GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

Auditing Application Controls

The Institute of
Internal Auditors

GTAG – Partners

AICPA – American Institute of
Certified Public Accountants
www.aicpa.org

CIS – Center for Internet Security
www.cisecurity.org

CMU/SEI – Carnegie-Mellon University
Software Engineering Institute
www.cmu.edu

ISSA – Information Systems Security Association
www.issa.org

ITPI – IT Process Institute
www.itpi.org

NACD – National Association of
Corporate Directors
www.nacd.org

SANS Institute
www.sans.org

Auditing Application Controls

Authors

Christine Bellino, Jefferson Wells

Steve Hunt, Enterprise Controls Consulting LP

July 2007

The IIA publishes this document for informational and educational purposes. This document is intended to provide information, but is not a substitute for legal or accounting advice. The IIA does not provide such advice and makes no warranty as to any legal or accounting results through its publication of this document. When legal or accounting issues arise, professional assistance should be sought and retained.

GTAG – Table of Contents

Over the last several years, organizations around the world have spent billions of dollars upgrading or installing new business application systems for different reasons, ranging from tactical goals, such as year 2000 compliance, to strategic activities, such as using technology as an enabler of company differentiation in the marketplace. An application or application system is a type of software that enables users to perform tasks by employing a computer's capabilities directly. According to The Institute of Internal Auditors' (IIA's) *GTAG 4: Management of IT Auditing*, these types of systems can be classified as either transactional applications or support applications.

Transactional applications process organizationwide data by:

- Recording the value of business transactions in terms of debits and credits.
- Serving as repositories for financial, operational, and regulatory data.
- Enabling various forms of financial and managerial reporting, including the processing of sales orders, customer invoices, vendor invoices, and journal entries.

Examples of transactional processing systems include SAP R/3, PeopleSoft, and Oracle Financials, which are often referred to as enterprise resource planning (ERP) systems, as well as countless other non-ERP examples. These systems process transactions based on programmed logic and, in many cases, in addition to configurable tables that store unique organizational business and processing rules.

On the other hand, support applications are specialized software programs that facilitate business activities. Examples include e-mail programs, fax software, document imaging software, and design software. However, these applications generally do not process transactions.[1]

As with any technology that is used to support business processes, transactional and support applications may pose risks to the organization, which stem from the inherent nature of the technology and how the system is configured, managed, and used by employees. With respect to transactional processing systems, risks can have a negative impact on the integrity, completeness, timeliness, and availability of financial or operational data if they are not mitigated appropriately. Furthermore, the business processes themselves will have some element of inherent risk, regardless of the application used to support them. As a result of these application technology and business process risks, many organizations use a mix of automated and manual controls to manage these risks in transactional and support applications. However, the degree of successful risk management is directly dependent upon:

- The organization's risk appetite or tolerance.
- The thoroughness of the risk assessment related to the application.
- The affected business processes.
- The effectiveness of general information technology (IT) controls.
- The design and ongoing extent of operating effectiveness of the control activities.

One of the most cost-effective and efficient approaches organizations use to manage these risks is through the use of controls that are inherent or embedded (e.g., three-way match on account, payable invoices) into transactional and support applications as well as controls that are configurable (e.g., accounts payables invoice tolerances). These types of controls are generally referred to as application controls — those controls that pertain to the scope of individual business processes or application systems, including data edits, separation of business functions, balancing of processing totals, transaction logging, and error reporting.[2]

It is also important for chief audit executives (CAEs) and their staff to understand the difference between application controls and IT general controls (ITGCs). The ITGCs apply to all organizationwide system components, processes, and data,[3] while application controls are specific to a program or system supporting a particular business process. The "Application Controls Versus IT General Controls" section will go into greater detail about these two types of controls.

Due to the importance of application controls to risk management strategies, CAEs and their teams need to develop and execute audits of application controls on a periodic basis to determine if they are designed appropriately and operating effectively. Therefore, the objective of this GTAG is to provide CAEs with information on:

1. What application controls are and their benefits.
2. The role of internal auditors.
3. How to perform a risk assessment.
4. Application control review scoping.
5. Application review approaches and other considerations.
6. Common application controls, suggested tests, and a sample review program.

To further assist CAEs or other individuals who use this guide, we also have included a list of common application controls, a sample audit plan, and a few application control review tools.

[1] *GTAG 4: Management of IT Auditing*, p. 5.

[2] *GTAG 1: Information Technology Controls*, p. 3.

[3] *GTAG 1: Information Technology Controls*, p. 3.

Defining Application Controls

Application controls are those controls that pertain to the scope of individual business processes or application systems, including data edits, separation of business functions, balancing of processing totals, transaction logging, and error reporting. Therefore, the objective of application controls is to ensure that:

- Input data is accurate, complete, authorized, and correct.
- Data is processed as intended in an acceptable time period.
- Data stored is accurate and complete.
- Outputs are accurate and complete.
- A record is maintained to track the process of data from input to storage and to the eventual output.[4]

Several types of application controls exist. These include:

- **Input Controls** – These controls are used mainly to check the integrity of data entered into a business application, whether the data is entered directly by staff, remotely by a business partner, or through a Web-enabled application or interface. Data input is checked to ensure that is remains within specified parameters.
- **Processing Controls** – These controls provide an automated means to ensure processing is complete, accurate, and authorized.
- **Output Controls** – These controls address what is done with the data and should compare output results with the intended result by checking the output against the input.
- **Integrity Controls** – These controls monitor data being processed and in storage to ensure it remains consistent and correct.
- **Management Trail** – Processing history controls, often referred to as an audit trail, enables management to identify the transactions and events they record by tracking transactions from their source to their output and by tracing backward. These controls also monitor the effectiveness of other controls and identify errors as close as possible to their sources.[5]

Additional application control components include whether they are preventive or detective. Although both control types operate within an application based on programmed or configurable system logic, preventive controls perform as the name implies — that is, they prevent an error from occurring within an application. An example of a preventive control is an input data validation routine. The routine checks to make sure that the data entered is consistent with the associated program logic and only allows correct data to be saved. Otherwise, incorrect or invalid data is rejected at the time of data entry.

Detective controls also perform as the name implies — that is, they detect errors based on a predefined program logic. An example of a detective control is one that discovers a favorable or unfavorable variation between a vendor invoice price and the purchase order price.

Application controls, particularly those that are detective in nature, are also used to support manual controls used in the environment. Most notably, the data or results of a detective control can be used to support a monitoring control. For instance, the detective control described in the previous paragraph can note any purchase price variances by using a program to list these exceptions on a report. Management's review of these exceptions can then be considered a monitoring control.

Application Controls Versus Information Technology General Controls (ITGCs)

It is important for CAEs and their staff to understand the relationship and difference between application controls and ITGCs. Otherwise, an application control review may not be scoped appropriately, thereby impacting the quality of the audit and its coverage.

ITGCs apply to all systems components, processes, and data present in an organization or systems environment.[6] The objectives of these controls are to ensure the appropriate development and implementation of applications, as well as the integrity of program and data files and of computer operations.[7] The most common ITGCs are:

- Logical access controls over infrastructure, applications, and data.
- System development life cycle controls.
- Program change management controls.
- Physical security controls over the data center.
- System and data backup and recovery controls.
- Computer operation controls.

Because application controls relate to the transactions and data pertaining to each computer-based application system, they are specific to each individual application. The objectives of application controls are to ensure the completeness and accuracy of records, as well as the validity of the entries made to each record, as the result of program processing.[8] In other words, application controls are specific to a given application, whereas ITGCs are not. Common application control activities include:

- Determining whether sales orders are processed within the parameters of customer credit limits.

[4, 5] GTAG 1: *Information Technology Controls*, p. 8.

[6] GTAG 1: *Information Technology Controls*, p. 3

[7] ISACA, IS Auditing Guideline — Application Systems Review, Document G14, p. 3.

[8] ISACA, IS Auditing Guideline — Application Systems Review, Document G14, p. 3.

- Making sure goods and services are only procured with an approved purchase order.
- Monitoring for segregation of duties based on defined job responsibilities.
- Identifying that received goods are accrued upon receipt.
- Ensuring fixed-asset depreciation is recorded accurately in the appropriate accounting period.
- Determining whether there is a three-way match between the purchase order, receiver, and vendor invoice.

In addition, it is important for CAEs to note the degree to which management can rely on application controls for risk management. This reliance depends directly on the design and operating effectiveness of the ITGCs. In other words, if these controls are not implemented or operating effectively, the organization may not be able to rely on its application controls to manage risk. For example, if the ITGCs that monitor program changes are not effective, then unauthorized, unapproved, and untested program changes can be introduced to the production environment, thereby compromising the overall integrity of the application controls.

Complex Versus Non-complex IT Environments

The sophistication or complexity of an organization's IT environment has a direct effect on the overall risk profile and related management strategies available. Organizations that have a more complex IT infrastructure are marked by the following characteristics:

- Changes to existing applications, databases, and systems.
- The creation of source code for critical in-house developed software.
- Customized pre-packaged software that is adapted to the organization's processing needs.
- Deployment of pre-packaged applications, changes, and code into production.[9]

On the other hand, organizations that have a less complex IT environment are marked by the following characteristics:

- Few changes to the existing IT environment.
- Implementation of a pre-packaged financial application with no significant modifications that is completed in the current year.
- User-configurable options that do not significantly alter the application's functioning.
- The lack of IT development projects.[10]

As these differences point out, there is a direct correlation between the complexity of transactional and support applications and the availability, use, and reliance on inherent and configurable application controls. In other words, a less complex IT infrastructure may not offer as many inherent or configurable application controls for risk management. Hence, the degree of transactional and support application complexity will drive the scoping, implementation, level of effort, and knowledge required to execute an application control review, as well as the degree to which internal auditors can assist in a consulting capacity.

Benefits of Relying on Application Controls

Relying on application controls can yield multiple benefits. Following is a description of key benefits.

Reliability

Application controls are more reliable than manual controls when evaluating the potential for control errors due to human intervention. Once an application control is established, and there is little change to the application, database, or supporting technology, the organization can rely on the application control until a change occurs.

Furthermore, an application control will continue to operate effectively if the ITGCs that have a direct impact on its programmatic nature are operating effectively as well. This is particularly true of controls pertaining to program changes and segregation of duties for IT administrators. As a result, the auditor will be able to test the control once and not multiple times during the testing period.

Benchmarking

Appendix B of the U. S. Public Company Accounting Oversight Board's adopted Auditing Standard, An Audit of Internal Control Over Financial Reporting That is Integrated With an Audit of Financial Statements, states that benchmarking of application controls can be used because these controls are generally not subject to breakdowns due to human failure. If general controls that are used to monitor program changes, access to programs, and computer operations are effective and continue to be tested on a regular basis, the auditor can conclude that the application control is effective without having to repeat the previous year's control test. This is especially true if the auditor verifies that the application control has not changed since the auditor last tested the application control.[11]

In addition, the nature and extent of the evidence the auditor should obtain to verify the control has not changed may vary, based on circumstances such as the strength of the organization's program change controls.[12] As a result, when

[9] The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's), *Internal Control Over Financial Reporting – Guidance for Smaller Companies*, Vol. III, p. 61.

[10] The Committee of Sponsoring Organizations of the Treadway Commission's (COSO's), *Internal Control over Financial Reporting – Guidance for Smaller Companies*, Vol. III, p. 56.

[11] Public Company Accounting Oversight Board, Proposed Auditing Standard, An Audit of Internal Control Over Financial Reporting That is Integrated With an Audit of Financial Statements, p. A1-57.

using a benchmarking strategy for a particular control, the auditor should consider the effect of related files, tables, data, and parameters on the application control's functionality. For example, an application that calculates interest income might depend on the continued integrity of a rate table that is used by the automated calculation.[13]

The auditor should evaluate the appropriate use of benchmarking of an automated control by considering how frequently the application changes. Therefore, as the frequency of code change increases, the opportunity to rely on an application control's benchmarking strategy decreases. Additionally, the auditor should evaluate the reliability of the information regarding the changes made to the system. Hence, if there is little to no verifiable information or reports available for the changes made to the application, database, or supporting technology, the application control is less likely to qualify for benchmarking.

However, benchmarking is particularly effective when companies use pre-packaged software that doesn't allow for any source code development or modification. In cases like these, the organization needs to consider more than just the code change. An application control within a complex application, such as SAP or Oracle Financials, can be changed, disabled, or enabled easily without any code change.

Finally, parameter changes and configuration changes have a significant impact on most application controls. For example, tolerance levels can be manipulated easily to disable tolerance-level controls, and purchase approval controls can be manipulated when their release strategy is modified, once again, without requiring any code changes.

Organizations need to evaluate each application control to determine how long benchmarking can be effective. Once the benchmark is no longer effective, it is important to re-establish the baseline by re-testing the application control. Auditors should ask the following questions when identifying if the application control is still operating effectively and as originally benchmarked:

- Have there been changes in the risk level associated with the business process and the application control from when it was originally benchmarked (i.e., does the business process provide substantially greater risk to financial, operational, or regulatory compliance than when the application control was originally benchmarked)?
- Are ITGCs operating effectively, including logical access, change management, systems development, acquisition, and computer operation controls?
- Can the auditor gain a complete understanding of the effects of changes, if any, on the applications, databases, or supporting technology that contain the application controls?
- Were changes implemented to the business process relying on the application control that could impact the design of the control or its effectiveness?

Time and Cost Savings

Application controls typically take less time to test than manual controls. This is because sample sizes for manual controls are tied to the frequency with which the controls are performed (i.e., daily, weekly, monthly, quarterly, or annually), while the sample size of the application controls often does not depend on the frequency of the control's performance (i.e., application controls are either operating effectively or not). In addition, application controls are typically tested one time, as long as the ITGCs are effective. As a result, all of these factors can potentially accumulate to a significant savings in the number of hours required to test an application control versus a manual control.

The Role of Internal Auditors

Knowledge

Today, organizations are relying more on application controls than in the past to manage risk due to their inherent efficient nature, cost effectiveness, and reliability. Traditionally, any kind of technology-related control was tested by an experienced IT auditor, while financial, operational, or regulatory controls were tested by a non-IT auditor. Although the demand for IT auditors has grown substantially in the past few years and shows no signs of subsiding, all internal auditors need to be able to evaluate all business process controls from end-to-end.

In addition, according to The IIA's *International Standards for the Professional Practice of Internal Auditing (Standards)* 1220 and 1210.A3, internal auditors need to apply the care and skill of a reasonably prudent and competent auditor[14], as well as have the necessary knowledge of key IT risks, controls, and audit techniques to perform their assigned work, although not all internal auditors are expected to have the expertise of an auditor whose primary responsibility is IT auditing.[15] In other words, every internal auditor needs to be aware of IT risks and controls and be proficient enough to determine if implemented application controls are appropriately designed and operating effectively to manage financial, operational, or regulatory compliance risks.

[12] Public Company Accounting Oversight Board, Proposed Auditing Standard, An Audit of Internal Control Over Financial Reporting That is Integrated With an Audit of Financial Statements, p. A1-57.

[13] Public Company Accounting Oversight Board, Proposed Auditing Standard, An Audit of Internal Control Over Financial Reporting That is Integrated With an Audit of Financial Statements, p. A1-57, 58.

Consultant or Assurance

Other than traditional assurance services, one of the greatest opportunities for the internal audit activity to add value to an organization is through consultative engagements, which can take on many forms and cover any part or business function. One example of a consultative engagement is assisting organization personnel with the design of controls during the implementation or upgrading of transactional or support applications.

Unfortunately, many internal auditors do not assist management with understanding how risks will change when the organization implements a new transactional or support application or conducts a major upgrade. In almost all cases, this lack of involvement is not due to a lack of desire or focus, but to the fact that internal auditors are not aware of any system development activity or management does not want them involved.

No matter what the reason is, it is the responsibility of the CAE to ensure internal auditors are aware of such activities and to properly position the value, knowledge, and expertise of internal auditors in providing risk management services. Also, it is important for internal auditors to be involved in these kinds of system development activities to help manage the risk the application presents, as well as make sure inherent and configurable controls are operating effectively prior to the application's live stage. Otherwise, it will be much more costly to conduct a review after the fact, find weaknesses, and retrofit controls. Below are examples of how internal auditors can provide value during system development efforts with a focus on application controls from a consultative perspective.

Independent Risk Assessment

Any time a new or significantly upgraded transactional or support application is implemented, two things can happen. First, many of the automated or manual controls that were in place to manage risk within the legacy environment will need to be replaced with new controls. Second, the application's risk profile might change. In other words, the new application will bring about new inherent risks (i.e., in the form of how the application is configured) and risks that cannot be mitigated within the application itself, thus requiring the use of manual controls. As a result, internal auditors can assist — if not lead — the organization's efforts to understand how current risks will change with the advent of the new application. This is because internal auditors are skilled at providing this level of service and are uniquely positioned to do so due to their independence from management.

For internal auditors to provide this service, as well as the others listed below, they need to have sufficient knowledge of the application under development. The number and type of auditors who need such knowledge depends on the application under development, the implementation's scope in terms of impacted business processes, the organization's size, and the number of auditable entities or areas once the application has been fully deployed across the organization. CAEs can take different avenues to ensure sufficient knowledge is obtained, including the use of books, online courses, classroom training, and external consultants.

Design of Controls

Another valuable service internal auditors can provide during a new system implementation or significant upgrade is an extension of the independent risk assessment. More specifically, auditors can assist management with the design of controls to mitigate the risks identified during the risk assessment. The internal auditors assigned to this activity should be a part of the implementation team, not an adjunct. Therefore, the tasks, time, and number of internal audit resources required for the design of application controls need to be built into the overall project plan.

It is important that CAEs assign the appropriate number of auditors, as well as auditors with the necessary skills and experience to perform the task. In many cases, auditors may be assigned to work on the project on a full-time basis. If that is the case, CAEs should assign current duties of the personnel chosen to work on the project to other internal auditors in the department so that the auditors assigned to the project can focus on the task. Furthermore, internal auditors working on the project should report to the project manager during the system's implementation life cycle.

In the event that auditors are assigned to assist management in the design of application controls, CAEs should note that independence and objectivity may be impaired if assurance services are provided within one year after a formal consulting engagement (The IIA's *Standard* 1130.C1). In addition, steps should be taken to minimize the effects of impairment by; assigning different auditors to perform each of the services, establishing independent management and supervision of the auditors, defining separate accountability for project results, and disclosing presumed auditor impairment. Finally, management should be responsible for accepting and implementing recommendations.[16] In other words, if an internal auditor is involved in the design of controls related to a transactional or support application, he or she should not be involved in the evaluation of the controls' operating effectiveness within the first 12 months of the consulting engagement's completion.

Education

The educational value internal auditors can provide to the organization is not limited to application controls. Another key opportunity for internal auditors to provide value to

[14] IIA *Standard* 1220

[15] IIA *Standard* 1210.A3

the organization is through controls education. From an application control perspective, internal auditors can educate management on:

- How the risk profile will change once the new application is brought online.
- Known inherent control weaknesses in the applications under development.
- Prospective solutions to mitigate identified weaknesses.
- The various services auditors can provide to management as part of the system's development efforts.

Controls Testing

If the implementation team has designed and deployed controls based on the risk assessment, or without the benefit of one, internal auditors can provide value by independently testing the application controls. This test should determine if the controls are designed adequately and will operate effectively once the application is deployed. If any of the controls are designed inadequately or do not operate effectively, auditors should present this information along with any recommendations to management to prevent the presence of unmanaged risks when the application is deployed fully.

Application Reviews

Transactional and support applications require control reviews from time to time based on their significance to the overall control environment. The frequency, scope, and depth of these reviews should vary based on the application's type and impact on financial reporting, regulatory compliance, or operational requirements, and the organization's reliance on the controls within the application for risk management purposes.

[16] The IIA *Standard* 1130.C1

Assess Risk

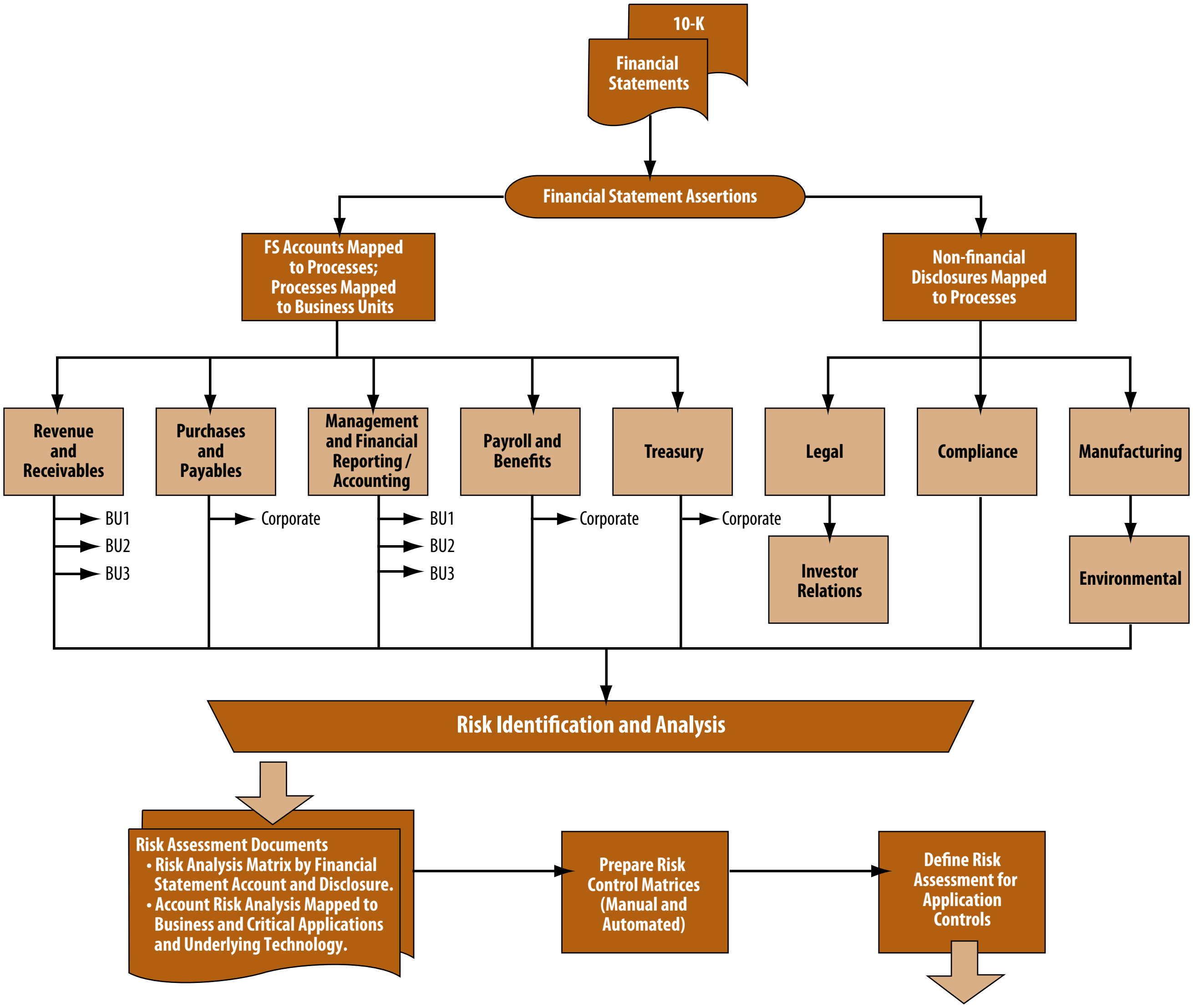
The auditor should use risk assessment techniques to identify critical vulnerabilities pertaining to the organization's reporting, and operational and compliance requirements when developing the risk assessment review plan. These techniques include:

- The review's nature, timing, and extent.
- The critical business functions supported by application controls.
- The extent of time and resources to be expended on the review.

In addition, auditors should ask four key questions when determining the review's appropriate scope:

1. What are the biggest organization wide risks and main audit committee concerns that need to be assessed and managed while taking management views into account?
2. Which business processes are impacted by these risks?
3. Which systems are used to perform these processes?
4. Where are processes performed?

When identifying risks, auditors may find it useful to employ an existing top-down risk assessment performed by management to determine which applications to include as part of the control review and what tests need to be performed. For instance, Figure 1 outlines an effective methodology for identifying financial reporting risks and the scope of the review. Please note this illustration does not represent the only way to conduct a financial reporting risk assessment.


10-K
Financial Statements
Financial Statement Assertions
FS Accounts Mapped to Processes; Processes Mapped to Business Units
Non-financial Disclosures Mapped to Processes
Revenue and Receivables
Purchases and Payables
Management and Financial Reporting / Accounting
Payroll and Benefits
Treasury
Legal
Compliance
Manufacturing
BU1
BU2
BU3
Corporate
BU1
BU2
BU3
Corporate
Corporate
Investor Relations
Environmental
Risk Identification and Analysis
Risk Assessment Documents
• Risk Analysis Matrix by Financial Statement Account and Disclosure.
• Account Risk Analysis Mapped to Business and Critical Applications and Underlying Technology.
Prepare Risk Control Matrices (Manual and Automated)
Define Risk Assessment for Application Controls

See Risk Assessment Approach in the following section.

Figure 1. Financial statement risk analysis approach.

Application Control: Risk Assessment Approach

To add value to organizationwide application control risk assessment activities, internal auditors:

- Define the universe of applications, databases, and supporting technology that use application controls, as well as summarize the risk and controls using the risk and control matrices documented during the risk assessment process.
- Define the risk factors associated with each application control, including:
  - Primary (i.e., key) application controls.
  - The design effectiveness of the application controls.
  - Pre-packaged or developed applications or databases. Pre-packaged applications that are not highly configured by the user pose a reduced risk to the organization compared to applications that are developed in-house or purchased applications that have been highly configured by the user.
  - Whether the application supports more than one critical business process.
  - The classification of data processed by the application (e.g., financial, private, or confidential).
  - Frequency of changes to the applications or databases.
  - Complexity of changes (e.g., table changes versus code changes).
  - Financial impact of the application controls.
  - Effectiveness of ITGCs residing within the application (e.g., change management, logical security, and operational controls).
  - The controls' audit history.
- Weigh all risk factors to determine which risks need to be weighed more heavily than others.
- Determine the right scale for ranking each application control risk by considering qualitative and quantitative scales, such as:
  - Low, medium, or high control risk.
  - Numeric scales based on qualitative information (e.g., 1 = low-impact risk, 5 = high-impact risk, 1 = strong control, and 5 = inadequate control).
  - Numeric scales based on quantitative information (e.g., 1 = < US $50,000 and 5 = > US $1,000,000).
- Conduct the risk assessment and rank all risk areas.
- Evaluate risk assessment results.
- Create a risk review plan that is based on the risk assessment and ranked risk areas.

Figure 2 shows an example of an application control risk assessment that uses a qualitative ranking scale (1 = low impact or risk and 5 = high impact or risk). Composite scores for each application are calculated by multiplying each risk factor and their weight in the application and adding the totals. For example, the composite score on the first line of 375 is computed by multiplying the risk factor rating times the specific application rating [(20 x 5) + (10 x 1) + (10 x 5) +…]. For this example, the auditor may determine that the application control review will include all applications with a score of 200 or above.

Risk Factor Weighting

	20	10	10	10	10	10	15	15	
Application	Application Contains Primary Controls	Design Effectiveness of the App Controls	Pre-packaged or Developed	Application Supports More Than One Critical Business Process	Frequency of Change	Complexity of Change	Financial Impact	Effectiveness of the ITGC Controls	Composite Score
APPA	5	1	5	5	3	3	5	2	375
APPB	1	1	2	1	1	1	4	2	170
APPC	5	2	2	1	5	5	5	2	245
APPD	5	3	5	1	5	5	5	2	395
APPE	5	1	1	1	1	1	3	2	225

Figure 2. Example of an application control risk assessment.

Following are several methods for determining the review scope of application controls. Internal auditors should keep in mind that the review's scope, depth, approach, and frequency depends on the results of the risk assessment and the availability of internal audit resources. No matter what scoping method is chosen, the review needs to cover an evaluation of data input controls, processing controls, and output controls.

Business Process Method

The business process scoping method is a top-down review approach used to evaluate the application controls present in all the systems that support a particular business process. Over the past several years, this method has grown in importance as the most common and widely accepted scoping methodology. This is primarily due to an increase in ERP transactional application use and a reduction in stand-alone, "best of breed" applications.

When using the business process method in the non-ERP world, internal auditors should include within the review's scope all of the applications used by the company that are involved in the business process under review because they are generally stand-alone systems. In other words, the auditor needs to include within the review's scope the separate applications that make up the different components of the business process cycle. The auditor can then identify the inbound and outbound interfaces within the application under review and complete the scoping activity.

Using the business process method to scope the review of application controls is different with integrated applications such as an ERP system because business processes cut across multiple modules. For example, consider the procurement to payment business process. In an ERP environment, this process generally consists of the procurement, inventory management, general ledger, and accounts payable modules or subapplications within the ERP system. Therefore, it is important to have a thorough understanding of the modules that comprise the business process and how the data is managed and flows from one module to the other.

Single Application Method

The single application scoping method is used when the auditor wants to review the application controls within a single application or module as opposed to taking a business process scoping approach. As discussed earlier, this is the most effective scoping method in a non-ERP or non-integrated environment because the auditor can more easily "draw a box" around the application (i.e., include the application within scope). In other words, the auditor can identify the inbound data inputs and outputs because data and related processing rules are contained and used only for one application.

However, in an ERP or integrated environment, this method is not desirable. Although it may appear to be fairly easy to draw a box around the module of an ERP or integrated transactional system, the reality is that this activity can be quite difficult. This is because there can be multiple data feeds into and out of any given module, and attempting to identify them could prove to be an exercise in futility. Therefore, using the module approach is likely to lead to an inadequate review; using the business process method is a more effective scoping method in an ERP or integrated environment.

Access Controls

No matter what method is chosen to scope the review of application controls, the module's or application's logical access controls need to be reviewed periodically. In most cases, the user and administrative access rights (i.e., read, write, and delete) are built using the inherent security platform and tools within the application. The strategies employed to determine the logical access rights to be assigned to users vary from a need-to-know basis to a need-to-withhold basis. Regardless, the access rights should be granted based on the user's job function and responsibilities.

How logical access rights are created vary from package to package. In some cases, the logical access rights are granted based on a transaction code or a screen name or number, while others use more complex object-based security protocols. When a review of an application's logical access controls is performed, it is important to ensure that the general application security controls are reviewed as well, including:

- The length of the username or user identification.
- The password's length.
- Password character combinations.
- Password aging (e.g., users must change their password every 90 days).
- Password rotation (e.g., users cannot use any of their last five passwords).
- User account lockout after a certain number of unsuccessful login attempts.
- Session timeout (e.g., the application automatically logs out a user if the user has not interacted with the application within 15 minutes).

Most of the latest application generations are created with parameters that can be configured by management such as the ones above. In some cases, however, management may forget to activate the parameter(s), or the settings used for each parameter may not be representative of best practice standards. For example, the password aging parameter could be set to work once every calendar year, while best practices today recommend a time frame between 60 and 90 days. In addition, auditors should review administrative access rights in development and testing environments periodically.

Once the review is scoped appropriately, the next task is to determine how it will be executed. Besides the standard audit methodology chosen, following are recommendations that can help auditors execute a properly scoped application controls review.

Planning

After completing the risk evaluation and determining the scope of the review, auditors need to focus on the development and communication of the detailed review plan. The first step in developing the detailed review plan is to create a planning memorandum that lists the following application control review components:

- All review procedures to be performed.
- Any computer-assisted tools and techniques used and how they are used.
- Sample sizes, if applicable.
- Review items to be selected.
- Timing of the review.

When preparing the memorandum, all of the required internal audit resources need to be included on the planning team. This is also the time when IT specialists need to be identified and included as part of the planning process.

After completing the planning memorandum, the auditor needs to prepare a detailed review program. (Refer to Appendix B for an example of detailed audit program development requirements.) When preparing the review program, a meeting should be held with management to discuss:

- Management's concerns regarding risks.
- Previously reported issues.
- Internal auditing's risk and control assessment.
- A summary of the review's methodology.
- The review's scope.
- How concerns will be communicated.
- Which managers will be working on the review team.
- Any preliminary information needed (i.e., reports).
- The length of the review.

Besides completing a summary of the risk assessment phase, an important part of this meeting is to obtain management support. Although discussions should be held at the beginning of the review's planning phase, key business processes, risks, and controls should be discussed throughout the review to ensure management is in agreement with the review's planning scope.

Management should be informed of any known concerns, specifically, any issues identified during the risk assessment or planning phase — even if these issues have not been substantiated. Discussions should be held to ensure management concurs with all identified risks and controls. By doing so, the team can influence management to take corrective action immediately and encourage the appropriate risk-conscious behavior throughout the company. To do this, auditors can send a letter to management announcing the review. This letter should include:

- The review's expected start date.
- The review's timeframe.
- The key business areas under review.

Need for Specialized Audit Resources

The internal auditor should evaluate the review's scope and identify whether an IT auditor will be required to perform some of the review. Adding an IT auditor to the review team, however, does not relieve the auditor from having to assess the adequacy of IT controls. The IT auditor will simply assess the organization's reliance on IT to determine the integrity of the data and the accuracy, completeness, and authorization of transactions. Another factor IT auditors could review is the number of transactions processed by the application. Special tools may be required to assess and report on the effectiveness of application controls. The information collected by the IT auditors, along with the knowledge of the internal auditor, will assist in determining if specialized resources are required.

An example of when specialized resources are required involves a segregation of duties' review during the installation of an Oracle eBusiness Suite application for a large manufacturing company. The complexity of the roles and functions contained within the application and database require the use of personnel with knowledge on the configuration capabilities of the Oracle application. Additional staff may be needed who know how to mine data from the Oracle application and database to facilitate the review. Furthermore, the review team may need a specialist who is familiar with a specific computer-assisted audit tool to facilitate data extraction and analysis.

Business Process Method

In the previous chapter, the business process method was identified as being the most widely used for application control review scoping. In today's world, many transactional applications are integrated into an ERP system. Because business transactions that flow through these ERP systems can touch several modules along their life cycle, the best way to perform the review is to use a business process or cycle approach (i.e., identifying the transactions that either create, change, or delete data within a business process and, at a minimum, testing the associated input, processing, and output application controls). The best way to approach the review is to break down the business processes using the four-level model shown in Figure 3:

- Mega process (i.e., level 1): This refers to the complete end-to-end process, such as procure-to-pay.
- Major process (i.e., level 2): This refers to the major components of the end-to-end process, such as

procurement, receiving, and payment of goods.

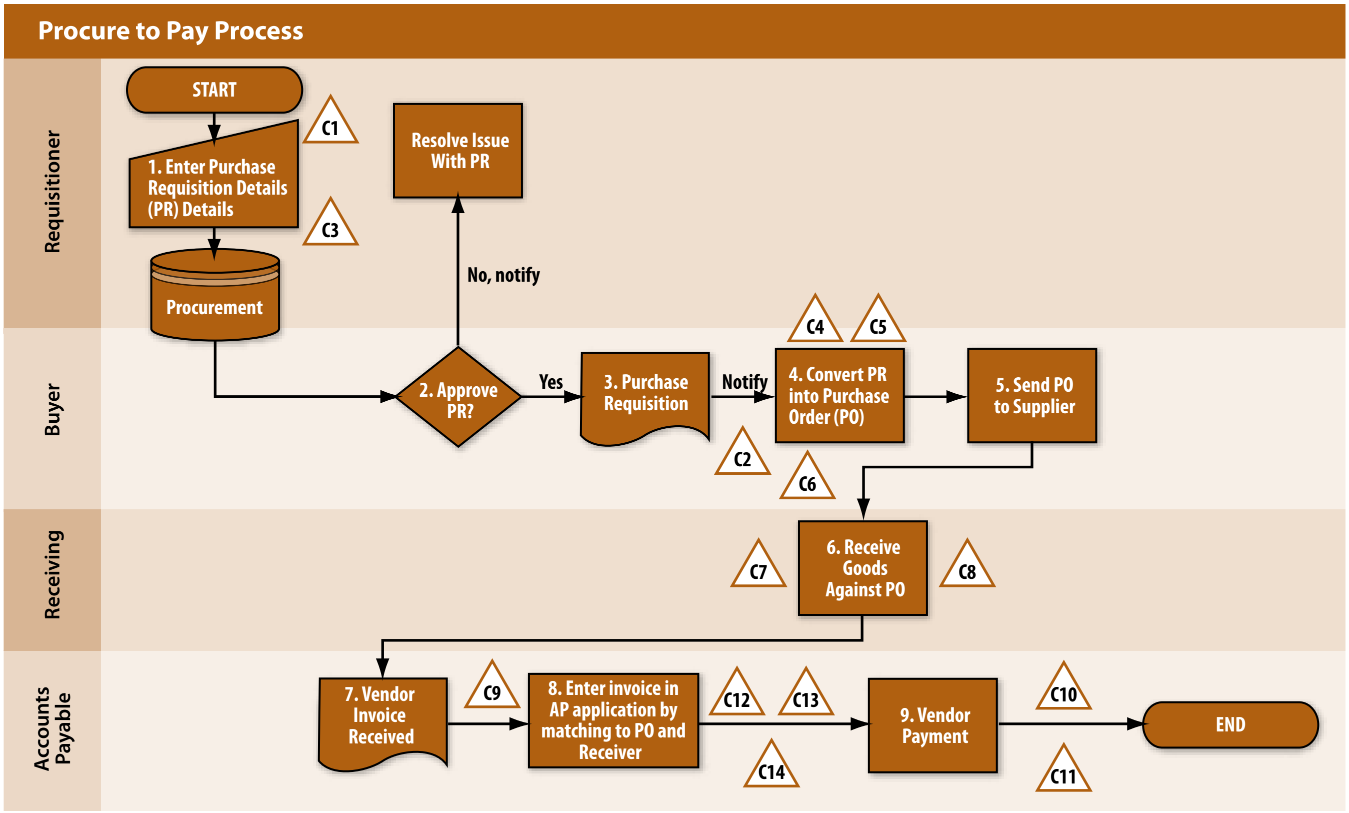
- Minor or subprocess (i.e., level 3): This level lists the minor or subprocess components of each of the major processes, such as requisitioning and purchase order creation.
- Activity (i.e., level 4): This final level lists the system transactions that result in the creation, change, or deletion of data for each of the minor or subprocess components.

Taking a business-centric view of application controls is essential to ensure that the review is comprehensive and meaningful to the organization. From this point forward, the review can be executed as a single engagement or as part of an integrated review.

Mega Process (Level 1): Procure-to-Pay

Major Process (Level 2)	Subprocess (Level 3)	Activity (Level 4)
Procurement	Requisition processing	Create, change, and delete
	Purchase order processing	Create, change, delete, approval, and release
Receiving	Goods receipt processing	Create, change, and delete
	Goods return processing	Create, change, and delete
Accounts Payable	Vendor management	Create, change, and delete
	Invoice processing	Create, change, and delete
	Credit memo processing	Create, change, and delete
	Process payments	Create, change, and delete
	Void payments	Create, change, and delete

Figure 3. Breakdown of a business process.



△ Triangles represent each control in the process. The number of each control ties to the activity represented on the Risk and Controls Matrix.

Figure 4. A flowchart of a procure-to-pay process.

Documentation Techniques

In addition to the documentation standards used by internal auditors, following are suggested approaches for documenting each application control.

Flowcharts

Flowcharts are one of the most effective techniques used to capture the flow of transactions and their associated application and manual controls used within an end-to-end business process because they illustrate transaction flows. Figure 4 shows an example of a flowchart for a procure-to-pay process. Due to the difficulty of fitting the actual control descriptions on the flowchart, it is prudent to instead simply number the controls on the flowchart and have a separate document, such as a risk and controls matrix (see Figure 6, pg. 14-17), that contains the control descriptions and associated information. However, flowcharts may not be practical for use all the time, and a process narrative would be more appropriate. This typically happens when an auditor is documenting the areas or work performed within the IT environment. In many cases, the work performed by IT and the related application controls do not flow in a linear manner as do business processes such as procure-to-pay.

Process Narratives

Process narratives are another technique available to document business process transaction flows with their associated applications, as shown in Figure 5. These narratives are best used as a documentation tool for relatively non-complex business processes and IT environments. This is because the more complex the business process is, the more difficult it is to create a process narrative that reflects the process' true nature adequately and accurately. Therefore, when relatively complex business processes are documented, auditors should create a flowchart with a corresponding process narrative that numbers the controls on the process narrative. Auditors also should create a separate document, such as a risk and controls matrix.

The following is an example process narrative that covers the procure-to-pay process.

Narrative	Procure-to-pay
Primary Contact(s)	
Key Components	C1, C2, C3, C4, C5, C6, C7, C8, C9, C10, C11, C12, C13, and C14

Figure 5. Risk and controls matrix.

1) Procurement

- **a) Requisitioning**
    - i) When employees need to buy goods or services, they will create a purchase requisition in the procurement application (**Control C1**). Once the requisition has been created, the buyer will review the purchase requisition for its appropriateness, completeness, and accuracy. Components of the purchase requisition that are reviewed include, but are not limited to, the vendor, item, quantity, and account coding. If the review does not reveal any errors, the buyer will approve the purchase requisition. If the buyer rejects the purchase requisition for any reason, the requisitioner will be notified. Finally, if issues with the original requisition are resolved as required, the buyer will approve the requisition.
    - ii) All purchase requisitions are reviewed on a monthly basis to detect any unauthorized requisitions as well as any excessive order quantities (**Controls C2 and C3**).
- **b) Purchase Order Processing**
    - i) Once the purchase requisition has been approved by the buyer, he or she will create a purchase order referencing the requisition in the procurement application (**Control C4**). The buyer will then forward a copy of the purchase order to the supplier.
    - ii) All purchase orders are reviewed on a monthly basis to detect any unauthorized purchase orders as well as any excessive order quantities (**Controls C5 and C6**).

2) Receiving

- a) All goods are received at the shipping and receiving dock. A warehouse employee will review the packing slip, make note of the purchase order number, and count the items that are physically received. The warehouse employee then logs onto the procurement application and enters the number of items received against the appropriate line item number on the purchase order.
- b) The appropriate member of the accounting department reviews and reconciles the inventory general ledger account on a monthly basis to determine the goods that have been received, but not invoiced by the vendor (**Control C7**).
- c) The appropriate buyer from the purchasing department reviews all unmatched purchase order reports on a monthly basis (**Control C8**).

3) Accounts Payable

- a) The accounts payable department receives invoices from the various suppliers on a daily basis. These invoices are sorted and assigned to each accounts payable clerk, based on the vendor's name. Each clerk is required to stamp each invoice with the date it was received by the accounts payable department. Each accounts payable clerk then matches the invoice quantities and prices to the purchase order and receiver and enters the invoice in the accounts payable application (**Controls C9 and C14**).

b) The accounts payable application automatically generates requests for payments based on the vendor payment terms, and an accounts payable check run is processed every Wednesday (**Controls C10, C12, and C13**).

c) At month-end, the accounts payable manager compares the accounts payable system's sub-ledger total to the general ledger control total. Any differences noted are then corrected (**Control C11**).

Risk and control matrices should capture all relevant information pertaining to a given business process. In addition, each of the control activities should be numbered, and this number should be linked back to the flowcharts or pro-cess narratives. Important control activity information that needs to be captured in the matrix includes:

- Identified risks.
- Control objectives.
- Control activities.
- Control attributes such as control type (i.e., automated or manual) and frequency (i.e., daily, weekly, monthly, quarterly, annually, etc.).
- Testing information.

Testing

The auditor should assess if application controls are working or if they are being circumvented by creative users or management override. Substantive testing on the efficacy of controls is needed rather than a review of control settings. Auditors should also identify the effectiveness of ITGCs and consider if application-generated change control logs, security logs, and administration logs need to be reviewed by the audit team.

The auditor may test application controls using several methods that are based on the type of application control. Depending on the nature, timing, and extent of testing, a specific control or report could be tested by:

- Inspection of system configurations.
- Inspection of user acceptance testing, if conducted in the current year.
- Inspection or re-performance of reconciliations with supporting details.
- Re-performance of the control activity using system data.
- Inspection of user access listings.
- Re-performance of the control activity in a test environment (i.e., using the same programmed procedures as production) with robust testing scripts.

An example of a system configuration test includes re-viewing the three-way match system parameters of the tested system by tracing through one transaction. Another example of a system configuration review is to query the underlying programming code of the application report ge-neration process for appropriate logic. Additionally, the auditor should observe a rerun of the query to compare the report to the one that management generated.

The auditor could test edit checks for key fields, which can be verified by stratifying or classifying transactions on the field values. In addition, by using audit software, it might be easy to recalculate and verify calculations made by the system. For example, if the system uses the quantity and unit price fields to calculate the total cost, the auditor could use audit software to perform the same calculation and identify any transactions where his or her calculated values differ from those of the application.

Finally, auditors can perform reasonableness checks to examine possible value data ranges for key fields. For example, by calculating the current age based on the date of birth field, auditors can identify ages, including negative values and values over 100 that fall outside expected ranges.

Computer-assisted Audit Techniques

Computer-assisted audit techniques (CAATs) make use of computer applications, such as ACL, IDEA, VIRSA, SAS, SQL, Excel, Crystal Reports, Business Objects, Access, and Word, to automate and facilitate the audit process. The use of CAATs helps to ensure that appropriate coverage is in place for an application control review, particularly when there are thousands or perhaps millions of transactions occurring during a test period. In these situations it would be impossible to obtain adequate information in a format that can be reviewed without the use of an automated tool. Because CAATs provide the ability to analyze large volumes of data, a well-designed audit supported by CAAT testing will perform a complete review of all transactions looking for abnormalities, such as duplicate vendors or transactions, or a set of predetermined control issues, such as segregation of duty conflicts.

Risk and Control Matrix: Procure-to-Pay

	BUSINESS PROCESS & CONTROL OBJECTIVES	RISKS		CONTROL ACTIVITIES	COSO COMPONENTS					CONTROL ATTRIBUTES				CONTROL CLASSIFICATION						TESTING		
Number	Control Objectives	Risks	Impact/ Likelihood	Control Activities	CE	RA	CA	I/C	M	K (Y/N)	Man/Auto	Pre/Det	Frequency	Real	Recorded	Valued	Timely	Classified	Posted	Test Results	Operational Effectiveness (Y/N)	Notes
	Major: Procurement																					
	Sub: Purchase Requisition Processing																					
	Activity: Create																					
C1	Controls provide reasonable assurance that purchase requisitions are created by authorized personnel completely and accurately.	Due to the lack of appropriate segregation of duties, a user is able to create, approve (i.e., release), assign, and convert a purchase requisition, resulting in the inappropriate rewarding of business to suppliers, overpayments, and excessive inventory levels.	H	Controls are such that access is granted only to those individuals with a business purpose for creating purchase requisitions.			X				A	P	Always	X	X	X		X	X			
C2	Controls provide reasonable assurance that purchase requisitions are created by authorized personnel completely and accurately.	Due to the lack of appropriate segregation of duties, a user is able to create, approve (i.e., release), assign, and convert a purchase requisition, resulting in the inappropriate rewarding of business to suppliers, overpayments, and excessive inventory levels.	H	Purchase requisitions are reviewed on a monthly basis to detect any unauthorized purchase requisitions.			X	X	X		M	D	Monthly	X	X	X		X	X			
C1	Controls provide reasonable assurance that purchase requisitions are created by authorized personnel completely and accurately.	Unauthorized or excessive purchase requisition quantities could lead to unfavorable prices, excessive inventory, and unnecessary product returns.	M	Controls are such that access is granted only to those individuals with a business purpose for creating purchase requisitions.			X				A	P	Always	X	X	X		X	X			
C3	Controls provide reasonable assurance that purchase requisitions are created by authorized personnel completely and accurately.	Unauthorized or excessive purchase requisition quantities could lead to unfavorable prices, excessive inventory, and unnecessary product returns.	M	Purchase requisitions are reviewed on a monthly basis to detect any excessive order quantities.			X	X	X		M	D	Monthly	X	X	X			X			

List of acronyms used in the chart:
COSO Components
1. CE: control environment
2. RA: risk assessment
3. CA: control activities
4. I/C: information and communication
5. M: monitoring

Control Attributes
6. K: key control
7. Man/Aut: manual or automatic
8. Pre/Det: prevent or detect

Figure 6. Risk and control matrix for a procure-to-pay process.

Risk and Control Matrix: Procure-to-Pay

	BUSINESS PROCESS & CONTROL OBJECTIVES	RISKS		CONTROL ACTIVITIES	COSO COMPONENTS					CONTROL ATTRIBUTES				CONTROL CLASSIFICATION						TESTING		
Number	Control Objectives	Risks	Impact/ Likelihood	Control Activities	CE	RA	CA	I/C	M	K (Y/N)	Man/Auto	Pre/Det	Frequency	Real	Recorded	Valued	Timely	Classified	Posted	Test Results	Operational Effectiveness (Y/N)	Notes
	Major: Procurement																					
	Sub: Purchase Order Processing																					
	Activity: Create																					
C4	Controls provide reasonable assurance that purchase orders are created by authorized personnel completely and accurately.	Due to the lack of appropriate segregation of duties, a user is able to create, approve (i.e., release), assign, and convert a purchase requisition, resulting in the inappropriate rewarding of business to suppliers, overpayments, and excessive inventory levels.	H	Controls are such that access is granted only to those individuals with a business purpose for creating purchase orders.			X				A	P	Always	X	X	X		X	X			
C5	Controls provide reasonable assurance that purchase orders are created by authorized personnel completely and accurately.	Due to the lack of appropriate segregation of duties, a user is able to create, approve (i.e., release), assign, and convert a purchase requisition resulting in the inappropriate rewarding of business to suppliers, overpayments, and excessive inventory levels.	H	Purchase orders are reviewed on a monthly basis to detect any unauthorized purchase orders.			X	X	X		M	D	Monthly	X	X	X		X	X			
C6	Controls provide reasonable assurance that purchase requisitions are created by authorized personnel completely and accurately.	Unauthorized or excessive purchase order quantities could lead to unfavorable prices, excessive inventory and unnecessarary product returns.	M	Purchase orders are reviewed on a monthly basis to detect any excessive order quantities.			X	X	X		M	D	Monthly	X	X	X		X	X			

List of acronyms used in the chart:

COSO Components

1. CE: control environment
2. RA: risk assessment
3. CA: control activities
4. I/C: information and communication
5. M: monitoring

Control Attributes

6. K: key control
7. Man/Aut: manual or automatic
8. Pre/Det: prevent or detect

Figure 6. Risk and control matrix for a procure-to-pay process.

Risk and Control Matrix: Procure-to-Pay

	BUSINESS PROCESS & CONTROL OBJECTIVES	RISKS		CONTROL ACTIVITIES	COSO COMPONENTS					CONTROL ATTRIBUTES				CONTROL CLASSIFICATION						TESTING		
Number	Control Objectives	Risks	Impact/ Likelihood	Control Activities	CE	RA	CA	I/C	M	K (Y/N)	Man/Auto	Pre/Det	Frequency	Real	Recorded	Valued	Timely	Classified	Posted	Test Results	Operational Effectiveness (Y/N)	Notes
	Major: Receiving																					
	Sub: Goods Receipt Processing																					
	Activity: Create																					
C7	Controls provide reasonable assurance that goods receipts are processed by authorized personnel completely, accurately, and in a timely manner.	Associating a goods receipt with an incorrect purchase order or incorrect line item could result in the inaccurate valuing of inventory and the goods received/not invoiced account, thereby causing delays in invoice and payment processing.	H	The goods received/not invoiced account is reconciled on a monthly basis.			X	X	X		M	D	Monthly	X	X	X		X	X			
C8	Controls provide reasonable assurance that goods receipts are processed by authorized personnel completely, accurately, and in a timely manner.	Goods receipts are not recorded appropriately.	M	Unmatched purchase order reports are reviewed on a monthly basis.			X	X	X		M	D	Monthly	X	X		X	X				
	Major: Accounts Payable																					
	Sub: Invoice Processing																					
	Activity: Create																					
C9	Controls provide reasonable assurance that vendor invoices are created by authorized personnel completely, accurately, and in a timely manner.	An invoice that should be paid by matching it to a purchase order is paid without a reference to a purchase order, which could result in an unacceptable payment for material or services, (i.e., unacceptable and unfavorable price variations).	M	Application security is such that access to the non-purchase order invoice entry transaction is limited as much as possible.			X				A	P	Always	X	X	X		X	X			
C10	Controls provide reasonable assurance that vendor invoices are processed by authorized personnel completely, accurately, and in a timely manner.	Incorrect invoice amounts are entered, resulting in incorrect payments to vendors.	H	Checks are matched to supporting documents (invoice, check requests, or expense reimbursements) based on a dollar threshhold.			X	X			M	P	As Required	X	X	X			X			
C11	Controls provide reasonable assurance that vendor invoices are processed by authorized personnel completely, accurately, and in a timely manner.	AP invoice sub-ledger postings are not posted to the GL.	L	The AP sub-ledger total is compared to the GL balance at the end of the month via an aging report. Any differences noted are corrected.			X	X	X		M	D	Monthly	X	X	X			X			

List of acronyms used in the chart:
COSO Components
1. CE: control environment
2. RA: risk assessment
3. CA: control activities
4. I/C: information and communication
5. M: monitoring

Control Attributes
6. K: key control
7. Man/Aut: manual or automatic
8. Pre/Det: prevent or detect

Figure 6. Risk and control matrix for a procure-to-pay process.

Risk and Control Matrix: Procure-to-Pay

	BUSINESS PROCESS & CONTROL OBJECTIVES	RISKS		CONTROL ACTIVITIES	COSO COMPONENTS					CONTROL ATTRIBUTES				CONTROL CLASSIFICATION						TESTING		
Number	Control Objectives	Risks	Impact/ Likelihood	Control Activities	CE	RA	CA	I/C	M	K (Y/N)	Man/Auto	Pre/Det	Frequency	Real	Recorded	Valued	Timely	Classified	Posted	Test Results	Operational Effectiveness (Y/N)	Notes
	Major: Accounts Payable																					
	Sub: Process Payments																					
	Activity: Create																					
C12	Controls provide reasonable assurance that vendor payments are processed by authorized personnel completely and accurately.	Disbursements recorded differ from amounts paid.	L	The AP application automatically writes checks or electronic payments based on the value of approved invoices according to vendor payment and system terms.			X				A	P	Always	X	X	X	X	X	X			
C13	Controls provide reasonable assurance that vendor payments are processed by authorized personnel completely and accurately.	Disbursements made are not recorded.	H	Access is restricted to authorized personnel to create checks.			X				A	P	Always	X	X	X			X			
C14	Controls provide reasonable assurance that vendor payments are processed by authorized personnel completely and accurately.	Fictitious disbursements are recorded.	M	The AP application performs a three-way match between the purchase order line item, the receiver, and the invoice when AP invoices are processed.			X	X			A	P	Always		X			X	X			

List of acronyms used in the chart:
COSO Components
1. CE: control environment
2. RA: risk assessment
3. CA: control activities
4. I/C: information and communication
5. M: monitoring

Control Attributes
6. K: key control
7. Man/Aut: manual or automatic
8. Pre/Det: prevent or detect

Figure 6. Risk and control matrix for a procure-to-pay process.

Appendix A: Common Application Controls and Suggested Tests

The following outlines common application controls and suggested tests for each control. The table was provided by the AXA Group.[17]

Input Controls

These controls are designed to provide reasonable assurance that data received for computer processing is appropriately authorized and converted into machine-sensible form and that data is not lost, suppressed, added, duplicated, or improperly changed. Computerized input controls include data checks and validation procedures such as check digits, record counts, hash totals, and batch financial total. While computerized edit routines, which are designed to detect data errors, include valid character tests, missing data tests, sequence tests, and limit or reasonableness tests. Input controls and suggested tests are identified in the table below.

Input and Access Controls

These controls ensure that all input transaction data is accurate, complete, and authorized.

Domain	Control	Possible Tests
Data checks and validation	• Reasonableness and limit checks on financial values. • Format and required field checks; standardized input screens. • Sequence checks (e.g., missing items) range checks, and check digits. • Cross checks (e.g., certain policies are only valid with certain premium table codes). • Validations (e.g., stored table and drop-down menu of valid items).	• Conduct a sample test of each scenario. • Observe attempts to input incorrect data. • Determine who can override controls. • If table driven, determine who can change edits and tolerance levels.
Automated authorization, approval, and override	• Authorization and approval rights (e.g., of expenses or claim payments or credit over a certain threshold) are allocated to users based on their roles and their need to use the application. • Override capability (e.g., approval of unusually large claims) is restricted by the user's role and need to use the application by management.	• Conduct tests based on user access rights. • Test access privileges for each sensitive function or transaction. • Review access rights that set and amend configurable approval and authorization limits.
Automated segregation of duties and access rights	• Individuals who set up approved vendors cannot initiate purchasing transactions. • Individuals who have access to claims processing should not be able to set up or amend a policy.	• Testing based on user access rights. • Review of access to set and amend configurable roles or menu structures.
Pended items	• Aging reports showing new policy items with incomplete processing are reviewed daily or weekly by supervisors. • Pending files where there is insufficient information available to process transactions.	• Review aging results and evidence of supervisor review procedures. • Walk through a sample of items to and from the aging report or pending file.

File and Data Transmission Controls

These controls ensure that internal and external electronically transmitted files and transactions are received from an identified source and processed accurately and completely.

Domain	Control	Possible Tests
File transmission controls	• Checks for completeness and validity of content, including date and time, data size, volume of records, and authentication of source.	• Observe transmission reports and error reports. • Observe validity and completeness parameters and settings. • Review access to set and amend configurable parameters on file transfers.
Data transmission controls	• Application of selected input controls to validate data received (e.g., key fields, reasonableness, etc.).	• Test samples of each scenario. • Observe attempts to input incorrect data. • Determine who can override controls. • If table driven, determine who can change edits and tolerance levels.

[17] Taken from AXA Group's Common Application Controls and Suggested Testing.

Processing Controls

These controls are designed to provide reasonable assurance that data processing has been performed as intended without any omission or double-counting. Many processing controls are the same as the input controls, particularly for online or real-time processing systems, but are used during the processing phases. These controls include run-to-run totals, control-total reports, and file and operator controls, such as external and internal labels, system logs of computer operations, and limit or reasonableness tests.

Processing Controls

These controls ensure that valid input data has been processed accurately and completely.

Domain	Control	Possible Tests
Automated file identification and validation	• Files for processing are available and complete.	• Review process for validation and test operation.
Automated functionality and calculations	• Specific calculations conducted on one or more inputs and stored data elements produce further data elements. • Use of existing data tables (e.g., master files or standing data such as rating tables).	• Compare input values and output values for all scenarios by walkthrough and re-performance. • Review table maintenance controls and determine who can change edits and tolerance levels. • Inputs and outputs may be from another process or calculation within the application and, therefore, a calculation can consist of a series of such calculations.
Audit trails and overrides	• Automated tracking of changes made to data, associating the change with a specific user. • Automated tracking and highlighting of overrides to normal processes.	• Review reports and evidence of reviews. • Review access to override normal processes.
Data extraction, filtering, and reporting	• Extract routine outputs are assessed for reasonableness and completeness. • Automated allocation of transactions (e.g., for reinsurance purposes, further actuarial processes, or fund allocation). • Evaluation of data used to perform estimation for financial reporting purposes.	• Review design of extract routine against data files used. • Review supervisory assessment of output from extract routine for evidence of regular review and challenges. • Review sample of allocations for appropriateness. • Review process to assess extracted data for completeness and validity.
Interface balancing	• Automated checking of data received from feeder systems (e.g., payroll, claims data, etc.) into data warehouses or ledger systems. • Automated checking that balances on both systems match or, if not, an exception report is generated and used.	• Inspect interface error reports. • Inspect validity and completeness parameters and settings. • Review access to set and amend configurable parameters on interfaces. • Inspect evidence of match reports checks and error file processing.
Automated functionality and aging	• File extracts from debtors listing to provide management with data on age transactions.	• Test sample of listing transactions to validate appropriateness of aging processing.
Duplicate checks	• Comparison of individual transactions to previously recorded transactions to match fields. • Comparison of individual files to expected dates, times, sizes, etc.	• Review access to set and amend configurable parameters on duplicate transactions or files. • Review process for handling rejected files or transactions.

Output Controls

These controls are designed to provide reasonable assurance that processing results are accurate and distributed to authorized personnel only. Control totals produced as output during processing should be compared and reconciled to input and run-to-run control totals produced during processing. Computer-generated change reports for master files should be compared to original source documents to assure information is correct.

Output Controls These controls ensure that output is complete, accurate, and distributed appropriately.		
Domain	Control	Possible Tests
General ledger posting	• All individual and summarized transactions posting to general ledger.	• Sample of input and subledger summary transactions traced to the general ledger.
Subledger posting	• All successful transactions posting to subledger.	• Sample of input transactions traced to subledger.

Master Files and Standing Data Controls These controls ensure the integrity and accuracy of master files and standing data.		
Domain	Control	Possible Tests
Update authorization	• Access to update allocated rights to senior users based on their roles and need to use the application.	• Review access to set and amend master files and standing data.

Appendix B: Sample Detailed Review Program

Note: Relevant ITGCs are included as needed.

Type Detailed audit program	**Audit Type** Application control review
Scope TBD	Effective date Enter date
Author Auditor name	Notes Add notes as required

Background Information

A. Technical and Information Systems

1. Determine what hardware is used to run the system. Classify the system as micro, local area network, client/server, or mainframe-based.

2. Determine if the software was purchased or developed in-house.

3. If the software was purchased, determine if any vendor warranties are still in force. In addition, determine if the vendor is financially sound and if the software is held in escrow.

4. If the software was developed in-house, verify that the software was developed and updated based on a sound system development methodology.

5. Determine if there are any third-party relationships involved in the processing or support of the application.

6. Identify the programming languages used in the application. Determine if the information systems (IS) department has programming staff knowledgeable in these programming languages.

7. Identify the types of data files used in processing (i.e., databases, sequential files, disks, tapes, etc.).

8. Identify the primary transaction, master, and reference files used in processing.

9. Determine how the IS department controls and secures access to the application programs.

10. Determine if passwords are entered in such a way that they are not displayed.

11. Evaluate the quality of the programmer's application documentation. This documentation should include system and program flowcharts, decision tables, file layouts, data element definitions, narratives, source program listings, and change records.

12. Evaluate the quality of the application operations documentation. This should include job and system flowcharts, input and output descriptions, job frequency and sequence of operations, job restart and recovery procedures, file backup requirements and procedures, error messages and reconciliation techniques, report distribution procedures, and data capture instructions.

13. Determine if backup copies of application programs and operation documentation files are stored offsite.

14. Determine if IS personnel monitor processing flows to verify application programs run according to schedule.

B. End Users

1. Determine the primary means of data entry and processing (e.g., batch, online, or real time).

2. Determine if the organization practices data ownership. If so, identify and interview data owners to determine if they understand their roles and responsibilities.

3. Interview a sample of end-user managers to identify end-user management attitudes regarding the system's quality and effectiveness.

4. Ask end-user managers what they perceive to be the risks, exposures, and limitations associated with the system.

5. Determine the number of end-users working with the system, their locations, and responsibilities associated with the system. Obtain an organizational chart for these positions.

6. Determine if this application generates data for legal or regulatory agencies. If so, pay extra attention to these transactions.

7. Evaluate the quality of end-user documentation. This should include a system description, a description of source documents and procedures for their preparation, job submission procedures, control procedures, error identification and correction procedures, and description of output reports and their use.

8. Identify the application training available for end users. Evaluate this training to determine if it is adequate, current, and available for new people.

9. Determine if end-user activity is supervised adequately.

C. System Interfaces

1. Determine what other applications interface manually or electronically with this application. Document what is received from and what is sent to these other applications.

2. Determine how end users verify or establish assurance that interfaces are providing complete, accurate, and authorized data.

D. File Handling

1. Determine the retention periods of key application data files. Evaluate if retention periods satisfy management reporting, U.S. Internal Revenue Service reporting, regulatory compliance, and internal accounting requirements.

2. Determine if end-user management and data owners are aware of key application data file retention periods and if these managers are satisfied with the length of the retention period.

E. Backup and Recovery

1. Determine how often key files are backed up. Determine if copies of these backup files are stored at a suitable off-site facility.

2. Verify that off-site backup file storage facilities are secure.

3. Determine if technical and end-user application recovery plans exist for restoring short-term and long-term computer processing interruptions. Verify that these plans address technical restoration needs and alternative end-user processing procedures.

4. Determine if these application recovery plans have been tested in the past year.

5. Establish how long the organization could comfortably function and avoid significant financial loss if the computerized aspects of the application failed. Verify that disaster recovery plans, as well as restart and recovery plans, specify how to restore this application to avoid significant financial loss.

6. Determine if the IS department has established data files and record retention periods and if these periods are reasonable for backup, disaster and recovery, and audit purposes.

7. Verify that restart and recovery plans from short-term computer interruptions include the ability to identify the status of all processing to the point of application failure to establish a cut-off for transaction re-entry.

F. Identify all subsystems.

G. Identify all transactions within each subsystem, including those automatically generated by the computer.

H. For each type of transaction, use Chart A's (page 22) transaction worksheet in this Appendix to record and evaluate application controls and procedures.

Chart A: A Checklist for Application Control Review

Note: The following checklist includes applicable ITGCs.

Application Controls Review Transaction Worksheet
System:
Subsystem:
Transaction:

A. Input Controls

Input controls ensure transactions are:

- Added into and accepted by the computer.
- Processed only once.
- Have no duplicates.

In addition, input controls make sure transaction errors in financial and non-financial data fields are:

- Identified.
- Segregated from valid transactions.
- Corrected in a timely manner.
- Returned to mainstream processing.

Questions internal auditors should ask during reviews of input controls include:

1. How does the transaction originate?

2. How is the transaction authorized (e.g., a manual signature, electronic signature, screen access authorization, etc.)?

3. Who inputs the source data? Are these individuals separate from those who reconcile the processing results?

4. How is the source data added into the application (e.g., batch, online, etc.)?

5. Is data entry conducted within a short time after the source document is created?

6. After source documents are entered into the application, are they marked or signed to indicate they were entered, thus reducing the risk of accidental duplication or reuse of the document?

7. Is there an appropriate segregation of duties for custody, authorization, recording, and periodic reconciliations for those authorized to update data?

8. How are source data documents controlled for completeness and accuracy — are documents pre-printed, sequentially pre-numbered, securely stored after being authorized, or tagged after input?

9. Is there a retention period for source data?

10. If input controls include the use of control totals, are computer-generated totals compared to independently established totals?

11. What reports do users receive to verify and monitor the operation of the application (e.g., controls totals, summaries, error counts, exception reports, etc.)?

12. How do supervisors or managers verify that production control total checking procedures are being performed?

13. How do users verify updates to the files against authorizations?

In addition, auditors need to:

1. Determine if there is an automatically triggered process that will change the application data. If yes, determine how updates of this kind are authorized, identified, and reconciled and what controls are in place to ensure the accuracy of the events that trigger the automatic process (e.g., date, inventory, reorder points, etc.).

2. Identify implemented controls to ensure completeness and accuracy of input (i.e., reconciliation of control totals, one-for-one checking, matching, sequence checking, duplicate processing, and programmed edit checks).

3. Describe any result comparisons of runs to previous runs for reasonableness checks.

4. Determine how duplicate transactions are prevented or identified.

5. Determine if and how data received from other applications is validated for completeness and accuracy.

6. Determine if and how the following automated edit checks are performed on the input data:
   - Reasonableness.
   - Dependency.
   - Range.
   - Existence.
   - Format.
   - Check digit.
   - Prior data matching.
   - Consistency.

7. Identify whether the following edit checks exist:
   - Format checks on numeric data.
   - Range checks on variable numeric fields.
   - Date tests on date fields.
   - Existence checks on key fields.
   - Check digits on identification keys.
   - Tests for missing data.
   - Tests for extraneous data.
   - Tests for record mismatches.
   - Tests for out of sequence conditions.

B. Processing Controls

Processing controls ensure transactions are:

- Accepted by the computer.
- Processed with valid logic.
- Carried through all phases of processing.
- Updated to the correct data files.

Questions internal auditors should ask during reviews of processing controls include:

1. Are users required to provide processing parameters and, if so, how are they authorized and verified?

2. Do implemented controls ensure completeness and accuracy of processing (e.g., run-to-run control totals, duplicate processing, etc.)?

3. Are end-user reconciliation procedures documented to facilitate completeness and accuracy of processing?

4. What reports do users receive to verify and monitor the application's operation (e.g., controls totals, summaries, error counts, exception reports, etc.)?

5. How do office personnel check production control totals?

6. How do supervisors or managers verify that production control totals checking procedures are being performed?

7. Are reasonableness checks performed for result comparisons of runs to previous runs? If so, describe.

8. How do users verify file updates against authorizations?

9. What is the cut-off point for special reconciliation procedures (i.e. is the cut-off point applied at the end of the month, the quarter, or at the end of the fiscal year)?

C. Error Correction

1. Identify data and processing errors that can be identified either through edits or routine processing.

2. Determine the impact data and processing errors have on processing activities (i.e., are errors corrected before processing continues or are they segregated from processing, so that good transactions may continue to be processed while errors are corrected?).

3. Determine if errors are segregated onto a suspense file and if the error suspense file is cumulative or non-cumulative.

4. Review error reports to determine if they are of a reasonable length by evaluating expected outage reports or prior period experience with respect to service level agreement.

5. Determine how errors are corrected.

6. Determine if the corrected transactions are authorized.

7. Verify that corrected transactions are reintroduced into mainstream processing at the original point of input or through a special error-correction process.

8. Determine if the error-correction process removes the items from the error suspense file.

9. Determine the timeliness of error-correction activities.

10. Identify how end users monitor the remaining errors and whether they conduct timely further investigations.

11. Is there an appropriate segregation of duties (i.e., custody, authorization, recording, and periodic reconciliations) for those authorized to update data?

12. Determine if reconciliation and error-correction procedures are documented in the end-user documentation.

13. Is an exception report generated for long-outstanding error transactions with an aging analysis?

D. Output Controls

Output controls ensure output data is:

- Reported in the correct manner.
- Viewable and available to authorized personnel only.
- Retained or destroyed appropriately.
- Subject to necessary processing audit trails.
- Segregated from valid transactions, corrected, and re-entered into mainstream processing if erroneous.

Questions internal auditors should ask during reviews of output controls include:

1. How is output distributed? Does this distribution increase the likelihood that sensitive information is viewed by unauthorized personnel by involving remote printers at end-user locations or using output distribution checklists?

2. How does the organization ensure that reports and files are distributed to the correct end users (i.e., does the organization use report routing or remote printers)?

3. Who receives the output reports? Are these individuals different from those performing the input?

4. How do end users verify that all reports were received and that report pages were included (i.e., do they use standard report titles, page numbering (1 of 10), or end-of-report indicators)?

5. Do output reports include the following identifying information:
   - Report titles?
   - Processing program names and numbers?
   - The date and time the report was produced?
   - The processing period covered?

6. How do end users verify that reports and files were received (i.e., do they use checklists, sign-off, etc.)?

7. Is there an appropriate segregation of duties in the areas of data custody, authorization, recording, and periodic reconciliations for those authorized to update the data?

8. How are confidential reports identified and distributed?

9. Are special forms used in processing and reporting? If so, determine if sensitive forms are secured (i.e., are they stored in secured areas?) and accounted for (i.e., are the forms pre-printed? Do the forms use sequentially pre-numbered forms, multipart forms, laser printed forms, etc.?).

10. Are the people responsible for securing sensitive documents different from those who maintain related accounting records?

11. Are there special disposal procedures for sensitive reports (i.e., shredding or special secured filing activities)?

E. End-user Documentation

User documentation is the primary source of information for all personnel responsible for the application's day-to-day use.

Questions internal auditors should ask during reviews of end-user documentation include:

1. Does end-user documentation exist explaining the source document's origination, authorization, data collection, input preparation, report handling, error correction, and report and data retention?

2. Are source documents retained so that data lost or destroyed during subsequent processing can be recreated?

3. Does each type of source document have a specific retention period?

F. Authorization

Authorization controls ensure that all information and data entered or used throughout processing activities is:

- Authorized by management.
- Representative of events that actually occurred.

Questions internal auditors should ask during reviews of authorization controls include:

1. Are transactions manually authorized? If so, what controls ensure that no unauthorized modifications take place after authorization and prior to establishing input controls? Is the appropriate level of management authorizing the transaction activity?

2. Is transaction authorization facilitated by logical access restrictions? If so, select a sample of access rules that apply to the transaction input and update, and verify that the correct authorized personnel have these capabilities.

3. Are allowable overrides or bypasses of data validation and edit checks (e.g., authorization, monitoring, etc.) taking place? If so, who does the overrides? Is this a manager with the appropriate authority to conduct the override? Are uses of override features automacally logged so these actions can be subsequently analyzed for appropriateness?

G. Security

Security controls ensure that access to information and facilities is restricted to only those individuals designated by management.

Questions internal auditors should ask during reviews of processing controls include:

1. Are the primary transaction, master, and reference files used in processing identified? If so, work with IS administrators to determine whether these files are secured from unauthorized access.

2. How are security access restrictions maintained? Items of importance that need to be evaluated for effectiveness include security administration, login and password management activities, security monitoring, and data ownership.

3. Is access to source documents and blank input forms restricted to authorized personnel only? If so, evaluate how access is restricted.

4. Are data entry terminals located in secured locations?

5. Are remote printers located in secure locations that protect against unauthorized access?

H. Segregation of Duties

Segregation of duty controls prevent errors and irregularities by assigning responsibility for initiating transactions, recording transactions and custody of assets to separate individuals. Segregation of duties is commonly used in organizations with a large number of employees so that no single person is in a position to commit fraud without detection.

Questions internal auditors should ask during reviews of segregation of duty activities include:

1. Are duties separated so that individuals do not perform more than one of the following operations:
   - Transaction originating?
   - Transaction authorization?
   - Transaction input?
   - Distributing output?

2. Are rejected transactions caused by entry errors that are not corrected by the user who originates the transaction?

3. Do end users have ultimate responsibility for the completeness and accuracy of all application data?

I. File Maintenance

Maintenance controls ensure data stored on computers is kept current and up-to-date and that unusual data requiring action or change is identified. This applies particularly to reference and standing data files.

Questions internal auditors should ask during reviews of file maintenance controls include:

1. Are reference and master files used in this application identified?

2. Are master file update notification procedures identified (i.e., turn-around documents, e-mail notices, control totals, etc.)? Are end users employing these update notification procedures to verify master file updates?

3. Are master files reviewed on a regular basis to verify that their contents are current and up-to-date?

Glossary

Application controls: Application controls are specific to each application and relate to the transactions and data pertaining to each computer-based application system. The objectives of application controls are to ensure the completeness and accuracy of records and the validity of the entries made resulting from programmed processing activities. Examples of application controls include data input validation, agreement of batch totals, and encryption of transmitted data.

Enterprise resource planning (ERP): ERP denotes the planning and management of resources in an enterprise, as well as the use of a software system to manage whole business processes and integrate purchasing, inventories, personnel, customer service activities, shipping, financial management, and other aspects of the business. An ERP system is typically based on a common database, integrated business process application modules, and business analysis tools. Taken from ISACA's Certified Information Systems Auditor (CISA) Glossary.

Information technology general controls (ITGCs): These controls apply to all systems components, processes, and data for a given organization or IT environment. The objectives of ITGCs are to ensure the proper development and implementation of applications, as well as the integrity of program, data files, and computer operations. The following are the most common ITGCs:

- Logical access controls over infrastructure, applications, and data.
- System development life cycle controls.
- Program change management controls.
- Data center physical security controls.
- System and data backup and recovery controls.
- Computer operation controls.

Data input controls: Data input controls ensure the accuracy, completeness, and timeliness of data throughout its conversion after it enters a computer or application. Data can be entered into a computer application through a manual online input or automated batch processing.

Data output controls: Data output controls are used to ensure the integrity of output information as well as the correct and timely distribution of any output produced. Outputs can be in hardcopy form, such as files used as input to other systems, or can be available for online viewing.

Data processing controls: Data processing controls are used to ensure the accuracy, completeness, and timeliness of data during an application's batch or real-time processing.

Risk: The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood. Taken from The IIA Professional Practices Framework.

Segregation of duties: Controls that prevent errors and irregularities by assigning responsibility to separate individuals for initiating transactions, recording transactions, and overseeing assets. Segregation of duties is commonly used in organizations with a large number of employees so that no single person is in a position to commit fraud without detection.

References

- GTAG 1: *Information Technology Controls*.
- GTAG 4: *Management of IT Auditing*.
- ISACA, IS Auditing Guideline Application Systems Review, Document G14.
- COSO's *Internal Control Over Financial Reporting Guidance for Smaller Public Companies*.
- PCAOB adopted Audit Standard No.5, "An Audit of Internal Control over Financial Reporting That Is Integrated With An Audit of Financial Statements."
- The IIA *Standard* 1220.
- The IIA Attribute *Standard* 1210.A3.
- The IIA Attribute *Standard* 1130.C1.
- AXA *Group*, *Common Application Controls and Suggested Testing*.

Christine Bellino, CPA, CITP
Christine Bellino is the director of technology risk management for the Jefferson Wells' Denver, Colorado practice and is a member of The IIA's Advanced Technology Committee. Christine is a member of the organization's Guide to the Assessment of IT General Controls Scope based on Risk (GAIT) core team. Her current responsibilities include the management of multiple business processes and ITGC reviews for small-, mid-, and large-size organizations.

Bellino has more than 25 years of finance, operations, and technology risk management experience and was co-chair of the COSO Task Force responsible for the recently released *Internal Control Over Financial Reporting — Guidance for Smaller Public Companies*.

Steve Hunt, MBA, CIA, CISA, CBM
Steve Hunt is the director of enterprise solutions for Enterprise Controls Consulting (ECC) and is a member of The IIA's Advanced Technology Committee, ISACA, and the Association of Professionals in Business Management. At ECC, Hunt works with Fortune 1000, mid-size, and small-market companies in different industries, directing the delivery of financial, operational, and IT risk management engagements.

Hunt has more than 20 years of experience working in various industries, including accounting, internal auditing, and management consulting. More specifically, he has performed in-depth Sarbanes-Oxley compliance audits and other internal and external audits, and participated in business process reengineering projects and business development initiatives. He also has several years experience configuring SAP R/3 applications and application security and business process controls and has been a featured speaker at several universities and organizations across the United States.

Reviewers
The IIA thanks the following individuals and organizations who provided valuable comments and added great value to this guide:

- IT Auditing Speciality Group, The IIA - Norway.
- The technical committees of The IIA - UK and Ireland.
- Helge Aam, Deloitte - Norway.
- Ken Askelson, JCPenney - USA.
- Rune Berggren, IBM - Norway.
- Shirley Bernal, AXA Equitable Life Insurance Company - USA.
- Lily Bi, The IIA.
- Claude Cargou - AXA, France.
- Maria Castellanos, AXA Equitable Life Insurance Company - USA.
- Nelson Gibbs, Deloitte & Touché, LLP.
- Steven Markus, AXA Equitable Life Insurance Company - USA.
- Peter B. Millar, ACL Services Ltd. - Canada.
- Stig J. Sunde, OAG - Norway.
- Jay R. Taylor, General Motors Corp. - USA.
- Karine Wegrzynowicz, Lafarge North America.
- Hajime Yoshitake, Nihon Unisys, Ltd. - Japan.
- Jim Zemaites, AXA Equitable Life Insurance Company - USA.
- Joe Zhou, GM Audit Services - China.

Advocate for the Profession of Internal Auditing!

To access the wealth of advocacy resources and tools available through The IIA, visit our home page at www.theiia.org. Press the "Start Here" button to begin making a difference today!

ADVOCATE INTERNAL AUDITING START HERE

The Institute of
Internal Auditors

GTAG®

Auditing Application Controls

Application controls are those controls that pertain to the scope of individual business processes or application systems, such as data edits, separation of business functions, balancing of processing totals, transaction logging, and error reporting. Effective application controls will help your organization to ensure the integrity, accuracy, confidentiality, and completeness of your data and systems. This guide provides chief audit executives (CAEs) with information on application control, its relationship with general controls, scope a risk-based application control review, the steps to conduct an application controls review, a list of key application controls, and a sample audit plan.

Visit www.theiia.org/guidance/technology/gtag/gtag8 to rate this GTAG or submit your comments.

What is GTAG?

Prepared by The Institute of Internal Auditors, each Global Technology Audit Guide (GTAG) is written in straightforward business language to address a timely issue related to information technology management, control, and security. The GTAG series serves as a ready resource for chief audit executives on different technology-associated risks and recommended practices.

Guide 1: *Information Technology Controls*

Guide 2: *Change and Patch Management Controls: Critical for Organizational Success*

Guide 3: *Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*

Guide 4: *Management of IT Auditing*

Guide 5: *Managing and Auditing Privacy Risks*

Guide 6: *Managing and Auditing IT Vulnerabilities*

Guide 7: *Information Technology Outsourcing*

Visit the technology section of The IIA's Web site at www.theiia.org/technology to download the entire series.

Order Number: 1033
IIA Member US $25
Nonmember US $30
IIA Event US $22.50

ISBN 978-0-89413-613-9
30000
9 780894 136139

The Institute of
Internal Auditors

www.theiia.org

07227