Information Systems Audit and Control Association

STANDARDS FOR INFORMATION SYSTEMS CONTROL PROFESSIONALS

Introduction

The Information Systems Audit and Control Association, Inc. (ISACA) has long recognised that the specialised nature of information systems (IS) auditing, and the skills necessary to perform such audits, require standards that apply specifically to IS auditing. However, as the proportion of members from the IS Control Professional community grows, the ISACA has perceived a need to produce further ethical guidance and standards for its non-audit membership.

The attached Standards for IS Control Professionals are the ISACA's first steps in meeting this need. In addition, a Draft Code of Professional Ethics for IS Control Professionals has been issued for re-exposure, alongside the revised Code of Professional Ethics for ISACA members and holders of the Certified Information Systems Auditor (CISA) designation.

Objectives

The objectives of the ISACA's Standards for IS Control Professionals are to inform

- IS Control Professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics for IS Control Professionals (currently issued as an exposure draft)
- Management and other interested parties of the profession's expectations concerning the work of practitioners

Scope and Authority of Standards for IS Control Professionals

ISACA's intent is to respond to the growing need for standards outside the IS Audit profession, including but not limited to the areas of:

- data security
- business continuity planning
- data and media administration
- quality assurance

The framework for the ISACA's Standards for IS Control Professionals provides for multiple levels of standards, as follows:

Standards define mandatory requirements for IS Control functions.

Guidelines provide guidance in applying standards for IS Control Professionals. The IS Control Professional should consider them in determining how to achieve implementation of the standards, use professional judgment in their application and be prepared to justify any departure.

Procedures provide examples of procedures an IS Control Professional might follow. The procedure documents provide information on how to meet the standards when performing IS Control Professional functions, but do not set requirements.

The Draft ISACA Code of Professional Ethics requires members of the ISACA and holders of the CISA designation when performing IS control functions, to comply with Standards for IS Control Professionals as issued by the ISACA. Failure to comply with these standards may result in an investigation into the member's or CISA holder's conduct by the ISACA Board or appropriate ISACA committee, and ultimately in disciplinary action.

Development of Standards, Guidelines and Procedures

The ISACA Standards Board is committed to wide consultation in the preparation of 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 on-going development programme, and would welcome the input of members of the ISACA and holders of the CISA designation to identify emerging issues requiring new standards products. Any suggestions should be e-mailed (research@isaca.org), faxed (+1.847. 253 .1443), or mailed (address at the end of the Standards) to ISACA's International Office for the attention of the Director of Research, Standards and Academic Relations.

This material was issued on 1 May 1999 and is effective for IS control functions carried out on or after 1 September 1999.

Standards for Information Systems Control Professionals

510. Statement of Scope

510.010 Responsibility, Authority and Accountability

The responsibility, authority and accountability of the information systems control functions are to be appropriately documented and approved by an appropriate level of management.

520. Independence

520.010 Professional Independence

In all matters related to information systems control, the information systems control professional is to be independent in attitude and appearance.

520.020 Organisational Relationship

The information systems control function is to be sufficiently independent of the area being controlled to permit objective completion of the information systems control professional's duties.

530. Professional Ethics and Standards

530.010 Code of Professional Ethics

The information systems control professional is to adhere to the Code of Professional Ethics for Information Systems Control Professionals issued by the Information Systems Audit and Control Association.

530.020 Due Professional Care

Due professional care and observance of applicable professional standards are to be exercised in all aspects of the information systems control professional's work.

540. Competence

540.010 Skills and Knowledge

The information systems control professional is to be technically competent, having the skills and knowledge necessary to perform the control professional's work.

540.020 Continuing Professional Education

The information systems control professional is to maintain competence through appropriate continuing professional education.

550. Planning

550.010 Control Planning

The information systems control professional is to use risk assessment and other tools as appropriate in planning and prioritising the information systems control work to address the control objectives.

560. Performance of Work

560.010 Supervision

Information systems control professionals are to be appropriately supervised and coordinated to provide assurance that control objectives are accomplished and applicable professional standards are met.

560.020 Evidence

The information systems control professional is to maintain sufficient, reliable, relevant and useful evidence of activities and tasks performed to achieve the control objectives. Control assessments are to be supported by appropriate analysis and interpretation of this evidence.

560.030 Effectiveness

In carrying out their duties, information systems control professionals are to establish appropriate measures of the effectiveness of their activities in achieving both the objectives of their role and the objectives defined in the Statement of Scope.

570. Reporting

570.010 Periodic Reporting

The information systems control professional is to report periodically to an appropriate level of management on the extent to which control objectives have been achieved.

580. Follow-Up Activities

580.010 Follow-Up

The information systems control professional is to monitor the performance of control procedures and review feedback on the efficiency and effectiveness of control activities and is to ensure appropriate corrective action is taken where necessary.

This material was issued on 1 May 1999 and is effective for information systems control activities carried out on or after 1 September 1999.

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: *research@isaca.org*
Web Site: *www.isaca.org*