

G16 EFFECT OF THIRD PARTIES ON AN ENTERPRISE'S IT CONTROLS

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 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 enterprises. It emphasises regulatory compliance, helps enterprises 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 and/or elements 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, 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.

1. BACKGROUND

1.1. Linkage to Standards

- 1.1.1. Standard S5 Planning states, 'The IS auditor should plan the information systems audit coverage to address the audit objectives and to comply with applicable professional auditing standards'.
- 1.1.2. Standard S6 Performance of Audit Work states, 'During the course of the audit, the IS auditor is to 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 COBIT

- 1.2.1 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 meet the responsibility, authority and accountability requirement 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.
- 1.2.2 Primary IT processes are:
 - PO4 *Define the IT processes, organisation and relationships*
 - PO7 *Manage IT human resources*
 - AI5 *Procure IT resources*
 - DS1 *Manage service levels*
 - DS2 *Manage third-party services*
 - DS5 *Ensure systems security*
 - ME2 *Monitor and evaluate internal control*
- 1.2.3 Secondary IT processed are:
 - PO1 *Define a strategic plan*
 - PO2 *Define the information architecture*
 - PO8 *Manage quality*
 - AI3 *Acquire and maintain technology infrastructure*
 - DS12 *Manage the physical environment*
 - ME4 *Provide IT governance*
- 1.2.4 The information criteria most relevant to responsibility, authority and accountability are:
 - Primary: Effectiveness, availability, integrity and reliability
 - Secondary: Efficiency and confidentiality

1.3 Definitions

- 1.3.1 Internet service provider (ISP): A third party that provides enterprises with a variety of Internet and Internet-related services
- 1.3.2 Application or managed service provider (ASP/MSP): A third party that delivers and manages applications and computer services, including security services, to multiple users via the Internet or a private network.
- 1.3.3 Business service provider (BSP): An ASP that also provides outsourcing of business processes such as payment processing, sales order processing and application development.
- 1.3.4 In this guideline, ISPs, ASP/MSPs and BSPs are referred to collectively as third parties. Third parties covered under this guideline include any organisation that is separate from the enterprise (such as shared service organisations) whether legally separate or not.

1.4 Guideline Application

- 1.4.1 When applying this guideline, the IS auditor should consider it in relation to other relevant ISACA guidelines.

1.5 Need for Guideline

- 1.5.1 This guideline sets out how the IS auditor should comply with the ISACA IS Auditing Standards and COBIT when assessing the effect a third party has on an enterprise's IS controls and related control objectives.
- 1.5.2 This guideline is not intended to provide guidance on how IS auditor's report on third-party provider controls in accordance with other standard-setting entities.

2. ROLE OF THIRD-PARTY SERVICE PROVIDERS

2.1 Services of Third-party Providers

2.1.1 Enterprises use third-party service providers in a variety of different capacities. These providers often perform important and critical functions for the enterprises and, therefore, usually require access to confidential information, applications and systems.

2.1.2 Third parties provide services such as:

- Business advisory and consulting services
- Connectivity and utility services to the enterprise's partners, suppliers and customers
- Security services
- Providing physical location for hardware (known as co-location)
- Monitoring of system and application access
- Backup and recovery services
- Application development, maintenance and hosting (e.g., enterprise resource planning (ERP) systems, e-commerce systems, web sites)
- Business services such as cash management, credit card services, order processing, call centre services as well as back-office transactional accounting services, such as accounts payable, fixed asset, HR/payroll and/or general ledger accounting/reporting processing

3. EFFECT ON CONTROLS

3.1 Third-party Providers Effect on Controls

3.1.1 When enterprises use third parties, they can become a key component in an enterprise's controls and its achievement of related control objectives.

3.1.2 IS auditors should evaluate the role that the third party performs in relation to the IT environment, related controls and control objectives.

3.1.3 An enterprise that uses third-party providers for limited purposes, such as co-location services, may rely upon these third parties for only limited purposes in achieving its control objectives. However, an enterprise that uses providers for other purposes, such as hosting financial accounting systems and e-commerce systems, utilises the third-party provider's controls wholly or in conjunction with its own controls to achieve its control objectives.

3.1.4 The effectiveness of third-party controls can enhance the ability of an enterprise to achieve its control objectives. Conversely, ineffective third-party controls can weaken the ability of an enterprise to achieve its control objectives. These weaknesses can arise from many sources including:

- Gaps in the control environment arising from the outsourcing of services to the third party
- Poor control design, causing controls to operate ineffectively
- Lack of knowledge and/or inexperience of personnel responsible for control functions
- Over reliance on the third party's controls (when there are no compensating controls within the enterprise)

4. PROCEDURES TO BE PERFORMED BY THE IS AUDITOR

4.1. Obtaining an Understanding

4.1.1 As part of the planning process, IS auditors should obtain and document an understanding of the relationship between the services provided by the third party and the enterprise's control environment. IS auditors should consider reviewing such things as the contract, service level agreements, and policies and procedures between the third party and the enterprise.

4.1.2 IS auditors should document the third party's processes and controls that have a direct effect on the enterprise's processes and control objectives.

4.1.3 IS auditors should thoroughly contemplate and identify risks involved with the process and whether those risks reside with the company and/or the third-party provider.

4.1.4 IS auditors should identify each control, its location in the combined control environment (internal or external), the type of control, its function (preventive, detective or corrective), and the organisation that performs the functions (internal or external) that offset or compensate for those risks.

4.1.5 IS auditors should assess the risk of the services provided by the third party to the enterprise, its controls and control objectives, and determine the significance of third-party controls on the ability of the enterprise to meet its control objectives.

4.2 Confirming the Understanding

4.2.1 IS auditors should confirm their understanding of the control environment.

4.2.2 IS auditors can confirm their understanding of the control environment through a variety of methods including such things as inquiry and observation and process walk-throughs.

4.3 Assessing the Role of Third-party Provider Controls

4.3.1 If the role or effect that the third party has on the enterprise's control objectives is significant, the IS auditor should assess these controls to determine whether they function as described, operate effectively and assist the enterprise in achieving its control objectives. Section 7, Review of Third-party Provider Controls, provides an approach to testing these controls.

5. RISKS ASSOCIATED WITH THIRD-PARTY PROVIDERS

5.1 Effects of Third-party Providers on an Enterprise

5.1.1 Third-party providers can affect an enterprise (including its partners), its processes, controls and control objectives on many different levels. This includes effects arising from such things as:

- The economic viability of the third-party provider
- Third-party provider access to information that is transmitted through their communication systems and applications
- Systems and application availability
- Processing integrity
- Application development and change management processes
- The protection of systems and information assets through backup recovery, contingency planning and redundancy

5.1.2 The lack of controls and/or weakness in their design, operation or effectiveness can lead to such things as:

- Loss of information confidentiality and privacy
- Systems not being available for use when needed
- Unauthorised access and changes to systems, applications or data
- Changes to systems, applications or data occurring that result in system or security failures, loss of data, loss of data integrity, loss of data protection, or system unavailability
- Loss of system resources and/or information assets
- Increased costs incurred by the enterprise as a result of any of the above

5.2 Assessing Identified Control Weaknesses

5.2.1 IS auditors should assess the likelihood (or control risk) that weaknesses in control, design or operation may exist in the IT environment. IS auditors should identify where the control weakness exists.

5.2.2 IS auditors should then assess whether control risk is significant and what effect it has on the control environment.

5.2.3 When weaknesses are identified, IS auditors should also determine if compensating controls exist and to what extent they counter the effect of identified weaknesses (compensating controls may exist at the enterprise, the third-party provider or in both entities). If compensating controls exist, IS auditors should determine if they mitigate the effect of identified control weaknesses.

6. CONTRACTS WITH THIRD-PARTY PROVIDERS

6.1 Roles and Responsibilities

6.1.1 The relationship between the enterprise and a third-party provider should be documented in the form of an executed contract. The contract is a critical element in the relationship between the enterprise and the service provider. These contracts contain many provisions that govern the actions and responsibilities of each party.

6.1.2 IS auditors should review the contract between the enterprise and the third party.

6.1.3 Within the context of this guideline, IS auditors should review the contract (possibly with the assistance of the enterprise's legal counsel) to determine the third party's role and responsibility for assisting the enterprise in achieving its control objectives. Guidance on how to review a contract is outside the scope of this guideline; however, the following list provides examples of issues that

should be considered by IS auditors when reviewing the contract:

- Level of service to be provided by the third party (whether to the enterprise, its partners or both)
- Reasonableness of fees charged by the third party
- Responsibilities for design, implementation, performance and monitoring of controls
- Responsibilities for data and application privacy and confidentiality
- Responsibilities for systems, communications, operating system, utility software, data, and application software access controls and administration
- Monitoring of assets and related data and response (enterprise and third party) and reporting procedures (routine and incident)
- Specification of ownership of information assets, including data and domain names
- Specification of ownership of custom programming developed by the third-party provider for the enterprise, including change documentation, source code and escrow agreements
- Provision for systems and data protection, including backup and recovery, contingency planning, and redundancy
- Right to audit clause (including such things as the ability to meet with the third-party provider's internal audit personnel and review their audit work papers and reports)
- Process for negotiation, review and approval of changes to the contract and related documents (such as service level agreements and procedures)

6.1.4 As a minimum, IS auditors should review the contract to determine the extent of responsibility for controls that the third party undertakes on behalf of the enterprise. This process should assess the sufficiency of identified controls and compliance monitoring/reporting, their design, and operating effectiveness.

6.2 Corporate Governance

6.2.1 Even when third-party providers are involved, management is still responsible for the achievement of related control objectives. As part of this responsibility, management should have a process to govern the relationship with and the performance of the third-party provider. IS auditors should identify and review the components of this process. IS auditors should review such things as the process management uses to identify risks associated with the third-party provider, the services provided by the third party and how management governs the relationship between the two entities.

6.2.2 IS auditors' review of the governance process should ascertain such things as whether management reviews the third-party providers against the performance standards or criteria set forth in the contract and any standards specified by regulatory bodies. The governance process should include review of such things as:

- Financial performance of the third-party provider
- Compliance with terms of the contract
- Changes to the control environment mandated by the third party, its auditors and/or regulators
- Results of control reviews performed by others, including the third party's auditors, consultants or others
- Maintaining adequate levels of insurance

7. REVIEW OF THIRD-PARTY PROVIDER CONTROLS

7.1 Contractual Limitations

7.1.1 When reviewing third-party provider controls, IS auditors should consider the contractual relationship between the enterprise and the third-party provider and the third-party provider's evaluation and reporting on the controls.

7.1.2 Contractual limitations such as 'right to audit' clauses may preclude IS auditors from reviewing controls at the third-party provider. In these circumstances, IS auditors should assess this limitation of scope on their ability to evaluate the IS control environment.

7.2 Independent Reports

7.2.1 Third-party providers may provide reports from independent sources on their controls. These reports may take the form of service bureau audit reports or other control-based reports. Service auditor's assurance reports are examples of reports issued by independent sources. IS auditors can use these reports as the basis for reliance on controls in the IS control environment.

7.2.2 If the IS auditor decides to use an independent report as the basis for reliance on IS controls at the third-party provider, then the IS auditor should review these reports to determine the following:

- Whether the independent party is qualified. This can include whether the independent party has appropriate professional certification or license, has relevant experience, and is in good standing with applicable professional and regulatory (if applicable) authorities
 - Whether the independent party has no relationship with the third-party provider that would impair their independence and objectivity
 - The period of coverage of the report
 - Whether the report is sufficient (i.e., the report covers the applicable systems and controls and includes tests of areas that an IS auditor would include when performing the work)
 - If the testing of the controls is sufficient to enable an IS auditor to rely upon the work of the independent party (i.e., the testing of the controls is sufficient as is the nature, timing and extent of procedures performed)
 - If testing exceptions were identified by the independent third party
 - Whether the report delineates between the responsibilities of the service provider and the responsibilities of the user enterprise
 - Whether the user enterprise has addressed its responsibilities with respect to proper controls
- 7.2.3** If exceptions exist in testing, IS auditors should determine their impact on control objectives, follow up on whether they have been remediated and assess whether additional testing is required to satisfy the control objective.

7.3 Testing Third-party Controls

7.3.1 If an IS auditor decides to directly review and test controls at the third-party provider, then the IS auditor should do the following:

- Work with management and, as applicable or considered appropriate, internal audit of both enterprises to plan the engagement and set its objectives and scope of review.
- Work with management and, as applicable or considered appropriate, internal audit and staff of both enterprises to determine timing, staffing needs and other issues.
- Address issues such as access to third-party systems and assets and confidentiality.
- Develop an audit programme, budget and engagement plan.
- Validate control objectives.

7.3.2 IS auditors should consider the following areas when setting scope and objectives of the audit:

- Location and environment where third-party services are performed. Remote locations may require special access exceptions that may impact security.
- Size and stability of the third-party provider. The number of employees and size of the company may adversely impact segregation of duties between functions as well as impact appropriateness of access of those employees.
- Housing and handling of data. If the third-party provider is responsible for handling or housing confidential data or assets for multiple clients, privacy, segregation and access controls for employees and customers should be reviewed.

7.3.3 Once the fieldwork has been completed, a conclusion on the operating effectiveness of tested controls should be made. IS auditors should review the effectiveness of the controls within each enterprise and the interplay of controls between the enterprise and the third party.

7.3.4 In most situations, controls overlap between the enterprise and the third-party provider. IS auditors should assess the operating effectiveness of the controls taken together vs. those taken individually.

7.3.5 Situations may also exist where controls for a particular objective in either enterprise may not exist or do not operate effectively. In this situation, IS auditors should assess the effect this weakness has on the overall control environment and on the extent of the procedures.

7.3.6 Situations may also exist where control strengths in one enterprise may be negated partially or completely by control weaknesses in another enterprise. IS auditors are responsible to assess this situation's impact on the overall control environment.

7.4 Internal Auditors of the Third-party Provider

7.4.1 IS auditor's should also consider whether the third-party provider has an internal audit department. The presence of third-party provider internal auditors can enhance the strength of the control environment at the third-party provider.

7.4.2 If an internal audit department exists, IS auditor's should ascertain the extent of their activities with regard to the systems and controls that effect the enterprise.

7.4.3 If possible, IS auditors should review relevant third-party provider internal audit reports.

7.4.4 In situations where it is not possible to review these reports, IS auditors should discuss the scope of

these reviews, identify what systems and controls were covered by the reviews, and identify the significant issues and weaknesses.

- 7.4.5 If the third-party provider is unwilling to grant access to the reports or their internal audit personnel, IS auditors should assess this restriction on the extent of their procedures.
- 7.4.6 IS auditors should also consider assessing the skills and expertise of the third-party provider's internal audit staff. This can be accomplished through discussions with these individuals and by additional procedures such as reviewing their work plans, work papers and reports.

8. SUBCONTRACTORS OF THIRD PARTIES

8.1 Effect on Controls

- 8.1.1 IS auditors should determine whether the third party uses subcontractors to provide systems and services.
- 8.1.2 In situations where subcontractors exist, IS auditors should review the significance of these subcontractors to determine the effect they may have on the primary third party's controls that relate to the enterprise.

8.2 Effect on an Engagement

- 8.2.1 If the subcontractor does not have a significant effect on the controls relevant to the enterprise, IS auditors should document this in their work papers.
- 8.2.2 If the subcontractor has a significant effect on the controls relevant to the enterprise, IS auditors should evaluate the processes used by the third party to manage and monitor the relationship with the subcontractor. IS auditors should consider sections 6 and 7 of this guideline when evaluating the third party's controls over its subcontractors.

9. REPORTING

9.1 Weaknesses

- 9.1.1 The IS auditor's report should indicate that the controls subject to the review extended to controls within the enterprise and those that exist at the third-party organisation. In addition, IS auditors should consider identifying the controls, control weaknesses and compensating controls that exist in each enterprise.
- 9.1.2 The extent to which conclusions and recommendations are communicated should be documented in the terms of reference. Some third parties may not be willing, or able, to implement recommendations. In these situations, the IS auditor should recommend compensating controls that the enterprise could implement to address control weaknesses at the third-party organisation. In some cases, the enterprise may have to refer back to contract language to determine the appropriate course of action with management if significant issues continue to exist.

10. EFFECTIVE DATE

- 10.1 This guideline is effective for all IS audits beginning on or after 1 March 2002. The guideline has been reviewed and updated effective 1 March 2009.

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 MacLeod, CISA, CIA, FCPA, MACS, PCP Brisbane City Council, Australia
John G. Ott, CISA, CPA AmerisourceBergen, USA
Edward Pelcher, CISA Office of the Auditor General, South Africa
Jason Thompson, CISA, CIA 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