Generic Application Audit/Assurance Program

ISACA
Serving IT Governance Professionals

ISACA®
With more than 86,000 constituents in more than 160 countries, ISACA (*www.isaca.org*) is a recognized worldwide leader in IT governance, control, security and assurance. Founded in 1969, ISACA sponsors international conferences, publishes the *ISACA Journal®*, and develops international information systems auditing and control standards. It also administers the globally respected Certified Information Systems Auditor™ (CISA®) designation, earned by more than 60,000 professionals since 1978; the Certified Information Security Manager® (CISM®) designation, earned by more than 10,000 professionals since 2002; and the new Certified in the Governance of Enterprise IT™ (CGEIT™) designation.

Disclaimer
ISACA has designed and created *Generic Application Audit/Assurance Program* (the "Work"), primarily as an informational resource for audit and assurance professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, audit/assurance professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or IT environment.

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: *info@isaca.org*
Web site: *www.isaca.org*

ISBN 978-1-60420-076-8
Generic Application Audit/Assurance Program
Printed in the United States of America

ISACA wishes to recognize:

Author
Norm Kelson, CISA, CGEIT, CPA, The Kelson Group, USA

Expert Reviewers
Robert B. Brenis, CISA, CGEIT, MCP, PMP, Skoda Minotti, USA
Samuel Chiedozie Isichei, CISA, CISM, CISSP, Protiviti, USA
Sandeep Godbole, CISA, CISM, CISSP, Syntel, India
Larry Marks, CISA, CGEIT, CISSP, CSTE, PMP, Resources Global Professionals, USA
Bharath Nallapu, CISA, PMP, Smith, Nallapu & Associates LLP. United States
Gbadamosi Folakemi Toyin, AMPDM, CPE, MCS, Flookytee Computers, Nigeria
Greet Volders, Voquals, Belgium

Table of Contents

I. Introduction

Overview

ISACA has developed the *IT Assurance Framework*™ (ITAF™) as a comprehensive and good-practice-setting model. ITAF provides standards that are designed to be mandatory and are the guiding principles under which the IT audit and assurance profession operates. The guidelines provide information and direction for the practice of IT audit and assurance. The tools and techniques provide methodologies, tools and templates to provide direction in the application of IT audit and assurance processes.

Purpose

The audit/assurance program is a tool and template to be used as a road map for the completion of a specific assurance process. The ISACA Assurance Committee has commissioned audit/assurance programs to be developed for use by IT audit and assurance practitioners. This audit/assurance program is intended to be utilized by IT audit and assurance professionals with the requisite knowledge of the subject matter under review, as described in ITAF, section 2200—General Standards. The audit/assurance programs are part of ITAF; section 4000—IT Assurance Tools and Techniques.

Control Framework

The audit/assurance programs have been developed in alignment with the IT Governance Institute® (ITGI™) framework *Control Objectives for Information and related Technology* (COBIT ®)—specifically COBIT 4.1— using generally applicable and accepted good practices. They reflect ITAF, sections 3400—IT Management Processes, 3600—IT Audit and Assurance Processes, and 3800—IT Audit and Assurance Management.

Many organizations have embraced several frameworks at an enterprise level, including the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Framework. The importance of the control framework has been enhanced due to regulatory requirements by the US Securities and Exchange Commission (SEC) as directed by the US Sarbanes-Oxley Act of 2002 and similar legislation in other countries. They seek to integrate control framework elements used by the general audit/assurance team into the IT audit and assurance framework. Since COSO is widely used, it

has been selected for inclusion in this audit/assurance program. The reviewer may delete or rename these columns to align with the enterprise's control framework.

IT Governance, Risk and Control

IT governance, risk and control are critical in the performance of any assurance management process. Governance of the process under review will be evaluated as part of the policies and management oversight controls. Risk plays an important role in evaluating what to audit and how management approaches and manages risk. Both issues will be evaluated as steps in the audit/assurance program. Controls are the primary evaluation point in the process. The audit/assurance program will identify the control objectives and the steps to determine control design and effectiveness.

Responsibilities of IT Audit and Assurance Professionals

IT audit and assurance professionals are expected to customize this document to the environment in which they are performing an assurance process. This document is to be used as a review tool and starting point. It may be modified by the IT audit and assurance professional; it *is not* intended to be a checklist or questionnaire. It is assumed that the IT audit and assurance professional holds the Certified Information Systems Auditor (CISA) designation, or has the necessary subject matter expertise required to conduct the work and is supervised by a professional with the CISA designation and necessary subject matter expertise to adequately review the work performed.

II. Using This Document

This audit/assurance program was developed to assist the audit and assurance professional in designing and executing a review. Details regarding the format and use of the document follow.

Work Program Steps

The first column of the program describes the steps to be performed. The numbering scheme used provides built-in work paper numbering for ease of cross-reference to the specific work paper for that section. The physical document was designed in Microsoft® Word. The IT audit and assurance professional is encouraged to make modifications to this document to reflect the specific environment under review.

Step 1 is part of the fact gathering and pre-fieldwork preparation. Because the pre-fieldwork is essential to a successful and professional review, this step has been itemized in this plan. The first level steps, e.g., 1.1, are in **bold** type and provide the reviewer with a scope or high-level explanation of the purpose for the substeps.

Beginning in step 2, the steps associated with the work program are itemized. To simplify the use of the program, the audit/assurance program describes the audit/assurance objective—the reason for performing the steps in the topic area. The specific controls follow and are shown in **blue** type. Each review step is listed below the control. These steps may include assessing the control design by walking through a process, interviewing, observing or otherwise verifying the process and the controls that address that process. In many cases, once the control design has been verified, specific tests need to be performed to provide assurance that the process associated with the control is being followed. The application audit requires significant customization to include operational issues specific to the application under review. Using the approach described above, the audit and assurance professional can modify this program to meet these needs.

The maturity assessment, which is described in more detail later in this document, makes up the last section of the program.

The audit/assurance plan wrap-up—those processes associated with the completion and review of work papers, preparation of issues and recommendations, report writing and report clearing—has been excluded from this document, since it is standard for the audit/assurance function and should be identified elsewhere in the enterprise's standards.

COBIT Cross-reference

The COBIT cross-reference provides the audit and assurance professional with the ability to refer to the specific COBIT control objective that supports the audit/assurance step. The COBIT control objective should be identified for each audit/assurance step in the section. Multiple cross-references are not uncommon. Processes at lower levels in the work program are too granular to be cross-referenced to COBIT. The audit/assurance program is organized in a manner to facilitate an evaluation through a structure parallel to the development process. COBIT provides in-depth control objectives and suggested control practices at each level. As the professional reviews each control, he/she should refer to COBIT 4.1 or the *IT Assurance Guide: Using COBIT* for good-practice control guidance.

COSO Components

As noted in the introduction, COSO and similar frameworks have become increasingly popular among audit and assurance professionals. This ties the assurance work to the enterprise's control framework. While the IT audit/assurance function has COBIT as a framework, operational audit and assurance professionals use the framework established by the enterprise. Since COSO is the most prevalent internal control framework, it has been included in this document and is a bridge to align IT audit/assurance with the rest of the audit/assurance function. Many audit/assurance organizations include the COSO control components within their report and summarize assurance activities to the audit committee of the board of directors.

For each control, the audit and assurance professional should indicate the COSO component(s) addressed. It is possible but generally not necessary, to extend this analysis to the specific audit step level.

The original COSO internal control framework contained five components. In 2004, COSO was revised as the *Enterprise Risk Management (ERM) Integrated Framework* and extended to eight components. The primary difference between the two frameworks is the additional focus on ERM and integration into the business decision model. ERM is in the process of being adopted by large enterprises. The two frameworks are compared in **figure 1**.

Figure 1—Comparison of COSO Internal Control and ERM Integrated Frameworks

Internal Control Framework	ERM Integrated Framework
Control Environment: The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.	**Internal Environment**: The internal environment encompasses the tone of an organization, and sets the basis for how risk is viewed and addressed by an entity's people, including risk management philosophy and risk appetite, integrity and ethical values, and the environment in which they operate.
	Objective Setting: Objectives must exist before management can identify potential events affecting their achievement. Enterprise risk management ensures that management has in place a process to set objectives and that the chosen objectives support and align with the entity's mission and are consistent with its risk appetite.
	Event Identification: Internal and external events affecting achievement of an entity's objectives must be identified, distinguishing between risks and opportunities. Opportunities are channeled back to management's strategy or objective-setting processes.

Figure 1—Comparison of COSO Internal Control and ERM Integrated Frameworks	
Internal Control Framework	**ERM Integrated Framework**
Risk Assessment: Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives and thus risk assessment is the identification and analysis of relevant risks to achievement of assigned objectives. Risk assessment is a prerequisite for determining how the risks should be managed.	**Risk Assessment**: Risks are analyzed, considering the likelihood and impact, as a basis for determining how they could be managed. Risk areas are assessed on an inherent and residual basis.
	Risk Response: Management selects risk responses – avoiding, accepting, reducing, or sharing risk – developing a set of actions to align risks with the entity's risk tolerances and risk appetite.
Control Activities: Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address risks to achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.	**Control Activities:** Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out.
Information and Communication: Information systems play a key role in internal control systems as they produce reports, including operational, financial and compliance-related information that make it possible to run and control the business. In a broader sense, effective communication must ensure information flows down, across and up the organization. Effective communication should also be ensured with external parties, such as customers, suppliers, regulators and shareholders.	**Information and Communication**: Relevant information is identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Effective communication also occurs in a broader sense, flowing down, across, and up the entity.
Monitoring: Internal control systems need to be monitored—a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities or separate evaluations. Internal control deficiencies detected through these monitoring activities should be reported upstream and corrective actions should be taken to ensure continuous improvement of the system.	**Monitoring**: The entirety of enterprise risk management is monitored and modifications made as necessary. Monitoring is accomplished through ongoing management activities, separate evaluations, or both.

Information for **figure 1** was obtained from the COSO web site *www.coso.org/aboutus.htm.*

The original COSO internal control framework addresses the needs of the IT audit and assurance professional: control environment, risk assessment, control activities, information and communication, and monitoring. As such, ISACA has elected to utilize the five-component model for these audit/assurance programs. As more enterprises implement the ERM model, the additional three columns can be added, if relevant. When completing the COSO component columns, consider the definitions of the components as described in **figure 1**.

Reference/Hyperlink

Good practices require the audit and assurance professional to create a work paper for each line item, which describes the work performed, issues identified and conclusions. The reference/hyperlink is to be used to cross-reference the audit/assurance step to the work paper that supports it. The numbering system of this document provides a ready numbering scheme for the work papers. If desired, a link to the work paper can be pasted into this column.

Issue Cross-reference

This column can be used to flag a finding/issue that the IT audit and assurance professional wants to further investigate or establish as a potential finding. The potential findings should be documented in a work paper that indicates the disposition of the findings (formally reported, reported as a memo or verbal finding, or waived).

Comments

The comments column can be used to indicate the waiving of a step or other notations. It is not to be used in place of a work paper describing the work performed.

III. Controls Maturity Analysis

One of the consistent requests of stakeholders who have undergone IT audit/assurance reviews is a desire to understand how their performance compares to good practices. Audit and assurance professionals must provide an objective basis for the review conclusions. Maturity modeling for management and control over IT processes is based on a method of evaluating the organization, so it can be rated from a maturity level of nonexistent (0) to optimized (5). This approach is derived from the maturity model that the Software Engineering Institute (SEI) of Carnegie Mellon University defined for the maturity of software development.

The *IT Assurance Guide Using COBIT*, Appendix VII—Maturity Model for Internal Control, in **figure 2**, provides a generic maturity model showing the status of the internal control environment and the establishment of internal controls in an enterprise. It shows how the management of internal control, and an awareness of the need to establish better internal controls, typically develops from an *ad hoc* to an optimized level. The model provides a high-level guide to help COBIT users appreciate what is required for effective internal controls in IT and to help position their enterprise on the maturity scale.

Figure 2—Maturity Model for Internal Control

Maturity Level	Status of the Internal Control Environment	Establishment of Internal Controls
0 Non-existent	There is no recognition of the need for internal control. Control is not part of the organization's culture or mission. There is a high risk of control deficiencies and incidents.	There is no intent to assess the need for internal control. Incidents are dealt with as they arise.
1 Initial/*ad hoc*	There is some recognition of the need for internal control. The approach to risk and control requirements is *ad hoc* and disorganized, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.	There is no awareness of the need for assessment of what is needed in terms of IT controls. When performed, it is only on an *ad hoc* basis, at a high level and in reaction to significant incidents. Assessment addresses only the actual incident.
2 Repeatable but Intuitive	Controls are in place but are not documented. Their operation is dependent on the knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weaknesses exist and are not adequately addressed; the impact can be severe. Management actions to resolve control issues are not prioritized or consistent. Employees may not be aware of their responsibilities.	Assessment of control needs occurs only when needed for selected IT processes to determine the current level of control maturity, the target level that should be reached and the gaps that exist. An informal workshop approach, involving IT managers and the team involved in the process, is used to define an adequate approach to controls for the process and to motivate an agreed-upon action plan.
3 Defined	Controls are in place and adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. While management is able to deal predictably with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilities for control.	Critical IT processes are identified based on value and risk drivers. A detailed analysis is performed to identify control requirements and the root cause of gaps and to develop improvement opportunities. In addition to facilitated workshops, tools are used and interviews are performed to support the analysis and ensure that an IT process owner owns and drives the assessment and improvement process.
4 Managed and Measurable	There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weaknesses. A limited, tactical use of technology is applied to automate controls.	IT process criticality is regularly defined with full support and agreement from the relevant business process owners. Assessment of control requirements is based on policy and the actual maturity of these processes, following a thorough and measured analysis involving key stakeholders. Accountability for these assessments is clear and enforced. Improvement strategies are supported by business cases. Performance in achieving the desired outcomes is consistently monitored. External control reviews are organized occasionally.
5 Optimized	An enterprisewide risk and control program provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.	Business changes consider the criticality of IT processes and cover any need to reassess process control capability. IT process owners regularly perform self-assessments to confirm that controls are at the right level of maturity to meet business needs and they consider maturity attributes to find ways to make controls more efficient and effective. The organization benchmarks to external best practices and seeks external advice on internal control effectiveness. For critical processes, independent reviews take place to provide assurance that the controls are at the desired level of maturity and working as planned.

The maturity model evaluation is one of the final steps in the evaluation process. The IT audit and assurance professional can address the key controls within the scope of the work program and formulate an objective assessment of the maturity levels of the control practices. The maturity assessment can be a part of the audit/assurance report and can be used as a metric from year to year to document progression in the enhancement of controls. However, it must be noted that the perception of the maturity level may vary between the process/IT asset owner and the auditor. Therefore, an auditor should obtain the concerned stakeholder's concurrence before submitting the final report to management.

At the conclusion of the review, once all findings and recommendations are completed, the professional assesses the current state of the COBIT control framework and assigns it a maturity level using the six-level scale. Some practitioners utilize decimals (x.25, x.5, x.75) to indicate gradations in the maturity model. As a further reference, COBIT provides a definition of the maturity designations by control objective. While this approach is not mandatory, the process is provided as a separate section at the end of the audit/assurance program for those enterprises that wish to implement it. It is suggested that a maturity assessment be made at the COBIT control level. To provide further value to the client/customer, the professional can also obtain maturity targets from the client/customer. Using the assessed and target maturity levels, the professional can create an effective graphic presentation that describes the achievement or gaps between the actual and targeted maturity goals. A graphic is provided on the last page of this document (section VII), based on sample assessments.

IV. Assurance and Control Framework

ISACA IT Assurance Framework and Standards

ITAF section 3650—Auditing Application Controls—is relevant to the audit/assurance of an application review. In addition, reliance is placed on section 3630—Auditing IT General Controls.

ISACA has long recognized the specialized nature of IT assurance and strives to advance globally applicable standards. Guidelines and procedures provide detailed guidance on how to follow those standards. IS Auditing Standard S15 IT Controls, IS Auditing Guidelines G14 Application Systems Review and G38 Access Controls, and IS Auditing Procedure P10 Business Application Change Control are relevant to this audit/assurance program.

ISACA Controls Framework

COBIT is an IT governance framework and supporting tool set that allows managers to bridge the gap among control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout enterprises.

Utilizing COBIT as the control framework on which IT audit/assurance activities are based, aligns IT audit/assurance with good practices as developed by the enterprise.

The COBIT application controls (ACs) address good practices for business applications. The COBIT areas for this evaluation include:

- AC1 *Source data preparation and authorization*—Ensure that source documents are prepared by authorized and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Errors and omissions can be minimized through good input form design. Detect errors and irregularities so they can be reported and corrected.
- AC2 *Source data collection and entry*—Establish that data input is performed in a timely manner by authorized and qualified staff. Correction and resubmission of data that were erroneously input should

be performed without compromising original transaction authorization levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time.

- AC3 *Accuracy, completeness and authenticity checks*—Ensure that transactions are accurate, complete and valid. Validate data that were input, and edit or send back for correction as close to the point of origination as possible.
- AC4 *Processing integrity and validity*—Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transactions does not disrupt the processing of valid transactions.
- AC5 *Output review, reconciliation and error handling*—Establish procedures and associated responsibilities to ensure that output is handled in an authorized manner, delivered to the appropriate recipient and protected during transmission; that verification, detection and correction of the accuracy of output occurs; and that information provided in the output is used.
- AC6 *Transaction authentication and integrity*—Before passing transaction data between internal applications and business/operational functions (inside or outside the enterprise), check it for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport.

Refer to the IT Governance Institute's *COBIT Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*, published in 2007, for the related control practice value and risk drivers.

V. Executive Summary of Audit/Assurance Focus

Generic Application

The application review provides the enterprise with an assessment of the design and effectiveness of the internal controls and operating efficiency and effectiveness of an existing application. The definition of an application review is specific to an enterprise and can encompass a business function, business unit or business process. "Application" does not specifically refer to the automated functions of a business process.

This audit/assurance program focuses on an existing application or business process. The *Systems Development and Project Management Audit/Assurance Program* is more suited for an application under development.

The application audit/assurance review is, by definition, an "integrated audit." The integrated team ensures that there are no gaps between automated and manual functions; therefore, the skill sets and planning require a project team consisting of both IT and business/operational professionals.

The audit/assurance process should be customized to the individual needs of the business and application under review. This generic application audit/assurance program requires customization by the assurance team to fit the business environment.

Business Impact and Risk

An application is the procedures and processes necessary to fulfill a business function. This may be financial (general ledger, accounts payable, accounts receivable, payroll), order entry (however an order is defined, i.e., claims, product orders, banking transactions), operational (inventory transfer and logistics), or involving intellectual property, human resources and other business-related processes. The volume of transactions necessitates the reliance on the functionality and internal controls of a business application.

Failure to implement effective, efficient and appropriate internal controls may result in the following general risks:

- Loss or underutilization of assets
- Invalid or incorrectly processed transactions
- Loss of reputation due to inability to deliver services or disclosure of internal issues
- Costly compensating controls
- Reduced system availability and questionable integrity of information
- Inability to satisfy audit/assurance charter, requirements of regulators or external auditors

Objective and Scope

Objective—The objectives of the applications review are to:

- Provide management with an independent assessment of efficiency and effectiveness of the design and operation of internal controls and operating procedures
- Provide management with the identification of application-related issues that require attention
- {Additional objectives customized to the specific business as determined by the audit and assurance professional}

Scope—The review will focus upon the {list specific applications}. The scope of the review will include the following:

- Identification and evaluation of the design of controls
- Evaluation of control effectiveness
- Assessment of compliance with regulatory requirements
- Identification of issues requiring management attention
- {Additional scope as determined by project team}

Based on the initial risk assessment, the scope will focus on the following transaction/business processes:

- {List relevant processes.}

The following will be excluded from the review:

- {List exclusions.}

Minimum Audit Skills

The IT audit and assurance professional should have an understanding of the good-practice process and controls in automated applications, and the operational audit professional should have an understanding of the good-practice control process and controls for the specific business processes addressed by the application. Professionals who have achieved CISA certification should have the appropriate skills for the automated scope, and professionals who have achieved either a Certified Internal Auditor (CIA) or a Certified Public Accountant/Certified Accountant (CPA/CA) should have the necessary skills for the operational scope.

VI. Audit/Assurance Program

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
1. PLANNING AND SCOPING THE AUDIT									
1.1 Define audit/assurance objectives. The audit/assurance objectives are high level and describe the overall audit goals.									
1.1.1 Review the audit/assurance objectives in the introduction to this audit/assurance program.									
1.1.2 Modify the audit/assurance objectives to align with the audit/assurance universe, annual plan and charter.									
1.2 Define boundaries of review. The review must have a defined scope. The reviewer must understand the operating environment and prepare a proposed scope, subject to a later risk assessment.									
1.2.1 Obtain an understanding of the services provided by the enterprise, including the scope of services and the effect the services have on the enterprise's activities.									
1.2.2 Establish initial boundaries of the audit/assurance review.									
1.2.2.1 Identify limitations and/or constraints affecting the audit/assurance review.									
1.3 Define assurance. The review requires two sources of standards. The corporate standards defined in policy and procedure documentation establish the corporate expectations. At minimum, corporate standards should be implemented. The second source, a good-practice reference, establishes industry standards. Enhancements should be proposed to address gaps between the two.									
1.3.1 Obtain company systems development standards, systems development methodology manual, project management standards, project methodology manual, and application or software manual.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
1.3.2 Determine if COBIT and the appropriate systems development framework will be used as a good-practice reference.									
1.4 Define the change process. The initial audit approach is based upon the reviewer's understanding of the operating environment and associated risks. As further research and analysis are performed, changes to the scope and approach will result.									
1.4.1 Identify the senior IT audit/assurance resource responsible for the review.									
1.4.2 Establish the process for suggesting and implementing changes to the audit/assurance program, and to the authorizations required.									
1.5 Define assignment success. The success factors need to be identified. Communication among the IT audit/assurance team, other assurance teams and the enterprise is essential.									
1.5.1 Identify the drivers for a successful review (this should exist in the assurance function's standards and procedures).									
1.5.2 Communicate success attributes to the process owner or stakeholder, and obtain agreement.									
1.6 Define audit/assurance resources required. The resources required are defined in the introduction to this audit/assurance program.									
1.6.1 Determine the audit/assurance skills necessary for the review.									
1.6.2 Determine the estimated total resources (hours) and time frame (start and end dates) required for the review.									
1.7 Define deliverables The deliverable is not limited to the final report. Communication between the audit/assurance teams and the process owner is essential to assignment success.									
1.7.1 Determine the interim deliverables, including initial findings, status reports, draft reports, due dates for responses and the final report.									

Generic Application Audit/Assurance Program

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
1.8 Communications The audit/assurance process is clearly communicated to the customer/client.									
1.8.1 Conduct an opening conference to discuss the review objectives with the executive responsible for operating systems and infrastructure.									
2. PLANNING THE APPLICATION AUDIT									
2.1 Planning team									
2.1.1 Establish the audit/assurance management team to plan the review.									
2.1.1.1 Assign an experienced IT audit and assurance professional and an operational audit and assurance professional as project managers.									
2.1.1.2 Consider knowledge of the business process area and IT operating environment when making assignments.									
2.1.1.3 Assign lead staff to the planning process.									
2.2 Understand the application.									
2.2.1 Obtain an understanding of the business and application process environment.									
2.2.1.1 Obtain an understanding of the application's business environment.									
2.2.1.1.1 Ensure that audit/assurance engagement managers meet with the business and IT executives responsible for the application and business processes.									
2.2.1.1.2 Identify the business process and data owners responsible for the application.									
2.2.1.1.3 Obtain an understanding of the strategic and operational significance of the application.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2.2.1.1.4 Determine if the application has been developed in- house or purchased, and if the application is maintained in-house or has been contracted/outsourced.									
2.2.1.1.5 Obtain an understanding of the warranties and support in the case of a purchased application.									
2.2.1.1.6 Through discussions and a walkthrough of the general business process, obtain an understanding of the business functions performed by the application and the interfaces with other applications; determine where the controls are located within the application and identify application limitations, where possible.									
2.2.1.1.7 Determine how the business process affects the financial statements of the enterprise (direct interface to the general ledger or mission-critical process that, if not operating correctly, could affect the enterprise's financial performance), or operational significance to the enterprise.									
2.2.1.1.8 Determine the regulatory requirements that impact the business process (external examiners, financial reporting requirements, privacy, data security, etc.).									
2.2.1.1.9 Determine known issues with the business process and application from the perspective of other executives.									
2.2.1.2 Obtain an understanding of the application's functionality.									
2.2.1.2.1 Audit/assurance engagement management and lead staff members meet with the business and IT managers responsible for the application and business processes.									
2.2.1.2.2 Through discussions, perform a walkthrough of the business process and application from source entry through output and reconciliation.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2.2.1.2.3 Determine how the business process affects the financial statements of the enterprise (direct interface to the general ledger or mission-critical process that, if not operating correctly, could affect the enterprise's financial performance), or operational significance to the enterprise.									
2.2.1.2.4 Determine the regulatory requirements that impact the business process (external examiners, financial reporting requirements, privacy, data security, etc.).									
2.2.1.2.5 Determine known issues with the business process and application from the perspective of other executives.									
2.2.1.3 Understand the application's technical infrastructure.									
2.2.1.3.1 Through discussions with senior management responsible for the development, implementation and operations of the application, obtain an understanding and documentation of the following and how they impact the application: • Technical infrastructure (host, client-server or web-based) • Network (intranet, Internet, or extranet), wireless or wired • Transaction processor (CICS or IMS) • Workstation (desktop/handheld/laptop/special devices) • Operating systems (IBM Mainframe, UNIX/LINUX, Windows, proprietary) • Database management systems (Oracle, DB2, IMS, SQL Server, other) • Insourced or outsourced • Real-time, store and forward, and/or batch • Test and development of operating environments	DS5.3 DS5.4 DS5.8 DS5.10 DS5.11								
2.2.1.4 Understand the volatility and level of change affecting the application.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2.2.1.4.1 Interview business management to determine planned changes, history of problem areas and other known operational issues that would affect the scope of the review.									
2.2.1.4.2 Obtain recent systems requests, incident reports and problem logs. Identify issues that were not identified in meetings with management.	DS5.6 DS8.2								
2.2.1.4.3 Evaluate how volatility and change issues affect the scope of the review, and determine if there are identifiable trends for certain issues.									
2.2.2 Obtain a detailed understanding of the application.									
2.2.2.1 Using the information obtained in management interviews and documentation provided by enterprise and IT, obtain and document a detailed understanding of the application. Consider the: • Source data – Manual input – Input interfaces from other applications • Processing cycle – Audit trails – Error reporting – Internal controls and edits – Frequency of application processes – Dependency of application on processing cycles and other applications – System setup parameters • Data edits – Initial edits – Data correction – Maintenance of master files • Output – Review and reconciliation									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
– Reports generated – Output interfaces to other applications – Report distribution									
2.2.3 Based on the detailed understanding, identify the transactions in the application and business flow.									
2.3 Risk assessment									
2.3.1 Perform a risk assessment of the effect the application has on the business, the IT organization and the potential scope of the review.	PO9.2								
2.3.1.1 Consider the importance of business processes and transactions.									
2.3.1.2 Consider financial and regulatory requirements.									
2.3.1.3 Prioritize business processes and transactions for evaluation.									
2.4 Scope									
2.4.1 Narrow the scope to business processes and transactions to be evaluated in review.									
2.4.2 Determine the operational audit scope and IT audit scope.									
2.4.3 Determine the audit/assurance resources required to perform the review.									
2.4.4 Determine computer-assisted audit techniques (CAATs) that may be required.									
2.4.5 Identify specific business processes and application transactions to be reviewed.									
2.4.6 Establish the proposed scope.									
2.5 General controls									
2.5.1 Evaluate general control reviews to determine the level of reliance that can be placed on the installation controls.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
2.5.1.1 Review the results from the following IT audit/assurance assessments: • Physical security • Identity and access management • Incident/problem management • Change management • Operating system configuration • Information security • Network perimeter management • Database management • IT contingency and business contingency planning	AI6 DS4 DS5 DS8 DS10								
2.5.1.2 If open audit/assurance findings remain and are considered material in the context of the application audit, consider what expanded review procedures will be required.									
2.6 Finalize scope									
2.6.1 Identify the business processes to be reviewed.									
2.6.1.1 Identify the transactions for the business process.									
2.6.1.2 Identify the control objectives for each business process.									
2.6.1.2.1 Identify the controls that address each control objective.									
2.6.1.2.2 Customize the work program for the controls identified and their control description.									
2.6.2 Assign staff based on skill sets to the various processes.									
2.6.3 Determine IT and operational audit/assurance roles, and establish project management.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3. SOURCE DATA PREPARATION AND AUTHORIZATION									
3.1 Source data preparation Audit/assurance objective: Source documents should be prepared by authorized and qualified personnel following established procedures, and should provide for adequate segregation of duties between the origination and approval of these documents and accountability.									
3.1.1 Source document design **Control: Source documents are designed in a way that they increase the accuracy with which data can be recorded, control the workflow and facilitate subsequent reference checking. Where appropriate, completeness controls in the design of the source documents are included.**	AC1			X					
3.1.1.1 Assess whether source documents and/or input screens are designed with predetermined coding, choices, etc., to encourage timely completion and minimize the potential for error.									
3.1.2 Source data procedures **Control: Procedures for preparing source data entry are documented, and are effectively and properly communicated to appropriate and qualified personnel.[1]**	AC1			X	X				
3.1.2.1 Determine if the design of the system provides for the identification and management of authorization levels.									
3.1.2.1.1 Verify, through inspection of authorization lists, that authorization levels are properly defined for each group of transactions. Observe that authorization levels are properly applied.									

[1] These procedures establish and communicate required authorization levels (input, editing, authorizing, accepting and rejecting source documents). The procedures also identify the acceptable source media for each type of transaction.

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3.1.2.2 Inspect and observe creation and documentation of data preparation procedures, and inquire whether and confirm that procedures are understood and the correct source media are used.									
3.1.2.3 Inquire whether and confirm that the design of the system provides for the use of preapproved authorization lists and related signatures for use in determining that documents have been appropriately authorized.									
3.1.2.4 Inquire whether and confirm that the design of the system encourages review of the forms for completeness and authorization, and identifies situations where attempts to process incomplete and/or unauthorized documents occur.									
3.1.3 Data entry authorization **Control: The function responsible for data entry maintains a list of authorized personnel, including their signatures.**	AC1			X					
3.1.3.1 Where required by procedures, verify that adequate segregation of duties between originator and approver exists.									
3.1.3.2 Inquire whether and confirm that a list of authorized personnel and their signatures is maintained by the appropriate departments. Where possible, use automated evidence collection, including sample data, embedded audit modules or CAATs, to trace transactions to verify that the list of authorized personnel is effectively designed to allow/restrict personnel to enter data.									
3.1.3.3 Determine if a separation of duties (SOD) table exists and review for adequate separation of key duties.									
3.1.3.3.1 Inspect documents, trace transactions through the process and, where possible, use automated evidence collection, including sample data, embedded audit modules or CAATs, to trace transactions to verify that authorization access controls are effective.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3.2 Form design Audit/assurance objective: Good input form design should be used to minimize errors and omissions.									
3.2.1 Transaction identifier **Control: Unique and sequential identifiers (e.g., index, date and time) are automatically assigned to every transaction.**	AC1			X					
3.2.1.1 Inquire whether and confirm that unique and sequential numbers are assigned to each transaction.									
3.2.2 Source document design **Control: Source documents include standard components, contain proper instructions for completion and are approved by management.**	AC1			X					
3.2.2.1 Verify that all source documents include standard components, contain proper documentation (e.g., timeliness, predetermined input codes, default values) and are authorized by management.									
3.3 Error detection Audit/assurance objective: Errors and irregularities should be detected so they can be reported and corrected.									
3.3.1 Document error detection **Control: Documents that are not properly authorized or are incomplete are returned to the submitting originators for correction and recorded in a log to document their return. Logs are reviewed periodically to verify that corrected documents are returned by originators in a timely fashion, and to enable pattern analysis and root cause review.**	AC1			X	X	X			
3.3.1.1 Inquire whether and confirm that, once identified, the system is designed to track and report upon incomplete and/or unauthorized documents that are rejected and returned to the owner for correction.									
3.3.1.2 Inquire and confirm whether logs are reviewed periodically, reasons for returned documents are analyzed and corrective action is initiated.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
3.3.1.3 Determine if the corrective action is monitored for its effectiveness.									
4. SOURCE DATA COLLECTION AND ENTRY									
4.1 Data input preparation input Audit/assurance objective: Data input should be performed in a timely manner by authorized and qualified staff.	AC2								
4.1.1 Source document criteria **Control: Criteria for defining and communicating for timeliness, completeness and accuracy of source documents are documented.**				X	X				
4.1.1.1 Inquire whether and confirm that criteria for timeliness, completeness and accuracy of source documents are defined and communicated.									
4.1.2 Source document preparation **Control: Procedures ensure that data input is performed in accordance with the timeliness, accuracy and completeness criteria.**	AC2			X					
4.1.2.1 Inspect documentation of policies and procedures to ensure that criteria for timeliness, completeness and accuracy are appropriately represented.									
4.2 Correction and reentry of erroneous data Audit/assurance objective: Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorization levels.									
4.2.1 Out-of-sequence and missing source documents **Control: Use only prenumbered source documents for critical transactions. If proper sequence is a transaction requirement, identify and correct out-of-sequence source documents. If completeness is an application requirement, identify and account for missing source documents.**	AC2			X					
4.2.1.1 Inquire whether and confirm that policies and processes are established to establish criteria for the identification of classes of critical transactions that require prenumbered source documents or other unique methods of identifying source data.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
4.2.1.2 Inquire and confirm whether critical source documents are prenumbered and out-of-sequence numbers are identified and taken into account.									
4.2.1.3 Identify and review out-of-sequence numbers, gaps and duplicates using automated tools (CAATs).									
4.2.2 Data editing **Control: Access rules define and communicate who can input, edit, authorize, accept and reject transactions, and override errors. Accountability is established through access controls and documented supporting evidence to establish accountability in line with role and responsibility definitions.**	AC2			X					
4.2.2.1 For each major group of transactions, inquire whether and confirm that there is documentation of criteria to define authorization for input, editing, acceptance, rejection and override.									
4.2.2.2 Inspect documents, trace transactions through the process and, where possible, use automated evidence collection, including sample data, embedded audit modules or CAATs, to trace transactions to verify that authorization controls are effective and that sufficient evidence is reliably recorded and reviewed.									
4.2.2.3 Identify critical transactions. From that population, select a set of critical transactions. Perform the following steps.									
4.2.2.3.1 Compare the actual state of access controls over transaction input, editing, acceptance, etc. with established criteria, policies or procedures.									
4.2.2.3.2 Inspect whether critical source documents are prenumbered or other unique methods of identifying source data are used.									
4.2.2.3.3 Inspect documentation or walk through transactions to identify personnel who can input, edit, authorize, accept and reject transactions, and override errors.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
4.2.2.3.4 Take a sample of transactions within this set for a specific period, and inspect the source documents for those transactions. Verify that all appropriate source documents are available.									
4.2.3 Error correction **Control: Procedures are formally established and documented to correct errors, override errors and handle out-of-balance conditions and to follow up on, correct, approve and resubmit source documents and transactions in a timely manner. These procedures should consider things such as error message descriptions, override mechanisms and escalation levels.**	AC2			X					
4.2.3.1 Inquire and confirm whether documented procedures for the correction of errors, out-of-balance conditions and entry of overrides exist.									
4.2.3.2 Determine that the procedures include mechanisms for timely follow-up, correction, approval and resubmission.									
4.2.3.3 Evaluate the adequacy of procedures addressing error message descriptions and resolution, and override mechanisms.									
4.2.4 Error correction monitoring **Control: Error messages are generated in a timely manner as close to the point of origin as possible. The transactions are not processed unless errors are corrected or appropriately overridden or bypassed. Errors that cannot be corrected immediately are logged in an automated suspense log, and valid transaction processing continues. Error logs are reviewed and acted upon within a specified and reasonable period of time.**	AC2			X		X			
4.2.4.1 Inquire whether and confirm that error messages are generated and communicated in a timely manner, transactions are not processed unless errors are corrected or appropriately overridden, errors that cannot be corrected immediately are logged and valid transaction processing continues, and error logs are reviewed and acted upon within a specified and reasonable period of time.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
4.2.5 Error condition monitoring **Control: Errors and out-of-balance reports are reviewed by appropriate personnel, followed up on and corrected within a reasonable period of time, and, where necessary, incidents are escalated for attention by a senior-level staff member. Automated monitoring tools may be used to identify, monitor and manage errors.**	AC2			X	X	X			
4.2.5.1 Inquire whether and confirm that reports on errors and out-of-balance conditions are reviewed by appropriate personnel; all errors are identified, corrected and checked within a reasonable period of time; and errors are reported until corrected.									
4.2.5.2 Determine if error reports are distributed to someone other than the originating person.									
4.2.5.3 Inspect error and out-of-balance reports, error corrections, and other documents to verify that errors and out-of-balance conditions are effectively reviewed, corrected, checked and reported until corrected.									
4.3 Source document retention Audit/assurance objective: Where appropriate for reconstruction, original source documents should be retained for an appropriate amount of time.									
4.3.1 Source document retention **Control: Source documents are safe-stored (either by the enterprise or by IT) for a sufficient period of time in line with legal, regulatory or business requirements.**	AC2			X					
4.3.1.1 Inquire whether and confirm that there are policies and procedures in place to determine document retention policies. Factors to consider in assessing the document retention policy include: • Criticality of the transaction • Form of the source data • Method of retention • Location of retention									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
• Time period for retention • Ease of and availability of document retreival • Compliance and regulatory requirements									
4.3.1.2 For a sample of transaction flows, inquire whether and confirm that retention of source documents is defined and applied in relation to established criteria for source document retention.									
5. ACCURACY, COMPLETENESS AND AUTHENTICITY CHECKS									
5.1 Accuracy of transactions Audit/assurance objective: Entered transactions should be accurate, complete and valid. Input data should be validated and edited; edit failures should be corrected interactively or sent back for correction as close to the point of origination as possible.									
5.1.1 Transaction edits **Control: Transaction data are verified as close to the data entry point as possible and interactively during online sessions. Transaction data, whether people-generated, system-generated or interfaced inputs, are subject to a variety of controls to check for accuracy, completeness and validity. Wherever possible, transaction validation continues after the first error is found. Understandable error messages are immediately generated to enable efficient remediation.**	AC3			X					
5.1.1.1 Inquire whether and confirm that validation criteria and parameters on input data are periodically reviewed, confirmed and updated in a timely, appropriate and authorized manner.									
5.1.1.2 Obtain functional description and design information on transaction data entry. Inspect the functionality and design for the presence of timely and complete checks and error messages. If possible, observe transaction data entry.									
5.1.1.3 Select a sample of source data input processes. Inquire whether and confirm that mechanisms are in place to ensure that the source data input processes have been performed in line with established criteria									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
for timeliness, completeness and accuracy.									
5.1.2 Transaction accuracy completeness and validity **Control: Controls ensure accuracy, completeness, validity and compliance with regulatory requirements of data input. Controls may include sequence, limit, range, validity, reasonableness, table look-ups, existence, key verification, check digit, completeness (e.g., total monetary amount, total items, total documents, hash totals), duplicate and logical relationship checks, and time edits. Validation criteria and parameters are subject to periodic reviews and confirmation.**	AC3			X					
5.1.2.1 Obtain functional description and design information on data input controls. Inspect the functionality and design for appropriate controls. Examples of controls include the presence of sequence, limit, range, validity, reasonableness, table look-ups, existence, key verification, check digit, completeness (e.g., total monetary amount, total items, total documents, hash totals), duplication, logical relationship checks and time edits, and transaction cutoffs.									
5.1.2.2 Obtain functional description and design information on transaction data validation.									
5.1.2.3 Select a sample of input source data of source documents. Using inspection, CAATs, or other automated evidence collection and assessment tools, validate that input data are a complete and accurate representation of underlying source documents.									
5.2 Transaction access control Audit/assurance objective: Access control and role and responsibility mechanisms should be implemented so that only authorized persons whose duties are appropriately segregated from conflicting functions may input, modify and authorize data.									
5.2.1 Transaction access control **Control: Access controls are implemented to assign access based on job function.**	AC3			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
5.2.1.1 Obtain the results from the latest identity management review, and determine if reliance can be placed on the reviews performed previously.									
5.2.1.2 Determine if requirements for segregation of duties for entry, modification and authorization of transaction data as well as for validation rules have been established.									
5.2.1.2.1 Obtain separation of duties tables that define job function and permitted transactions. Determine that no controls or asset protection principles will be violated due to the transaction access assignments.									
5.2.1.2.2 Inquire whether and confirm that processes and procedures are established for the segregation of duties for entry, modification and approval of transaction data as well as for validation rules. Factors to consider in the assessment of segregation of duties policies include criticality of the transaction system and methods for the enforcement of segregation of duties.									
5.2.1.2.3 For important or critical systems, inspect the data input design to ensure that the authorization controls allow only appropriately authorized persons to input or modify data.									
5.3 Transaction error reporting Audit/assurance objective: Transactions failing edit and validation routines should be subject to follow-up procedures to ensure that they are ultimately remediated. Any root cause should be identified and procedures should be modified.									
5.3.1 Suspending and reporting erroneous transactions **Control: Transactions failing validation are identified and posted to a suspense file in a timely fashion, and valid transactions are not delayed from processing.**	AC3			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
5.3.1.1 Inquire whether and confirm that policies and procedures exist for the handling of transactions that fail edit and validation checks.									
5.3.1.2 Inspect error corrections, out-of-balance conditions, entry overrides and other documents to verify that the procedures are followed.									
5.3.2 Suspended transaction follow-up **Control: Transactions failing edit and validation routines are subject to appropriate follow-up until errors are remediated. Follow-up includes aging transactions to ensure follow-up and conducting root cause analysis to help adjust procedures and automated controls.**	AC3			X		X			
5.3.2.1 Inspect error and out-of-balance reports, error corrections, and other documents to verify that errors and out-of-balance conditions are effectively reviewed, corrected, checked and reported until corrected.									
5.3.2.2 Inquire whether and confirm that transactions failing edit and validation routines are subject to appropriate follow-up until they are remediated.									
6. PROCESSING INTEGRITY AND VALIDITY									
6.1 Data integrity and validity Audit/assurance objective: The integrity and validity of data should be maintained throughout the processing cycle and the detection of erroneous transactions should not disrupt processing of valid transactions.									
6.1.1 Transaction authorization **Control: Mechanisms are established and implemented to authorize the initiation of transaction processing and to enforce that only appropriate and authorized applications and tools are used.**	AC4			X					
6.1.1.1 Inquire whether and confirm that transaction processing takes place only after appropriate authorization is given.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
6.1.1.2 For a sample application, inquire whether and confirm that segregation of duties is in place. Verify whether segregation of duties is implemented for entry, modification and approval of transaction data as well as for validation rules.									
6.1.1.3 For a sample of critical transactions processes, test whether access controls prevent unauthorized data entry. With searching tools, identify cases where unauthorized personnel are able to input or modify data.									
6.1.1.4 For a sample of critical transactions processes, test whether access controls prevent unauthorized data entry. With searching tools, identify cases where unauthorized personnel are able to input or modify data.									
6.1.2 Processing integrity **Control: Processing is completely and accurately performed routinely with automated controls, where appropriate. Controls may include checking for sequence and duplication errors, transaction/record counts, referential integrity checks, control and hash totals, range checks, and buffer overflow.**	AC4			X					
6.1.2.1 Inquire whether and confirm that adjustments, overrides and high-value transactions are promptly reviewed in detail for appropriateness by a supervisor who does not perform data entry. Inspect the audit trail, other documents, plans, policies and procedures to verify that adjustments, overrides and high-value transactions are designed effectively to be promptly reviewed in detail.									
6.1.2.2 Inspect the audit trail, other documents, plans, policies and procedures to verify that adjustments, overrides and high-value transactions are designed effectively to be promptly reviewed in detail. Inspect the audit trail, transactions (or batches), reviews and other documents; trace transactions through the process; and, where possible, use automated evidence collection, including sample data, embedded audit									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
modules or CAATS, to verify that supervisor reviews are effective to ensure the validity of adjustments, overrides and high-value transactions in a timely manner.									
6.1.2.3 Review the documentation of the tools and applications to verify that they are applicable and suitable for the task. Where appropriate for critical transactions, review the code to confirm that controls in the tools and applications operate as designed. Reprocess a representative sample to verify that automated tools operate as intended.									
6.1.2.4 For highly critical transactions, set up a test system that operates like the live system. Process transactions in the test system to ensure that valid transactions are processed appropriately and in a timely fashion.									
6.1.2.5 Inspect error messages upon data entry or online processing.									
6.1.2.6 Use automated evidence collection, including sample data, embedded audit modules or CAATS, to verify that valid transactions are processed without interruption. Inspect whether and confirm that invalid transactions are reported in a timely manner.									
6.1.3 Transaction error processing **Control: Transactions failing validation routines are reported and posted to a suspense file. Where a file contains valid and invalid transactions, the processing of valid transactions is not delayed and all errors are reported in a timely fashion. Information on processing failures is kept to allow for root cause analysis and help adjust procedures and automated controls.**	AC4			X	X	X			
6.1.3.1 Inquire whether and confirm that reconciliation of file totals is performed on a routine basis and that out-of-balance conditions are reported.									
6.1.3.1.1 Inspect reconciliations and other documents, and trace transactions through the process to verify that reconciliations effectively determine whether file totals									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
match or the out-of-balance condition is reported to the appropriate personnel.									
6.1.3.2 Inspect the functional description and design information on transaction data entry to verify whether transactions failing edit and validation routines are posted to suspense files.									
6.1.3.2.1 Verify that suspense files are correctly and consistently produced and that users are informed of transactions posted to suspense accounts.									
6.1.3.2.2 Verify that the processing of transactions is not delayed by data entry or transaction authorization errors. Use automated evidence collection, including sample data, base cases (prepared transactions with an expected outcome), embedded audit modules or CAATS to trace transactions to verify that transactions are processed effectively, valid transactions are processed without interruption from invalid transactions and erroneous transactions are reported.									
6.1.3.3 For a sample of transaction systems, verify that suspense accounts and suspense files for transactions failing edit and validation routines contain only recent errors. Confirm that older failing transactions have been appropriately remediated.									
6.1.3.4 For a sample of transactions, verify that data entry is not delayed by invalid transactions.									
6.1.3.5 For highly critical transactions, set up a test system that operates like the live system. Enter different types of errors.									
6.1.3.6 Determine if transactions failing edit and validation routines are posted to suspense files.									
6.1.3.7 Verify that suspense files are correctly and consistently produced.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
6.1.3.8 Verify that the user is informed of transactions posted to suspense accounts.									
6.1.4 Error monitoring and follow-up **Control: Transactions failing validation routines are subject to appropriate follow-up until errors are remediated or the transaction is canceled.**	AC4			X		X			
6.1.4.1 Analyze a representative sample of error transactions on suspense accounts and files, and verify that transactions failing validation routines are checked until remediation.									
6.1.4.2 Verify that suspense accounts and files for transactions failing validation routines contain only recent errors, confirming that older ones have been appropriately remediated.									
6.1.4.3 Verify that error detection and reporting are timely and complete and that they provide sufficient information to correct the transaction.									
6.1.4.4 Ensure that errors are reported appropriately and in a timely fashion.									
6.1.4.5 Take a sample of data input transactions. Use appropriate automated analysis and search tools to identify cases where errors were identified erroneously and cases where errors were not detected.									
6.1.4.6 Ensure that error messages are appropriate for the transaction flow. Examples of appropriate attributes of messages include understandability, immediacy and visibility.									
6.1.5 Process flow **Control: The correct sequence of jobs is documented and communicated to IT operations. Job output includes sufficient information regarding subsequent jobs to ensure that data are not inappropriately added, changed or lost during processing.**	AC4			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
6.1.5.1 Obtain functional description and design information on data input controls.									
6.1.5.1.1 Inspect the functionality and design for the presence of sequence and duplication errors, referential integrity checks, control, and hash totals.									
6.1.5.1.2 With searching tools, identify cases where errors were identified erroneously and cases where errors were not detected.									
6.1.5.2 Determine whether and confirm that jobs sequence is indicated to IT operations.									
6.1.5.2.1 Inquire whether and confirm that jobs provide adequate instructions to the job scheduling system so data are not inappropriately added, changed or lost during processing. Inspect source documents; trace transactions through the process; and, where possible, use automated evidence collection, including sample data, embedded audit modules or CAATS to trace transactions to verify that production job scheduling software is used effectively so that jobs run in the correct sequence and provide adequate instructions to the systems.									
6.1.5.2.2 Inspect source documents; trace transactions through the process; and, where possible, use automated evidence collection, including sample data, embedded audit modules or CAATS to trace transactions to verify that production job scheduling software is used effectively so that jobs run in the correct sequence and provide adequate instructions to the systems.									
6.1.6 Unique transaction identifier **Control: Each transaction has a unique and sequential identifier (e.g., index, date and time).**	AC4			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
6.1.6.1 Inquire whether and confirm that every transaction is assigned a unique and sequential number or identifier (e.g., index, date, time).									
6.1.6.1.1 Inspect source documents; trace transactions through the process; and, where possible, use automated evidence collection, including sample data, embedded audit modules or CAATS to trace transactions to verify that production job scheduling software is used effectively so that jobs run in the correct sequence and provide adequate instructions to the systems.									
6.1.7 Audit trails **Control: The audit trail of transactions processed is maintained. Include date and time of input and user identification for each online or batch transaction. For sensitive data, the listing should contain before-and-after images and should be checked by the business owner for accuracy and authorization of changes made.**	AC4			X					
6.1.7.1 Inquire whether and confirm that the audit trail of transactions processed is maintained, including who can disable or delete the audit trails.									
6.1.7.1.1 Inspect the audit trail and other documents to verify that the audit trail is designed effectively. Use automated evidence collection, including sample data, embedded audit modules or CAATS, to trace transactions to verify that the audit trail is maintained effectively.									
6.1.7.1.2 Verify that before-and-after images are maintained and periodically reviewed by appropriate personnel.									
6.1.7.2 Inquire whether and confirm that the transaction audit trail is maintained and periodically reviewed for unusual activity.									
6.1.7.2.1 Verify that the review is done by a supervisor who does not perform data entry. Inspect the audit trail, transactions (or									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
batches), reviews and other documents; trace transactions through the process; and, where possible, use automated evidence collection, including sample data, embedded audit modules or CAATS, to verify that periodic review and maintenance of the audit trail effectively detects unusual activity and supervisor reviews are effective to verify the validity of adjustments, overrides and high-value transactions in a timely manner.									
6.1.7.3 Determine that access to sensitive audit trails is restricted to authorized personnel and that access is monitored.									
6.1.8 Data integrity during system interruptions **Control: The integrity of data during unexpected interruptions in data processing is maintained.**	AC4			X					
6.1.8.1 Inquire whether and confirm that utilities are used, where possible, to automatically maintain the integrity of data during unexpected interruptions in data processing.									
6.1.8.1.1 Inspect the audit trail and other documents, plans, policies and procedures to verify that system capabilities are effectively designed to automatically maintain data integrity.									
6.1.8.1.2 Review the records of actual interruptions involving data integrity issues, and verify that appropriate tools were used effectively.									
6.1.9 Monitoring of high-value and adjustment transactions **Control: Adjustments, overrides and high-value transactions are reviewed promptly in detail for appropriateness by a supervisor who does not perform data entry.**	AC4			X		X			
6.1.9.1 Inquire whether and confirm that appropriate tools are used and maintenance of thresholds complies with the security requirements.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
6.1.9.2 Inquire whether and confirm that a supervisor periodically reviews system output and thresholds.									
6.1.9.3 Use automated evidence collection, including sample data, embedded audit modules or CAATS, to trace transactions to verify that the tools work as designed.									
6.1.10 Reconcile file totals **Control: A parallel control file that records transaction counts or monetary value as data is processed and then compared to master file data once transactions are posted. Reports are generated to identify out-of-balance conditions.**	AC4			X		X			
6.1.10.1 Inquire whether and confirm that control files are used to record transaction counts and monetary values, and that the values are compared after posting.									
6.1.10.2 Determine if other file total controls are in use.									
6.1.10.3 Verify that reports are generated identifying out-of-balance conditions and that the reports are reviewed, approved and distributed to the appropriate personnel.									
7. OUTPUT REVIEW, RECONCILIATION AND ERROR HANDLING									
7.1 Output review, reconciliation and error handling Audit/assurance objective: Procedures and associated responsibilities to ensure that output is handled in an authorized manner, delivered to the appropriate recipient and protected during transmission should be established and implemented; verification, detection and correction of the accuracy of output should occur; and information provided in the output should be used.									
7.1.1 Output retention and handling procedures **Control: Defined procedures for the handling and retaining of output from IT applications are implemented and communicated, follow defined**	AC5			X					

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
procedures, and consider privacy and security requirements.									
7.1.1.1 Review output handling and retention procedures for privacy and security.									
7.1.2 Data retrieval interfaces **Control: Data retrieval processes utilize access control security to prevent unauthorized access to data.**	AC5			X					
7.1.2.1 Determine if data retrieval tools including data extract generators, open database connectivity interfaces (to Microsoft® Access and Excel) are restricted to data by job function.									
7.1.2.2 Verify that data retrieval security tools are effective by performing appropriate tests of the controls.									
7.1.3 Sensitive output monitoring **Control: Physical inventories of all sensitive output, such as negotiable instruments, are routinely performed and compared with inventory records. Procedures with audit trails to account for all exceptions and rejections of sensitive output documents have been created.**	AC5			X					
7.1.3.1 Review the documentation and ensure that procedures specify that periodic inventories should be taken of key sensitive documents and differences should be investigated.									
7.1.3.2 Inquire whether and confirm that physical inventories of sensitive outputs are taken at appropriate intervals.									
7.1.3.3 Verify that physical inventories of sensitive outputs are compared to inventory records and that any differences are acted upon.									
7.1.3.4 Confirm that audit trails are created to account for all exceptions and rejections of sensitive output documents.									
7.1.3.5 Inspect a representative sample of audit trails using automated									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
evidence collection, if possible, to identify exceptions; verify whether they have been detected and action has been taken.									
7.1.3.6 Take a physical inventory sample, and compare it to the associated audit trails to verify that detection operates effectively.									
7.1.4 Distribution of sensitive output **Control: If the application produces sensitive output, the recipients who may receive it are defined and the output is clearly labeled so it is recognizable by people and machines, and is distributed accordingly. Where necessary, the sensitive data are sent it to special access-controlled output devices.**	AC5			X					
7.1.4.1 Inquire whether and confirm that sensitive information is defined, agreed upon by the process owner and treated appropriately. This may include labeling sensitive application output and, where required, sending sensitive output to special access-controlled output devices.									
7.1.4.2 For a sample of sensitive data, search output files and confirm that they are properly labeled.									
7.1.4.3 Review the distribution methods of sensitive information and the access control mechanisms of sensitive output devices.									
7.1.4.4 Verify that the mechanisms correctly enforce preestablished access rights.									
7.1.5 Control total reconciliation **Control: Control totals in the header and/or trailer records of the output are balanced to the control totals produced by the system at data entry to ensure completeness and accuracy of processing. If out-of-balance control totals exist, they are reported to the appropriate level of management.**	AC5			X	X				
7.1.5.1 Review design criteria and confirm that they require the use of integrity-based control processes, such as the use of control totals in header and/or trailer records and the balancing of output back to									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
control totals produced by the system.									
7.1.5.2 Inquire whether and confirm that procedures require that out-of-balance conditions and other abnormalities require prompt investigation and reporting.									
7.1.5.3 Inquire whether and confirm that control totals are properly implemented in header and/or trailer records of output to balance back to control totals produced by the system.									
7.1.5.4 Inquire whether and confirm that detected out-of-balance conditions are reported to the appropriate level of management. Inspect out-of-balance reports. Where possible, use automated evidence collection to look for control total errors, and verify that they were acted upon correctly and in a timely manner.									
7.1.6 Process validation **Control: Validation of completeness and accuracy of processing is performed before other operations are executed. If electronic output is reused, validation is performed prior to subsequent processing.**	AC5			X					
7.1.6.1 Inquire whether and confirm that procedures have been developed to ensure that output is reviewed for reasonableness, accuracy or other criteria established by the process owner prior to use.									
7.1.6.2 Inquire whether and confirm that procedures have been designed to ensure that the completeness and accuracy of application output are validated prior to the output being used for subsequent processing, including use in end-user processing.									
7.1.6.3 Obtain a list of all electronic outputs that are reused in end-user applications. Verify that the electronic output is tested for completeness and accuracy before the output is reused and reprocessed.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
7.1.6.4 Select a representative sample of electronic output, and trace selected documents through the process to ensure that completeness and accuracy are verified before other operations are performed.									
7.1.6.5 Reperform completeness and accuracy tests to validate that they are effective.									
7.1.7 Business owner output review **Control: Procedures to ensure that the business owners review the final output for reasonableness, accuracy and completeness are defined and implemented, and output is handled in line with the applicable confidentiality classification. Potential errors are reported and logged in an automated, centralized logging facility, and errors are addressed in a timely manner.**	AC5			X	X	X			
7.1.7.1 Inquire whether and confirm that detected out-of-balance conditions are reported, reports have been designed into the system and procedures have been developed to ensure that reports are provided to the appropriate level of management.									
7.1.7.2 Assess whether procedures have been defined that require the logging of potential errors and their resolution prior to distribution of the reports.									
7.1.7.3 Inquire whether and confirm that output is reviewed for reasonableness and accuracy.									
7.1.7.4 Select a representative sample of output reports, and test the reasonableness and accuracy of the output. Verify that potential errors are reported and centrally logged.									
7.1.7.5 Select a sample of representative transactions, and verify that errors are identified and addressed in a timely manner.									
7.1.7.6 Inspect error logs to verify that errors are effectively addressed in a timely manner.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
8. TRANSACTION AUTHENTICATION AND INTEGRITY									
8.1 Transaction authentication and integrity Audit/assurance objective: Before passing transaction data between internal applications and business/operational functions (inside or outside the enterprise), transactions should be checked for proper addressing, authenticity of origin and integrity of content. Authenticity and integrity should be maintained during transmission or transport.									
8.1.1 Data exchange standards **Control: Where transactions are exchanged electronically, an agreed-upon standard of communication and mechanisms necessary for mutual authentication is established, including how transactions will be represented, the responsibilities of both parties and how exception conditions will be handled.**	AC6			X					
8.1.1.1 Inquire whether and confirm that a process has been designed to ensure that, for critical transactions, appropriate agreements have been made with counterparties that include communication and transaction presentation standards, responsibilities, authentication, and security requirements.									
8.1.1.2 Select a sample of counterparty agreements for critical transactions and verify that they are complete.									
8.1.1.3 Inquire whether and confirm that systems are designed to incorporate appropriate mechanisms for integrity, authenticity and nonrepudiation, such as adoption of a secure standard or one that is independently verified.									
8.1.1.4 Review documentation and perform a walkthrough to identify applications that are critical for transaction authenticity, integrity and nonrepudiation. For these applications, inquire whether and confirm that an appropriate mechanism for integrity, authenticity and nonrepudiation is adopted (i.e., a secure standard or one that is independently verified).									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
8.1.1.5 Perform a walkthrough of the code of a sample of applications to confirm that this specification and design are applied. Verify that these specifications have been tested with good results.									
8.1.1.6 Review error logs for transactions that failed authentication, and verify the cause.									
8.1.1.7 Perform a walkthrough of the code of a sample of applications to confirm that specifications for authenticity have been applied. Verify that these specifications have been tested with good results.									
8.1.2 Tag output **Control: Tag output from transaction-processing applications in accordance with industry standards to facilitate counterparty authentication, provide evidence of nonrepudiation and allow for content integrity verification upon receipt by the downstream application.**	AC6			X					
8.1.2.1 Obtain and inspect agreements made with counterparties for critical transactions, and ensure that the agreements specify requirements for communication and transaction presentation standards, responsibilities, and authentication and security requirements.									
8.1.2.2 Inquire whether and confirm that systems are designed to incorporate industry standard output tagging to identify authenticated information.									
8.1.2.3 Inspect application manuals and documentation for critical applications to confirm that text regarding specifications and design states that output is appropriately tagged with authentication information.									
8.1.2.4 Select a representative sample of transactions, and verify that authenticity and integrity information is correctly carried forward throughout the processing cycle.									

Audit/Assurance Program Step	COBIT Cross-reference	COSO					Reference Hyper-link	Issue Cross-reference	Comments
		Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring			
8.1.2.5 Select a sample of authentication failures to verify that the counterparty agreements operate effectively.									
8.1.3 Transaction integration with interfacing applications Control: Input received from other transaction-processing applications is analyzed to determine authenticity of origin and the maintenance of the integrity of content during transmission.	AC6			X					
8.1.3.1 Inspect manuals and documentation for critical applications to confirm that design specifications require that input be appropriately verified for authenticity.									
8.1.3.2 Inquire whether and confirm that systems are designed to identify transactions received from other processing applications, and analyze that information to determine authenticity of origin of the information and whether integrity of content was maintained during transmission.									
8.1.3.3 Review error logs for transactions that failed authentication and verify the cause.									

VII. Maturity Assessment

The maturity assessment is an opportunity for the reviewer to assess the maturity of the processes reviewed. Based on the results of audit/assurance review, and the reviewer's observations, assign a maturity level to each of the following COBIT control practices.

COBIT Control Practice	Assessed Maturity	Target Maturity	Reference Hyper-link	Comments
AC1 Source Data Preparation and Authorization 1. Design source documents in a way that they increase accuracy with which data can be recorded, control the workflow and facilitate subsequent reference checking. Where appropriate, include completeness controls in the design of the source documents. 2. Create and document procedures for preparing source data entry, and ensure that they are effectively and properly communicated to appropriate and qualified personnel. These procedures should establish and communicate required authorisation levels (input, editing, authorising, accepting and rejecting source documents). The procedures should also identify the acceptable source media for each type of transaction. 3. Ensure that the function responsible for data entry maintains a list of authorised personnel, including their signatures. 4. Ensure that all source documents include standard components and contain proper documentation (e.g., timeliness, predetermined input codes, default values) and are authorised by management. 5. Automatically assign a unique and sequential identifier (e.g., index, date and time) to every transaction. 6. Return documents that are not properly authorised or are incomplete to the submitting originators for correction, and log the fact that they have been returned. Review logs periodically to verify that corrected documents are returned by originators in a timely fashion, and to enable pattern analysis and root cause review.				

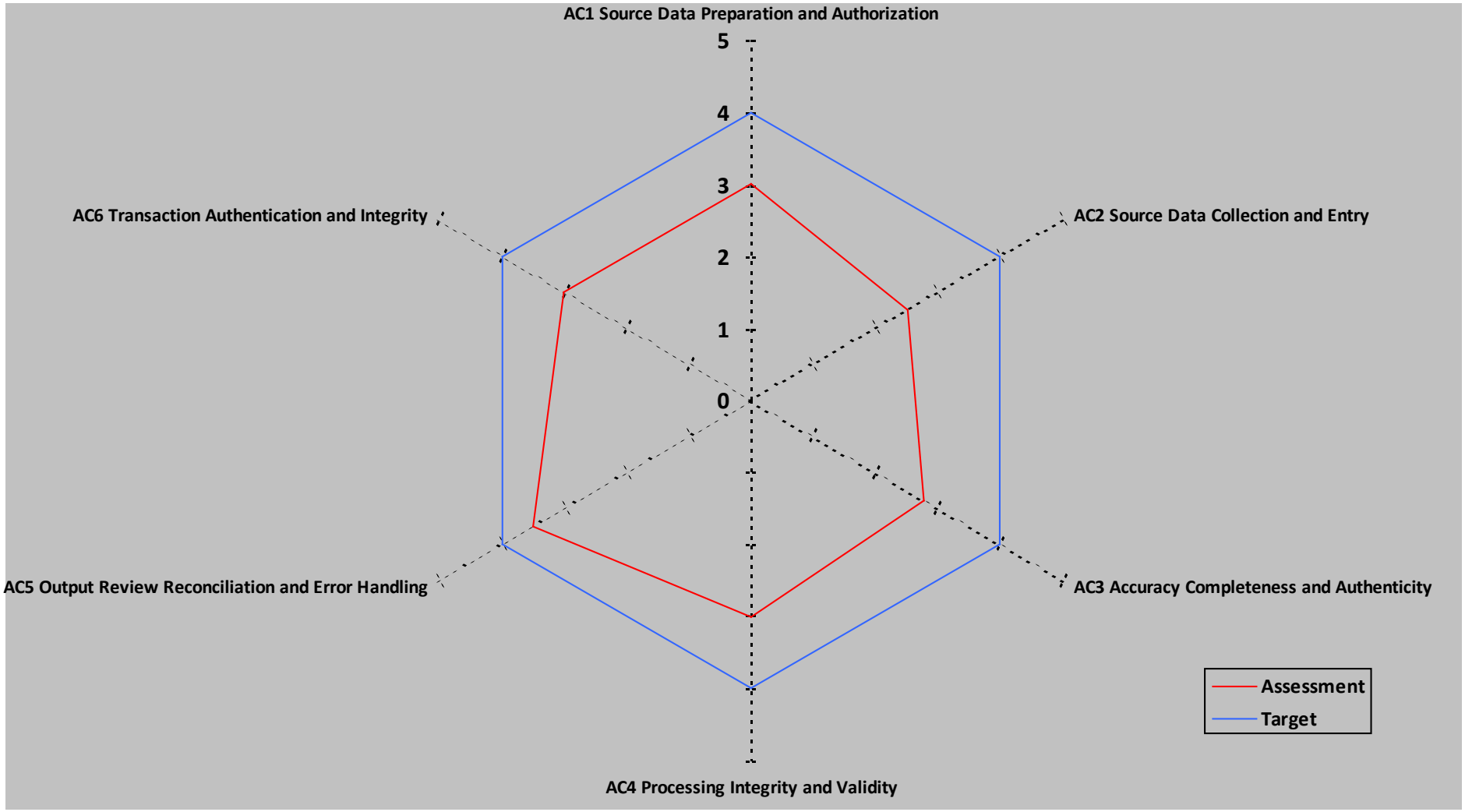
COBIT Control Practice	Assessed Maturity	Target Maturity	Reference Hyper-link	Comments
AC2 Source Data Collection and Entry 1. Define and communicate criteria for timeliness, completeness and accuracy of source documents. Establish mechanisms to ensure that data input is performed in accordance with the timeliness, accuracy and completeness criteria. 2. Use only prenumbered source documents for critical transactions. If proper sequence is a transaction requirement, identify and correct out-of-sequence source documents. If completeness is an application requirement, identify and account for missing source documents. 3. Define and communicate who can input, edit, authorise, accept and reject transactions, and override errors. Implement access controls and record supporting evidence to establish accountability in line with role and responsibility definitions. 4. Define procedures to correct errors, override errors and handle out-of-balance conditions, as well as to follow up, correct, approve and resubmit source documents andtransactions in timely manner. These procedures should consider things such as error message descriptions, override mechanisms and escalation levels. 5. Generate error messages in a timely manner as close to the point of origin as possible. The transactions should not be processed unless errors are corrected or appropriately overridden or bypassed. Errors that cannot be corrected immediately should be logged in an automated suspense log, and valid transaction processingshould continue. Error logs should be reviewed and acted upon within a specified and reasonable period of time. 6. Ensure that errors and out-of-balance reports are reviewed by appropriate personnel, followed up and corrected within a reasonable period of time, and that, where necessary, incidents are raised for more senior attention. Automated monitoring tools should be used to identify, monitor and manage errors. 7. Ensure that source documents are safe-stored (either by the business or by IT) for a sufficient period of time in line with legal, regulatory or business requirements.				

COBIT Control Practice	Assessed Maturity	Target Maturity	Reference Hyper-link	Comments
AC3 Accuracy, Completeness and Authenticity Checks 1. Ensure that transaction data are verified as close to the data entry point as possible and interactively during online sessions. Ensure that transaction data, whether people-generated, system-generated or interfaced inputs, are subject to a variety of controls to check for accuracy, completeness and validity. Wherever possible, do not stop transaction validation after the first error is found. Provide understandable error messages immediately such that they enable efficient remediation. 2. Implement controls to ensure accuracy, completeness, validity and compliancy to regulatory requirements of data input. Controls may include sequence, limit, range, validity, reasonableness, table look-ups, existence, key verification, check digit, completeness (e.g., total monetary amount, total items, total documents, hash totals), duplicate and logical relationship checks, and time edits. Validation criteria and parameters should be subject to periodic reviews and confirmation. 3. Establish access control and role and responsibility mechanisms so that only authorised persons input, modify and authorise data. 4. Define requirements for segregation of duties for entry, modification and authorisation of transaction data as well as for validation rules. Implement automated controls and role and responsibility requirements. 5. Report transactions failing validation and post them to a suspense file. Report all errors in a timely fashion, and do not delay processing of valid transactions. 6. Ensure that transactions failing edit and validation routines are subject to appropriate follow-up until errors are remediated. Ensure that information on processing failures is maintained to allow for root cause analysis and help adjust procedures and automated controls.				

COBIT Control Practice	Assessed Maturity	Target Maturity	Reference Hyper-link	Comments
AC4 Processing Integrity and Validity 1. Establish and implement mechanisms to authorise the initiation of transaction processing and to enforce that only appropriate and authorised applications and tools are used. 2. Routinely verify that processing is completely and accurately performed with automated controls, where appropriate. Controls may include checking for sequence and duplication errors, transaction/record counts, referential integrity checks, control and hash totals, range checks, and buffer overflow. 3. Ensure that transactions failing validation routines are reported and posted to a suspense file. Where a file contains valid and invalid transactions, ensure that the processing of valid transactions is not delayed and that all errors are reported in a timely fashion. Ensure that information on processing failures is kept to allow for root cause analysis and help adjust procedures and automated controls, to ensure early detection or to prevent errors. 4. Ensure that transactions failing validation routines are subject to appropriate follow-up until errors are remediated or the transaction is cancelled. 5. Ensure that the correct sequence of jobs has been documented and communicated to IT operations. Job output should include sufficient information regarding subsequent jobs to ensure that data are not inappropriately added, changed or lost during processing. 6. Verify the unique and sequential identifier to every transaction (e.g., index, date and time). 7. Maintain the audit trail of transactions processed. Include date and time of input and user identification for each online or batch transaction. For sensitive data, the listing should contain before and after images and should be checked by the business owner for accuracy and authorisation of changes made. 8. Maintain the integrity of data during unexpected interruptions in data processing with system and database utilities. Ensure that controls are in place to confirm data integrity after processing failures or after use of system or database utilities to resolve operational problems. Any changes made should be reported and approved by the business owner before they are processed. 9. Ensure that adjustments, overrides and high-value transactions are reviewed promptly in detail for appropriateness by a supervisor who does not perform data entry. 10. Reconcile file totals. For example, a parallel control file that records transaction counts or monetary value as data should be processed and then compared to master file data once transactions are posted. Identify, report and act upon out-of-balance conditions.				

COBIT Control Practice	Assessed Maturity	Target Maturity	Reference Hyper-link	Comments
AC5 Output Review, Reconciliation and Error Handling 1. When handling and retaining output from IT applications, follow defined procedures and consider privacy and security requirements. Define, communicate and follow procedures for the distribution of output. 2. At appropriate intervals, take a physical inventory of all sensitive output, such as negotiable instruments, and compare it with inventory records. Create procedures with audit trails to account for all exceptions and rejections of sensitive output documents. 3. Match control totals in the header and/or trailer records of the output to balance with the control totals produced by the system at data entry to ensure completeness and accuracy of processing. If out-of-balance control totals exist, report them to the appropriate level of management. 4. Validate completeness and accuracy of processing before other operations are performed. If electronic output is reused, ensure that validation has occurred prior to subsequent uses. 5. Define and implement procedures to ensure that the business owners review the final output for reasonableness, accuracy and completeness, and that output is handled in line with the applicable confidentiality classification. Report potential errors, log them in an automated, centralised logging facility, and address errors in a timely manner. 6. If the application produces sensitive output, define who can receive it, label the output so it is recognisable by people and machines, and implement distribution accordingly. Where necessary, send it to special access-controlled output devices.				
AC6 Transaction Authentication and Integrity 1. Where transactions are exchanged electronically, establish an agreed-upon standard of communication and mechanisms necessary for mutual authentication, including how transactions will be represented, the responsibilities of both parties and how exception conditions will be handled. 2. Tag output from transaction processing applications in accordance with industry standards to facilitate counterparty authentication, provide evidence of non-repudiation, and allow for content integrity verification upon receipt by the downstream application. 3. Analyse input received from other transaction processing applications to determine authenticity of origin and the maintenance of the integrity of content during transmission.				

VIII. Assessment Maturity vs. Target Maturity



IT Audit Basics

Auditing Applications, Part 1

Tommie W. Singleton, Ph.D., CISA, CGEIT, CITP, CPA, is an associate professor of information systems (IS) at Columbus State University (Columbus, Georgia, USA). Prior to obtaining his doctorate in accountancy from the University of Mississippi (USA) in 1995, Singleton was president of a small, value-added dealer of accounting using microcomputers. Singleton is also a scholar-in-residence for IT audit and forensic accounting at Carr Riggs & Ingram, a large regional public accounting firm in the southeastern US. In 1999, the Alabama Society of CPAs awarded Singleton the 1998–1999 Innovative User of Technology Award. His articles on fraud, IT/IS, IT auditing and IT governance have appeared in numerous publications.

Auditing applications is a common type of audit for medium and large companies, especially when some of the applications are developed in-house. There are some basic principles of auditing applications that IT auditors need to know and understand. This two-part article describes one framework for performing effective audits of applications.

A FRAMEWORK

A process-oriented framework includes steps similar to the following:

- Plan the audit.
- Determine audit objectives.
- Map systems and data flows.
- Identify key controls.
- Understand application's functionality.
- Perform applicable tests.
- Avoid/consider complications.
- Include financial assertions.
- Consider beneficial tools.
- Complete the report.

Some of the steps, such as mapping systems and data flows, are comprehensive. While mapping should occur near the beginning of the audit, it has a role in most of the other steps. Others, such as financial assertions, may or may not apply. However, the noted framework represents a fair body of steps that should allow for the effective audit of applications.

> "The noted framework represents a fair body of steps that should allow for the effective audit of applications."

The remainder of this article details the first three steps: planning, determining objectives and mapping. The remaining steps will be detailed in this space in volume 4, 2012.

PLAN THE AUDIT

Planning the audit includes the consideration of all the relevant factors that frame the purpose of the audit. This consideration is necessary to properly plan the audit.

Consideration of Purpose

One of the key drivers of an application audit throughout the process is the conditions or circumstances by which the audit arose. That is, what is driving the need for the audit? Is it a regular audit plan? Is it an *ad hoc* audit? The need is usually directly associated with the primary objective of the audit. For example, if management wants to gain assurance that a new application is performing as designed, that fact will drive the audit objectives and plan.

Consideration of Risk

A second key factor and driver is consideration of risk associated with a particular audit, given the purpose of the audit that was determined previously. The IT auditor, or the audit team, needs to identify risk associated with the application and its associated data, sources, infrastructure and systems. To follow the previous example, possible risk scenarios include a lack of functionality (i.e., does not actually meet the information requirements), errors and/or bugs, an inability to properly integrate/interface with other applications or systems, data errors, and other similar risk.

Naturally, once the risk scenarios are properly identified, the IT auditor needs to assess the impact on the audit objectives, audit plan, audit scope and audit procedures. For instance, if lack of functionality is a risk, the IT auditor should examine the original information requirements, review tests, review a user acceptance document (if one exists), test the application and perform other similar procedures.

Consideration of the Control Environment

Usually, the audit plan should take into account the control environment surrounding the application, within the context of the audit purpose. If the primary purpose of the audit is auditing proper

functionality, the controls might be application development controls or systems development life cycle (SDLC) controls. In particular, controls for testing the application are important.

Consideration of Pre/Postimplementation
Sometimes the application audit involves a preimplementation application, but most likely, it will be a postimplementation situation. A preaudit tends to involve proprietary objectives, scope and procedures that are peculiar to that application and purpose. Postaudits often follow a general set of objectives (see the Determine Audit Objectives section).

Consideration of Scope
A very important consideration in planning is to establish the boundaries of scope. That means determining the relevant technologies and controls associated with auditing the applications, such as:
- Interfaces to other applications
- Source systems
- Target/destination systems
- Infrastructure or components thereof
- Databases
- Staging area/testing facility

Consideration of Competencies
As in all audits, one of the leaders or managers of the audit team will need to assess the competencies of the staff against the needs of the audit. For example, if the interface involves Oracle, it is possible that an expert in Oracle will be needed to properly audit the application.

DETERMINE AUDIT OBJECTIVES

The objectives are somewhat tied to the consideration of pre/postimplementation. As stated previously, the objectives tend to be proprietary for preimplementation applications. The same could be true for certain purposes. For others, the objective tends to be one of those that are typical for audits:

> "Mapping is one of the most effectual tools that the IT auditor has for any IT audit."

- Efficiency (related to development cost, operational performance, etc.)
- Effectiveness (related to meeting information requirements/functionality, the original authorization purpose, integration with other IT, operational performance, etc.)
- Compliance (laws and regulations, contractual, etc.)
- Alerts (if alerts are involved with the application)
- Financial reporting implications

MAP SYSTEMS AND DATA FLOWS

Mapping is one of the most effectual tools that the IT auditor has for any IT audit. In auditing applications, it is important to properly scope other IT that either affects or is affected by the application. Experts believe that mapping can assist the IT auditor in gaining a thorough understanding of the relevant technologies, the process, the controls and how they all fit together. It also empowers the IT auditor to best perform the steps in this framework from planning to reporting—that is, it has a comprehensive impact on the quality of the IT audit.

Items that should be considered in properly mapping the application include, among others:

- Relevant IT components (description)
- The business owners or business lines
- Change management policies and procedures
- The role and impact of vendors
- Business processes
- Controls
- Access and security administration

These factors can guide the IT auditor in creating the map, determining what should be on the map or determining what columns should be used in a spreadsheet that depicts the mapping. **Figure 1** shows one way to map the auditing of an application.

Documenting and mapping risk may involve items such as the risk, risk area, objective, reference, procedures, audit days, percent done, days to complete, scope of systems and notes. **Figure 2** shows a spreadsheet document that may be helpful in mapping risk, and demonstrates how such a map may be useful throughout the audit and may assist in managing the audit.

IT auditors need to map the process and data flow using conventional data flow diagrams (DFD), use cases, systems flowcharts or Unified Modeling Language (UML). A nonconventional diagram may serve as a better model for depicting processes and data flows. For example, the matrix in **figure 3** may serve as a better model because it incorporates the time/delivery as well as systems, processes and data flows.

The particular schematic shown in **figure 3** depicts controls in such a way as to make them clear and understandable, e.g., the automatic reconciliation, error-checking system (IT-dependent) and manual review of CRM data before the target data are uploaded as a control in the flow of data and processes.

This process/data flow framework might be more effective if it is presented using the system model vs. the timeline and process dimensions. Inputs include the source data, such as the source data for the middleware application. They

Figure 3—Mapping Processes and Data Flows

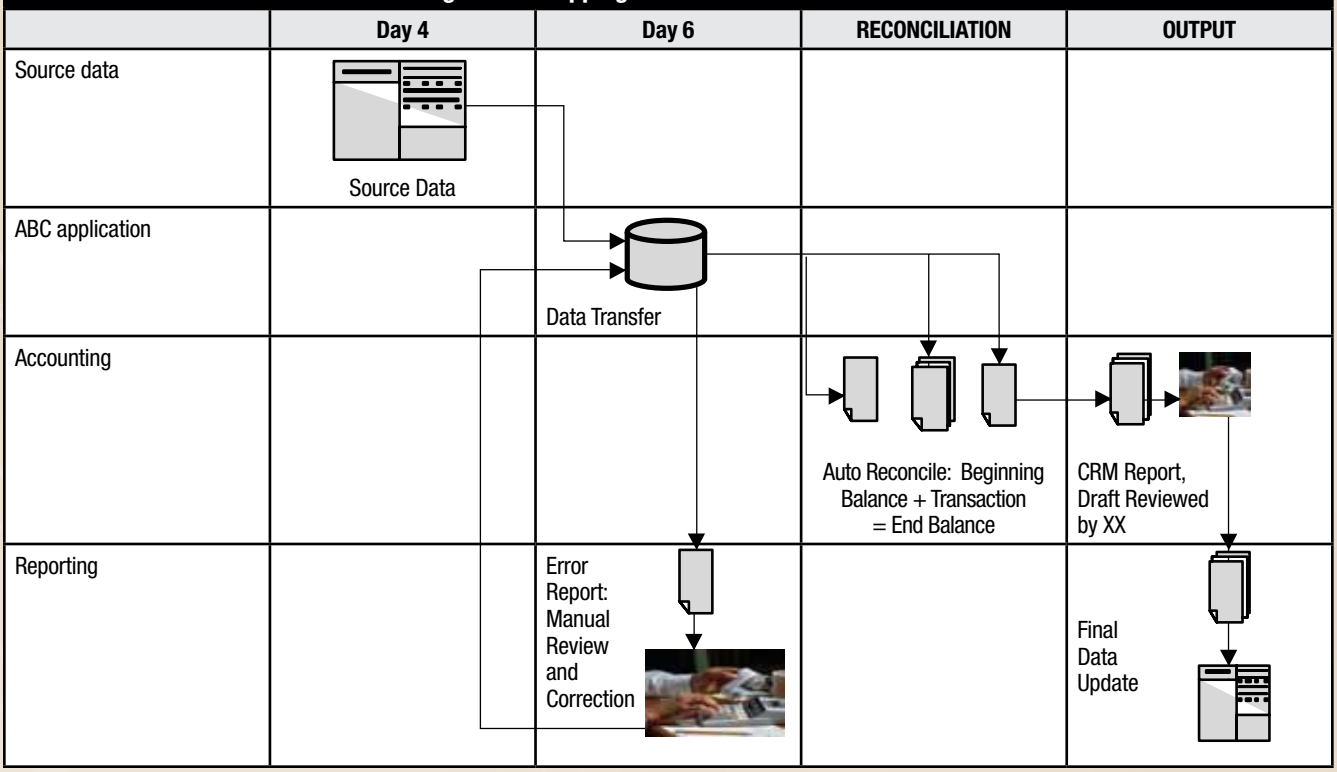


Figure 1—Mapping Example Using Spreadsheet, Part I					
IT	**Description**	**O/S**	**DBMS**	**DB Server**	**Data Location**
ABC App	Middleware designed to ...	N.A.	N.A.	XYZ	Birmingham
DEF App	CRM, target ...	Z/OS	DB2	Z mainframe	Nashville

Figure 1— Mapping Example Using Spreadsheet, Part II					
Developed	**Maintained**	**Owner**	**Access Admin**	**Change Control**	**Notes**
In-house	In-house	Sue	Active directory ...	Controls include ...	
Vendor	Vendor, SOC1/2 available	John	Security admin ...	Vendor ...	

Figure 2—Documenting and Mapping Risks, Part I					
Ref.	**Risk**	**Risk Area**	**Objective**	**W/P Ref.**	**Procedures**
1	Invalid, inaccurate or incomplete data may cause errors in reports or accounting.	Data integrity	Evaluate data integrity checks and controls between inputs and outputs.	CO.1.1	
2	Unauthorized or unintended changes to middleware may cause errors in reports/accounting.	Change management	Evaluate changes to the application for appropriate approvals, tests and segregation of duties (SoD).	CO.1.2	
3	Unauthorized access may cause unauthorized changes to middleware or target data, causing errors in reports/accounting.	Security	Evaluate logical access controls to the application and its folder.	CO.1.3	
4	Invalid, inaccurate or incomplete processing may cause errors in reports/accounting.	Operations	Evaluate processing and documentation for appropriate controls on development and support, and error identification and resolution.	CO.1.4	

Figure 2—Documenting and Mapping Risks, Part II					
Ref.	**Audit Days**	**Percent Done**	**Days to Complete**	**Scope of Systems**	**Notes**
1	0.5	100%	0	Middleware, stored procedures, views, CRM, DB2	
2	1.5	33%	1	Middleware	
3	1.0	0%	1	Active directory, middleware	
4	2.0	0%	2	INPUT: Source file PROCESS: Middleware OUTPUT: Target file/DB2, error report	

FIGURE 2—Documenting and Mapping Risks, Part III				
Ref.	**Inherent Risk**	**Control Risk**	**Assessed Risk**	**Notes**
1	High	Medium	Medium–High	To date, facts are ...
2	Medium	Low	Low	
3	High	Medium	Medium–High	
4	Medium	Low	Low–Medium	

also include intermediate data. Sources include the internal databases (DBs) and external providers of data—something not uncommon in data warehouses (DWs), for example.

The processing segment includes the processing function of the application (see **figure 3**, including automatic reconciliations and the error detection/correction routine). It also includes any process documents being created for the process functions. Certain processes are similar to those associated with DWs, such as ETL (extract, transform and load), which basically describe the process data go through to get into the DW from various sources. The ABC application example in **figure 3** is fairly consistent with ETL. Processing logic is of particular interest in auditing applications, as they are usually a chief component of data integrity and reliability.

Outputs include reports, screen information and other printed documents. Outputs also include the need to evaluate tools and templates being used to create those reports and screens.

CONCLUSION

This article explains the first portion of the framework. One of the key beneficial steps in this part of the application audit is to generate thorough and accurate maps or diagrams.

In the next issue (volume 4, 2012), the remaining steps of the framework will be explained. It is in these final steps that the bulk of the actual procedures and tests occur.

ADDITIONAL RESOURCES

Bitterli, Peter R., *et al*; "Guide to Audit of IT Applications," ISACA Switzerland Chapter, 2010

ERP Seminars, "Auditing Application Controls," 2008, *www.auditnet.org/docs/Auditing_Application_Controls.pdf*

SANS Institute, "The Application Audit Process," InfoSec Reading Room, *www.sans.org/reading_room/whitepapers/auditing/application-audit-process-guide-information-security-professionals_1534*

Auditing Applications, Part 2

Tommie W. Singleton, Ph.D., CISA, CGEIT, CITP, CPA, is an associate professor of information systems (IS) at Columbus State University (Columbus, Georgia, USA). Prior to obtaining his doctorate in accountancy from the University of Mississippi (USA) in 1995, Singleton was president of a small, value-added dealer of accounting using microcomputers. Singleton is also a scholar-in-residence for IT audit and forensic accounting at Carr Riggs & Ingram, a large regional public accounting firm in the southeastern US. In 1999, the Alabama Society of CPAs awarded Singleton the 1998–1999 Innovative User of Technology Award. His articles on fraud, IT/IS, IT auditing and IT governance have appeared in numerous publications.

This is the second part of a two-part article on a process-oriented framework for auditing applications. Part 1 (volume 3, 2012) detailed the first three steps: planning, determining objectives and mapping. The remaining steps are described here. The full framework includes the following steps:

- Plan the audit.
- Determine audit objectives.
- Map systems and data flows.
- Identify key controls.
- Understand application's functionality.
- Perform applicable tests.
- Avoid/consider complications.
- Include financial assertions.
- Consider beneficial tools.
- Complete the report.

IDENTIFY KEY CONTROLS

When evaluating the relevant controls, the IT auditor will want to distinguish between customized controls and those contained in commercial off-the-shelf software (COTS). For custom-built controls, inquiry is a good place to begin the evaluation. One of the key questions is to ask management the specific nature of controls expertise being injected into the application development process. That is, who or what group is providing the expertise that makes sure adequate controls are embedded in new applications? How is that goal achieved? And, finally, the IT auditor should make sure those controls have been properly documented and tested.

For COTS, the IT auditor would probably start with a walk-through to determine what controls are actually in the application and how they function. A walk-through would involve following transactions or processes step by step, keystroke by keystroke, with the data-entry person explaining what they are doing and why. Such a process should enable the IT auditor to gain a general understanding of the applications' controls, the adequacy of controls and the nature of them (i.e., effectiveness). This walk-through is especially necessary the first time an application is used by the entity.

Also for COTS, the IT auditor should establish a baseline of controls—tests to understand reliability and effectiveness. These would include configurations for applications, such as SAP and Oracle.

For COTS, the IT auditor needs to determine the responsibility of vendors involved. That goal is why **figure 1**, which is part of the mapping step and detailed in part 1 of this article, has information about the vendor and the nature of maintenance of the application. When a problem occurs with the application, management needs to have assurance of exactly who to rely upon to solve the problem. Obviously, vendor management practices apply.

Figure 1—Mapping Example Using Spreadsheet, Part I

IT	Description	O/S	DBMS	DB Server	Data Location
ABC App	Middleware designed to ...	N.A.	N.A.	XYZ	Birmingham
DEF App	CRM, target ...	Z/OS	DB2	Z mainframe	Nashville

Figure 1— Mapping Example Using Spreadsheet, Part II

Developed	Maintained	Owner	Access Admin	Change Control	Notes
In-house	In-house	Sue Z.Q.	Active directory ...	Controls include ...	Yada ...
Vendor	Vendor, SOC1/2 available	John D.	Security admin ...	Vendor ...	Yada ...

The types of controls can be assessed by using the typical systems model: input, process and output. Input controls include:

- Access security
- Logical segregation of duties (SoD)
- Data validation
- Data integrity
- Coding
- Input error correction
- Batch controls (where applicable)

Typical process controls include:

- The level of automation (e.g., fully automated, IT-dependent, fully manual)
- Job scheduler dependencies (for job processing)
- Job scheduler monitoring
- Auto calculations
- Auto reconciliations
- Auto notifications

Typical output controls include:

- Reconciliations
- Reviews
- Approvals
- Error detection/error reports or lists
- Control over physical reports (ancillary control)

UNDERSTAND APPLICATION'S FUNCTIONALITY

Normally, auditing functionality is a chief audit goal. The procedures involve verifying the operational functionality, which should be described in the information requirements in the application development (AppDev) process. Besides reviewing the authorization document for the application, the IT auditor should review the end-user acceptance report—if one exists. If one does not exist, that says something about the adequacy of control procedures for AppDev: They are lacking a best practice.

Some typical objectives are related to the purpose of the application. When testing the application, consideration is given to the various scenarios needed to properly test the application. If the purpose of the application leads to a dichotomous outcome, a test of one might suffice (yes or no, approved or not approved, etc.). But, if the application is an update to payroll processing, for example, there are a large number of scenarios to consider to test all of the various combinations of factors that go into calculating payroll taxes. The same is likely to be true of testing security and access controls.

Some special considerations include at least a couple of things that the typical end user and business manager tend to overlook in the information-requirements-gathering stage: security and proper scope of data captured. The proper level of security is obviously a critical success factor in AppDev and, thus, needs to be evaluated. Typically, users and managers do not fully grasp the scope of data that need to be captured at the point of events and transactions. This fact is especially important if the entity has any plans to ever employ, for example, business intelligence (BI) or business analytics. A richness of data becomes necessary to "slice and dice" data with data mining tools to gain the maximum benefit of the data in employing BI.

> "The problem can usually be traced back to an improper testing phase."

Operational controls might be in scope, depending on the consideration of purpose. The same is true for financial reporting controls.

Using the system model is likely to make analysis and testing of the application's functionality easier and more complete.

PERFORM APPLICABLE TESTS

When an application fails to perform correctly, when there are errors created, when processes embedded in the application fail to work properly, the problem can usually be traced back to an improper testing phase. Testing the application is more than just performing a single test.

The best practice for testing involves multiple levels of testing. First, the application is tested stand-alone. That is usually done by a senior programmer or analyst who is chiefly responsible for the AppDev project. Then, the application goes through some quality control in the IT department. That is, it is independently tested by some expert in the IT department.

Next, the application is tested by actual users. Often, these end users are involved in a cyclical manner as the application is being developed. But, at a minimum, one or more end users should test the application once it is fully developed in order to determine its functionality, completeness, accuracy and efficiency. After completion, it is customary to have those end

users sign an end-user acceptance report, documenting the results of the test.

Then, the application is tested in conjunction with other applications in the same module, cycle, or class of transactions. That often requires a more robust environment than earlier testing of the application as stand-alone. A staging area has become one of the best ways to perform this test, where a simulator is created of the entity's infrastructure, applications, systems and databases. But, that is not the end either. The application should be tested in the context of the enterprise system, with all of the data transfers and interfacing that goes on in actual IT operations. That process in particular needs a staging area.

AVOID/CONSIDER COMPLICATIONS

There are a number of complications that are inherently risky and, thus, need consideration during the application audit. First, proprietary (custom-built) applications have a high inherent risk. This fact affects the objectives, planning, controls and risks steps.

If a data warehouse (DW) is involved, there is a relatively high inherent risk. Almost universally, when a DW is initially implemented, data being imported into the DW have a high risk due to, for example, inconsistencies in data (same field with different names), missing data and bad data (i.e., errors). Thus, when data are extracted from the transaction processing systems (TPS), care should be taken in mapping the data and using the ETL (extract, transform and load) process to identify and correct the previously mentioned data anomalies.

For the ongoing DW, data owners could, for example, change field names and add fields, and if change controls are not effective, the data cannot pass through the next ETL process successfully. Thus, change management controls for DW are highly important. The same is true for other similar integration functions.

Some distinction should be made between two types of risk with DWs. First, there is process integrity. This integrity is about whether the processing is successful. Does the application do what it should do regarding its processing function? Second, there is data integrity or data quality, which involves the reliability and integrity of the data being processed, transferred and recorded. Were the data entered valid? Are the source data valid, accurate and complete? Was the data transfer from source to target completed effectively, with no errors?

INCLUDE FINANCIAL ASSERTIONS

When financial reporting is in scope, the application needs to address the primary assertions of the account balance, class of transactions or disclosure. Does the application include the appropriate controls related to the primary assertions of the end result account balance or class of transactions? The IT auditor, if applicable, should test the application against the appropriate assertion(s). For instance, if the assertion is accuracy, testing might include things such as:

- Data entry validation controls
- Automatic calculations
- Automatic reconciliations

Existence assertions might be tested for data entry validation controls. Completeness assertions might be tested for job/batch processing controls or reconciliations.

CONSIDER BENEFICIAL TOOLS

Some useful tools for testing applications are computer-assisted audit techniques (CAATs) and ETL. CAATs are helpful in conducting procedures, such as data mining, that examine results in data from posting by the application to determine if the application's controls are working, if the application is working properly and if the application produced any errors. CAATs are also useful in analyzing data for objectives such as data integrity.

ETL is useful in detecting flawed data that can be traced back to the application that produced it and, thus, provide the opportunity to correct the flaw in the application.

Tests of Controls

Some possible tests of controls include:

- Reconciliation
- Recalculation
- Duplication
- Gaps

An example of reconciliation might be verifying the customer ID in the transaction file against the customer ID in the master file. That is, do the customers in the transaction file actually exist in the authorized customer list? Another example is recalculating where the IT auditor might extend the inventory database to see if the total inventory costs match the control total in the general ledger (i.e., the account balance). Duplicates and gaps are useful in detecting errors in data processing.

CAATs

CAATs could be used to reperform automatic calculations or automatic reconciliations.

Data Mining

Data mining could be used to support the audit objectives. In particular, it is useful in conducting IT-related substantive procedures, such as testing approvals or classification errors related to proper codes.

Purchase Order Thresholds

Any time an application involves a threshold where initial/additional approval is needed, CAATs are useful in determining if that control is operating effectively. For instance, if the application is either purchase orders or disbursements, and if purchases and payments are one-to-one (i.e., disbursements are paid by invoice and not statements), a simple test of extracting all disbursements over the threshold against the data file containing the approval (e.g., purchase order file) would expose any exceptions to the control/threshold. This also has the added benefit of fraud detection if someone is frustrating the threshold deliberately to perpetrate a fraud.

Inventory Anomalies

If the app is recording receipt of inventory, CAATs could be used to show whether the application allows zero or negative quantities to be recorded. Obviously that constitutes an error (anomaly) and, thus, the application would be seen as containing a control deficiency and in need of either a change in the application or a compensating control. There are other applications that could make use of this test.

Second, if the application is a file maintenance program, the system would (hopefully) minimize situations in which an employee could make undocumented changes to the inventory data that lead to discrepancies and data errors. Controls are needed to prevent this anomaly. For example, use of logical SoD could limit employees who can make file maintenance changes. Also, the application/system could track changes by recording data before the change and after the change. Without such tracking, employees could falsify changes and create errors or fraud in the data. Data mining could spot differences in account balances by taking the beginning balance, adding up all transactions and verifying the sum against the ending balance. A similar situation exists for any file maintenance application.

> "The successful audit of applications is dependent on a reliable approach."

COMPLETE THE REPORT

Obviously all audits end with some kind of report. Those reports are generally proprietary in format. But, they tend to include the audit objectives, tests conducted, results of tests (usually) and recommendations.

CONCLUSION

The successful audit of applications is dependent on a reliable approach. This two-part article demonstrates a reliable approach and some tools that should be helpful in conducting the audit, especially mapping and CAATs.

ADDITIONAL RESOURCES

Bitterli, Peter R., *et al*; "Guide to Audit of IT Applications," ISACA Switzerland Chapter, 2010

ERP Seminars, "Auditing Application Controls," 2008, *www.auditnet.org/docs/Auditing_Application_Controls.pdf*

SANS Institute, "The Application Audit Process," InfoSec Reading Room, *www.sans.org/reading_room/whitepapers/auditing/application-audit-process-guide-information-security-professionals_1534*