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® (ISACA®) is to advance globally applicable standards to meet this need. The development and dissemination of the 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 the IS Auditing Procedures 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 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 auditors 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. A full glossary of terms can be found on the ISACA web site at www.isaca.org/glossary.htm.

Holders of the Certified Information Systems Auditor™ (CISA®) designation are to comply with the 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 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 following CobiT® resources should be used as a source of best practice guidance:
- 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

Each of these is organised by the IT management process, as defined in the CobiT Framework. CobiT is intended for use by businesses and IT management as well as IS auditors. Its usage allows for the understanding of business objectives and for the communication of best practices and recommendations around a commonly understood and well-respected standard reference.

The Standards Board has an ongoing development programme, and welcomes the input of ISACA members and other interested parties to help identify emerging issues requiring new standards. Any suggestions should be e-mailed (research@isaca.org), faxed (+1.847.253.1443) or mailed (address at the end of this procedure) to ISACA International Headquarters, for the attention of the director of research standards and academic relations.

This material was issued on 1 May 2003.
1. **BACKGROUND**

1.1 **Linkage to ISACA Standards**

1.1.1 Standard S5 Planning states, “The IS auditor should plan the information systems audit coverage to address the audit objectives and comply with applicable laws and professional auditing standards.”

1.1.2 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.”

1.1.3 Standard S7 Reporting states, “The IS auditor should provide a report, in an appropriate form, upon the completion of the audit. The report should identify the organisation, the intended recipients and any restrictions on circulation. The audit report should state the findings, conclusions and recommendations and any reservations, qualifications or limitations in scope that the IS auditor has with respect to the audit. The IS auditor should have sufficient and appropriate audit evidence to support the results reported. When issued, the IS auditor’s report should be signed, dated and distributed according to the terms of the audit charter or engagement letter.”

1.1.4 Standard S8 Follow-Up Activities states, “After the reporting of findings and recommendations, the IS auditor should request and evaluate relevant information to conclude whether appropriate action has been taken by management in a timely manner.”

1.1.5 Guideline G13 Use of Risk Assessment in Audit Planning provides guidance.

1.2 **Linkage to COBIT**

1.2.1 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.”

1.2.2 The COBIT Management Guidelines 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?
- 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?

1.2.3 The 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.

1.2.4 The 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.

1.2.5 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’s information criteria.

1.2.6 Refer to the COBIT reference located in the appendix of this document for the specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance.

1.3 **Need for Procedure**

1.3.1 This procedure is designed to provide the following:
- A definition of control risk self-assessment (CRSA)
- Guidance on the use of CRSA methodology
- Guidance on implementing CRSA

2. **CRSA**

2.1 **Definition of CRSA**

2.1.1 CRSA is an empowering method/process by which management and staff of all levels collectively identify and evaluate IS-related risks and controls under the guidance of a facilitator who could be an IS auditor. The IS auditor can utilise CRSA for gathering relevant information about risks and controls and to forge greater collaboration with management and staff. The terms control risk self-assessment and risk and control self-assessment can be used instead of CRSA. CRSA provides a framework and tools for management and employees to:
- Identify and prioritise their business objectives
- Assess and manage high risk areas of business processes
- Self-evaluate the adequacy of controls
- Develop risk treatment action plans
- Ensure that the identification, recognition and evaluation of business objectives and risks are consistent across all levels of the organisation

2.2 **Objective**

2.2.1 CRSA is a technique that adds value by increasing an operating unit’s involvement in designing and maintaining control and risk systems as well as identifying risk exposures and determining corrective action. The CRSA process supports the following IS Auditing Standards: Audit Planning, Performance of Audit Work and Reporting.
2.3 Involvement of the IS Auditor
2.3.1 The IS auditor’s involvement in CRSA exercises can be significant and may involve sponsoring, designing, implementing and, in effect, managing the CRSA process, conducting CRSA training, supplying facilitators, orchestrating the participation of key management and staff, and scribing and reporting CRSA outcomes. In other CRSA exercises, the IS auditor’s involvement may be minimal, serving as an interested party and consultant to the whole process and as an ultimate verifier of the evaluations produced by the teams. In most exercises, the IS auditor’s involvement in CRSA exercises will be somewhere between these extremes.

2.3.2 Whatever the role of the IS auditor in the CRSA process, the IS auditor maintains professional independence and objectivity, in accordance with standard S20.010 Independence and guideline G12 Organisational Relationship and Independence. Ordinarily, the IS auditor acts as a facilitator, drawing on the functional expertise of line management and staff in identifying and assessing risks and developing action plans. The IS auditor contributes expertise in relation to the assessment, implementation and effectiveness of internal controls, just as he/she would in applying other auditing techniques. Line management remains responsible for the effective operation of internal controls and for considering and making decisions on the basis of advice received in the form of a CRSA report and proposed risk management action plan.

2.3.3 A CRSA exercise augments the traditional role of the IS auditor by assisting management in fulfilling its responsibilities to establish and maintain risk management and control processes and to evaluate the adequacy of that system. Through a CRSA exercise, the IS auditor and the business units and functions collaborate to produce better information about how well the control processes are working and how significant the residual risks are.

2.3.4 CRSA should not be seen as a substitute for more traditional auditing techniques, but rather should be considered as one tool within the overall IS assurance and audit framework, which includes CRSA, conventional IS audit techniques, reporting and follow-up activities.

2.3.5 Where a CRSA exercise has been conducted independently of the internal audit function, or the IS auditor has had minimal involvement, it is desirable for the IS auditor to review the CRSA outcomes, as a means of helping to validate the risk assessments and proposed action plans and also to help ensure the IS auditor remains up to date with the risk profile of the area or function concerned.

2.4 Benefits/Advantages of CRSA
2.4.1 CRSA aims to integrate risk management practices and culture into the way staff undertake their jobs, and business units achieve their objectives. The successful implementation of CRSA has a number of specific benefits:

- Directly involves the audit customer in risk assessment and control evaluation activities, and thereby assists in creating a partnership approach between the customer and the IS auditor
- Allows the IS auditor to better allocate scarce resources by involving the customer in the risk assessment and control evaluation process
- Educates management and employees in risk management and control evaluation
- Aligns business unit objectives with corporate goals
- Fosters a sense of ownership of risks and controls
- Builds teamwork in addressing risks
- Improves communication within business units and across the organisation
- Provides a mechanism for raising the awareness of management and staff with respect to the effect that soft controls such as organisational values, ethical standards, competence and leadership styles can have on the overall health of the corporate control system

2.5 Limitations of CRSA
2.5.1 CRSA is not a technique to find fraud and may not be appropriate for regulatory audits that require testing of attributes and documentation of the attribute tested.

2.5.2 The particular style of management may mean that when issues are presented for discussion, participants may not be candid in terms of risk disclosure and may not trust each other and work effectively as a team.

2.5.3 CRSA works well in an organisational environment of devolved management and empowerment. It does not work well in an organisation that does not value innovation and collaboration.

2.5.4 Difficulties may be experienced in attempting to introduce new management practices, techniques or concepts to an organisation. The CRSA process involves initial and continuous investment and its cost/benefit ratio is not easy to determine.

2.5.4 Some of the major obstacles/restraints/pitfalls to the conducting of CRSA exercises are:

- Lack of top management support
- Selection of facilitators who lack skills and experience in facilitation, consensus oriented techniques, and knowledge of the theory and application of controls, or who do not adequately prepare for the CRSA workshop by familiarising themselves with the system under review
- Underestimation of the investment, learning or planning necessary to mount a successful workshop or series workshops
- Narrowing the focus and thereby limiting the potential of the CRSA exercise to be effective
- Starting off with a huge first project

2.6 Possible IS Areas Suitable for the CRSA Process
2.6.1 CRSA can be used in many areas that include system development projects, project development teams, data centre operations, system security for operating systems, networks, databases and application systems, help desk and call centres, telephone systems, business continuity and disaster preparedness, IS documentation, electronic data interchange, web server management, and IT governance.

2.6.2 CRSA can be used to identify and assess risks and controls in a target area or function and to develop a comprehensive risk management action plan.

2.6.3 Alternatively, or in addition to developing an action plan, CRSA can be used to highlight risk areas and issues that need additional
testing. The additional testing can be carried out using traditional IS audit techniques, or it can be made the subject of follow up CRSA activity.

2.6.4 CRSA can be a valuable tool to assist in the planning of major projects, by providing early identification and evaluation of risks and development of risk management action plans.

2.7 Ownership of CRSA

2.7.1 The participants of CRSA are process owners, i.e., management and staff who are directly involved with or affected by the particular systems and issues under examination, who know them best and are critical to the implementation of appropriate process controls. CRSA highlights the fact that managers and staff at all levels of the organisation are responsible for effective and continuous risk management and internal control.

2.8 CRSA Approach

2.8.1 The primary forms of CRSA are facilitated workshops and structured questionnaires or surveys. Organisations can combine more than one approach.

2.8.2 Frequently facilitated workshops are preferred and are a powerful means of obtaining excellent results in a short time.

2.8.3 The survey or questionnaire approach is often used if the desired respondents are too numerous or widely dispersed to be readily brought together for a workshop. They are also preferred if the culture of the organisation might hinder open, candid discussions in workshop settings or if management desires to minimise the initial time spent and cost incurred in gathering the information.

2.9 Selecting Areas and Management Buy-in

2.9.1 CRSA can be implemented at different levels of an organisation. Strategically, senior management and the board can assess the risks and controls affecting the achievement of corporate objectives. Similarly, business units and functions within the organisation can identify risks and evaluate controls against their own objectives and outcomes. A guiding principle in selecting a business unit or function is that a set of objectives or results can be defined for the group concerned. This is important because there must be a common understanding and acceptance of what the group needs to achieve, against which risks and controls can be assessed and evaluated.

2.9.2 As with any major initiative, management buy-in and commitment is essential to CRSA’s success. Senior management interest and involvement demonstrates the organisation’s commitment to integrating risk management and control evaluation into the way the organisation does business at all levels. This commitment can be demonstrated through senior management issuing a policy or directive on the implementation of CRSA or briefing CRSA workshops in person.

3. CRSA WORKSHOP

3.1 Suggested Procedures

3.1.1 The purpose of CRSA is to give business units the knowledge, skills and support to assess and monitor their own risks. The process can assist the IS auditor in developing a strong control environment in organisation areas as well as encouraging a partnership approach to the management of risk. It enables the IS auditor to provide proactive and value-adding services in assisting business units to manage the achievement of their objectives and, consequently, meeting the organisation’s goals.

<table>
<thead>
<tr>
<th>Suggested Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning a CRSA workshop</td>
</tr>
<tr>
<td>Business objectives—Focuses on the best way to accomplish a business objective. The workshop ordinarily identifies business objectives and then identifies the controls presently in place to help achieve the objective and then assesses the residual risks that might mitigate against achievement of the objectives</td>
</tr>
<tr>
<td>Business risks—Focuses in the first instance on identifying all risks that impinge on the business or system, often with reference to a generic checklist of risks or risk categories. Having listed all possible obstacles, threats or exposures, the workshop examines the existing control procedures to determine if they are sufficient to manage the key risks. Risks that are not sufficiently mitigated are escalated upwards.</td>
</tr>
<tr>
<td>Internal controls—Focuses initially on identifying current controls and then assessing how well they are working to mitigate risk and promote the achievement of the business objectives. The workshop produces an analysis gap between how controls are working and how well management expects these controls to work.</td>
</tr>
<tr>
<td>Business processes—The workshop starts by examining key processes and assessing whether each process or subprocess is producing appropriate results. Where results are considered to be unacceptable or inadequate, then the controls are analysed to identify causes.</td>
</tr>
<tr>
<td>Estimate the completion date of the workshop and the reporting schedule.</td>
</tr>
<tr>
<td>Suggested Procedures</td>
</tr>
<tr>
<td>-----------------------</td>
</tr>
<tr>
<td><strong>Planning a CRSA workshop continued</strong></td>
</tr>
<tr>
<td><strong>Selecting participants</strong></td>
</tr>
<tr>
<td><strong>Workshop preparation</strong></td>
</tr>
<tr>
<td><strong>Workshop tools</strong></td>
</tr>
<tr>
<td><strong>Facilitated workshop using the process-based approach—</strong></td>
</tr>
<tr>
<td><strong>Examining the current control framework for each of the risks identified.</strong> If the group is conducting a control examination workshop, they should prepare a control framework for each of the risks identified. This framework should include the controls in place, the effectiveness of those controls and any control weaknesses. The control examination process should be documented.</td>
</tr>
</tbody>
</table>
Suggested Procedures

| Validating workshop results | Examine and assess information from the CRSA workshop as to whether it is valid and legitimate. The extent to which the IS auditor needs to independently validate controls is based on the level of the residual risk, the importance of the issue, the consistency of the testimonies from one participant to the other and any other supporting information from the workshop, as well as the IS auditor’s professional judgment. The IS auditor should give particular consideration to validating controls where the workshop has converted high-level inherent risks to low-level residual risks. Validation also may include using follow-up questionnaires/surveys and gathering audit evidence. The IS auditor should discuss, with the appropriate management level, his evaluation of the soft controls to get any valuable feedback to better accomplish business objectives. |
| Workshop reporting | Each CRSA exercise should produce a report. In general, the substance of the report will be created during the deliberations, by way of a listing and description of relevant risks, control weaknesses and remedial actions proposed. A group consensus will be recorded for the various issues discussed and the group will review the proposed final report before the end of the session. One of the outputs of the CRSA workshop will be a remedial action plan, the format of which will depend on users’ requirements. The IS auditor should also issue a formal report on the CRSA process and outcomes, including relevant background, context, risk ratings and other material in accordance with ISACA IS Auditing Standard 070 Reporting. |
| Ongoing monitoring | An important part of CRSA is that business units or process owners must revisit their risk assessments regularly and monitor the implementation of action plans. The tools provided for CRSA can act as support in achieving this. Follow-up workshops also can be considered, as should network meetings with business unit representatives to discuss risk management issues and concerns. Monitor the implementation of the agreed actions, in accordance with normal audit and assurance practice and ISACA IS Auditing Standard 58 Follow-Up Activities. |

4. EFFECTIVE DATE

4.1 This procedure is effective for all information systems audits beginning on or after 1 August 2003. A full glossary of terms can be found on the ISACA web site at www.isaca.org/glossary.htm.

APPENDIX

COBIT Reference
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 information criteria.

COBIT provides a detailed set of controls and control techniques for the information systems management environment. Under the Monitoring domain, COBIT has a high-level control objective—“Assess Internal Control Adequacy (M2)”—that has a number of detailed control objectives, such as Internal Control Monitoring, Timely Operation of Internal Controls and Internal Control Reporting, underlying it. The achievement of each of these detailed control objectives could be assisted by the use of control risk self-assessment techniques. Control risk self-assessment techniques can be used both to assess the extent to which an area or function is meeting these detailed control objectives and also to help the area or function to improve its performance in meeting the objectives.

Under the Planning & Organisation domain, COBIT has a high-level control objective—“Assess Risks (PO9)”—that has a number of detailed control objectives, such as Risk Identification, Risk Measurement, and Risk Action Plan, underlying it. Also, the achievement of each of these detailed control objectives could be assisted by the use of control risk self-assessment techniques. Control risk self-assessment techniques can be used to identify and assess inherent and residual risks in an area or function and to help develop an action plan for the effective management of these risks.

Example of Risks Associated With an IT Project

- **Business**
  - Project/system requirements not adequately defined
  - Changes to Project/system requirements cannot be managed
  - Project outcomes do not satisfy business needs
  - Timing of project outcomes does not satisfy business needs
  - Required business changes are not managed

- **Contract**
  - Price changes
  - Contractor’s resources not available as needed
  - Product or services do not meet expectations
  - Contractor fails
  - Contract conditions and terms not enforceable
- Emergence of new technologies
- Failure of key technologies
- Failure of essential services, such as telecommunications or power
- Change or failure of supplier or other input provider
- Organisation is taken over

- Funding becomes partially or totally unavailable
- Project budget proves inaccurate
- Significant input cost increases
- Contract variations not managed
- Project budget exceeded

- Interdependent projects fail or are delayed
- Poor project management methodology
- Poor systems development methodology
- Ineffective project reporting
- Project not completed on time

- Anticipated business benefits from the project are not realised
- Poor systems documentation
- Post-implementation problems and costs
- Long term system maintenance problems and costs

- Skills inadequate to successfully complete implementation
- Skilled resources unavailable
- Skilled resources not retained
- Hardware not available as required

- Project outcomes prove to be inconsistent with corporate objectives and priorities
- Change of corporate priorities or direction
- Expansion of project scope

- Platform not suitable
- Associated existing systems, processes or hardware are not compatible with the project

- Project inputs do not perform as expected
- Project outputs do not perform as expected