IS AUDITING PROCEDURE #1
IS RISK ASSESSMENT MEASUREMENT

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 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 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 material was issued on 1 April 2002.

1 BACKGROUND

1.1 Linkage to Standards/Guidelines

1.1.1 Standard 050.010 (Audit Planning) states, "The information systems auditor is to plan the information systems audit work to address the audit objectives and to comply with applicable professional auditing standards."

1.1.2 Standard 060.020 (Evidence) states, "During the course of the audit, the Information Systems Auditor is to obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by the appropriate analysis and interpretation of this evidence."

1.1.3 Guideline 050.010.030 (Use of Risk Assessment in Audit Planning)

1.2 Need for Procedure

1.2.1 This procedure is designed to provide:

- A definition of IS audit risk assessment
- Guidance on the use of a IS audit risk assessment methodology for use by internal audit functions
- Guidance on the selection of risk ranking criteria and the use of weightings

2. IS RISK

2.1 Risk is the possibility of an act or event occurring that would have an adverse effect on the organisation and its information systems. Risk can also be the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss of, or damage to, the assets. It is ordinarily measured by a combination of effect and likelihood of occurrence.

2.2 Inherent risk refers to the risk associated with an event in the absence of specific controls.

2.3 Residual risk refers to the risk associated with an event when the controls in place to reduce the effect or likelihood of that event are taken into account.

3. IS RISK ASSESSMENT MEASUREMENT

3.1 Risk assessment measurement is a process used to identify and evaluate risks and their potential effect.

4. IS AUDIT RISK ASSESSMENT MEASUREMENT METHODOLOGY

4.1. IS audit risk assessment measurement is a methodology to produce a risk model to optimise the assignment of IS audit resources through a comprehensive understanding of the organisation's IS environment and the risks associated with each auditable unit. See Section 9 for details of auditable units.

4.2. The objective of a risk model is to optimise the assignment of IS audit resources through a comprehensive understanding of the IS audit universe and risks associated with each universe item.

5. RISK-BASED IS AUDIT APPROACH

5.1. More and more organisations are moving to a risk-based audit approach that can be adapted to develop and improve the continuous audit process. This approach is used to assess risk and to assist an IS auditor's decision to do either compliance testing or substantive testing. In a risk based audit approach, IS auditors are not just relying on risk. They are also relying on internal and operational controls as well as knowledge of the organisation. This type of risk assessment decision can help relate the cost/benefit analysis of the control to the known risk, allowing practical choices.

5.2. By understanding the nature of the business, IS auditors can identify and categorise the types of risks that will better determine the risk model or approach used in conducting the review. The risk assessment model can be as simple as creating weights for the types of risks associated with the business and identifying the risk in an equation. On the other hand, risk assessment can be a scheme where risks have been given elaborate weights based on the nature of the business or the significance of the risk.

5.3 The IS auditor is interested in uncontrolled risks and in critical controls. Thus in a risk-based audit approach the IS auditor will be interested in technology-based systems which provide controls for business functions where there is a high inherent risk and in technology-based functions where there is a higher than acceptable residual risk.

5.4 Defining the IS audit universe is the first prerequisite to risk ranking. The determination of the audit universe will be based on knowledge of the organisation's IT strategic plan and organisation operations, a review of organisation charts and function and responsibility statements of all organisation affiliates, and discussions with responsible management personnel.

5.5 Audit planning cycles are ordinarily aligned with business planning cycles. Often, an annual audit planning cycle is selected—either a calendar year or another twelve-month period. Some organisations have planning cycles other than for twelve month periods such as six or eighteen months. Rather than have a fixed planning cycle, some organisations have rolling planning cycles that keep rolling forward a set period. For consistency, this procedure will assume an annual audit planning cycle.

5.6 Selection of audit projects to be included in the IS audit plan is one of the most important problems confronting IS audit management. The audit planning process presents the opportunity to quantify and justify the amount of IS audit resources needed to complete the annual IS audit plan. Failure to select appropriate projects results in unexploited opportunities to enhance control and operational efficiency.

5.7 The assumption underlying the IS audit plan is that an evaluation of prospective audit reviews/projects will be more effective if a formal process is followed for gathering the information necessary to make review/project selection decisions. The approaches described herein are basically a framework in which to apply common sense and professional judgment.

5.8 The methodology presented is relatively simple. However, in a great majority of cases, it should suffice to reach reasonable, prudent and defensible IS audit review/project selection decisions. A framework to use in performing a risk exposure analysis and establishing an audit review/project priority schedule is detailed in this procedure.

5.9 As used here, risk assessment is a technique used to examine auditable units and choose reviews/projects that have the greatest risk exposure. A risk assessment approach to audit review/project selection is important in that it affords a means of providing reasonable assurance that IS audit resources are deployed in an optimal manner, i.e., the IS audit plan allocates IS audit resources in a manner likely to achieve maximum benefits. To this end, the risk assessment approach provides explicit criteria for systematically selecting audit projects. The IS audit plan is often attached with the financial and operational audit plan to detail the complete planned IS audit coverage.

6. IS RISK ASSESSMENT MEASUREMENT TECHNIQUES

6.1 When determining which functional areas should be audited, the IS auditor could face a large variety of audit subjects. If possible all IS areas of the organisation should be included in the risk assessment exercise. Some organisations only rate IS projects. Others rate every IS auditable area/system. Each of these may represent different types of audit risks. The IS auditor should evaluate these various risk candidates to determine which are the high-risk areas and therefore should be audited. The purpose of this process is to:

- Identify areas where the residual risk is unacceptably high
- Identify critical control systems that address high inherent risks
- Assess the uncertainty that exists in relation to the critical control systems

6.2 Using risk assessment to determine IS areas to be audited:

- Enables management to effectively allocate limited IS audit resources
- Provides reasonable assurance that relevant information has been obtained from all levels of management, including the board of directors and functional area management. Generally, the information includes areas that will assist management in effectively discharging their responsibilities and provides reasonable assurance that the IS audit activities are directed to high business risk areas and will add value to management.
- Establishes a basis for effectively managing the IS audit function
- Provides a summary of how the individual review subject is related to the overall organisation as well as to the business plans

7. IS RISK ASSESSMENT MEASUREMENT METHODS

7.1 Several methods are currently employed to perform IS risk assessments. One such risk assessment approach is a scoring system that is useful in prioritising IS audits based on an evaluation of risk factors that consider variables such as technical complexity, extent of system and process change and materiality. These variables may or may not be weighted. These risk values are then compared to each other and ordinarily an annual IS audit plan is prepared. Often the IS audit plan is approved by the audit committee and or the chief executive officer. Reviews are then scheduled according to the IS audit plan. Another form of IS risk assessment is judgmental. This entails making an independent decision based upon executive management directives, historical perspectives and business climate.

8. COLLECTION OF DATA

8.1 Information describing all aspects of the organisation's operation will be used to define the various auditable units and to model the IS risks inherent in the unit's operations. Sources of this data include:

- Interviews conducted with senior management for the purpose of gathering data for the development of the IS risk model
- Returns of structured questionnaires sent to management to facilitate the gathering of IS risk model data
- Recent review reports
- The IT strategic plan
- The budgetary process may be a useful source of information
- Issues raised by the external auditors
- IS audit knowledge and awareness of significant issues gathered from any other sources
- The specific methods used to collect the data, whether they will be sufficient considering the time and resources available for the task

9. IS AUDITABLE UNITS

9.1 The model is meant to include and provide a risk rating for every IS auditable unit in the organisation (the IS audit universe). An auditable unit can be defined as the discrete segments of every organisation and its systems. There are no specific rules for determine or differentiate an individual auditable unit. However, the following are guidelines for use in this audit risk model for each unit/topic/function:

- Auditable in a reasonable timeframe
- A system, i.e., have recognisable inputs, processes, outputs, outcome
- Separable, i.e., able to be audited with minimal reference to other systems (This may be difficult if an application system under review has many interfaced systems.)

10. EXAMPLES

10.1 There are many different methods of performing IS risk assessment measurements. Sections 11 through 14 contain several types of IS risk assessments.

11. EXAMPLE I

11.1 Example I shows an IS risk assessment measurement evaluation with eight key variables. Each unit/area in the IS audit universe will be rated on these eight key variables using a numeric descriptive value ranking of 1 (low) to 5 (high). The results of these ranking judgments are then multiplied by significance weighting factors that range from 1 (low) to 10 (high) to give an extended value. Arbitrary examples of significance weighting factors are included in example I. These extended values are added together to give a total. Once the totals for each auditable unit/area have been obtained, the auditable units/areas are ranked by risk. The framework of the annual IS audit plan is then built from these rankings. The eight key variables are listed in sections 11.1.1 to 11.1.3 with a brief explanation of each.

11.1.1 Measures of Effect

- **Character of activity**—The criticality of the activity and the part of the organisation that utilises the activity. Infrequent or unusual activities or projects are more likely to result in error or inefficiency and are of greater audit interest.
- **Fall back arrangements**—This factor relates to the measures that have been put in place to continue operations if the new system has problems. Factors to consider include business continuity plans, disaster recovery plans, manual procedures, and the old system.

Generally speaking, if the above issues have been addressed, are achievable or are cost beneficial, then the risk is lowest.

- **Sensitivity of the function to executive management**—This factor relates to how important the unit, function or area is viewed by executive management.
- **Materiality**—A concept regarding the importance of an item of information with regard to the effect on the functioning of the organisation. An expression of the relative significance or importance of a particular matter in the context of the organisation as a whole.

11.1.2 Measures of Likelihood

- **Extent of system or process change**—A dynamic environment in terms of system or process change increases the probability of errors and consequently increases audit interest. A considerable amount of process re-engineering may have taken place. System or process change ordinarily occurs to effect improvement in the long term but often has short-term offsets that require increased audit coverage**.**
- **Complexity**—This risk factor reflects the potential for errors or misappropriation to go undetected because of a complicated environment. The rating for complexity will depend on many factors. Extent of automation, complex calculations, interrelated and interdependent activities, number of products or services, the time spans of estimates, dependency on third parties, customer demands, processing times, applicable laws and regulations and many other factors, some not recognised, affect judgments about the complexity of a particular audit.
- **Project management**—Consideration should be given to the following when ranking project management:
  - In-house or outside developers
  - Project structure
  - Personnel skills
  - Project timeframes

Generally speaking, the risk is shared if the project is outsourced.

11.1.3 Measures of Uncertainty about the Controls

- **Period since last review**—As the time since the last review coverage lengthens, the value of a new review is likely to increase. The beneficial effects of a review are greatest immediately before or after system implementation.

EXAMPLE I—**IS RISK ASSESSMENT MEASUREMENT EVALUATION**

KEY VARIABLES	DESCRIPTIVE VALUE 1 (low) to 5 (high)	SIGNIFICANCE WEIGHTING 1 (low) to 10 (high)	EXTENDED VALUE
1. **Character of activity**	**Consider:** Core activity = 4 to 5 Business unit = 2 to 3 Local system = 1	8*	
2. **Fall back**	**Consider:** Business continuity plans Disaster recovery plans Manual procedures Old system	5*	
3. **Sensitivity of the function to executive management**	Major interest = 4 to 5 Moderate interest = 2 to 3 Minor interest = 1	6*	
4. **Materiality**	**Significance of expenditures or revenues generated or resources consumed.** Project budget >$500,000 = 4 to 5 Project budget $100,000 to $500,000 = 2 to 3 Project budget <$100,000 = 1 Revenue/expenditure >$500,000 = 4 to 5 Revenue/expenditure $100,000 to $500,000 = 2 to 3 Revenue/expenditure <$100,000 = 1	5*	
5. Extent of system, procedure and process change	**Consider:** The extent of reengineering. Major reengineering = 4 to 5 Moderate reengineering = 2 to 3 Minor reengineering = 1 Or No procedures = 4 or 5 Local procedures = 3 or 2 Corporate procedures = 1	8*	
6. **Complexity**	**Consider:** Transactions volume Number of users Centralised or decentralised Number of interfaces Very complex = 4 to 5 Moderately complex = 2 to 3 Simple = 1	7*	
7. **Project management**	**Consider:** In-house or outside developers Project structure Personnel skills Project timeframes	7*	
8. **Period since last review**	Rating of 5 indicates 5 years or more since last audit or never	1*	
	Total		

* Uses arbitrary Significance Weighting Example

12. EXAMPLE II

12.1 Example II extends the IS risk assessment measurement evaluation used in example I by incorporating business risks as well as the eight IS audit key variables used in example I. The IS audit risk ranking factor (from example I) is multiplied by business risk in this example. The business risk factors (financial, strategic, operational, and legal compliance) are considered regarding their relevance to each auditable unit/area.

12.2 Each unit/area in the IS audit universe will be rated on these eight key variables using a numeric rating of 1 (low) to 5 (high). The results of these rating judgments are then multiplied by a significance weighting factor, which ranges from 1 (low) to 10 (high) as in example I. These extended values are added together to give a total (using the arbitrary significance weightings used in example I). This total is the IS audit risk ranking factor.

12.3 The four business risk factors are defined below:

- **Financial risk**—As most systems potentially have some effect on the organisation's financial performance, the level and likelihood of such an effect needs to be considered. If the anticipated effect is indirect and relatively minor in comparison with other effects and purposes of the system and/or in comparison with other auditable areas/systems then we would probably score 0 rather then 1 for the financial risk factor.
- **Strategic risk**—Systems may have direct strategic effect on the organisation. Some that would be expected to score 1 on the risk factor are those identified by executive management.
- **Operational risk**—Operational risk will probably be rated 1 more commonly than any of the other business risk factors since most systems are designed to affect the manner in which, and the effectiveness with which, the organisation conducts its day-to-day business.
- **Legal compliance**—Systems can have a direct effect on how the organisation complies with statutory obligations.

12.4 Insert a score of 1 (relevant) or 0 (not relevant) for each *business risk factor.* Then multiply each score by the respective weighting and add, to give the total *business risk ranking factor* for each audit topic.

12.5 In assigning scores consider the following three issues:

- What are the anticipated purpose and objectives of the system being audited?
- What are the anticipated scope and objectives of the audit?
- Does the system directly effect the organisation's financial/strategic/operational/compliance performance? For example, if the system does not operate as intended, is it probable that the organisation will suffer financial loss, experience strategic disadvantage, have operational problems or contravene relevant legal requirements?

12.6 The final step in this example is to multiply the *audit risk* ranking factor by the *business risk ranking factor*, to give the *total risk ranking*. See the example in the table below. Once the *total risk rankings* for each auditable unit/area have been obtained the auditable units/areas are ranked by risk. The framework of the annual IS audit plan is then built from these rankings.

EXAMPLE II—IS RISK ASSESSMENT MEASUREMENT EVALUATION INCORPORATING BUSINESS RISK FACTORS

AUDITABLE UNIT	AUDIT RISK RANKING (from Example I)	BUSINESS RISK FACTORS (RATE 0 OR 1)				BUSINESS RISK RANKING FACTOR	TOTAL RISK RANKING
		FINANCIAL	STRATEGIC	OPERATIONAL	LEGAL COMPLIANCE		
Business	**Risk weighting**	**5***	**4***	**3***	**2***		
Treasury system	158	1	1	1	0	12	1896
Business continuity	162	0	0	1	1	5	810
Payroll	165	0	0	1	0	3	495
Local area networks	159	0	0	1	0	3	477
Computer operations	146	0	0	1	0	3	438
Software licencing	123	0	0	0	1	2	246
RACF	152	0	0	1	0	3	456

For Example-Treasury System: 158 *(5*1+4*1+3*1+2*0)=158*(5+4+3)=158*12=1896

13. EXAMPLE III

13.1 Some IS auditors prefer to just rank IS projects and not the whole IS auditable universe. Example III provides a methodology to rank IS projects. Each IS project in the IS audit universe will be rated on these eight key variables using a numeric risk value ranking of 1 (low) to 5 (high). The results of these ranking judgments are then multiplied by a Weighting factor that ranges from 1 (low) to 10 (high) to give an extended value. These extended values are added together to give a total. Once the totals for each project have been obtained, the projects are ranked by risk. The framework of the annual IS audit project coverage is then built from these rankings. The categories used in Example III are listed in 13.2 and 13.3.

13.2 Measures of Effect

- **Project budget**—The total budget of an IS project is an important factor to consider. As a guide, some organisations rank project budgets over US$500,000 as a risk level of 4 or 5. These organisations rank budgets between US $100,000 to US$ 500,000 as a risk ranking of 2 or 3 and budgets under US $100,000 as a risk level of 1.
- **Transaction volume**—The total volume of transactions that are estimated to be processed by the system in a given period.
- **Character of activity**—The criticality of the activity and the part of the organisation that utilises the activity. Infrequent or unusual activities or projects are more likely to result in error or inefficiency and are of greater audit interest.
- **Executive management interest**—This factor relates to how important the unit, function or area is viewed by executive management.
- **Fall back arrangements**—This factor relates to the measures that have been put in place to continue operations if the new system has problems. Factors to consider include:
  - Business continuity plans
  - Disaster recovery plans
  - Manual procedures
  - Old system

Generally speaking, if the above issues have been addressed, are achievable or are cost beneficial then the risk is lowest.

13.3 Measures of Likelihood

- **Changes in procedures**—The extent of procedural change or reengineering accompanying the system implementation.
- **Complexity of system**—Factors such as number of users, number of system modules, mainframe versus a client-server environment (centralised versus a decentralised environment), and the number of interfaces are considered.
- **Project management**—Consideration should be given to the following when ranking project management:
  - In-house or outside developers
  - Project structure
  - Personnel skills
  - Project timeframes

Generally, speaking the risk is shared if the project is outsourced.

EXAMPLE III—**IT PROJECT RISK RANKING**

Category	**Risk level** 1(Low) to 5(High)	**Significance weighting** 1(Low) to 10(High)	**Total**
1. Project budget >$500,000 = 4 to 5 $100,000 to $500,000 = 2 to 3 <$100,000 = 1		**5**	
2. Transaction volume		**2**	
3. Character of activity Core council 4 to 5 Business unit 2 to 3 Local system 1		**8**	
4. Executive management interest Major interest = 4 to 5 Moderate interest = 2 to 3 Minor interest = 1		**6**	
5. Fall-back arrangements Business continuity/ disaster recovery plans Manual procedures Old system		**7**	
6. Changes in **procedures** (Extent of reengineering) Major reengineering = 4 to 5 Moderate reengineering = 2 to 3 Minor reengineering = 1		**8**	
7. Complexity of system Number of users Number of modules Centralised or decentralised (mainframe v. client-server) Interfaces		**7**	
8. Project management In-house Outside developers Structure Skills Timeframe		**7**	
		Total	

14. EXAMPLE IV—IS Risk Assessment of Auditable Units

14.1 Example IV ranks various categories of auditable units in the IS auditable universe after they have been identified. The categories are listed based on the nature of risk that these units are exposed to. Relevant information, such as, financial exposure, effect on business, and scope is collected. The categories are as follows:

i. Data centre operations
ii. Application systems (production)
iii. Application systems (development)
iv. IS procurement (manpower and material)
v. Software package acquisition
vi. Other IS functions

14.2 Under each category, major risk components are enumerated. Depending on the type of risk a weight is assigned to each risk element. Each risk element is then further subdivided and a score attached to it. This risk score of a particular risk element is the product of the *score* and its weight. The total risk score of the function is the sum of the scores of all its risk elements. For ease of comparison, the risk score is measured on a scale of 100. Separate risk assessment sheets can been prepared for each of the auditable unit. Finally the scores obtained for each of the auditable units are consolidated and audits prioritised.

EXAMPLE IV—RISK ASSESSMENT—IS AUDIT
i. DATA CENTRE OPERATIONS

	Rating factor	Weight	Score	Assigned score
1.	**Number of data centre staff** Very small under 2 Small 3—7 Moderate 7—15 Large 16—25 Very large Above 25	1	1 2 3 4 5	5
2.	**Effect on the group's business** No effect Small Moderate High Put Group out of business	5	1 2 3 4 5	25
3.	**Number of applications** Single Under 5 5—15 16—25 Above 25	5	1 2 3 4 5	25
4.	**Number of users** Below 25 26—50 51—100 100—250 Above 250	2	1 2 3 4 5	10
5.	**Prior audit findings** No significant findings A few insignificant findings Many Insignificant findings A few significant findings Many significant findings	1	1 2 3 4 5	5
6.	**Sophistication of processing** Batch Batch/real-time Batch/real-time/online Client/server Parallel/distributed	2	1 2 3 4 5	10
7.	**Changes in equipment/platform/staff** No changes Moderate changes/low turnover Platform changes/low turnover High turnover Platform changes and high turnover	1	1 2 3 4 5	5
8.	**Number of platforms** 1 2 3 4 5+	3	1 2 3 4 5	15
	Total risk score		100	100

EXAMPLE IV—RISK ASSESSMENT—IS AUDIT
ii. APPLICATION SYSTEMS (PRODUCTION)

	Rating factor	Weight	Score	Assigned score
1.	**Effect of system failure (criticality)** No immediate effect Inconvenience to users Loss of goodwill Loss of revenue Loss of business/revenue/goodwill	**5**	 1 2 3 4 5	25
2.	**Financial exposure (AED)** None Small (<100,000) Moderate (100,000—1 m) High (1m—10 m) Very high (>10 m)	**5**	 1 2 3 4 5	25
3.	**Scope of the system** Part of a department Complete department Multidepartment Organisationwide Organisation and external	**2**	 1 2 3 4 5	10
4.	**Age of the application** Over 10 years 7—10 years 4—6 years 1—3 years Less than one year	**1**	 1 2 3 4 5	5
5.	**Prior audit findings** Recent Audit—no weaknesses Recent Audit—minor weaknesses Audit—Some weaknesses Audit—Many weaknesses No previous audit	**2**	 1 2 3 4 5	10
6.	**Size of the application (number of programs)** Below 25 25—50 50—100 100—250 Above 250	**3**	 1 2 3 4 5	15
7.	**Changes in environment/staff** No changes Moderate changes/low turnover Significant changes/low turnover High turnover Significant changes and high turnover	**1**	 1 2 3 4 5	5
8.	**Number of locations implemented** 1 2 3 4 5+	**1**	 1 2 3 4 5	5
	Total risk score		**100**	100

EXAMPLE IV—RISK ASSESSMENT—IS AUDIT
iii. APPLICATION SYSTEMS (DEVELOPMENT)

	Rating factor	Weight	Score	Assigned score
1.	**Size, organisation and experience of team** Small, dedicated and experienced team Average size, centralised and experienced team Average, experienced and mixed priorities Average, mostly centralised with other priorities Large, decentralised, inexperienced and unclear reporting	**3**	 1 2 3 4 5	15
2.	**Size of the system** Small number of programs for 1 department Moderate number of programs for 1 department Large number of programs for many departments Moderate number of programs for entire organisation Large number of programs for entire organisation	**3**	 1 2 3 4 5	15
3.	**Duration of the development cycle** Less than 3 months 3—6 months 6—12 months 1—1 1/2 years 2 or more years	**2**	 1 2 3 4 5	10
4.	**Development platform** Tried and widely used Fairly new but accepted worldwide Fairly new but not accepted worldwide Tried and proprietary New, untried proprietary	**3**	 1 2 3 4 5	15
5.	**Prior audit involvement** Controls building exercise Requirement analysis phase Project schedule monitoring Project cost monitoring None	**2**	 1 2 3 4 5	10
6.	**System development methodology** Standard methodology with documented standards and procedures Standard methodology without documented standards and procedures No standard methodology but experienced team Experimental untried methodology No development methodology used and no documented development standards and guidelines	**3**	 1 2 3 4 5	15
7.	**Project management experience** Very high Above average Average Below average No experience/multiproject	**1**	 1 2 3 4 5	5
8.	**Manpower outsourcing** Small quantity, single supplier Small quantity, heterogeneous suppliers Significant quantity, single suppliers Significant quantity, heterogeneous suppliers 100%	**1**	 1 2 3 4 5	5
	Total risk score		**100**	**100**

EXAMPLE IV—RISK ASSESSMENT—IS AUDIT
iv. IS PROCUREMENT (MANPOWER AND MATERIAL)

	Rating factor	Weight	Score	Assigned score
1.	**Effect** No immediate effect Inconvenience to users Loss of goodwill Loss of revenue Loss of business/revenue/goodwill	**5**	 1 2 3 4 5	25
2.	**Financial exposure (AED)** None Small (<100,000) Moderate (100,000—1 m) High (1m—10 m) Very high (>10 m)	**5**	 1 2 3 4 5	25
3.	**Procedures and guidelines** Documented and tested procedures Procedures not documented Procedures but not implemented fully No set procedures but controlled No set procedures and uncontrolled	**5**	 1 2 3 4 5	25
4.	**Prior audit findings** Recent audit—No weaknesses Recent audit—Minor weaknesses Audit—Some weaknesses Audit—Many weaknesses No previous audit	**2**	 1 2 3 4 5	10
5.	**Complexity** Local sourcing for one department Local sourcing for entire organisation International sourcing for one technology International sourcing for multitechnology International and local sourcing for multitechnology	**3**	 1 2 3 4 5	15
	Total risk score		**100**	**100**

EXAMPLE IV—RISK ASSESSMENT—IS AUDIT
v. SOFTWARE PACKAGE ACQUISITION

	Rating factor	Weight	Score	Assigned score
1.	**Scope of the system** Part of a department Complete department Multidepartment Organisationwide Organisation and external	**5**	 1 2 3 4 5	25
2.	**Financial exposure (AED) associated with the system** None Small (<100,000) Moderate (100,000—1 m) High (1m—10 m) Very high (>10 m)	**5**	 1 2 3 4 5	25
3.	**Nature of package** Off the shelf product Custom built by vendor, maintained by vendor Vendor developed, in-house maintained Jointly developed, vendor maintained Jointly developed, in-house maintained	**2**	 1 2 3 4 5	10
4.	**Type of evaluation** By the user department/IS/consultant By IS/user By consultant By IS By the user department	**1**	 1 2 3 4 5	5
5.	**Cost and complexity of the package** Negligible Small Moderate Significant Very high	**2**	 1 2 3 4 5	10
6.	**Evaluation methodology** Vendor/product evaluated Only product evaluated Only supplier evaluated Not evaluated both purchased conditionally Not evaluated purchased unconditionally	**3**	 1 2 3 4 5	15
7.	**Selection** Selected from many candidates Selected from few reputed vendors Selected from few known systems Selected a familiar system Selected an unfamiliar system	**1**	 1 2 3 4 5	5
8.	**Business effect** No immediate effect Inconvenience to users Loss of goodwill Loss of revenue Loss of business/goodwill/revenue	**1**	 1 2 3 4 5	5
	Total risk score		**100**	**100**

EXAMPLE IV—RISK ASSESSMENT—IS AUDIT
vi. OTHER IS FUNCTIONS

	Rating factor	Weight	Score	Assigned score
1.	**Effect of the function failure (criticality)** No immediate effect Inconvenience to users Loss of goodwill Loss of revenue Loss of business/revenue/goodwill	**5**	 1 2 3 4 5	25
2.	**Financial exposure (AED)** None Small (<100,000) Moderate (100,000—1 m) High (1m—10 m) Very high (>10 m)	**5**	 1 2 3 4 5	25
3.	**Scope of the function** Part of a department Complete department Multidepartments Organisationwide Organisation and external	**2**	 1 2 3 4 5	10
4.	**Age of the function** Over 10 years 7—10 years 4—6 years 1—3 years Less than one year	**1**	 1 2 3 4 5	5
5.	**Prior audit findings** Recent audit—No weaknesses Recent audit—Minor weaknesses No previous audit Audit—Some weaknesses Audit—Many weaknesses	**2**	 1 2 3 4 5	10
6.	**Complexity of the function** Very low Low Moderate High Very high	**3**	 1 2 3 4 5	15
7.	**Number of staff** One Less than 5 6—10 11—25 Above 25	**1**	 1 2 3 4 5	5
8.	**Number of locations** 1 2 3 4 5+	**1**	 1 2 3 4 5	5
	Total risk score		**100**	**100**

15. EFFECTIVE DATE

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

APPENDIX - GLOSSARY

Inherent risk—The susceptibility of an audit area to error which could be material, individually or in combination with other errors, assuming that there were no related internal controls.

Residual risk—The risk associated with an event when the controls in place to reduce the effect or likelihood of that event are taken into account.

Risk—The possibility of an act or event occurring that would have an adverse effect on the organisation and its information systems.

Risk assessment—A process used to identify and evaluate risks and their potential effect.

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*