



Information Systems
Audit and Control
Association

IS AUDITING GUIDELINE

IT GOVERNANCE

DOCUMENT G18

Introduction

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, Inc.[®] (ISACA[™]) is to advance globally applicable standards to meet this need. The development and dissemination of IS Auditing Standards are a cornerstone of the ISACA professional contribution to the audit community.

Objectives

The objectives of the ISACA IS Auditing Standards are to 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* for IS auditors
- Management and other interested parties of the profession's expectations concerning the work of practitioners

The objective of IS auditing guidelines is to provide further information on how to comply with the IS Auditing Standards.

Scope and Authority of IS Auditing Standards

The framework for the ISACA IS Auditing Standards provides multiple levels of guidance:

- **Standards** define mandatory requirements for IS auditing and reporting.
- **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 judgment in their application and be prepared to justify any departure.
- **Procedures** provide examples of procedures an IS auditor might follow in an audit engagement. Procedures should not be considered inclusive of any proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtain the same results. In determining the appropriateness of any specific procedure, group of procedures or test, the IS auditor should apply their own professional judgment to the specific circumstances presented by the particular information systems or technology environment. The procedure documents provide information on how to meet the standards when performing IS auditing work, but do not set requirements.

The words audit and review are used interchangeably.

Holders of the Certified Information Systems Auditor[™] (CISA[®]) designation are to comply with IS Auditing Standards adopted by ISACA. 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.

Development of Standards, Guidelines and Procedures

The ISACA Standards Board is committed to wide consultation in the preparation of 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 would welcome the input of members of the ISACA and holders of the CISA designation and other interested parties 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 provided at the end of this guideline) to ISACA International Headquarters, for the attention of the director of research standards and academic relations.

This guideline replaces the previously issued IS Auditing Guideline Corporate Governance of Information Systems, which will be withdrawn on the date which this guideline becomes effective. This material was issued on 1 April 2002.

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION 2001-2002 STANDARDS BOARD

Chair, Claudio Cilli, CISA, Ph.D. KPMG, Italy
Claude Carter, CISA, CA Nova Scotia Auditor General's Office, Canada
Sergio Fleginsky, CISA PricewaterhouseCoopers, Uruguay
Alonso Hernandez, CISA, ROAC Colegio Economistas, Spain
Marcelo Hector Gonzalez, CISA Central Bank of Argentina Republic, Argentina
Andrew MacLeod, CISA, FCPA, MACS, PCP, MIIA Brisbane City Council, Australia
Peter Niblett, CISA, CA, MIIA, FCPA Day Neilson, Australia
Venkatakrisnan Vatsaraman, CISA, ACA, AICWA, CISSPEmirates Airlines, United Arab Emirates
Sander S. Wechsler, CISA, CPA Ernst & Young, USA

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 the appropriate analysis and interpretation of this evidence."

1.2 Need for Guideline

1.2.1 The COBIT® *Executive Summary* states: "Organisations must satisfy the quality, fiduciary and security requirements for their information, as for all assets. Management must also optimise the use of available resources including data, application systems, technology, facilities and people. To discharge these responsibilities, as well as to achieve its objectives, management must establish an adequate system of internal control."

1.2.2 Use of technology in all aspects of economic and social endeavours has created a critical dependency on Information technology to initiate, record, move, and manage all aspects of economic transactions, information and knowledge, creating a critical place for IT governance within enterprise governance.

1.2.3 High profile problems (for example: system failures resulting from virus attacks, loss of trust or systems availability due to web site hacking) experienced by a variety of public and private sector organisations have focussed attention on enterprise governance issues. The formal means by which management discharges its responsibility to establish an effective system of internal control over an organisation's operational and financial activities can be subject to public scrutiny and often forms part of the audit scope for both internal and external IS auditors.

1.2.4 The purpose of this guideline is to provide information on how an IS auditor should approach an audit of the IT governance, covering the appropriate organisational position of the IS auditor concerned, issues to consider when planning the audit, and evidence to review when performing the audit. This guideline also provides guidance on reporting lines and content and the follow-up work to be considered.

2. AUDIT CHARTER

2.1 Mandate

2.1.1 IT governance, as one of the domains of the enterprise governance, comprises the body of issues addressed in considering how IT is applied within the enterprise. IT is now intrinsic and pervasive within enterprises, rather than being a separate function marginalised from the rest of the enterprise. How IT is applied within the enterprise will have an immense effect on whether the enterprise will attain its mission, vision, or strategic goals. For this reason, an enterprise needs to evaluate its IT governance, as it is becoming an increasingly important part of the overall enterprise governance. Reporting on IT governance involves auditing at the highest level in the organisation, and may cross divisional, functional or departmental boundaries. The IS auditor should confirm that the terms of reference state the:

- Scope of work, including a clear definition of the functional areas and issues to be covered
- Reporting line to be used where IT governance issues are identified to the highest level of the organisation
- IS auditor's right of access to information

3. INDEPENDENCE

3.1 Organisational Status

3.1.1 The IS auditor should consider whether his or her organisational status is appropriate for the nature of the planned audit. Where this is not considered to be the case, the hiring of an independent third party to manage or perform this audit should be considered by the appropriate level of management.

4. PLANNING

4.1 Fact Finding

4.1.1 The IS auditor should obtain information on the IT governance structure, including the levels responsible for:

- Governing the enterprise
- Setting the enterprise strategic directions
- Assessing performance of the Chief Executive Officer/executive management in implementing enterprise strategies
- Assessing the performance of senior management and subordinates who report on the strategies in operation (including the knowledge, information and technology involved)
- Determining whether the enterprise has developed the skills and IT infrastructure required to meet the strategic goals set for the enterprise
- Assessing the enterprise's capability to sustain its current operations

4.1.2 The IS auditor should identify and obtain a general understanding of the processes which enable the IT governance structure to perform the functions listed in 4.1.1 including the communication channels used to set goals and objectives to lower levels (top-down) and the information used to monitor its compliance (bottom-up).

4.1.3 The IS auditor should obtain information on the organisation's information systems strategy (whether documented or not), including:

- Long and short range plans to fulfil the organisation's mission and goals
- Long and short range strategy and plans for IT and systems to support those plans
- Approach to setting IT strategy, developing plans and monitoring progress against those plans
- Approach to change control of IT strategy and plans

- IT mission statement and agreed goals and objectives for IT activities
- Assessments of existing IT activities and systems

4.2 IS Audit Objectives

4.2.1 The objectives of an audit of IT governance may be affected by the intended audience's needs and the level of dissemination intended. The IS auditor should consider the following options in establishing the overall objectives of the audit:

- Reporting on the system of governance and/or its effectiveness
- Inclusion or exclusion of financial information systems
- Inclusion or exclusion of nonfinancial information systems

4.2.2 The detailed objectives for an IS audit of IT governance will ordinarily depend upon the framework of internal control exercised by top-level management. In the absence of any established framework, the COBIT framework should be used as a minimum basis for setting the detailed objectives.

4.3 Scope of the Audit

4.3.1 The IS auditor should include in the scope of the audit the relevant processes for planning and organising the IT activity and the processes for monitoring that activity.

4.3.2 The scope of the audit should include control systems for the use and protection of the full range of IT resources defined in the COBIT *Framework*. These include:

- Data
- Application systems
- Technology
- Facilities
- People

4.4 Staffing

4.4.1 The IS auditor should provide reasonable assurance that the staff used to perform this review includes persons of appropriate seniority and competence.

5. PERFORMANCE OF AUDIT WORK

5.1 Review of Top-Level Management Activities

5.1.1 IT governance, as part of enterprise governance should be driven by business goals and objectives. The IS auditor should evaluate whether there is a business strategic planning process in place by considering whether:

- There is a clear definition of business vision and mission
- There is a business strategic planning methodology used
- The level of the individuals involved in this process is appropriate
- This planning is periodically updated

5.1.2 In reviewing the IT strategic planning process, the IS auditor should consider whether:

- There is a clear definition of IT mission and vision
- There is a strategic information technology planning methodology in place
- The methodology correlates business goals and objectives to IT business goals and objectives
- This planning process is periodically updated (at least once per year)
- This plan identifies major IT initiatives and resources needed
- The level of the individuals involved in this process is appropriate

5.1.3 In reviewing the IT tactical planning, the IS auditor should consider the project management practices in place, considering:

- The extent of project management methodologies used
- The project management controls applied
- The project management tools used
- The integration of IT and business staff along the various stages of the projects
- Change management methodologies used for large projects, involving significant changes in the organisations

5.1.4 In reviewing the delivery process the IS auditor should consider:

- Operational controls in place (COBIT objectives related to application development)
- The development or modification process
- The project management process (as discussed above in 5.1.3)

5.1.5 Focusing on the application development methodology and practices, and the controls applied over the development process. The IS auditor may include in the review the:

- Application development methodology (considering its quality, for example if it is highly structured and covers all aspects of the system development life cycle and take into consideration special features of the environment such as outsourcing or distributed systems)
- Development metrics used to estimate project size and its progress
- Techniques used to examine testing issues, learning from them and enhancing the methodology and controls for future projects

5.1.6 In reviewing the processes used to administer the current systems portfolio, the IS auditor should consider the coverage of organisational strategic and support areas by the current systems. The IS auditor may include in the review:

- The overall coverage of the policies issued providing the strategic areas defined by the business strategic planning process
- The process followed by top level management to elaborate, communicate, enforce and monitor the policy compliance
- Documented policies on the following that may be appropriate: security, human resources, data ownership, end-user computing, intellectual property, data retention, system acquisition and implementation, outsourcing, independent assurance, continuity planning, insurance and privacy
- The definition of roles and responsibilities of the people involved in the processes under review (for example, data owners, IT management, executive management) and assess whether they are appropriate to support the processes involved in the review
- If the people involved in the processes under review have the skills, experience and resources needed to fulfil their roles
- Whether the appropriate level of involvement of internal audit has been provided (if the organisation has internal audit resources)
- Assessing whether the position in the organisation of IT specialist staff or functions is appropriate to enable the organisation to make the best use of IT to achieve its business objectives
- Assessing whether the organisation and management of IT specialists, and non-specialists with IT responsibilities, is adequate to address the risks to the organisation of error, omissions, irregularities or illegal acts

5.1.7 The IS auditor should consider whether the audit evidence obtained from the above reviews indicates coverage of the appropriate areas. Topics which should be considered are set by COBIT in the IT Governance Management Guideline. This guideline includes the key goal indicators, critical success factors and key performance indicators that drive IT governance to its goals. Examples of the information that should be considered are:

- The existence of an IT mission statement and agreed goals and objectives for IT activities
- Assessment of risks associated with the organisation's use of IT resources, and approach to managing those risks
- IT strategy plans to implement the strategy and monitoring of progress against those plans
- IT budgets and monitoring of variances
- High level policies for IT use and protection and monitoring of compliance with those policies
- Comparison of relevant performance indicators for IT, such as benchmarks from similar organisations, functions, appropriate international standards, maturity models or recognised best practices
- Regular monitoring of performance against agreed performance indicators
- Evidence of periodic reviews of IT by the governance function with action items identified, assigned, resolved, and tracked.
- Evidence of effective and meaningful links between the process described from 5.1.1 (above) to 5.1.5

5.1.8 The IS auditor should consider whether top-level management has initiated the appropriate management activities in relation to IT, and whether these activities are being appropriately monitored.

6. REPORTING

6.1 Addressees

6.1.1 The IS auditor should address reports on IT governance to the audit committee and top-level management.

6.1.2 Where inadequacies in IT governance are identified, these should be reported immediately to the appropriate individual or group defined in the audit charter.

6.2 Contents

6.2.1 In addition to compliance with other ISACA standards on reporting, the audit report on IT governance should include, in accordance with the terms of reference:

- A statement that top-level management is responsible for the organisation's system of internal control
- A statement that a system of internal control can only provide reasonable and not absolute assurance against material misstatement or loss
- A description of the key procedures that top-level management has established to provide an effective IT governance system and the related supporting documentation
- Information on any noncompliance with the organisation's policies or any relevant laws and regulations or industry codes of practice for enterprise governance
- Information on any major uncontrolled risks
- Information on any ineffective or inefficient control structures or controls or procedures, together with the IS auditor's recommendations for improvement
- The IS auditor's overall conclusion on the IT governance, as defined in the terms of reference

7. FOLLOW-UP ACTIVITIES

7.1 Timeliness

7.1.1 The effects of any weaknesses in the system of enterprise governance are ordinarily wide-ranging and high-risk. The IS auditor should therefore, where appropriate, carry out sufficient, timely follow-up work to verify that management action to address weaknesses is taken promptly.

8. EFFECTIVE DATE

8.1 This Guideline is effective for all information systems audits beginning on or after 1 July 2002.

APPENDIX – GLOSSARY

COCO—*Criteria of Control*, published by the Canadian Institute of Chartered Accountants in 1995.

Combined Code on Corporate Governance—The consolidation in 1998 of the "Cadbury," "Greenbury" and "Hampel" Reports. Named after the Committee Chairs, these reports were sponsored by the UK Financial Reporting Council, the London Stock Exchange, the Confederation of British Industry, the Institute of Directors, the Consultative Committee of Accountancy Bodies, the National Association of Pension Funds and the Association of British Insurers to address the Financial Aspects of Corporate Governance, Directors' Remuneration and the implementation of the Cadbury and Greenbury recommendations.

Control Objectives for Enterprise Governance—A discussion document which sets out an "Enterprise Governance Model" focussing strongly on both the enterprise business goals and the Information Technology enablers which facilitate good enterprise governance, published by the Information Systems Audit and Control Foundation in 1999.

Corporate Governance—"... [T]he structure through which the objectives of an organisation are set, and the means of attaining those objectives, and determines monitoring performance guidelines. Good corporate governance should provide proper incentives for board and management to pursue objectives that are in the interests of the company and stakeholders and should facilitate effective monitoring, thereby encouraging firms to use resources more efficiently." (Source: *Principles of Corporate Governance*, issued by the Organisation for Economic Cooperation and Development (OECD) in 1999)

COSO Report—A report on "Internal Control - An Integrated Framework" sponsored by the Committee of Sponsoring Organisations of the Treadway Commission in 1992. It provides guidance and a comprehensive framework of internal control for all organisations.

Enterprise Governance—A broad and wide-ranging concept of corporate governance, covering associated organisations such as global strategic alliance partners (Source: *Control Objectives for Enterprise Governance Discussion Document*, published by the Information Systems Audit and Control Foundation in 1999)

Internal Control—"The policies, procedures, practices and organisational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected." (Source: *COBIT Framework*)

IT Governance—A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.

Performance Indicators—A set of metrics designed to measure the extent to which performance objectives are being achieved on an on-going basis. They can include service level agreements, critical success factors, customer satisfaction ratings, internal or external benchmarks, industry best practices and international standards.

Reasonable Assurance—A level of comfort short of a guarantee but considered adequate given the costs of the control and the likely benefits achieved.

Terms of Reference—A document that confirms the client's and the IS auditor's acceptance of a review assignment.

Top-Level Management—The highest level of management in the organisation, responsible for direction and control of the organisation as a whole (such as director, general manager, partner, chief officer, executive manager)

© Copyright 2002
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