agreement between an ASP and a user that describes the level of service expected during the duration of the contract.
SLA	see Service Level Agreement.
SPAM	a term used to describe unsolicited and unwanted messages sent to an e-mail address or to an online discussion group.
Splash Page	an initial web page that is used to capture the user's attention and is usually as a lead-in to the home page.
SSL	see Secure Sockets Layer.
Stickiness	a term used to describe the ability of a web site to keep users on the site. Usually measured by the average length of time visitors spend on a web site.
T1 (also T3)	high speed, high bandwidth, dedicated connections to the internet. T1 offers 20 times the bandwidth of a 56K modem. A T3 connection is made up of 28 T1 lines.
24/7	refers to services offered 24 hours a day, 7 days a week.
Traffic	refers to the amount of visitors that a web site receives.
URL	see Uniform Resource Locator

Uniform Resource Locator (URL)	is another way of describing a web page address. When a URL is entered into a web browser, it will be bring the user to that site.
Viral Marketing	involves using the customer as a sales person to encourage others to use a product/service.
Web Site	generally a set of web pages all located within the same URL.
World Wide Web (or WWW or the Web)	a series of html documents all connected using the Internet.
www	see World Wide Web.

Appendix 2: Bibliography

Auditing Practices Board [UK]. *Draft Bulletin on the Electronic Publication of Auditors' Reports.* London, 2001.

E-Business: Identifying Financial Statements Risks. London, 2001.

Australian Accounting Research Foundation. *Audit Issues Relating to the Electronic Presentation of Financial Reports AGS 1050.* Melbourne, 2000.

Electronic Commerce and Its Impact on Audits AAA8. Melbourne, 2000.

Auditing Guidance Statement (AGS) 1050, Audit Issues Relating to the Electronic Presentation of Financial Report. Melbourne, December 1999.

Auditing Guidance Statement (AGS) 1056, Electronic Commerce: Audit Risk Assessments and Control Considerations. Melbourne, August 2000.

British Computer Society. *E-Commerce (A World of Opportunity*). London, 1999.

Canadian Institute of Chartered Accountants. *Information Technology Control Guidelines, 3rd edition.* Toronto, 1998.

Fröhlich, Dipl.-Kfm. Dr. Martin, und WP StB Dipl.-Kfm. Klaus Heese. *Ordnungsmäßigkeit und Sicherheit der rechnungslegungsbezogenen Informationssysteme im E-Business [Appropriateness and Security of Accounting Information Systems in an E-Business Environment]*. Düsseldorf: Die Wirtschaftsprüfung, 2001.

Greenstein, Marilyn and Todd Feinman. *Electronic commerce: Security, Risk Management and Control.* London: Irwin McGraw Hill, 1999.

Institute of Chartered Accountants of England and Wales — Faculty of Information Technology. *Introducing Information Security.* London, 1998.

A Practical Guide to Implementing Information Security, London, 1998.

Information Security Myths and Reality. London, 1999.

Establishing an E-Business. London, 2000.

Business on the Web. London, 1998.

Institut der Wirtschaftsprüfer in Deutschland e.V. Entwurf IDW Stellungnahme zur Rechnungslegung: Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie (IDW ERS FAIT 1) *[Draft IDW Accounting Principle: Principles of Proper Accounting When Using Information Technology (Draft IDW AcP FAIT 1)]*. Düsseldorf, 2001.

Entwurf IDW Prüfungsstandard: Abschlussprüfung bei Einsatz von Informationstechnologie (IDW EPS 330) *[Draft IDW Auditing Standard: The Audit of Financial Statements in an Information Technology Environment (Draft IDW AuS 330)]*. 2001.

International Auditing Practices Committee (of the International Federation of Accountants). *Electronic Commerce Using the Internet or Other Public Networks— Effect on the Audit of Financial Statements. Exposure Draft.* New York, 2001.