

G39 IT ORGANISATION

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 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 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 15 March 2008.

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S10 IT Governance states, 'The IS auditor should review and assess whether the IS function aligns with the organisation's mission, vision, values, objectives and strategies. The IS auditor should review whether the IS function has a clear statement about the performance expected by the business (effectiveness and efficiency) and assess its achievement'.

1.2 Linkage to COBIT

- 1.2.1 PO1 *Define a strategic IT plan* states, 'control over the IT process of *Define a strategic IT plan* that satisfies the business requirement for IT of sustaining or extending the business strategy and governance requirements while being transparent about benefits, costs and risks by focusing on incorporating IT and business management in the translation of business requirements into service offerings, and the development of strategies to deliver these services in a transparent and effective manner'.
- 1.2.2 PO4 *Define the IT processes, organisation and relationships*) states, 'control over the IT process of *Define the IT processes, organisation and relationships* that satisfies the business requirement for IT of being agile in responding to the business strategy while complying with governance requirements and providing defined and competent points of contact by focusing on establishing transparent, flexible and responsive IT organisational structures and defining and implementing IT processes with owners, roles and responsibilities integrated into business and decision processes'.
- 1.2.3 PO5 *Manage the IT investment* states, 'control over the IT process of *Manage the IT investment* that satisfies the business requirement for IT of continuously and demonstrably improving IT's cost-efficiency and its contribution to business profitability with integrated and standardized services that satisfy end user expectations by focusing on effective and efficient IT investment and portfolio decisions, and by setting and tracking IT budgets in line with IT strategy and investment decisions'.
- 1.2.4 ME4 *Provide IT governance* states, 'control over the IT process of *Provide IT governance* that satisfies the business requirement for IT of integrating IT governance with corporate governance objectives and complying with laws and regulations by focusing on preparing board reports on IT strategy, performance and risks, and responding to governance requirements in line with board directions'.
- 1.2.5 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 responsibility, authority and accountability requirement of IS auditors, the processes in COBIT most likely to be relevant, selected and adapted are classified below 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.
- 1.2.7 The following specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance are secondary:
- PO2 *Define the information architecture*
 - PO3 *Determine the technological direction*
 - PO6 *Communicate management aims and direction*
 - PO7 *Manage IT human resources*
 - PO8 *Manage quality*
 - PO9 *Assess and manage IT risks*
 - PO10 *Manage projects*
 - DS1 *Define and manage service levels*
 - DS2 *Manage third-party services*
 - DS3 *Manage performance and capacity*
 - DS6 *Manage and allocate costs*
 - DS7 *Educate and train users*
 - DS8 *Manage service desk and incidents*
 - DS9 *Manage the configuration*
 - DS10 *Manage problems*
 - DS12 *Manage the physical environment*
 - DS13 *Manage operations*

- A12 *Acquire and maintain application software*
- A13 *Acquire and maintain technology infrastructure*
- A16 *Manage changes*
- ME1 *Monitor and evaluate IT performance*

1.2.8 The information criteria most relevant to the IT organisation:

- Primary: Effectiveness and efficiency
- Secondary: Confidentiality, availability, integrity, compliance and reliability

1.3 Purpose of the Guideline

1.3.1 Structure can be a distinct enabler or inhibitor of organisational effectiveness but it alone will not determine organisational success. There is no one right structure, because no two organisations are exactly alike. All IT organisations serve similar purposes and have similar accountabilities, but their profiles, management systems, processes, constraints, strengths and weaknesses make each IT organisation unique. There are, however, certain attributes for verifying an optimised IT organisational structure.

1.3.2 This guideline provides guidance in applying IS Auditing Standard S10 IT Governance. The IS auditor should consider this guideline in determining how to achieve implementation of the above standard, use professional judgement in its application and be prepared to justify any departure.

1.4 Guideline Application

1.4.1 When applying this guideline, the IS auditor should consider it in relation to other relevant ISACA standards and guidelines.

2. THE IT ORGANISATION

2.1 Types of Organisations

2.1.1 The boundaries of today's organisations are more flexible and dynamic and, in most cases, more extensive. Organisations and industries realise that they must start focusing on whole processes, including those that transcend the physical walls of the organisation. They must reach out to business partners, suppliers and customers. Accurate, appropriate and timely information is the indispensable component in the new economy or what is commonly referred to as the extended enterprise. Information/knowledge-sharing activity amongst stakeholders of the extended enterprise is a key success factor in delivering workable enterprise governance. An overall competitive strategy must drive an effective knowledge management strategy and leadership. An organisation must build an appropriate information organisation to provide the information required by senior management in decision making, while maintaining an appropriate level of control over it.

2.2 IT Alignment

2.2.1 There is no one-size-fits-all approach for maximising the alignment of IT with the business and all of its components. Much depends upon the nature of the business, its size, its markets, its dependence upon IT, its leadership style and its culture. Additional factors that help dictate the organisation's alignment components and structure include the in-house IT capabilities, the dependence upon outsourcing, the nature of that outsourcing and the overall governance structure.

2.2.2 In recent years, IT has moved from providing largely back-office support to becoming the prime facilitator and enabler of the total business. Without proper alignment of IT, it is unlikely that any enterprise will achieve and sustain long-term success through the delivery of value to its stakeholders. The alignment of IT with the overall strategy of the enterprise does not happen by accident. It requires full and active involvement from many levels and activities within the enterprise, and active and focused management. It is a continuous effort and requires world-class skills and expertise, either in-house or outsourced. Risk taking, but with appropriate risk management is required along with strong and demonstrable governance.

2.2.3 Proper governance over the achievement of IT alignment requires leadership and commitment from the highest levels of the enterprise. This requires the proactive engagement of the chief executive officer and board. This requires the board to take responsibility for:

- Ensuring that IT strategy is aligned with business strategy
- Ensuring that IT delivers against the strategy

- Directing IT strategy to balance investments appropriately amongst systems that support the enterprise as it is, transform the enterprise or grow the enterprise

2.3 IT Strategic Plan

2.3.1 An organisation should establish an IT strategy committee at the board level. This committee should verify that IT governance, as part of corporate governance, is adequately addressed, advises on strategic direction and reviews major investments on behalf of the full board.

2.3.2 The IT strategy committee should create an IT strategic plan that defines, in co-operation with the relevant stakeholders, how IT will contribute to the enterprise's strategic objectives (goals) and related costs and risks. It includes how IT will support IT-enabled investment programmes and operational service delivery. The plan defines how the objectives will be met and measured and receives formal sign-off from the stakeholders. The IT strategic plan should cover investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements.

2.3.3 The strategic plan should be sufficiently detailed to allow the definition of tactical IT plans. A portfolio of tactical IT plans that are derived from the IT strategic plan should be created. These tactical plans describe required IS initiatives, resource requirements, and how the use of resources and achievement of benefits will be monitored and managed. The tactical plans should be sufficiently detailed to allow for the definition of project plans. The set tactical IS plans and initiatives should be actively managed through analysis of project and service portfolios. This ordinarily encompasses balancing requirements and resources on a regular basis, comparing them to achievement of strategic and tactical goals and the expected benefits, and taking appropriate action on deviations.

2.4 IT Steering Committee

2.4.1 An IT steering committee (or equivalent) composed of executive, business and IT management should be established to:

- Determine prioritisation of IT-enabled investment programmes in line with the enterprise's business strategy and priorities
- Track status of projects and resolve resource conflicts
- Monitor service levels and service improvements

2.4.2 The IT steering committee in its strategy implementation oversight role should have amongst its members at least one board member (sitting as the chair) supported by heads of operational and support departments, the chief information officer (CIO) and chief technical officer (or equivalent) together with other key contributors including legal, audit, finance, etc. Its discussions will be at a greater level of detail than would be expected of the IT strategy committee, and it will be expected to provide a great deal of input to the strategy committee's higher-level deliberations, for example, including recommendations on:

- The annual level of IT spending
- Alignment of the enterprise's IT architecture with business goals
- Portfolio management, including approval of projects plans for significant IT-related business investments
- Monitoring project plans and verifying that internal and external changes are appropriately factored into the updated plans
- The acquisition and divestment of IT-related resources
- Monitoring conflicts for IT resources based upon clearly articulated business priorities
- Communicating strategic goals to project teams through its representation of the operating and support departments
- Formulating plans for, and overseeing the results from, the IT dashboard, IT balanced scorecard or other key metrics
- Communicating the value of IT to all stakeholders. This may be done through articles on the corporate intranet or staff publications and, more importantly, to stakeholders and external analysts through the corporate web site or stakeholder communications.

2.5 Organisational Placement of the IT Function and Supporting Functions

2.5.1 The IT function should be placed in the overall organisational structure with a business model contingent on the importance of IT within the enterprise. Specifically, its criticality to business

strategy and the level of operational dependence on IT should be considered. The reporting line of the CIO should be commensurate with the importance and potential benefits of IT within the enterprise.

2.6 IT Organisational Structure

- 2.6.1** An internal and external IT organisational structure should be established that reflects business needs. In addition, a process should be put in place for periodically reviewing the IT organisational structure to adjust staffing requirements and sourcing strategies to meet expected business objectives and changing circumstances.
- 2.6.2** An IT organisation should be defined taking into consideration requirements for staff, skills, functions, accountability, authority, roles and responsibilities, and supervision. This organisation should be embedded into an IT process framework that verifies transparency and control as well as the involvement of senior executives and business management.
- 2.6.3** An IT strategy committee should verify board oversight of IT and one or more steering committees, in which business and IT participate, should determine prioritisation of IT resources in line with business needs. Processes, administrative policies and procedures need to be in place for all functions, with specific attention to control, quality assurance, risk management, information security, data and systems ownership, and segregation of duties. To verify timely support of business requirements, IT should be involved in relevant decision processes.
- 2.6.4** An IT process framework should be put in place to execute the IT strategic plan. This framework should include an IT process structure and relationships (e.g., to manage process gaps and overlaps), ownership, maturity, performance measurement, improvement, compliance, quality targets and plans to achieve them. It should provide integration amongst the processes that are specific to IT, enterprise portfolio management, business processes and business change processes. The IT process framework should be integrated in a quality management system and the internal control framework.

2.7 Roles and Responsibilities

- 2.7.1** Roles and responsibilities for all personnel in the organisation in relation to IS should be defined and communicated to allow sufficient authority to exercise the role and responsibility assigned to them. Role descriptions should be created and updated regularly. These descriptions should delineate both authority and responsibility, include definitions of skills and experience needed in the relevant positions, and are suitable for use in performance evaluation. Role descriptions should contain the responsibility for internal control.

2.8 Responsibility for IT Quality Assurance

- 2.8.1** Responsibility for the performance of the quality assurance function should be assigned, and the quality assurance group should be provided with appropriate quality assurance systems, controls and communications expertise. The organisational placement and the responsibilities and size of the quality assurance group should satisfy the requirements of the organisation.

2.9 Process Outsourcing

- 2.9.1** In most enterprises, the bulk of IT spending is devoted to operations and user support. Although in-house IT departments can provide these services, top executives are increasingly aware that service providers, both local and offshore, offer value and often a more disciplined approach to customer service.
- 2.9.2** With the increasing strategic importance of IT, the expectations of top executives in relation to IT have increased. Due to this situation, new and creative uses of outsourcing, which keep a balance with the internal organisation, have arisen. In many cases, the internal IT organisation is committed to delivering everyday services, such as user support, data centre operations and applications development, whilst contributing to strategy or leading innovation is left to external consultants (that can be seen as specialised and flexible). These tendencies may sometimes be supported by top executives due to increasing work supporting regulation. Because of the time it takes to change IT systems, the proportion of deficiencies in compliance attributed to the IT organisation will increase, exacerbating these tendencies, focusing internal resources even more to resolve these issues. Top executives recognise the need for advice about the strategic use of IT, and if they cannot get it from the IT organisation, they will go elsewhere. The use of third-party suppliers and consultants to give advice may risk a lack of objectivity, as they may recommend their own products and services for

both strategic and routine activities. If the IT organisation cannot deliver strategic advice, it may lose the opportunity even to deliver routine services. Process outsourcing could also be the result of a management decision to focus on its core activities and because it is more cost-effective to outsource the IT process vs. using in-house expertise.

2.10 IT Infrastructure and Computer Operations

- 2.10.1** Complete and accurate processing of data requires effective management of data processing and maintenance of hardware. This process includes defining operations' policies and procedures for effective management of scheduled processing, protection of sensitive output, monitoring infrastructure and preventive maintenance of hardware. Effective operations management helps maintain data integrity and reduces business delays and IT operating costs.
- 2.10.2** Protection for computer equipment and personnel requires well-designed and well-managed physical facilities. The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities, and designing effective processes for monitoring environmental factors and managing physical access. Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel. A good preventive maintenance schedule also helps ensure the normal running of equipment.
- 2.10.3** Verifying the integrity of hardware and software configurations requires establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimises production issues and resolves issues faster.
- 2.10.4** Timely and effective response to IT user queries and problems requires a well-designed and well-executed service desk and incident management process. This process includes setting up a service desk function with registration, incident escalation, trend and root cause analysis, and resolution. The business benefits include increased productivity through quick resolution of user queries. In addition, the business can address root causes (such as poor user training) through effective reporting.
- 2.10.5** The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, offsite backup storage and periodic continuity plan training. An effective continuous service process minimises the probability and effect of a major IT service interruption on key business functions and processes.
- 2.10.6** The need to manage performance and capacity of IS resources requires a process to periodically review current performance and capacity of IS resources. This process includes forecasting future needs based on workload, storage and contingency requirements. This process provides assurance that information resources supporting business requirements are continually available.
- 2.10.7** Effective communication between IS management and business customers regarding services required is enabled by a documented definition and agreement of IS services and service levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels. This process enables alignment between IS services and the related business requirements.

2.11 Operations Procedures and Tasks

- 2.11.1** Standard procedures for IT operations should be defined, implemented and maintained and the operations staff should be familiar with all tasks assigned to them. Operational procedures should cover shift handover (i.e., formal handover of activity, status updates, operational problems, escalation procedures, reports on current responsibilities) to verify continuous operations. Also, procedures to monitor the IT infrastructure and related events should be defined.

2.12 Application Development

- 2.12.1** Application systems could be acquired/developed through various modes, including:
- Custom development using internal resources
 - Custom development using fully or partly outsourced resources located onsite or offsite (locally or at an offshore location)
 - Vendor software packages implemented as-is with no customisation
 - Vendor software packages customised to meet the specific requirements

At times, large complex applications (which may include enterprise resource planning systems) may involve a combination of the above.

2.13 Contract Adherence of the IT Function Utilising an Outsourcing Arrangement

2.13.1 A large number of IT services from IT help desk to IT operations can be outsourced to third-party providers. The need to assure that services provided by third parties meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimises business risk associated with non-performing suppliers.

2.14 Procedures Regarding Third Parties

2.14.1 All third-party supplier services should be identified and categorised according to supplier type, significance and criticality. Formal documentation of technical and organisational relationships covering the roles and responsibilities, goals, and expected deliverables should include credentials of representatives of these suppliers. The third-party relationship management process for each supplier should be formalised. The relationship owners must liaise on customer issues and verify the quality of the relationship based on trust and transparency, for example, through service level agreements (SLAs). When a new third-party supplier service is being entered into, the service provider's ability to enhance and adapt its services to reflect business changes should be considered.

2.14.2 A process should be established to monitor service delivery to verify that the supplier is meeting current business requirements and is continuing to adhere to the contract agreements and SLAs, and that performance is competitive with alternative suppliers and market conditions.

2.15 Responsibility for Risk, Security and Compliance

2.15.1 Ownership and responsibility for IT-related risks should be embedded within the business at an appropriate senior level. Roles for managing critical IT risks including the specific responsibility for information security, physical security and compliance should be defined and assigned. Risk and security management responsibilities should be established at the enterprise level to deal with organisationwide issues. Additional security management responsibilities may need to be assigned at a system-specific level to deal with related security issues. Direction or guidelines should be obtained from (via consultation with) senior management on the appetite for IT risk and approval of any residual IT risks.

2.16 Personnel Recruitment and Retention

2.16.1 Staffing requirements should be evaluated on a regular basis or upon major changes to the business, operational or IT environments to verify that the IT function has a sufficient number of competent IT staff. Staffing should take into consideration co-location of business/IT staff cross-functional training, job rotation and outsourcing opportunities.

2.16.2 Key IT personnel should be defined and identified, and overreliance on them should be minimised. A plan for contacting key personnel in case of emergency should be established. Also, policies and procedures should be defined and implemented for controlling the activities of consultants and other contract personnel by the IT function to assure the protection of the organisation's information assets and meet agreed contractual requirements. Key performance indicators should be included to help verify that staff is performing to expectations.

3. AUDIT PROCESS

3.1 Planning

3.1.1 An audit programme should be developed based on the organisation's risk assessment and risk management strategy, including the scope, objectives and timing of the audit. Reporting arrangements should be clearly documented in the audit programme. Consideration should be given to the nature and size of the organisation and its stakeholders. The IS auditor should gain an understanding of the organisation's mission and business objectives, the types of technical infrastructure, and business critical data.

3.1.2 Risk assessment methodologies should be used to define the scope of the review, focusing on high-risk areas.

- 3.1.3** Any previous audit reports should be reviewed, and the level of resolution should be assessed on each issue according to the management action plan.
- 3.1.4** The IS auditor should obtain information on the IT organisation including:
- The roles and responsibilities of key staff, including the information managers, owners and supervisors
 - Senior management steering roles and responsibilities
 - Organisational objectives and long- and short-range plans
 - Setting the enterprise strategic directions
 - IT objectives and long- and short-range plans
 - Status reports and minutes of planning/steering committee meetings
 - Information architecture model
 - Policies and procedures relating to the IT organisation and relationships
 - Position descriptions, training and development records
 - Contracts with third-party service providers
 - Determining whether the enterprise has developed the skills and IT infrastructure required to meet the strategic goals set for the enterprise
- 3.1.5** The IS auditor should identify and obtain a general understanding of the processes that enable the IT organisation to perform the functions listed in section 4.1.1, including the communication channels used to set goals and objectives to lower levels (top-down) and the information used to monitor its compliance (bottom-up).
- 3.1.6** The IS auditor should obtain information on the organisation's IS strategy (whether documented or not), including:
- Long- and short-range plans to fulfil the organisation's mission and goals
 - Long- and short-range strategy and plans for IT and systems to support those plans
 - An approach to setting IT strategy, developing plans and monitoring progress against those plans
 - An approach to change control of IT strategy and plans
 - An IT mission statement and agreed goals and objectives for IT activities
 - Assessments of existing IT activities and systems

3.2 IS Audit Objectives

- 3.2.1** The objectives of an audit of the IT organisation may be affected by the intended audience's needs and the level of dissemination intended. The IS auditor should consider the following options in establishing the overall objectives of the audit:
- Reporting on the IT organisation and/or its effectiveness
 - Whether IT initiatives support the organisation mission and goals
 - Evaluation of alternate strategies for applications, technology and the organisation
- 3.2.2** The detailed objectives for an IS audit of the IT organisation ordinarily depends upon the framework of internal control exercised by top-level management. In the absence of any established framework, the COBIT framework should be used as a minimum basis for setting the detailed objectives.

3.3 Scope of the Audit

- 3.3.1** The IS auditor should include in the scope of the audit the relevant processes for planning and organising IT activity and the processes for monitoring that activity.
- 3.3.2** The scope of the audit should include control systems for the use and protection of the full range of IT resources defined in the COBIT framework. These include:
- Data
 - Application systems
 - Technology
 - Facilities
 - People
 - IT governance

3.4 Staffing

- 3.4.1** The IS auditor should provide reasonable assurance that the staff used to perform this review

includes persons of appropriate seniority and competence.

4. PERFORMANCE OF AUDIT WORK

4.1 Review of the IT Organisation and the Strategic Planning Process

4.1.1 In reviewing the IT organisation and relationships, the IS auditor should consider whether the IT organisation has the right mix of staff and skills, with roles and responsibilities defined and communicated and aligned with business. The IS auditor may include in the review whether:

- Policy statements and communications from senior management verify the independence and authority of the IT function
- Membership and functions of the IT planning/steering committee have been defined and responsibilities identified
- The IT planning/steering committee charter aligns the committee's goals with the organisation's objectives and long- and short-range plans and the IT objectives and long- and short-range plans
- The CIO reporting line is commensurate with the importance of the function in relation with the business of the enterprise and follows the trends of the enterprise industry and its market
- Policies address the need for evaluation and modification of organisational structure to meet changing objectives and circumstances
- Senior management verifies that roles and responsibilities are carried out
- Policies exist outlining roles and responsibilities for all personnel within the organisation with respect to information systems, internal control and security
- A quality assurance function and policies exists for the IT organisation
- Policies and procedures exist covering data and system ownership for all major data sources and systems
- Policies and procedures exist describing supervisory practices to verify that roles and responsibilities are appropriately exercised and all personnel have sufficient authority and resources to perform their roles and responsibilities
- Segregation of duties exist between systems development and maintenance, systems development and operations, systems development/maintenance and information security, operations and data control, operations and users, and operations and information security
- IT staffing and competence is maintained to verify its ability to provide effective technology solutions
- Appropriate roles and responsibilities exist for key processes, including system development life cycle activities, information security, acquisition and capacity planning
- Appropriate and effective key performance indicators and/or critical success factors are used in measuring results of the IT function in achieving organisational objectives
- IT policies and procedures exist to control the activities of consultants and other contract personnel, and thereby verify the protection of the organisation's assets
- Procedures are applicable to contracted IT services for adequacy and consistency with organisation acquisition policies
- Processes exist to coordinate, communicate and document interests both inside and outside the IT function
- Policies and procedures are in place to guarantee the delivery of services by the IT function is cost justified and in line with industry costs
- Organisational hiring and termination procedures including background checks

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

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

4.1.3 In reviewing the processes used to administer the current systems portfolio, the IS auditor should consider the coverage of organisational strategic and support areas by the current systems. The IS

auditor may include in the review whether:

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

5. REPORTING

5.1 Report Generation and Follow-up

- 5.1.1** The draft audit report should be generated and discussed with relevant personnel. Only those issues supported by clear audit evidence should be included. Recommendations developed for remediation should be discussed with appropriate personnel representing management.
- 5.1.2** The report should be finalised following ISACA guidelines and presented to management with recommendations to resolve/improve issues and follow-up options.
- 5.1.3** Follow-up activities, action plans, responsibilities, target dates, resources and priorities given by senior management should be agreed upon.

6. EFFECTIVE DATE

- 6.1** This guideline is effective for all IS audits beginning 1 May 2008.

References

IT Governance Institute, *IT Alignment: Who's in Charge?*, USA, 2005

2007-2008 ISACA Standards Board

Chair, Ravi Muthukrishnan, CISA, CISM, FCA, ISCA	Ikanos Communications, India
Brad David Chin, CISA, CPA	Google Inc., USA
Sergio Fleginsky, CISA	AKZO Nobel, Uruguay
Maria Gonzalez, CISA, CISM	Department of Defence, Spain
John Ho Chi, CISA, CISM, CBCP, CFE	Ernst & Young, Singapore
Andrew MacLeod, CISA, CIA, FCPA, MACS, PCP	Brisbane City Council, Australia
John G. Ott, CISA, CPA	AmerisourceBergen, USA
Jason Thompson, CISA, CIA	KPMG, USA
Meera Venkatesh, CISA, CISM, ACS, CISSP, CWA	Microsoft Corp., USA

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