

G40 REVIEW OF SECURITY MANAGEMENT PRACTICES

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 enterprises. It emphasises regulatory compliance, helps organisations increase the value attained from IT, enables alignment and simplifies implementation of the CobIT framework's concepts. CobIT is intended for use by business and IT management as well as IS auditors; therefore, its usage enables the understanding of business objectives and communication of good practices and recommendations to be made around a commonly understood and well-respected framework. CobIT is available for download on the ISACA web site, www.isaca.org/cobit. As defined in the CobIT framework, each of the following related products and/or elements is organised by IT management process:

- Control objectives—Generic statements of minimum good control in relation to IT processes
- Management guidelines—Guidance on how to assess and improve IT process performance, using maturity models; Responsible, Accountable, Consulted and/or Informed (RACI) charts; goals; and metrics. They provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:
 - Performance measurement
 - IT control profiling
 - Awareness
 - Benchmarking
- *CobIT[®] Control Practices*—Risk and value statements and 'how to implement' guidance for the control objectives
- *IT Assurance Guide*—Guidance for each control area on how to obtain an understanding, evaluate each control, assess compliance and substantiate the risk of controls not being met

A **glossary** of terms can be found on the ISACA web site at www.isaca.org/glossary. The words audit and review are used interchangeably in the IS Auditing Standards, Guidelines and Procedures.

Disclaimer: ISACA has designed this guidance as the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics. ISACA makes no claim that use of this product will assure a successful outcome. The publication should not be considered inclusive of all proper procedures and tests or exclusive of other procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific procedure or test, the controls professional should apply his/her own professional judgement to the specific control circumstances presented by the particular systems or IT environment.

The ISACA Standards Board is committed to wide consultation in the preparation of the IS Auditing Standards, Guidelines and Procedures. Prior to issuing any documents, the Standards Board issues exposure drafts internationally for general public comment. The Standards Board also seeks out those with a special expertise or interest in the topic under consideration for consultation where necessary. The Standards Board has an ongoing development programme and welcomes the input of ISACA members and other interested parties to identify emerging issues requiring new standards. Any suggestions should be e-mailed (standards@isaca.org), faxed (+1.847. 253.1443) or mailed (address at the end of document) to ISACA International Headquarters, for the attention of the director of research, standards and academic relations. This material was issued on 15 October 2008.

1. BACKGROUND

1.1 Linkage to Standards

- 1.1.1 Standard S1 Audit Charter states, 'The purpose, responsibility, authority and accountability of the information systems audit function or information systems audit assignments should be appropriately documented in an audit charter or engagement letter'.
- 1.1.2 Standard S3 Professional Ethics and Standards states, 'The IS auditor should adhere to the ISACA Code of Professional Ethics'.

1.2 Linkage to COBIT

- 1.2.1 Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's control objectives and associated management practices. To review security management practices by IS auditor, 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.
- 1.2.2 The primary specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance are:
 - PO2 *Define the information architecture*
 - PO9 *Assess and manage IT risks*
 - DS5 *Ensure systems security*
 - DS7 *Educate and train users*
 - ME2 *Monitor and evaluate internal control*
 - ME3 *Ensure compliance with external requirements*
 - ME4 *Provide IT governance*
- 1.2.3 The secondary specific objectives or processes of COBIT that should be considered when reviewing the area addressed by this guidance are:
 - PO6 *Communicate management aims and direction*
 - PO7 *Manage IT human resources*
 - DS1 *Define and manage service levels*
 - DS2 *Manage third-party services*
 - DS9 *Manage the configuration*
 - DS10 *Manage problems*
 - DS12 *Manage the physical environment*
 - AI1 *Identify automated solutions*
 - AI2 *Acquire and maintain application software*
 - AI3 *Acquire and maintain technology infrastructure*
 - AI6 *Manage changes*
 - ME1 *Monitor and evaluate IT performance*
- 1.2.4 The information criteria most relevant to responsibility, authority and accountability are:
 - Primary: Effectiveness, efficiency and confidentiality
 - Secondary: Availability, integrity and reliability

1.3 Purpose of the Guideline

- 1.3.1 Information is a most valuable asset in business. Information is increasingly vital for competitive success, and essential for economic survival. In the actual interconnected world, organisations should protect their information assets from unauthorised use, not only to protect its investments but also to protect information assets from the risks generated by the misuse of resources, intentionally or unintentionally. Such protection of information assets can be achieved only by implementing formal, detailed information security management framework in an enterprise. This guideline provides detailed guidance to assess and conclude on the design and operating effectiveness of the information security management practices implemented by management.

1.4 Guideline Application

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

1.5 Definitions

- 1.5.1 Information is an asset that has value to any organisation that needs to be protected suitably. Information can be in any form, including paper, stored electronically in any electronic media, or transmitted by means suitable to the media.
- 1.5.2 Information security is a set of measures that are in place ensure that only authorised users (confidentiality) have access to accurate and complete information (integrity) when required (availability).
- 1.5.3 An information security management system (ISMS) is an overall management system, based on a business-risk approach to establish, implement, operate, monitor, review, maintain and improve information security. The organisational structure to implement security management practices includes policies, planning activities, responsibilities, procedures, processes and resources.
- 1.5.4 ISO 27001 *Information Security Management—Specification with Guidance for Use* is the replacement for BS7799-2. It is intended to provide the foundation for third-party audit and is harmonised with other management standards, such as ISO/IEC 9001:2000 and 14001:2004.

2. SECURITY MANAGEMENT PRACTICES IMPLEMENTATION

2.1 Planned Approach

- 2.1.1 Enterprise's that consider adoption of an ISMS should follow a processed approach for the implementation of the security management practices. Such implementation of security management practices should include all activities such as establishing, implementing and operating, monitoring and reviewing and maintaining and improving the ISMS. The organisation may choose to adopt the Plan, Do, Check and Act (PDCA) model to implement the framework.

2.2 Establish Security Management Practices

- 2.2.1 The IS auditor should verify whether the enterprise has documented and implemented the information security policies and procedures relevant to manage the risks identified through a proper risk assessment process and improve information security performance, ensure compliance with organisation policies, and achieve its objectives.

2.3 Implement and Operate Security Management Practices

- 2.3.1 The IS auditor should verify whether the enterprise has identified appropriate controls, responsibilities and prioritisation of information security risks and has implemented all controls needed to address the risks and related objectives to protect information security. In addition, the IS auditor should verify whether the personnel have appropriate training and awareness programmes related to information security to implement and operate the security management practices. Also, the IS auditor should verify whether the enterprise has appropriate processes in place to operate the controls as intended including measures to detect and respond to security incidents.

2.4 Monitor and Review Security Management Practices

- 2.4.1 The IS auditor should verify whether the organisation has procedures to monitor the effectiveness and efficiency of the security management practices.

2.5 Maintain and Improve Security management Practices

- 2.5.1 The IS auditor should verify whether the enterprise has a process to ensure that management performs a review of the ISMS on a periodic basis to confirm its continuing applicability, adequacy, effectiveness and efficiency. Also, the IS auditor should verify whether the enterprise has a process to act upon the results and recommendations resulting from such periodic review and a continuous process to improve the effectiveness of ISMS.

3. REVIEW OF SECURITY MANAGEMENT PRACTICES

3.1 Security Management Practices

- 3.1.1 The IS auditor should verify whether the enterprise has a set of security management practices including policies, practices, procedures, security organisation, and security roles and responsibilities. The IS auditor should verify if the security management practices were established by the enterprise after identifying the security requirements through the risk assessment process and also with an understanding toward legal, statutory and regulatory requirements related to information protection and to meeting the information processing requirements needed for an enterprise.

3.2 Information Security Organisational Structure

- 3.2.1** The IS auditor should verify if the enterprise has set a clear security policy direction as a commitment to implementing security management practices by publishing and communicating a detailed information security policy that is approved by management.
- 3.2.2** The IS auditor should verify if the Information security policy includes, at minimum, the following:
- Definition of information security, objectives and scope
 - Management's intent, in the form of a security policy statement, to implement security management practices
 - A list of security policies, principles, standards and compliance requirements
 - Information security management structure and related responsibilities
 - Supporting documents in implementing security management practices such as more detailed policies and procedures
- 3.2.3** The IS auditor should verify whether the enterprise has documented and implemented ongoing training and awareness programmes to communicate the information security policy to the entire enterprise.
- 3.2.4** The IS auditor should verify whether the enterprise has documented and implemented a process to periodically evaluate the information security policy to ensure the effectiveness and applicability of the security policies.
- 3.2.5** The IS auditor should verify whether the enterprise has defined the responsibilities for implementation of security management practices, continuous evaluation, monitoring and improvement and to facilitate resourcing and implementing the security controls to achieve information security.
- 3.2.6** The IS auditor should verify whether the enterprise has a process for reviewing new information processing facilities prior to approving the implementation.

3.3 Third-party Access to Information and Outsourcing

- 3.3.1** The IS auditor should verify whether the enterprise has implemented appropriate access controls processes to prevent unauthorised access or misuse of information by third parties. Such controls should have been implemented prior to providing access to third parties.
- 3.3.2** The IS auditor should verify whether the enterprise has incorporated all control requirements, such as:
- Confidentiality and integrity
 - Acceptable use
 - Legal requirements, if any
 - Arrangements for ensuring awareness of security responsibilities by all parties
 - Controls to ensure integrity and confidentiality of the enterprise's business assets
 - Physical and logical security requirements
 - Outsourcing services availability
 - Background screening of employees
 - Auditing outsourced facilities, the right for which should be included within the contract with any third parties

3.4 Asset Classification and Control

- 3.4.1** IS auditor should verify whether the enterprise has identified owners and assigned accountability for all information assets, for protection of the assets. Such an asset ownership and accountability process should include an inventory of assets to help decide several protection measures, including insurance and financial management, apart from defining protection mechanisms. Also, the IS auditor should verify if the assets in the enterprise include the following categories:
- Information assets (e.g., databases, data files, the business continuity plan, network diagram and security architecture)
 - Software assets (e.g., application and system software, tools and utilities, and relevant licences)
 - Physical assets (e.g., computer and communications equipment and electronic media)
 - Services (e.g., general utilities, heating and lighting)
- 3.4.2** The IS auditor should verify whether the enterprise has classified all information assets based on their sensitivity and criticality to the business; value of information, including legal requirements to protect and retain; and the impact on the business upon losing the information or its integrity or non-availability.
- 3.4.3** The IS auditor should verify whether the enterprise has labelled all classified information assets and

defined appropriate handling procedures including procedures to copy, store, transmit by various means and destroy. Such labelling can be by physical or electronic. Also, the IS auditor should verify whether appropriate monitoring procedures have been introduced to ensure that information classification, labelling and handling processes are appropriately implemented.

3.5 Personnel Security

3.5.1 The IS auditor should verify whether the enterprise has:

- Addressed the security responsibilities at the recruitment stage, including defining security job responsibilities within the job descriptions
- Introduced practices to perform security screening of all employees, especially for sensitive jobs
- Required confidentiality or non-disclosure agreements to be signed by employees or any third party
- Specified the responsibility for information security under the terms and conditions of employment

3.5.2 The IS auditor should verify whether the enterprise has an appropriate training programme on security policies and procedures to provide training to all employees and non-employees, as appropriate. The IS auditor should also verify, at least on a sample basis, with select users within the organisation, whether the users are aware of all security procedures and know how to adhere to these procedures to minimise the possibility of security risks.

3.5.3 The IS auditor should verify whether the enterprise has:

- Documented and implemented reporting and incident response procedures
- Communicated and trained the entire enterprise regarding the security reporting and incident response procedures
- Required users to report security weaknesses identified in information systems to take appropriate remediation action
- Documented and implemented procedures for reporting software malfunctions
- Introduced appropriate incident-reporting functionalities that would enable management to identify recurring incidents and enhance security control requirements accordingly
- Documented and implemented a formal disciplinary process for employees who have committed a security breach

3.5.4 The IS auditor should verify whether the enterprise has proper procedures in place to collect evidence. Such procedures should include follow-up actions against a person or enterprise after an information security incident involves legal action (either civil or criminal) in order to collect, retain and present (as needed) appropriate evidence, as laid down in the relevant jurisdiction(s).

3.5.5 The IS auditor should verify whether the enterprise has a formal process for termination of employment in case of actions to be taken due to security breach. Such formal processes should include:

- Circumstances in which termination of employment would occur and responsibility for deciding terminations
- Requirement that all employees, contractors and third parties return all of the enterprise's assets in their possession upon termination of their employment, contract or agreement
- Removal (or adjusted upon change) of access rights of all employees, contractors and third parties to information and information processing facilities upon termination of their employment, contract or agreement

3.6 Physical Security

3.6.1 The IS auditor should verify whether the enterprise has introduced appropriate security controls to secure the office buildings from physical security threats. Such controls include:

- Security perimeters to protect areas that contain information and information processing facilities
- Appropriate entry procedures to secure areas to allow authorised personnel only
- Physical security for offices, rooms and facilities
- Physical protection against damage from nature or man-made disasters
- Physical protection for working in secure areas
- Physical access controls to network closets (including telecom closets)
- Segregation of physical locations and access areas such as loading and unloading sections where potential for unauthorised access exists to information processing facilities

3.6.2 The IS auditor should verify whether the enterprise has adequately implemented physical security controls to prevent loss, damage or compromise of assets and interruption to business activities.

Such controls include:

- Protection of all equipment, including telecom and network equipment, to reduce risks from environmental threats and hazards and opportunities for unauthorised access
- Proper maintenance of supporting utilities to ensure that disruptions are not caused to the equipment by their failures
- Protection of power and telecommunications cabling carrying data or supporting information services from interception or damage
- Proper maintenance of equipment to ensure its continued availability and integrity
- Proper protection measures for offsite equipment, taking into account the different risks of working outside the enterprise's premises
- Controls to ensure that any sensitive data and licensed software within any equipment or storage media has been removed or securely overwritten prior to disposal
- Prior to disposal of access devices, such as access cards or tokens, remove sensitive information
- Proper authorisation requirements for equipment, information or software prior to taking them offsite

3.7 Communications and Operations Management

3.7.1 The IS auditor should verify the following while reviewing the operational procedures of the enterprise:

- Operating procedures should be documented, maintained and made available to all users who need them.
- Changes to information processing facilities and systems should be controlled.
- Duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the enterprise's assets.
- Development, test and operational facilities should be separated to reduce the risk of unauthorised access or changes to the operational system.
- Security controls, service definitions and delivery levels included in the third-party service delivery agreement should be implemented, operated and maintained by the third party. The services, reports and records provided by the third party should be regularly monitored, reviewed and audited.

3.7.2 The IS auditor should verify whether the enterprise has documented and implemented:

- Procedures to monitor, tune and project the future capacity requirements for all information resources to ensure the required system performance
- Acceptance criteria for new information systems, upgrades and new versions, including performing suitable tests of the system(s) during development and prior to acceptance

3.7.3 The IS auditor should verify whether the enterprise has the following in place to protect against malicious software:

- Controls for detection, prevention and recovery to protect against malicious code and appropriate user-awareness procedures. Such protection measures could include installation of antivirus software and software that could detect and remove spyware and adware
- Controls to ensure authorisation of use of mobile code, appropriate configuration to ensure that the authorised mobile code operates according to a clearly defined security policy, and controls to prevent unauthorised mobile code from executing

3.7.4 The IS auditor should verify whether the enterprise has documented and implemented routine procedures to execute the agreed-upon backup strategy: test for recovery as needed for timely restoration, logging backup failures and remediation; monitor the equipment environment as needed. Such procedures should include backing up of information, operator logs and fault logging.

3.7.5 The IS auditor should verify whether the enterprise has established appropriate controls to manage and protect networks, in order to be protected from threats and to maintain security for the systems and applications using the network, including information in transit. The IS auditor should verify whether the network services agreement, whether the services are in-house or outsourced, should include security features, service levels and management requirements of all network services. Protection measures could include installation of firewalls and scanning of the networks, including penetration testing as needed.

3.7.6 The IS auditor should verify whether the enterprise has established the following formal procedures for:

- Disposal of media securely and safely when no longer required

- Handling and storage of information to protect this information from unauthorised disclosure or misuse
- Protection of system documentation against unauthorised access
- 3.7.7** The IS auditor should verify whether the enterprise has established the following:
 - Formal exchange policies, procedures and controls to protect the exchange of information through the use of all types of communication facilities
 - Agreements for the exchange of information and software between the organisation and external parties
 - Protection of media containing information against unauthorised access, misuse or corruption during transportation beyond the enterprise's physical boundaries
- 3.7.8** The IS auditor should verify whether the enterprise has established the following:
 - Policies and procedures to protect information associated with the interconnection of business information systems
 - Appropriate protection measures for information involved in electronic messaging
 - Appropriate protection measures to protect information involved in electronic commerce passing over public networks, from fraudulent activity, contract dispute, and unauthorised disclosure and modification
 - Protection to ensure that online transactions are transmitted completely and that misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay does not occur
 - Protection to ensure the integrity of information available on a public system

3.8 Access Controls to Information Assets

- 3.8.1** The IS auditor should verify whether the enterprise has a documented access-control policy based on business and security requirements for access.
- 3.8.2** The IS auditor should verify whether the enterprise has documented and implemented a formal user registration and de-registration procedure for granting and revoking access to all information systems and services. Such process should include: a) restricted and controlled allocation and use of privileges, b) review of users' access rights at regular intervals and c) timely revocation of access.
- 3.8.3** The IS auditor should verify whether the enterprise has documented and implemented controls to ensure that:
 - Information users are required to follow good security practices in the selection and use of passwords
 - Those with administrator/privileged access have stronger passwords and change their passwords more regularly (while stronger passwords are best practice for all users)
 - Information users have ensured that unattended equipment has appropriate protection
 - Information users have adopted a clear-desk policy for papers and removable storage media and a clear-screen policy for information-processing facilities
- 3.8.4** The IS auditor should verify whether the enterprise has documented and implemented the following related to network access control:
 - Appropriate authentication and authorisation methods to control access by remote users
 - Controlled physical and logical access to diagnostic and configuration ports
 - Segregated groups of information services, users and information systems on networks. This should include appropriate restrictions for shared networks, especially those extending across the enterprise's boundaries, to ensure that the capability of users to connect to the network is in line with the access-control policy and requirements of the business applications.
 - Routing controls to ensure that computer connections and information flows do not breach the access control policy of the business applications
- 3.8.5** The IS auditor should verify whether the enterprise has documented and implemented the following to protect access to the operating system:
 - Secure logon procedure for access to operating systems
 - Unique identifier (user ID) for all users within the enterprise for individual use only, and a suitable authentication technique to substantiate the claimed identity of a user
 - Interactive system for managing passwords and to ensure quality passwords
 - Controls to restrict access to utility programmes that might be capable of overriding system and application controls
 - Controls to shut down inactive sessions after a defined period of inactivity
 - Restrictions on connection times to provide additional security for high-risk applications

- 3.8.6** The IS auditor should verify whether the enterprise has documented and implemented the following to protect access to the applications:
- Access to information and application system functions by users and support personnel provided in accordance with the defined access-control policy
 - Dedicated (isolated) computing environment for protecting sensitive applications
- 3.8.7** The IS auditor should verify whether the enterprise has documented and implemented the following to monitor system access and use:
- A formal policy and appropriate security measures to protect against the risks of using mobile computing and communication facilities
 - Audit logs to record user activities, exceptions, and information security events and procedures to maintain the logs for an agreed-upon period to assist in future investigations and access control monitoring
 - Procedures to monitor use of information processing facilities and to review the results of the monitoring activities
 - Controls to protect logging facilities and log information against tampering and unauthorised access
 - Procedures to log system administrator and system operator activities and monitor the activities of the IT administrators on a regular basis
 - Procedures to log, analyse and act upon faults
 - Synchronisation of clocks of all relevant information processing systems within the enterprise or security domain to an agreed-upon accurate time source
- 3.8.8** The IS auditor should verify whether the enterprise has completed the following:
- A formal assessment of threats and vulnerabilities, from internal or external attacks, and their impact on the enterprise's network, information systems and applications
 - Implementation of an intrusion detection mechanism for timely identification of any intrusions within the enterprise's network
 - Adequate procedures to apply security patches and other patches required for the system without compromising the current security level of the information systems
 - Preventive, detective and corrective plans for any security incidents
- 3.9 Systems Development and Maintenance Documentation and Implementation**
- 3.9.1** The IS auditor should verify whether statements of business requirements for new information systems, or enhancements to existing information systems, specify the requirements for security controls, including:
- Access controls to application systems
 - Validation requirements for data inputs to applications to ensure that these data are correct and appropriate
 - Validation checks within applications to detect any corruption of information through processing errors or deliberate acts
 - Requirements for ensuring authenticity and protecting message integrity in applications
 - Validation of data output from an application validated to ensure that the processing of stored information is correct and appropriate to the circumstances
- 3.9.2** The IS auditor should verify whether the enterprise has documented and implemented a policy on the use of cryptographic controls for the protection of information. Such controls should include key management to support the enterprise's use of cryptographic techniques.
- 3.9.3** The IS auditor should verify whether the enterprise has established procedures to control the installation of software on operational systems and access to program source code.
- 3.9.4** The IS auditor should verify whether the enterprise has established formal change control procedures. Such procedures should include:
- Review and test of business critical applications when operating systems are changed to ensure that there is no adverse impact on organisational operations or security.
 - Limit and control modifications to software packages to necessary changes.
 - Monitor outsourced software development.
 - Input processes to obtain timely information about technical vulnerabilities of the information systems being used, including a process to evaluate the exposure to such vulnerabilities, and introduce appropriate measures to address risk.
- 3.9.5** The IS auditor should perform a post-implementation review of the system, after it has been developed and implemented, to assess if the system meets the business and control requirements.

The IS auditor in some cases, can also perform a pre-implementation review of the system, prior to the system implementation, to identify weaknesses or control improvements for timely remediation.

3.10 Business Continuity Management

3.10.1 The IS auditor should verify whether the enterprise has established the following:

- A managed process for business continuity throughout the organisation to address the information security requirements needed for the enterprise's business continuity
- A process to identify events that can cause interruptions to business processes, along with the probability and impact of such interruptions and their consequences for information security. This should include disaster incident response management and related procedures.
- Plans to maintain or restore operations and ensure availability of information, at the required level and in the required time scales, following interruption to, or failure of, critical business processes
- A single framework of business continuity plans to ensure that all plans are consistent, consistently address information security requirements, and identify priorities for testing and maintenance
- A test and regular update of all business continuity plans to ensure that they are up to date and effective. Where appropriate, the IS auditor can observe management's testing process of the business continuity plan.
- Plans to provide training/awareness specifically on responsibilities for those identified to be involved in the business continuity process within the enterprise

3.11 Compliance

3.11.1 The IS auditor should verify whether the enterprise has:

- Defined, documented, and kept up to date all relevant statutory, regulatory and contractual requirements and the enterprise's approach to meet these requirements for each information system and the enterprise as a whole.
- Implemented appropriate procedures to ensure compliance with legislative, regulatory and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products
- Protected important records from loss, destruction and falsification in accordance with statutory, regulatory, contractual and business requirements
- Implemented data protection and privacy controls as required in relevant legislation, regulations, and, if applicable, contractual clauses
- Implemented controls to deter users from using information processing facilities for unauthorised purposes
- Implemented controls to require that all software installed in the enterprise be either licensed or open source
- Implemented cryptographic controls in compliance with all relevant agreements, laws and regulations

3.11.2 The IS auditor should verify whether the enterprise has established a process to confirm that the:

- Managers have ensured that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards
- Information systems are regularly checked for compliance with security implementation standards

3.11.3 The IS auditor should verify whether the enterprise has established a process to ensure that the

- Audit requirements and activities involving checks on operational systems are planned and agreed-upon to minimise the risk of disruptions to business processes
- Access to information systems audit tools is protected to prevent any possible misuse or compromise

4. AUDIT PROCESS

4.1 Planning

4.1.1 The IS auditor should prepare an audit program for reviewing the security management practices of the enterprise based on the enterprise'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 enterprise and

its stakeholders. The IS auditor should gain an understanding of the enterprise's mission and business objectives, enterprise information assets, technology infrastructure, and security management practices.

- 4.1.2 An understanding of the organisational structure is needed, specifically of the roles and responsibilities of key staff responsible for creating, communicating and monitoring security management practices and their compliance within the company. Other key staff members include information managers, owners and supervisors.
- 4.1.3 A primary objective of the audit planning phase is to understand the security-related threats and risks that the enterprise faces to arrive at audit objectives and to define the scope of the review with an emphasis on high-risk areas.
- 4.1.4 Appropriate sampling techniques should be considered in the planning of the audit to quantify the results of testing, if applicable.
- 4.1.5 A previous audit report should be required and the level of resolution should be assessed on each issue according to the management action plan.

5. PERFORMANCE OF WORK

5.1 Audit Tasks

- 5.1.1 The IS auditor should perform a detailed and independent review of the security management practices and their implementation, to provide assurance that the enterprise security management objectives are appropriately achieved.
- 5.1.2 The IS auditor should review all aspects of the security management practices as outlined in this guideline to provide such assurance

6. REPORTING

6.1 Report Generation and Follow-up

- 6.1.1 The draft audit report should be generated and discussed with relevant personnel. Only include those issues supported by clear evidence
- 6.1.2 The report should be finalised following ISACA guidelines and presented to management or the governance board, if available and appropriate, with recommendations to resolve/improve issues and follow-up options. Specifically, for sensitive security deficiencies, distribution of the report should be restricted to the governance board or appropriate level of management
- 6.1.3 Follow-up activities, action plans, responsibilities, target dates, resources and priorities given by senior management and/or the governance board should be agreed upon.

7. EFFECTIVE DATE

- 7.1 This guideline is effective for all IS audits beginning on or after 1 December 2008.

2008-2009 ISACA Standards Board

Chair, Ravi Muthukrishnan, CISA, CISM, FCA, ISCA	Capco IT Services India Private Limited, India
Shawn Chaput, CISA, CISM, CISSP, PMP	IBM, Canada
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
Edward Pelcher, CISA	Office of the Auditor General, South Africa
Jason Thompson, CISA, CIA	KPMG LLP, 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