



# IS AUDITING STANDARD PROFESSIONAL ETHICS AND STANDARDS DOCUMENT #S3

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 the Information Systems Audit and Control Association® (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.

**CobIT®** resources should be used as a source of best practice guidance. The *CobIT Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility as well as to achieve its expectations, management must establish an adequate system of internal control." CobIT provides a detailed set of controls and control techniques for the information systems management environment. 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 information criteria.

As defined in the *CobIT Framework*, each of the following is organised by IT management process. CobIT is intended for use by business and IT management, as well as IS auditors; therefore, its usage enables the understanding of business objectives, communication of best practices and recommendations to be made around a commonly understood and well-respected standard reference. CobIT includes:

- Control objectives—High-level and detailed generic statements of minimum good control
- Control practices—Practical rationales and "how to implement" guidance for the control objectives
- Audit guidelines—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
- Management guidelines—Guidance on how to assess and improve IT process performance, using maturity models, metrics and critical success factors. They provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:
  - Performance measurement—How well is the IT function supporting business requirements? Management guidelines can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.
  - IT control profiling—What IT processes are important? What are the critical success factors for control?
  - Awareness—What are the risks of not achieving the objectives?
  - Benchmarking—What do others do? How can results be measured and compared? Management guidelines provide example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.

**Glossary** of terms can be found on the ISACA web site at [www.isaca.org/glossary](http://www.isaca.org/glossary). The words audit and review are used interchangeably.

**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 professional should apply his/her own professional judgement to the specific control circumstances presented by the particular systems or information technology 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](mailto: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. This material was issued 15 October 2004.

## Professional Ethics and Standards S3

### Introduction

- 01 ISACA Standards contain the basic principles and essential procedures, identified in bold, that are mandatory, together with related guidance.
- 02 The purpose of this IS Auditing Standard is to establish a standard and provide guidance to the IS auditor to adhere to the ISACA Code of Professional Ethics and exercise due professional care.

### Standard

- 03 The IS auditor should adhere to the ISACA Code of Professional Ethics.**
- 04 The IS auditor should exercise due professional care, including observance of applicable professional auditing standards.**

### Commentary

- 05 The Code of Professional Ethics issued by ISACA will be amended from time to time to keep pace with emerging trends and demands of the auditing profession. ISACA members and IS auditors should keep abreast of the latest Code of Professional Ethics and adhere to the same while discharging duties as IS auditors.
- 06 The IS Auditing Standards issued by ISACA are periodically reviewed for continual improvement and amended as necessary to keep pace with the evolving challenges in the auditing profession. ISACA members and IS auditors should be aware of the latest applicable IS Auditing Standards and exercise due professional care while conducting audit assignments.
- 07 Failure to comply with the ISACA Code of Professional Ethics and/or IS Auditing Standards can result in investigation into a member's or CISA holder's conduct and, ultimately, in disciplinary measures.
- 08 ISACA members and IS auditors should communicate with their team members and ensure the teams adherence to the Code of Professional Ethics and observance of applicable IS Auditing Standards in conducting audit assignments.
- 09 IS auditors should appropriately deal with all concerns encountered, with regard to the application of professional ethics or IS Auditing Standards during the conduct of the audit assignment. If adherence to professional ethics or IS Auditing Standards is impaired or appears impaired, the IS auditor should consider withdrawing from the engagement.
- 10 The IS auditor should maintain the highest degree of integrity and conduct, and not adopt any methods that could be seen as unlawful, unethical or unprofessional to obtain or execute audit assignments.
- 11 The following guidance should be referred to for further information on professional ethics and standards:
  - IS Auditing Guideline G19 Irregularities and Illegal Acts
  - IS Auditing Guideline G7 Due Professional Care
  - IS Auditing Guideline G12 Organisational Relationship and Independence
  - COBIT *Framework*, Control objective M4

### Operative Date

- 12 This IS Auditing Standard is effective for all information systems audits beginning on 1 January 2005.

#### **Information Systems Audit and Control Association 2004-2005 Standards Board**

Chair, Sergio Fleginsky, CISA PricewaterhouseCoopers, Uruguay  
Svein Aldal Aldal Consulting, Norway  
John Beveridge, CISA, CISM, CFE, CGFM, CQA Office of the Massachusetts State Auditor, USA  
Claudio Cilli, Ph.D., CISA, CISM, CIA, CISSP Value Partners, Italy  
Christina Ledesma, CISA, CISM Citibank NA Sucursal, Uruguay  
Andrew MacLeod, CISA, CIA, FCPA, MACS, PCP Brisbane City Council, Australia  
V. Meera, CISA, CISM, ACS, CISSP, CWA Microsoft Corporation, USA  
Ravi Muthukrishnan, CISA, CISM, FCA, ISCA NextLinx India Private Ltd., India  
Peter Niblett, CISA, CISM, CA, CIA, FCPA WHK Day Neilson, Australia  
John G. Ott, CISA, CPA Aetna Inc., USA  
Thomas Thompson, CISA Ernst & Young, UAE

© Copyright 2004  
Information Systems Audit and Control Association  
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](mailto:standards@isaca.org)  
Web site: [www.isaca.org](http://www.isaca.org)