

G37 CONFIGURATION MANAGEMENT PROCESS

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 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.

As defined in the CobIT framework, each of the following is organised by IT management process. CobIT is intended for use by business and IT management, as well as IS auditors; therefore, its usage enables the understanding of business objectives, communication of best practices and recommendations to be made around a commonly understood and well-respected standard reference. CobIT and related products include:

- **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, metrics and critical success factors. They provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:
 - **Performance measurement**—How well is the IT function supporting business requirements? Management guidelines can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.
 - **IT control profiling**—What IT processes are important? What are the critical success factors for control?
 - **Awareness**—What are the risks of not achieving the objectives?
 - **Benchmarking**—What do others do? How can results be measured and compared? Management guidelines provide example goals and metrics enabling assessment of IT performance in business terms. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.
- **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.

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 document should not be considered inclusive of any 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 information technology 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 15 September 2007.

1. BACKGROUND

1.1 Linkage to Standards

1.1.1 Standard S6 Performance of Audit Work states, 'IS audit staff should be supervised to provide reasonable assurance that audit objectives are accomplished and applicable professional auditing standards are met. During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence'.

1.2 Linkage to COBIT

1.2.1 Control process A12 *Acquire and maintain application software*, which satisfies the business requirement for IT of aligning available applications in line with business requirements, and doing so in a timely manner and at a reasonable cost by focusing on ensuring that there is a timely and cost-effective development process, is achieved by:

- Translating business requirements into design specifications
- Adhering to development standards for all modifications
- Separating development, testing and operational activities

A12 is measured by:

- Number of production problems per application causing visible down time
- Percentage of users satisfied with functionality delivered'

1.2.2 Control process DS9 *Manage the configuration*, which satisfies the business requirement for IT of optimising the IT infrastructure, resources and capabilities, and accounting for IT assets by focusing on establishing and maintaining an accurate and complete repository of asset configuration attributes and baselines, and comparing against actual asset configuration, is achieved by:

- Establishing a central repository of all configuration items
- Identifying configuration items and maintaining them
- Reviewing integrity of configuration data

DS9 is measured by:

- Number of business compliance issues caused by improper configuration of assets
- Number of deviations identified between configuration repository and actual asset configurations
- Percent of licences purchased and not accounted for in repository'

1.2.3 Control objective DS 9.1 *Configuration repository and baseline* states, 'establish a supporting tool and a central repository to contain all relevant information on configuration items. Monitor and record all assets and changes to assets. Maintain a baseline of configuration items for every system and service as a checkpoint to which to return after changes.'

1.2.4 Control objective DS 9.2 *Identification and maintenance of configuration items* states, 'establish configuration procedures to support management and logging of all changes to the configuration repository. Integrate these procedures with change management and problem management procedures.'

1.2.5 Control objective DS 9.3 *Configuration integrity review* states, 'periodically review the configuration data to verify and confirm the integrity of the current and historical configuration Periodically review installed software against the policy for software usage to identify personal or unlicensed software or any software instances in excess of current license agreements. Report, act on and correct errors and deviations.'

1.3 COBIT Reference

1.3.1 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.

1.3.2 The process and control objectives to be selected and adapted may vary depending on the specific scope and terms of reference of the assignment. To meet the requirement, the processes in COBIT likely to be the selected and adapted are classified as follows.

1.3.3 Primary:

- PO9 *Assess and manage IT risks*
 - AI6 *Manage changes*
 - DS9 *Manage the configuration*
 - ME2 *Monitor and evaluate internal control*
- 1.3.4** Secondary:
- PO1 *Define a strategic IT plan*
 - PO3 *Determine technological direction*
 - PO6 *Communicate management aims and direction*
 - DS4 *Ensure continuous service*
- 1.3.5** The information criteria most relevant to configuration management are:
- Primary: Effectiveness
 - Secondary: Efficiency, availability, and reliability
- 1.3.6** The IT governance focus areas most relevant to configuration management are:
- Primary: Value delivery
 - Secondary: Risk management

1.4 Purpose of the Guideline

- 1.4.1** Managing the configuration means providing reasonable assurance that the integrity of hardware and software configurations that require 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.
- 1.4.2** Modern businesses are organised as a set of core processes. Almost every organisation in the world is faced with increasing pressure for effectiveness and efficiency (i.e., higher-quality requirements for products and services, increased revenue, cost reduction, new product development), a pressure for better, faster and cheaper enterprisewide system and network change control process that provides high-quality software for the business owners. However, changing various components, such as desktop software, networks, middleware, system software for operating system and database, that introduce significant risk should be managed.
- 1.4.3** This guideline is intended to aid the IS auditor in performing a review of the configuration management process. Primarily intended for IS auditors—internal as well as external auditors—this document can be used by other IS professionals with responsibilities for information systems availability, data integrity and information confidentiality.
- 1.4.4** This guideline describes configuration management from the perspective of:
- Process flow
 - Roles and responsibilities
 - Asset tracking and tools
 - Control and logging of changes
 - Communication requirements including release management
 - Metrics to be reported

1.5 Background and General Process Flow

- 1.5.1** The goals of the configuration management process are to:
- Manage and effectively control change to the enterprise IT systems, resources and networks whilst maintaining or improving system availability.
 - Increase accuracy of predications of effect and manage the risks that changes can cause.
 - Create and maintain a central repository of all configuration items and historical information of the effect from of changes to the baseline configuration (e.g., success or failure of specific types of changes especially in large-scale and complex environments)
 - Communicate the number and types of changes planned in the short and long term; thereby establishing a process that communicates the status and existence of changes to all affected parties.

- 1.5.2** Effective configuration management enables management to reduce the risk of requiring back-out due to inadequate preparation and/or incompatible changes affecting system availability and data processing integrity.

2. AUDIT CONSIDERATIONS

2.1 Typical Configuration Management Review Points

- 2.1.1** Depending upon the size and complexity of the organisation, the IS auditor should gather audit evidence of a configuration management control process. The IS auditor should obtain senior management expectations regarding configuration management. Typically, weak configuration management poses a significant threat to system availability and data integrity. Specifically, there is a high correlation between configuration changes to enterprise systems, resources and networks; critical system outages; poor data integrity; and/or lack of confidentiality of organisation information.
- 2.1.2** The IS auditor should understand the configuration management policy and procedures that outline communication requirements, including documentation requirements for changing software and hardware of individual component to the enterprise systems and networks.
- 2.1.3** The IS auditor should obtain a general understanding of all elements, including all software (such as business application software, middleware and database system software) and hardware interrelationships and integration, that comprise the enterprise systems and networks. For example, the hardware type, model number and serial number for uniqueness identification.
- 2.1.4** The IS auditor should obtain all hardware and software information (model and serial number) from the IT asset tracking system, or comparable information, that are verified as complete. If this is not available, a complete inventory may need to be taken.
- 2.1.5** The IS auditor should understand the relevance of each component and how they fit together including the interrelationships with all other components.
- 2.1.6** Review of the configuration management process typically includes:
- Verifying the establishment of a central repository for all configuration items
 - Identifying configuration items and maintaining configuration data
 - Determining whether the repository contains all necessary information about components, interrelationships and events
 - Determining whether the configuration data are aligned with vendor/service provider catalogues
 - Determining whether there is a complete integration of interrelated processes, and that the organisation uses and updates configuration data in an automated fashion
 - Providing reasonable assurance of the integrity of configuration data
 - Verifying the existence of formal change request to the system including complete change documentation
 - Determining whether a formalised method is consistently employed to identify and categorise changes into levels of risk to the enterprise systems, resources and networks
 - Determining audit evidence of risk assessments for requested changes as deemed necessary by the configuration management committee, or appropriate level of the management. Risk assessment should denote if the change is restricted to specific environments or networks, the potential number of business users affected and the criticality of the business information processing.
 - Verifying business and IT management formal approval of results of the risk assessment (i.e., changes to firewall rule settings)
 - Determining that there is controlled development or installation of vendor upgrade for the change in development (i.e., systems engineer's sandbox)
 - Testing resulting in a required unqualified sign-off of configuration changes in a test environment, which mirrors the production environment in infrastructure and business software, noted no effect on other elements of the enterprise systems, resources and networks
 - Scheduling of changes based on the co-ordination of other changes to minimise potential effect to the enterprise systems, resources and networks. This scheduling occurs through the release management subprocess that controls batching of the software program elevations including synchronising of changes that minimises the effect on the business.

- Determining that the elevation of the change into the production processing environment is made in a controlled manner (off hours) where there is additional testing of the change in the live production processing environment (i.e., upgrade of database system software is evaluated by executing critical, stored procedures and triggers with an evaluation of data integrity).
- Establishing a repository of all assets, configuration attributes and baselines. Verify that a baseline of configuration items is kept as a checkpoint to return to after changes.
- Verifying the baseline report provides essential hardware and software data for repair, service, warranty, upgrade and technical assessment of each individual component
- Reviewing actual asset configuration for compliance with baselines in the repository and establishing integrity of the configuration repository
- Determining whether rules are in place and enforced for preventing the installation and detecting unauthorised software.
- Determining whether there is a system to forecast repairs and upgrades and also provide scheduled upgrades and technology refreshment capabilities
- Providing reasonable assurance of a linkage between the change management process and configuration management, so that all aspects of changes are understood in the configuration review process

2.2 Roles and Responsibilities

- 2.2.1** The IS auditor should obtain a listing of roles and responsibilities that support configuration management. These roles and responsibilities should be embedded in the job descriptions of the members of IT management who are responsible for each IT component and the correlated scope. If this is not present, the IS auditor should investigate responsibility for configuration management (i.e., identification of the overall process owner).
- 2.2.2** The IS auditor should obtain and verify that management has identified resources to measure the number and nature of changes being made to the enterprise systems, resources and networks.
- 2.2.3** Accountability should be established regarding first-and second tier-support for configuration changes.

2.3 Assets Tracking and Tools

- 2.3.1** Assets should be tracked and individual assets should be monitored to protect them from theft, abuse or misuse.
- 2.3.2** Software should be labeled, inventoried and appropriately licensed. Library management software should be used to produce audit trails of program changes and to maintain program version numbers, creation-date information and copies of previous versions.
- 2.3.3** The IS auditor should obtain a listing of all authorised software, if possible, from the use of automated tools that scan all hardware devices including servers and desktops computers. This software provides critical details, such as:
- Hardware type and model number
 - Software elements, including interface programs and controls to verify that Inter-operability
 - Vendor software:
 - Version
 - Documentation of current vendor support requirements
 - Documentation of any customisation made from vendor-provided baseline that could affect the interface with other software
- 2.3.4** The IS auditor should obtain a general understanding of the software acquisition controls used to verify that all software purchased is recorded in the IT asset tracking system.

2.4 Control and Logging of Changes

- 2.4.1** Procedures should be in place to verify that only authorised and identifiable configuration items are recorded in the inventory upon acquisition. These procedures should also provide for the authorised disposal and consequential sale or destruction of configuration items.
- 2.4.2** Procedures should be in place to keep track of changes to the configuration (e.g., new item, status change from development to prototype). Logging and control should be an integrated part of the configuration recording system including reviews of change records.

2.5 Communication Requirements Including Release Management

- 2.5.1** Senior IT management with selected senior business management should form a steering committee to evaluate high-risk configuration changes (i.e., business applications). Minutes should be documented including decisions regarding the implementation of changes.
- 2.5.2** The IS auditor should obtain audit evidence of a schedule of changes including a 'release calendar' that denotes the dates and times that various changes are elevated into the production-processing environment. Typically, the IS auditor should observe separation and elevation of changes, so computer operations can more easily identify system problems.
- 2.5.3** Audit evidence of communication to business owners to be on notice to detect unusual system events for significant configuration changes.

2.6 Metrics to be Reported

2.6.1 All measurements including dashboards should result from measuring the number and nature of changes being made to the enterprise, systems, resources and networks. Some typical instances for measurement:

- Average time period (lag) between identifying a discrepancy and rectifying it
- Number of discrepancies relating to incomplete or missing configuration information
- Percent of configuration items in line with service levels for performance, security and availability
- Number of deviations identified between configuration repository and actual asset configurations
- Percent of licences purchased and not accounted for in repository
- Percent of unauthorised licences vs. purchased licences in use
- Percent of business compliance issues caused by improper configuration of assets

2.6.2 Performance including service levels statistics such as response time, system uptime (availability), quality of data integrity, etc., should be formally documented and circulated amongst IT management. Employee or contractor performance (in cases where IT department is outsourced) should be measured on this metric.

2.6.3 For changes, whether management measures the amount of lead-time and if it affects the success or failure of making non-disruptive changes should be ascertained:

- When lead-time is important, identifying sensitive types and volumes of changes to reduce disruptions
- Determining a better method of identifying and categorising changes into levels of risk
- Verifying every record has technical and management accountability
- Establishing a process verifying that the record has been reviewed for technical merit and business readiness in a consistent manner while allowing flexibility based on business needs

3. EFFECTIVE DATE

3.1 This guideline is effective for all information systems audits effective 1 November 2007

ISACA 2007-2008 STANDARDS BOARD	
Chair, Ravi Muthukrishnan, CISA, CISM, FCA, ISCA	Ikanos Communications, India
Brad David Chin, CISA, CPA	Google Inc., USA
Sergio Fleginsky, CISA	ICI Paints, Uruguay
Maria Gonzalez, CISA	HomeLand Office, Spain
John Ho Chi, CISA, CISM, CBCP, CFE	Ernst & Young, Singapore
Andrew J. MacLeod, CISA, FCPA, MACS, PCP, CIA	Brisbane City Council, Australia
Meera Venkatesh, CISA, CISM, ACS, CISSP, CWA	Microsoft Corp., USA
John G. Ott, CISA, CPA	AmerisourceBergen, USA
Jason Thompson, CISA	Ford Motor Company, USA

© 2007 ISACA. All rights reserved.

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