IS AUDITING GUIDELINE

# G9 AUDIT CONSIDERATIONS FOR IRREGULARITIES AND ILLEGAL ACTS

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 information technology (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 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 all 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 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. This material was issued on 1 August 2008.

## 1. BACKGROUND

### 1.1 Linkage to Standards

**1.1.1** Standard S3 Professional Ethics and Standards states: ‘The IS auditor should exercise due professional care, including observance of applicable professional auditing standards’.

**1.1.2** Standard S5 Planning states: ‘The IS auditor should plan the information systems audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards’.

**1.1.3** 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’.

**1.1.4** Standard S7 Reporting states: ‘The IS auditor should provide a report, in an appropriate form, upon the completion of the audit. The audit report should state the scope, objectives, period of coverage, and the nature, timing and extent of the audit work performed. The report should state the findings, conclusions and recommendations and any reservations or qualifications or limitations in scope that the IS auditor has with respect to the audit’.

**1.1.5** Standard S9 Irregularities and Illegal Acts elaborates on requirements and considerations by IS auditors regarding irregularities and illegal acts.

### 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 audit considerations of IS auditors for irregularities and illegal acts, 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** The primary COBIT references are:

- PO5 *Manage the IT investment*
- PO7 *Manage IT human resources*
- PO9 *Assess and manage IT risks*
- PO10 *Manage projects*
- AI1 *Identify automated solutions*
- AI5 *Procure IT resources*
- ME2 *Monitor and evaluate internal controls*
- ME3 *Ensure regulatory compliance*
- ME4 *Provide IT governance*

**1.2.3** The secondary COBIT references are:

- PO3 *Determine technological direction*
- PO4 *Define the IT processes, organisation and relationships*
- PO8 *Manage quality*
- DS7 *Educate and train users*
- DS10 *Manage problems*
- ME1 *Monitor and evaluate IT performance*

**1.2.4** The most relevant COBIT information criteria are:

- Primary: Compliance, confidentiality, integrity and availability
- Secondary: Reliability, efficiency and effectiveness

### 1.3 Need for Guideline

**1.3.1** The purpose of this guideline is to provide guidance to IS auditors to deal with irregular or illegal activities they may come across during the performance of audit assignments.

**1.3.2** Standard S9 Irregularities and Illegal Acts elaborates on requirements and considerations by IS auditors for irregularities and illegal acts. This guideline provides guidance in applying IS auditing standards. The IS auditor should consider it in determining how to achieve implementation of the previously identified standards, use professional judgement in its application and be prepared to justify any departure.

## 2. DEFINITIONS

### 2.1 Non-fraudulent Irregular Activities

**2.1.1** Not all irregularities should be considered fraudulent activities. The determination of fraudulent activities depends on the legal definition of fraud in the jurisdiction pertaining to the audit. Irregularities include, but are not limited to, deliberate circumvention of controls with the intent to conceal the perpetuation of fraud, unauthorised use of assets or services, and abetting or helping to conceal these types of activities. Non-fraudulent irregularities may include:

- Intentional violations of established management policy
- Intentional violations of regulatory requirements
- Deliberate misstatements or omissions of information concerning the area under audit or the organisation as a whole
- Gross negligence
- Unintentional illegal acts

### 2.2 Irregularities and Illegal Acts

**2.2.1** Irregularities and illegal acts may include activities such as, but not limited to:

- Fraud, which is any act involving the use of deception to obtain illegal advantage
- Acts that involve non-compliance with laws and regulations, including the failure of IT systems to meet applicable laws and regulations
- Acts that involve non-compliance with the organisation’s agreements and contracts with third parties, such as banks, suppliers, vendors, service providers and stakeholders
- Manipulation, falsification, forgery or alteration of records or documents (whether in electronic or paper form)
- Suppression or omission of the effects of transactions from records or documents (whether in electronic or paper form)
- Inappropriate or deliberate leakage of confidential information
- Recording of transactions in financial or other records (whether in electronic or paper form) that lack substance and are known to be false
- Misappropriation and misuse of IS and non-IS assets
- Acts whether intentional or unintentional that violate intellectual property (IP), such as copyright, trademark or patents
- Granting unauthorised access to information and systems
- Errors in financial or other records that arise due to unauthorised access to data and systems

**2.2.2** The determination of whether a particular act is illegal generally would be based on the advice of an informed expert qualified to practice law or may have to await final determination by a court of law. The IS auditor should be concerned primarily with the effect or potential effect of the irregular action, irrespective of whether the act is suspected or proven as illegal.

## 3. RESPONSIBILITIES

### 3.1 Responsibilities of Management

**3.1.1** It is primarily management’s responsibility to prevent and detect irregularities and illegal acts.

**3.1.2** Management typically use the following means to obtain reasonable assurance that irregularities and illegal acts are prevented or detected in a timely manner:

- Designing, implementing and maintaining internal control systems to prevent and detect irregularities or illegal acts. Internal controls include transaction review and approval and management review procedures.
- Polices and procedures governing employee conduct
- Compliance validation and monitoring procedures
- Designing, implementing and maintaining suitable systems for the reporting, recording and management of incidents relating to irregularities or illegal acts

**3.1.3** Management should disclose to the IS auditor its knowledge of any irregularities or illegal acts and areas affected, whether alleged, suspected or proven, and the action, if any, taken by management.

**3.1.4** Where an act of irregularity or illegal nature is alleged, suspected or detected, management should aid the process of investigation and inquiry.

### 3.2 Responsibilities of IS Auditors

**3.2.1** The IS auditor should consider defining in the audit charter or letter of engagement the responsibilities of management and audit with respect to preventing, detecting and reporting irregularities, so that these are clearly understood for all audit work. Where these responsibilities are already documented in the organisation's policy or similar document, the audit charter should include a statement to that effect.

**3.2.2** The IS auditor should understand that control mechanisms do not completely eliminate the possibility of irregularities or illegal acts occurring. The IS auditor is responsible for assessing the risk of irregularities or illegal acts occurring, evaluating the impact of identified irregularities, and designing and performing tests that are appropriate for the nature of the audit assignment. The IS auditor can reasonably be expected to detect:

- Irregularities or illegal acts that could have a material effect on either the area under audit or the organisation as a whole
- Weaknesses in internal controls that could result in material irregularities or illegal acts not being prevented or detected

**3.2.3** The IS auditor is not professionally responsible for the prevention or detection of irregularities or illegal acts. An audit cannot guarantee that irregularities will be detected. Even when an audit is appropriately planned and performed, irregularities could go undetected, e.g., if there is collusion between employees, collusion between employees and outsiders, or management involvement in the irregularities. The IS auditor should also consider documenting this point in the audit charter or letter of engagement.

**3.2.4** Where the IS auditor has specific information about the existence of an irregularity or illegal act, the auditor has an obligation to perform procedures to detect, investigate and report it.

**3.2.5** The IS auditor should inform the audit committee (or equivalent) and management when he/she has identified situations where a higher level of risk exists for a potential irregularity or illegal act, even if none is detected.

**3.2.6** The IS auditor should be reasonably conversant with the subject to be able to identify risk factors that may contribute to the occurrence of irregular or illegal acts.

**3.2.7** IS auditors should ensure that they are independent of the subject during the entire audit assignment.

**3.2.8** IS auditors are required to refer to standard S9 Irregularities and Illegal Acts for a detailed discussion on IS auditors' responsibilities.

## 4. RISK ASSESSMENT

### 4.1 Planning the Risk Assessment

**4.1.1** The IS auditor should assess the risk of occurrence of irregularities or illegal acts connected with the area under audit following the use of the appropriate methodology. In preparing this assessment, the IS auditor should consider factors such as:

- Organisational characteristics, e.g., corporate ethics, organisational structure, adequacy of supervision, compensation and reward structures, the extent of corporate performance pressures, organisation direction
- The history of the organisation, past occurrences of irregularities, and the activities subsequently taken to mitigate or minimise the findings related to irregularities
- Recent changes in management, operations or IS systems and the organisation's current strategic direction
- Impacts resulting from new strategic partnerships
- The types of assets held, or services offered, and their susceptibility to irregularities
- Evaluation of the strength of relevant controls and vulnerabilities to circumvent or bypass established controls
- Applicable regulatory or legal requirements
- Internal policies such as a whistle-blower policy, insider trading policy, and employee and management code of ethics
- Stakeholder relations and financial markets
- Human resources capabilities

- Confidentiality and integrity of market-critical information
- The history of audit findings from previous audits
- The industry and competitive environment in which the organisation operates
- Findings of reviews carried out outside the scope of the audit, such as findings from consultants, quality assurance teams or specific management investigations
- Findings that have arisen during the day-to-day course of business
- Process documentation and a quality management system
- The technical sophistication and complexity of the information system(s) supporting the area under audit
- Existence of in-house developed/maintained application systems, compared with packaged software, for core business systems
- The effect of employee dissatisfaction
- Potential layoffs, outsourcing, divestiture or restructuring
- The existence of assets that are easily susceptible to misappropriation
- Poor organisational financial and/or operational performance
- Management’s attitude with regard to ethics
- Irregularities and illegal acts that are common to a particular industry or have occurred in similar organisations

**4.1.2** The risk assessment should take into consideration only those factors that are relevant to the organisation and the subject of the engagement, including risk factors relating to:

- Irregularities or illegal acts that affect the financial accounting records
- Irregularities or illegal acts that do not effect the financial records, but affect the organisation
- Other irregularities or illegal acts that relate to the sufficiency of the organisation’s controls

**4.1.3** As part of the planning process and performance of the risk assessment, the IS auditor should inquire of management with regard to such things as:

- Their understanding regarding the level of risk of irregularities and illegal acts in the organisation
- Whether they have knowledge of irregularities and illegal acts that have or could have occurred against or within the organisation
- How the risk of irregularities or illegal acts is monitored or managed
- What processes are in place to communicate to appropriate stakeholders about the existence of risk of irregularities or illegal acts
- Applicable national and regional laws in the jurisdiction the company operates and extent of co-ordination of the legal department with the risk committee and audit committee

## ~~5~~. PLANNING OF AUDIT WORK

### 5.1 Planning the Engagement

**5.1.1** While the IS auditor has no explicit responsibility to detect or prevent illegal acts or irregularities, the IS auditor should design the procedures to detect illegal acts or irregularities based on the assessed level of risk that they could occur.

**5.1.2** When planning the engagement, the IS auditor should obtain an understanding of such things as:

- A basic understanding of the organisation's operations and objectives
- The internal control environment
- The policies and procedures governing employee conduct
- Compliance validation and monitoring procedures
- The legal and regulatory environment in which the organisation operates
- The mechanism that the organisation uses to obtain, monitor and ensure compliance with the laws and regulations that affect the organisation

### 5.2 Engagement Procedure

**5.2.1** The IS auditor should design procedures for the engagement that take into account the level of risk for irregularities and illegal acts that have been identified.

**5.2.2** The results of the risk assessment and other procedures performed during planning should be used to determine the nature, extent and timing of the procedures performed during an engagement.

**5.2.3.** The IS auditor should inquire of IT and user management (as appropriate) concerning compliance with laws and regulations.

**5.2.4**. The IS auditor should use the results of the risk assessment, to determine the nature, timing and extent of the testing required to obtain sufficient audit evidence of reasonable assurance that:

- Irregularities that could have a material effect on the area under audit, or on the organisation as a whole, are identified
- Control weaknesses that would fail to prevent or detect material irregularities are identified
- All significant deficiencies in the design or operation of internal controls that could potentially affect the issuer's ability to record, process, summarise and report business data are identified

### 5.3 Evaluating the Results of Engagement Procedures

**5.3.1** The IS auditor should review the results of engagement procedures to determine whether indications of irregularities or illegal acts may have occurred.

**5.3.2** When this evaluation is performed, risk factors identified in section 4 should be reviewed against the actual procedures performed to provide reasonable assurance that all identified risks have been addressed.

**5.3.3** The evaluation should also include an assessment of the results of the procedures to determine if undocumented risk factors exist.

## 6. PERFORMANCE OF AUDIT WORK

### 6.1 Responding to Possible Illegal Acts

**6.1.1** During an engagement, indications that the existence of irregularities or illegal acts may come to the attention of the IS auditor. If indications of an illegal act are identified, the IS auditor should consider the potential effect on the subject matter of the engagement, the report and the organisation.

**6.1.2** When the IS auditor becomes aware of information concerning a possible illegal act, the IS auditor should consider taking the following steps:

- Obtain an understanding of the nature of the act.
- Understand the circumstances in which it occurred.
- Obtain sufficient supportive information to evaluate the effect of the irregularity or illegal act.
- Perform additional procedures to determine the effect of the irregularity or illegal act and whether additional acts exist.

**6.1.3** The IS auditor should work with appropriate personnel in the organisation (such as organisational security personnel), including management (at an appropriate level above those involved, if possible), to determine whether an irregularity or illegal act has occurred and its effect.

**6.1.4** When an irregularity involves a member of management, the IS auditor should reconsider the reliability of representations made by management. As stated previously, typically, the IS auditor should work with an appropriate level of management above the one associated with the irregularity or illegal act.

**6.1.5** Unless circumstances clearly indicate otherwise, the IS auditor should assume that an irregularity or illegal act is not an isolated occurrence.

**6.1.6** The IS auditor should also review applicable portions of the organisation's internal controls to determine why they failed to prevent or detect the occurrence of an irregularity or illegal act.

**6.1.7** The IS auditor should reconsider the prior evaluation of the sufficiency, operation and effectiveness of the organisation's internal controls.

**6.1.8** When the IS auditor has identified situations where an irregularity or illegal act exists (whether potential or in fact), the IS auditor should modify the procedures performed to confirm or resolve the issue identified during the engagement's performance. The extent of such modifications or additional procedures depends on the IS auditor's judgement as to the:

- Type of irregularity or illegal act that may have occurred
- Perceived risk of its occurrence
- Potential effect on the organisation, including such things as financial effects and the organisation's reputation
- Likelihood of the recurrence of similar irregularities or illegal acts
- Possibility that management may have knowledge of, or be involved with, the irregularity or illegal act

- Actions, if any, that the governing body and/or management is taking
- Possibility that non-compliance with laws and regulations has occurred unintentionally
- Likelihood that a material fine or other sanctions, e.g., the revocation of an essential licence, may be imposed as a result of non-compliance.
- Effect on the public interest that may result from the irregularity

### 6.2 Effect of Finding Irregularities

**6.2.1** If irregularities have been detected, the IS auditor should assess the effect of these activities on the audit objectives and on the reliability of audit evidence collected. In addition, the IS auditor should consider whether to continue the audit when:

- The effect of irregularities appears to be so significant that sufficient, reliable audit evidence cannot be obtained
- Audit evidence suggests that management, or employees who have a significant role in the issuer's internal controls, have participated in or condoned irregularities

### 6.3 Effect of Finding Indicators of Irregularities

**6.3.1** If the audit evidence indicates that irregularities could have occurred, the IS auditor should:

- Recommend to management that the matter be investigated in detail or the appropriate actions taken. If the IS auditor suspects that management is involved in the irregularity, he/she should identify the appropriate responsible figure in the organisation to whom these conclusions should be reported. If reporting internally proves impossible, the IS auditor should consider consulting the audit committee and legal counsel about the advisability and risks of reporting the findings outside the organisation.
- Perform adequate actions to support the audit findings, conclusions and recommendations

### 6.4 Legal Considerations

**6.4.1** If audit evidence indicates that an irregularity could involve an illegal act, the IS auditor should consider seeking legal advice directly or recommending that management seek legal advice. The IS auditor may want to define responsibility for legal costs in the audit charter or letter of engagement.

## 7. REPORTING

### 7.1 Internal Reporting

**7.1.1** The detection of irregularities should be communicated to appropriate persons in the organisation in a timely manner. The notification should be directed to a level of management above that at which the irregularities are suspected to have occurred. In addition, irregularities should be reported to the board of directors, audit committee of the board, or equivalent body, except for matters that are clearly insignificant in terms of both financial effect and indications of control weaknesses. If the IS auditor suspects that all levels of management are involved, then the findings should be confidentially reported to governing bodies of the organisation, such as the board of directors/ governors, trustees or audit committee, according to the local applicable regulations and laws.

**7.1.2** The IS auditor should use professional judgement when reporting an irregularity or illegal act. The IS auditor should discuss the findings and the nature, timing and extent of any further procedures to be performed with an appropriate level of management that is at least one level above the persons who appear to be involved. In these circumstances, it is particularly important that the IS auditor maintains independence. In determining the appropriate persons to whom to report an irregularity or illegal act, the IS auditor should consider all relevant circumstances, including the possibility of senior management involvement.

**7.1.3** The internal distribution of reports of irregularities should be considered carefully. The occurrence and effect of irregularities is a sensitive issue and reporting them carries its own risks, including**:**

- Further abuse of the control weaknesses as a result of publishing details of them
- Loss of customers, suppliers and investors when disclosure (authorised or unauthorised) occurs outside the organisation
- Loss of key staff and management, including those not involved in the irregularity, as confidence in management and the future of the organisation falls

**7.1.4** The IS auditor should consider reporting the irregularity separately from any other audit issues if this would assist in controlling distribution of the report.

**7.1.5** The IS auditor's report should include:

- Critical policies and practices adopted by the organisation
- If any deviations from generally accepted standards, management's reason for such deviation and the auditor's opinions on such deviations

**7.1.6** The IS auditor should seek to avoid alerting any person who may be implicated or involved in the irregularity or illegal act, to reduce the potential for those individuals to destroy or suppress evidence.

### 7.2 External Reporting

7**.2.1** External reporting may be a legal or regulatory obligation. The obligation may apply to the management of the organisation, or the individuals involved in detecting the irregularities, or both. Not withstanding an organisation's responsibility to report an illegal act or irregularity, the IS auditor's duty of confidentiality to the organisation precludes reporting any potential or identified irregularities or illegal acts. However, in certain circumstances, the IS auditor may be required to disclose an irregularity or illegal act. These include such things as:

- Compliance with legal or regulatory requirements
- External auditor requests
- Subpoena or court order
- Funding agency or government agency in accordance with requirements for the audits of entities that receive governmental financial assistance

**7.2.2** Where external reporting is required, the report should be approved by the appropriate level of audit management prior to external release and should also be reviewed with auditee management in advance, unless the applicable regulations or specific circumstances of the audit prevent this. Examples of specific circumstances that may prevent obtaining auditee management's agreement include:

- Auditee management's active involvement in the irregularity
- Auditee management's passive acquiescence to the irregularity

**7.2.3** If auditee management does not agree to the external release of the report, and external reporting is a statutory or a regulatory obligation, then the IS auditor should consider consulting the audit committee and legal counsel about the advisability and risks of reporting the findings outside the organisation. In some jurisdictions, the IS auditor may be protected by qualified privilege. Even in situations where IS auditor's are protected by privilege, IS auditors should seek legal advice and counsel prior to making this type of disclosure to ensure that they are in fact protected by this privilege.

**7.2.4** The IS auditor, with the approval of audit management, should submit the report to appropriate regulators on a timely basis. If the organisation fails to disclose a known irregularity or illegal act or requires the IS auditor to suppress these findings, the IS auditor should seek legal advice and counsel.

**7.2.5** Where the IS auditor is aware that management is required to report fraudulent activities to an outside organisation, the IS auditor should formally advise management of this responsibility.

**7.2.6** If an irregularity has been detected by an IS auditor who is not part of the external audit team, then the IS auditor should consider submitting the report to the external auditors in a timely manner.

### 7.3 Restriction of Audit Scope

**7.3.1** Where the audit scope has been restricted, the IS auditor should include an explanation of the nature and effect of this restriction in the audit report. Such a restriction may occur if:

- The IS auditor has been unable to carry out the further work considered necessary to fulfil the original audit objectives and support the audit conclusions, e.g., because of unreliable audit evidence, lack of resource or restrictions placed on the audit activities by management
- Management has not carried out the investigations recommended by the IS auditor

## 8 EFFECTIVE DATE

**8.1** This guideline is effective for all IS audits beginning on or after 1 March 2000. This guideline has been reviewed and updated, combined with and replaces G19 Irregularities and Illegal Acts, effective 1 September 2008.

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*