

G22 BUSINESS-TO-CONSUMER E-COMMERCE REVIEWS

The specialised nature of information systems (IS) auditing and the skills necessary to perform such audits require standards that apply specifically to IS auditing. One of the goals of ISACA[®] is to advance globally applicable standards to meet its vision. The development and dissemination of the IS Auditing Standards are a cornerstone of the ISACA professional contribution to the audit community. The framework for the IS Auditing Standards provides multiple levels of guidance:

- **Standards** define mandatory requirements for IS auditing and reporting. They inform:
 - IS auditors of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
 - Management and other interested parties of the profession's expectations concerning the work of practitioners
 - Holders of the Certified Information Systems Auditor[™] (CISA[®]) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.
- **Guidelines** provide guidance in applying IS Auditing Standards. The IS auditor should consider them in determining how to achieve implementation of the standards, use professional judgement in their application and be prepared to justify any departure. The objective of the IS Auditing Guidelines is to provide further information on how to comply with the IS Auditing Standards.
- **Procedures** provide examples of procedures an IS auditor might follow in an audit engagement. The procedure documents provide information on how to meet the standards when performing IS auditing work, but do not set requirements. The objective of the IS Auditing Procedures is to provide further information on how to comply with the IS Auditing Standards.

Control Objectives for Information and related Technology (CobIT[®]) is published by the IT Governance Institute[®] (ITGI[™]). It is an IT governance framework and supporting tool set that allows managers to bridge the gaps amongst control requirements, technical issues and business risks. CobIT enables clear policy development and good practice for IT control throughout organisations. It emphasises regulatory compliance, helps organisations increase the value attained from IT, enables alignment and simplifies implementation of the CobIT framework's concepts. CobIT is intended for use by business and IT management as well as IS auditors; therefore, its usage enables the understanding of business objectives and communication of good practices and recommendations to be made around a commonly understood and well-respected framework. CobIT is available for download on the ISACA web site, www.isaca.org/cobit. As defined in the CobIT framework, each of the following related products is organised by IT management process:

- **Control objectives**—Generic statements of minimum good control in relation to IT processes
- **Management guidelines**—Guidance on how to assess and improve IT process performance, using maturity models; Responsible, Accountable, Consulted and/or Informed (RACI) charts; goals; and metrics. They provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:
 - Performance measurement
 - IT control profiling
 - Awareness
 - Benchmarking
- **CobIT Control Practices**—Risk and value statements and 'how to implement' guidance for the control objectives
- **IT Assurance Guide**—Guidance for each control area on how to obtain an understanding, evaluate each control, assess compliance and substantiate the risk of controls not being met

A **glossary** of terms can be found on the ISACA web site at www.isaca.org/glossary. The words audit and review are used interchangeably in the IS Auditing Standards, Guidelines and Procedures.

Disclaimer: ISACA has designed this guidance as the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics. ISACA makes no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the controls professionals should apply their own professional judgement to the specific control circumstances presented by the particular systems or IT environment.

The ISACA Standards Board is committed to wide consultation in the preparation of the IS Auditing Standards, Guidelines and Procedures. Prior to issuing any documents, the Standards Board issues exposure drafts internationally for general public comment. The Standards Board also seeks out those with a special expertise or interest in the topic under consideration for consultation where necessary. The Standards Board has an ongoing development programme and welcomes the input of ISACA members and other interested parties to identify emerging issues requiring new standards. Any suggestions should be e-mailed (standards@isaca.org), faxed (+1.847. 253.1443) or mailed (address at the end of document) to ISACA International Headquarters, for the attention of the director of research, standards and academic relations. The material was issued 15 October 2008.

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states, 'During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.2 Linkage to Guidelines

1.2.1 Guideline G14 Application Systems Review provides guidance.

1.2.2 Guideline G16 Effect of Third Parties on Organisation's IT Controls provides guidance.

1.2.3 Guideline G17 Effect of Nonaudit Roles on the IS Auditor's Independence provides guidance.

1.3 Linkage to COBIT

1.3.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To help meet the business-to-consumer (B2C) e-commerce review requirements of IS auditors, the processes in COBIT most likely to be relevant, selected and adapted are classified here as primary and secondary. The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment.

1.3.2 For B2C e-commerce and IT-based businesses, all of the IT processes relating to the COBIT domains—Plan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS) and Monitor and Evaluate (ME) are relevant. Primary IT processes are:

- PO1 *Define a strategic IT plan*
- PO2 *Define the information architecture*
- PO3 *Determine technological direction*
- PO9 *Assess and manage IT risks*
- AI2 *Acquire and maintain application software*
- AI3 *Acquire and maintain technology infrastructure*
- AI4 *Enable operation and use*
- AI6 *Manage changes*
- AI7 *Install and accredit solutions and changes*
- DS1 *Define and manage service levels*
- DS2 *Manage third-party services*
- DS3 *Manage performance and capacity*
- DS4 *Ensure continuous service*
- DS5 *Ensure systems security*
- ME2 *Monitor and evaluate internal control*
- ME3 *Ensure compliance with external requirements*

1.3.3 The information criteria most relevant to a B2C audit are:

- Primary: Availability, compliance, confidentiality, effectiveness and integrity
- Secondary: Efficiency and reliability

1.4 Purpose of the Guideline

1.4.1 This guideline describes the recommended practices in carrying out the review of B2C e-commerce initiatives and applications, so the relevant IS Auditing Standards are complied with during the course of the review.

2. B2C E-COMMERCE

2.1 Definition

2.1.1 The term e-commerce is used by different parties to mean different things. ISACA defines e-commerce as the processes by which organisations conduct business electronically with their customers, suppliers and other external business partners, using the Internet as an enabling technology. Therefore, it

encompasses both business-to-business (B2B) and business-to-consumer (B2C) e-commerce models, but does not include existing non-Internet e-commerce methods that are based on private networks, such as EDI and SWIFTnet.

2.1.2 For the purpose of this guideline, ISACA's definition of e-commerce is used as the basis to arrive at the following definition of B2C e-commerce: B2C e-commerce refers to the processes by which organisations conduct business electronically with their customers and or public at large using the Internet as the enabling technology.

2.2 B2C E-commerce Models

2.2.1 More and more organisations are transforming their businesses using Internet technology in B2C relationships. The extent to which the Internet technology is used in an organisation for B2C relationships depends on the relative Internet maturity of the organisation, its customers, the Internet usage in its geographical market area, the nature of the organisation's products/services and the relative urgency to which the Internet is used to either achieve competitive advantage or to catch up with the competition. Accordingly, an organisation may be resorting to a B2C e-commerce model, covering one or more of the following broad e-commerce activities:

- Informational (public)—Making information regarding the organisation and its products available on the Internet for whoever wants to access the information
- Customer self-service (informational)—Making information, such as products/services and prices, available on the Internet for the customers of the organisation
- Customer self-service (transactional other than payments)—In addition to making information available on the Internet, accepting customer transactions, such as orders and cancellations, through the Internet, but payments are handled through conventional means
- Customer self-service (payments)—Accepting customer transactions including payments or fund transfers (in the case of banks) through the Internet
- Customer reporting—Providing reports, such as statement of accounts and order status to customers online
- Interactive self-service—Providing interactive responses through e-mails for requests/queries logged through a web site
- Direct selling—Selling products and services directly to prospective buyers through the Internet
- Auctioning—Auctioning the products online

2.3 Special Focus Required in a B2C E-commerce Review

2.3.1 In the case of B2C e-commerce initiatives, the business and the information systems are coupled tightly. Therefore, a review of B2C e-commerce should, in general, address the business risks as well as the IS risks.

2.3.2 COBIT has laid down seven information criteria to be met by information systems. Better compliance with these help to mitigate the IS risks and contribute towards minimising business risks. These are:

- Effectiveness
- Efficiency
- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

The relevance of these may be greater in the case of B2C e-commerce, depending on the extent of the broad e-commerce activities (as specified in section 2.2.1) carried out by the organisation. Accordingly, a review of B2C e-commerce should address how COBIT's information criteria are met by the B2C e-commerce application and how the related risks are mitigated.

2.3.3 Being connected to the Internet, B2C e-commerce applications are faced with inherent external threats, such as hackers, viruses and impersonation, which could affect the confidentiality, integrity and availability of the B2C e-commerce application. If the B2C e-commerce application is integrated with back-end systems, there is risk of even those systems becoming affected. In the event of the organisation's B2C e-commerce application being affected by such attacks, the reputation and image of

the organisation could be seriously impaired. In this context, the B2C e-commerce reviews should pay significant attention to the adequacy of the protection against such threats.

- 2.3.4** Non-repudiation of the transaction is an essential requirement of B2C e-commerce. With reference to COBIT's seven information criteria, one of the criteria is integrity. In cases where B2C e-commerce involves transactions and/or payments, authenticity of source and integrity during communication need to be ensured, so there is no subsequent repudiation of the transaction. The review of B2C e-commerce, in such cases, should address the effectiveness of the B2C e-commerce application in ensuring non-repudiation.
- 2.3.5** B2C e-commerce, in general, involves obtaining details about the customers and prospects using and or transacting through the B2C e-commerce applications. The data protection of such details should be ensured. In other words, the details gathered should be used for the intended purposes only and as per the agreement with the persons providing the information. There are various legal provisions evolving in various countries. In this context, any review of B2C e-commerce should address compliance with the legal provisions of the relevant countries as well as best practices relating to privacy and data protection.
- 2.3.6** Application audit trails have more significance in the B2C e-commerce environment due to the absence of paper trails for transactions and payments. In this context, the review of B2C e-commerce should address the adequacy of audit trails as well as the processes for reviewing the audit trails. This is important from the point of confirming the authenticity and integrity (including non-repudiation) of the transactions.
- 2.3.7** As against other channels of business, B2C e-commerce depends largely on the availability of the application and access to the Internet. In this context, there should be appropriate capacity planning processes, redundancies and fallback options as well as disaster recovery procedures in place for both the system and communication link. These should be given due attention while evaluating the availability aspects of the B2C e-commerce application.
- 2.3.8** Integrity of data between the B2C e-commerce application and the related back-end applications and processes (including manual processes, such as delivery/dispatch and receipt of non-electronic payments) is an important aspect. The adequacy of the automated application and manual controls to ensure such integrity should be an essential part of a B2C e-commerce review.
- 2.3.9** Where B2C e-commerce involves receiving online payments, there should be appropriate processes to obtain authorisations for the payments and to ensure that the considerations are duly received. In such cases, the appropriateness and adequacy of the controls need to be evaluated as part of the B2C e-commerce review.
- 2.3.10** Quite often, B2C e-commerce involves use of third-party service providers for various aspects, such as application development and maintenance, and managing the web site and related databases. In such cases, the appropriateness and adequacy of the controls and contractual protection, which ensure appropriate levels of service and the protection of the information relating to the organisation and its customers, needs to be evaluated as part of the B2C e-commerce review.
- 2.3.11** Data handling, storage, retention and disposal arising from B2C e-commerce activities become a greater concern as most, if not all, data originates and terminates electronically.
- 2.3.12** Some B2C e-commerce involve use of credit cards and other forms of payment and may be subject to standards set by those providers and processors. Awareness and adherence to those standards is important when enabling B2C e-commerce.

3. CHARTER

3.1 Mandate

- 3.1.1** Before commencing a review of B2C e-commerce, the IS auditor should provide reasonable assurance of the requisite mandate, by virtue of the IS auditor's position or the required written mandate provided by the organisation, to carry out the envisaged review. In case the review is initiated by the organisation, the IS auditor should also obtain reasonable assurance that the organisation has the appropriate authority to commission the review.

4. INDEPENDENCE

4.1 Professional Objectivity

4.1.1 Before accepting the assignment, the IS auditor should provide reasonable assurance that the IS auditor's interests, if any, in the B2C e-commerce application being reviewed would not in any manner impair the objectivity of the review. In the event of any possible conflict of interests, the same should be communicated explicitly to the organisation, and a written statement of the organisation's awareness of the conflict should be obtained before accepting the assignment.

4.1.2 In case the IS auditor has/had any non-audit roles in the B2C e-commerce application being reviewed, the IS auditor should consider the guideline G17 Effect of Non-audit Roles on the IS Auditor's Independence.

5. COMPETENCE

5.1 Skills and Knowledge

5.1.1 The IS auditor should provide reasonable assurance of the necessary business knowledge to review the B2C e-commerce application. Understanding the business catered to by the B2C e-commerce application is important for evaluating the B2C e-commerce applications/initiatives.

5.1.2 The IS auditor should also provide reasonable assurance of access to the relevant technical skill and knowledge to carry out the review of a B2C e-commerce application. Such reviews would call for technical knowledge to evaluate aspects, including the encryption technologies used, network security architecture and security technologies, such as firewalls, intrusion detection and virus protection. The IS auditor should have adequate knowledge to review these aspects. Where expert inputs are necessary, appropriate inputs should be obtained from external professional resources. The fact that external expert resources would be used should be communicated to the organisation in writing.

6. PLANNING

6.1 High-level Risk Assessment

6.1.1 The IS auditor should gather information regarding the industry in general (since the B2C e-commerce risks would vary from industry to industry), the organisation's B2C e-commerce objectives and policies, its strategy to achieve the objectives, the business processes involved and the underlying flow of information, the scope of the B2C e-commerce system, the extent of usage of the system, and the development process used for building the B2C e-commerce solution. The information gathered should help in carrying out a high-level assessment of the business risks as well as the risks with reference to COBIT's information criteria and the aspects referenced in section 2.3 of this document. This high-level risk assessment will help determine the scope and coverage of the review.

6.2 Scope and Objectives of the Review

6.2.1 The IS auditor, in consultation with the organisation, where appropriate, should define clearly the scope and objectives of the review of the B2C e-commerce. The aspects to be covered by the review should be stated explicitly as part of the scope. The high-level risk assessment referred to in section 6.1.1 would dictate which aspects need to be reviewed and the extent and depth of the review.

6.2.2 For the purpose of the review, the stakeholders in the B2C e-commerce solution should also be identified and agreed upon with the organisation.

6.3 Approach

6.3.1 The IS auditor should formulate the approach, so the scope and objectives of the review can be fulfilled in an objective and professional manner. The approach followed should depend on whether the review is a pre- or a post-implementation review. The approach should be documented appropriately. When and where external expert inputs would be used should also be specified as part of the approach.

6.4 Sign-off for the Plan

6.4.1 Depending on the organisational practices, the IS auditor may obtain the concurrence of the organisation for the plan and approach.

7. PERFORMANCE OF THE B2C E-COMMERCE REVIEW

7.1 General

7.1.1 This section addresses the wide spectrum of aspects to be addressed during the execution of a B2C e-commerce review. For a specific B2C e-commerce review, aspects relevant to the review should be

identified from this wide spectrum of aspects depending on the envisaged scope and objectives of the review.

- 7.1.2 The B2C e-commerce review should be carried out per the defined approach (with refinements as appropriate), so the envisaged objectives of the review are fulfilled.
- 7.1.3 In general, study of available documentation (i.e., business case, system documentation, contracts, service level agreements, logs), discussions with the stakeholders, use of the B2C e-commerce application and observation should be used appropriately to gather, analyse and interpret the data. Where appropriate, the IS auditor should test the significant processes in the test and/or production environment to verify that the processes are functioning as intended (i.e., test purchases or test ordering using the e-commerce system and test the security mechanisms using penetration testing).
- 7.1.4 Where necessary and agreed upon with the organisation, external expert inputs could be used suitably in the collection, analysis and interpretation of the data.
- 7.1.5 The inferences and recommendations should be based on an objective analysis and interpretation of the data.
- 7.1.6 Appropriate audit trails should be maintained for the data gathered, analysis made, inferences arrived at and corrective actions recommended.

7.2 Evaluating the Business Aspects

- 7.2.1 The IS auditor should evaluate the e-commerce objectives, strategy and business model critically. The existing and emerging competition should also be considered in evaluating the relative position of the organisation's business. This is essential for evaluating the appropriateness of the objectives and strategies and the effectiveness and efficiency of the B2C e-commerce application in fulfilling these objectives and strategies.
- 7.2.2 The IS auditor should evaluate whether the B2C e-commerce initiative is a new business by itself, or an additional channel to the existing line of business, and to what extent the success and financial viability of the organisation depends on the B2C e-commerce initiative being reviewed. The greater the dependency on the B2C e-commerce, the higher the effects of the risks should they materialise.
- 7.2.3 The IS auditor should review the business case to assess whether the costs and benefits of the B2C e-commerce are reflected in an objective manner. Considering the huge and ever-increasing number of Internet users, at times the business potential and volume are projected at levels way beyond what could be achieved pragmatically. If the IS auditor has concerns regarding the underlying assumptions, the same should be clarified with appropriate management.

7.3 Detailed Risk Assessment

- 7.3.1 The IS auditor should map the key processes relating to the B2C e-commerce application—automated as well as manual processes—in case these are not readily available.
- 7.3.2 The IS auditor should then assess the likely risks—business and IS risks—pertaining to these processes and their likely effect, and document these along with the aspects that mitigate/could mitigate the risks. The criticality of the residual risk should also be assessed.
- 7.3.3 Depending on the criticality of the risks, the IS auditor should determine aspects that need to be reviewed further and the depth of the review.
- 7.3.4 The IS auditor should identify applicable controls to mitigate risks identified. If multiple controls can be identified to mitigate risk, controls can be ranked in order of effectiveness. Primary or 'key' controls should be tested before secondary controls.

7.4 Development Process

- 7.4.1 The IS auditor should review the appropriateness of the development process followed to determine whether appropriate controls were built into the B2C e-commerce application.
- 7.4.2 The capabilities of the team developing/maintaining the B2C e-commerce application and the tools being used should be reviewed to assess their adequacy and to verify appropriate controls in the B2C e-commerce application.
- 7.4.3 In this context, the IS auditor should consider the guideline G23 System Development Life Cycle Reviews to the extent it is appropriate for the review being carried out.

7.5 Change Management Process

- 7.5.1 Uncontrolled changes to the B2C e-commerce applications could result in unplanned outages and could affect the integrity of data and processing. In this context, the IS auditor should review the

appropriateness of the change management process to evaluate its adequacy in ensuring controlled changes to the B2C e-commerce application environment. As part of testing the change management process, the IS auditor should review an adequate number of changes, to verify that the processes are functioning as intended. Adequacy is based on population of changes made within the period and complexity of the change.

7.5.2 The IS auditor should ascertain whether the development, testing, staging and production environments are segregated adequately to minimise the risks arising out of changes. The effects of any inadequacies in this aspect need to be evaluated.

7.6 Content Management Process

7.6.1 The contents appearing in B2C e-commerce web sites—those merely providing information as well as those relating to transactions—should be published through a controlled content management process to ensure appropriateness of language and presentation, correctness of information, and appropriate approvals for the data published, particularly those relating to product and service offering, pricing, contractual obligations, legal terms and conditions, etc.. The IS auditor should understand this process and review its adequacy.

7.6.2 The IS auditor should verify whether adequate audit trails relating to the key contents (i.e., terms, conditions and prices) are maintained and reviewed to verify the integrity and accuracy of the data.

7.6.3 The IS auditor should verify whether the terms and conditions of use of the B2C e-commerce application, as well as the privacy and data protection policies of the organisation, as published on the site, have been vetted by legal experts to confirm that adequate attention has gone into legal compliance and contractual protection.

7.7 Identification and Authentication

7.7.1 Depending on the e-commerce activities permitted by the B2C e-commerce application—particularly where transactions and payments are processed—the user should be identified and authenticated uniquely to ensure non-repudiation and to preserve confidentiality. The IS auditor should evaluate whether the controls/mechanisms/technologies (such as ID and passwords, challenge/response procedure, tokens, digital certificates and digital signatures), deployed regarding identification and authentication, are commensurate with the intended use of the B2C e-commerce application.

7.8 Data Validations and Authorisations

7.8.1 If the B2C e-commerce application accepts data from the users by way of transactions and/or information, the IS auditor should verify whether adequate validations built into the application ensure the appropriateness of the data being entered and that such validations are being performed.

7.8.2 If the B2C e-commerce application accepts electronic payments (such as credit cards), the IS auditor should verify whether there are adequate validation and payment authorisation processes to ensure the authenticity as well as the actual receipt of the payments.

7.9 Communication Controls

7.9.1 In the case of B2C e-commerce applications processing transactions and payments as well as accepting and/or displaying any personal details confidential in nature (such as statement of accounts), the IS auditor should verify whether an appropriate encryption technology/mechanism (such as Secure Socket Layer or IPSec) is being used to encrypt the transmission between the user and the application.

7.9.2 Where appropriate and necessary, the IS auditor should ascertain whether the communication across the network is made secure using a virtual private network (VPN) and related encryption.

7.10 Processing Controls

7.10.1 In the case of B2C e-commerce applications processing transactions and payments, the IS auditor should verify whether there are adequate application controls to ensure the integrity and correctness of the processing.

7.11 Integration With Back-end Processes and Applications

7.11.1 Some of the B2C e-commerce applications require back-end processes for fulfillment of orders, receipt of money and accounting for transactions. While some of this may be handled through detached applications or manual processes, they may call for integration of the B2C e-commerce application with some of the other applications. In such instances, the IS auditor should verify whether there are

sufficient controls, including reconciliation processes to ensure integrity of original data across the related applications and processes (including manual processes).

7.12 Data Storage Integrity

- 7.12.1** Behind any B2C e-commerce application is a database, the integrity and confidentiality of which is crucial. The IS auditor should evaluate the controls over the database to confirm that there are adequate checks and balances to prevent intentional or inadvertent damage, destruction or modification of data. In this context, the IS auditor should review the database access privileges and the access logs.
- 7.12.2** The IS auditor should also review the controls over the archived data to provide reasonable assurance that the confidentiality and integrity are protected adequately.

7.13 Audit Trails and Their Review

- 7.13.1** As indicated previously, in the absence of paper trails, the role of automated audit trails is critical in B2C e-commerce applications. The IS auditor should review the adequacy of the audit trails relating to transactions, including payments, changes to critical master data (such as rates, prices and actions) and any changes carried out by staff with system administration privilege.
- 7.13.2** Mere availability of audit trails would not suffice. There should be processes for reviewing the audit trails to provide reasonable assurance that the actions, as reflected in the audit trails, are valid and duly authorised. In this context, the IS auditor should look for audit evidence that the audit trails are being reviewed and acted upon.

7.14 Protection Against External IS Threats

- 7.14.1** The IS auditor should evaluate the external IS threats to the B2C e-commerce environment, taking into account the nature of the business of the organisation. The external threats to be addressed should include denial of service, unauthorised access to data and unauthorised use of the computer equipment. These could arise from various sources (such as casual hackers, competitors, alien governments and terrorists). The characteristics of the business of the organisation (such as intensity of competition, market share, nature, timing and extent of technology usage, and innovative/strategic products and/or services) should be used to determine the possible sources of such threats. The likely damage associated with these threats is linked closely to the dependence of the business on the e-commerce processes.
- 7.14.2** The IS auditor should assess whether the protective measures in place to counter the external threats are commensurate with the level of the assessed risk. In this process, the IS auditor should review the following:
- Technical architecture of the application, including the choice of protocols
 - Security architecture of the application
 - Virus protection mechanisms
 - Firewall implementation, appropriateness of the firewall solution, location of firewall, firewall policies, connections to the firewall and any external connections bypassing the firewall
 - Intrusion detection and prevention mechanisms
 - Existence of relevant logs as well as their ongoing review by competent staff
 - Processes in place, such as penetration and vulnerability testing, to verify the compliance with the envisaged architectures, policies and procedures.

7.15 Compliance With Regulations and Best Practices

- 7.15.1** The IS auditor should evaluate whether the relevant privacy and data protection requirements imposed by the relevant laws and best practices relating to privacy and data protection are being complied with by the organisation. As indicated previously, the IS auditor should verify whether the privacy and data protection policies and practices are displayed appropriately on the web site.
- 7.15.2** The IS auditor should evaluate whether the B2C e-commerce activity is subject to other governmental laws and regulations and identify processes and controls to ensure compliance. Appropriate measures should be taken to verify adherence to local and other applicable laws depending on jurisdiction, such as those related to anti-money laundering, taxation and industry regulations/standards such as PCI. The IS auditor should also evaluate whether goods and services sold via B2C activity violate export law. Encryption technology or weapons are examples of goods that may trigger export restrictions.

7.16 Availability of the B2C E-commerce Application and Business Continuity

7.16.1 Since B2C e-commerce depends largely on the availability of the application and access to the Internet, the IS auditor should evaluate whether there are appropriate capacity planning processes, redundancies and fallback options, offsite storage, rotation of media, and disaster recovery procedures in place for both the system and communication link.

7.16.2 Where relevant, the IS auditor should also review the fallback arrangements with reference to automated and other related manual processes to ascertain their appropriateness in ensuring business continuity and fast recovery in the event of any disruptions.

7.17 Effectiveness and Efficiency

7.17.1 The IS auditor should evaluate the effectiveness of the B2C e-commerce application with reference to the intended objectives of the initiative. Certain aspects, such as volume of transactions, value of business, number of customers/prospects/visitors attracted, volume and value of repeat business, and attrition of customers, would help in assessing the effectiveness of the system.

7.17.2 The IS auditor should compare, where relevant, the actual costs and benefits against what was envisaged, to assess whether the B2C e-commerce application is sufficiently cost-efficient. The processing performance, customer feedback and ease of use of the application (as indicated by the use of the system) also help in assessing the efficiency of the B2C e-commerce application.

7.17.3 The IS auditor should ascertain whether there are appropriate mechanisms to monitor the effectiveness and efficiency of B2C e-commerce on an ongoing basis. This should include the processes to detect and report exceptions so as to prevent errors and frauds.

7.18 Third-party Services

7.18.1 Where the B2C e-commerce solution depends on any third-party service providers, such as an Internet service provider (ISP), certificate authority (CA), registration authority (RA) and web-hosting agency, the IS auditor should ascertain whether the security procedures at their ends are appropriate and adequate.

7.18.2 Where such third-party service providers are used, the IS auditor should review the related contracts and service level agreements (SLAs) as well as the SLA reporting, to assess whether the interests of the organisation are being protected adequately.

7.18.3 In this context, the IS auditor should consider whether the guideline G16 Effect of Third Parties on Organisation's IT Controls provides the appropriate guidance.

7.18.4 When third parties are used for certification in B2C, the IS auditor should provide due diligence in reviewing how the information is collected and used for those seals of control (e.g., BetterBusiness, Webtrust).

7.19 Nonrepudiation

7.19.1 Where the B2C e-commerce solution involves processing of transactions and payments, the IS auditor should evaluate the relevant controls referred to previously (sections 7.7, 7.9 and 7.10) with reference to authentication, communication, processing, and ensuring non-repudiation.

8. REPORTING

8.1 Report Content

8.1.1 The report on the B2C e-commerce review should address the following aspects depending on the scope of its coverage:

- The scope, objective, methodology followed and assumptions
- Overall assessment of the solution in terms of key strengths and weaknesses as well as the likely effects of the weaknesses
- Recommendations to overcome the weaknesses and improve the solution
- The extent of compliance with COBIT's information criteria and criteria specific to B2C e-commerce (such as non-repudiation) and the effect of any noncompliance
- Recommendations regarding how the experience could be used to improve similar future solutions or initiatives

8.1.2 The observations and recommendations should be validated with the stakeholders and organisation, as appropriate, before finalising the report.

9. EFFECTIVE DATE

9.1 This guideline is effective for all IS audits beginning on or after 1 August 2003. The guideline has been reviewed and updated effective 1 December 2008.

APPENDIX

References

- ISACA, E-commerce Security Series publications, 2000-2002
- Australian Accounting Research Foundation, Auditing Guidance Statement AGS1056 E-commerce: Audit Risk Assessments and Control Considerations

2008-2009 ISACA Standards Board	
Chair, Ravi Muthukrishnan, CISA, CISM, FCA, ISCA	Capco IT Services India Private Ltd., India
Shawn Chaput, CISA, CISM, CISSP,PMP	IBM, Canada
Maria Gonzalez, CISA, CISM	Department of Defence, Spain
John Ho Chi, CISA, CISM, CBCP, CFE	Ernst & Young, Singapore
Andrew J. MacLeod, CISA, FCPA, MACS, PCP, CIA	Brisbane City Council, Australia
John G. Ott, CISA, CPA	AmerisourceBergen, USA
Edward Pelcher, CISA	Office of the Auditor General, South Africa
Jason Thompson, CISA	KPMG LLP, USA
Meera Venkatesh, CISA, CISM, ACS, CISSP, CWA	Microsoft Corp., USA

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Telephone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: standards@isaca.org
Web Site: www.isaca.org