GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

Auditing Application Controls

The Institute of
Internal Auditors

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.

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 payable 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 of this chapter 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.

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

[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 IT General Controls

It is important for CAEs and their staff to understand the relationship and difference between application controls and Information Technology General Controls (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

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

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

[7,8] ISACA, IS Auditing Guideline — Application Systems Review, Document G14, p. 3.

within the parameters of customer credit limits.

- 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 among 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.
- 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 (PCAOB) Auditing Standard No. 5, 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]

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

[10] COSO's, *Internal Control over Financial Reporting — Guidance for Smaller Public Companies*, Vol. III, p. 56.

[11] PCAOB, Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting That is Integrated with An Audit of Financial Statements, paragraph B29.

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 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 (e.g., 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)* — specifically 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

[12] PCAOB, Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting That is Integrated with An Audit of Financial Statements, paragraph B29.

[13] PCAOB, Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting That is Integrated with An Audit of Financial Statements, paragraphs B29 - 30.

[14] IIA Standard 1220: Due Professional Care.

[15] IIA Standard 1210.A3.

proficient enough to determine if implemented application controls are appropriately designed and operating effectively to manage financial, operational, or regulatory compliance risks.

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 upgrade 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. 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.

[16] IIA Standard 1130.C1

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 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.

Assess Risk

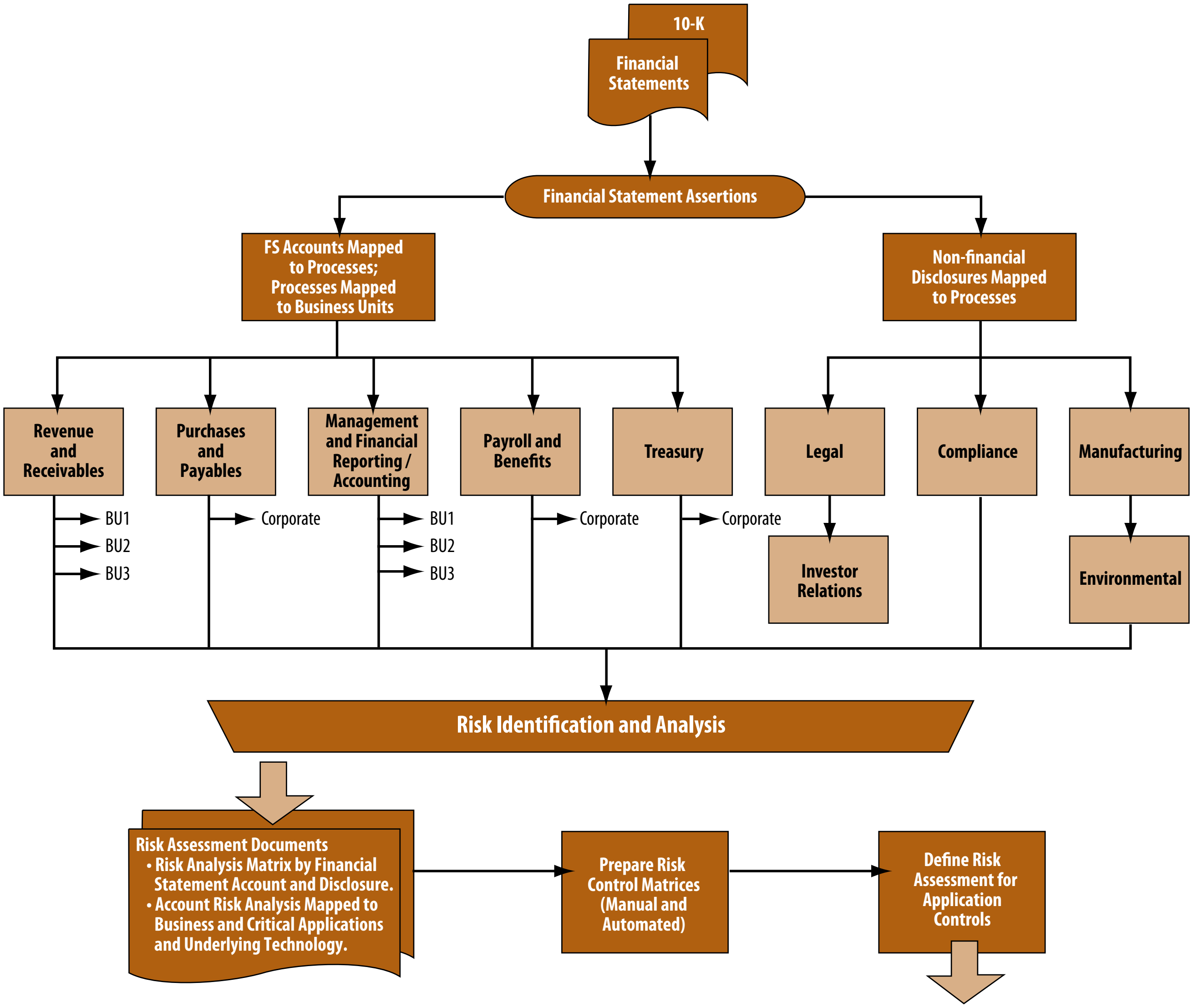
The auditor should use risk assessment techniques to identify critical vulnerabilities pertaining to the organization's reporting, and operational and compliance requirements when developing the risk assessment review plan. These techniques include:

- 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 organizationwide 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 a top-down risk assessment 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 all types of 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. Unconfigured pre-packaged or developed applications as opposed to highly configured in-house or purchased applications.
    - 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 its weight in the application and adding the totals. For example, the composite score of 375 on the first line 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 greater.

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 ITGCs	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 two 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 (e.g., read, write, and delete) are built using the inherent security platform and tools within the application. The strategies employed to determine which logical access rights will 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, such as SAP R/3, 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 user name 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).

The latest generation of applications are often 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 configured to require a password change every 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, the 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 page 21, for a sample audit program.) 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 (e.g., 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 planned 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 of the configuration capabilities of the Oracle application. Additional staff who know how to mine data from the Oracle application and database to facilitate the review may be needed. 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 (Level 1): This refers to the complete end-to-end process, such as procure-to-pay.
- Major Process (Level 2): This refers to the major components of the end-to-end process, such as procurement, receiving, and payment of goods.

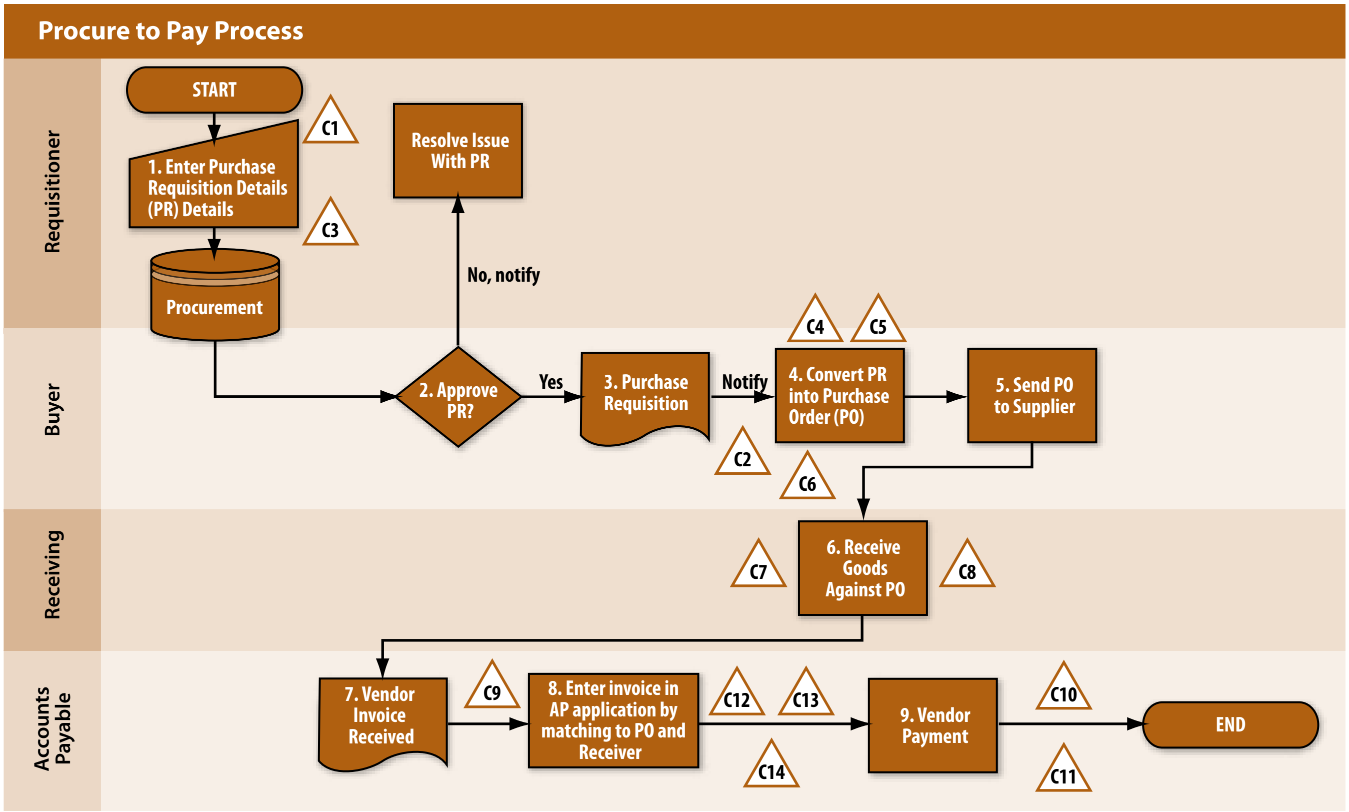
- Minor, or Subprocess (Level 3): This level lists the minor, or subprocess, components of each of the major processes, such as requisitioning and purchase order creation.
- Activity (Level 4): This final level lists the system transactions that result in the creation, change, or deletion of data for 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, the 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, pages 14–17), that contains the control descriptions and associated information. However, flowcharts may not be practical all of the time, and a process narrative is sometimes 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.

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 control matrix.

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

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 process 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 (e.g., automated or manual) and frequency (e.g., 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 (using the same programmed procedures as production) with robust testing scripts.

An example of a system configuration test includes reviewing 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 generation 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 of 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 can perform a complete review of all transactions and uncover abnormalities (e.g., duplicate vendors or transactions) or a set of predetermined control issues (e.g., 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. Continued.

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. Continued.

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. Continued.

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 a 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 totals, 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.	• Conduct tests based on user access rights. • Review access rights that 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.
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 aged 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 Audit Program

Internal auditors should develop and record a plan for each audit engagement, including objectives, scope, resource considerations, and audit work program. Objectives allow the auditor to determine whether the application controls are appropriately designed and operating effectively to manage financial, operational, or regulatory compliance risks. The objectives of application controls include the following, as outlined on page two of this guide:

- 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 that tracks the process of data input, storage, and output.

Here are the steps to achieve the above objectives:

- Step 1. Perform a risk assessment (see page 7 of this guide).
- Step 2. Determine the scope of the review (see page 9 of this guide).
- Step 3. Develop and communicate the detailed review plan (see page 10 of this guide).
- Step 4. Determine the need for specialized resources (see page 10 of this guide).
- Step 5. Determine whether computer-assisted audit techniques will be required (see page 13 of this guide).
- Step 6. Conduct the audit (see the following sample audit program). Please note that the sample program is not intended to cover all tests applicable to your organization.

Sample Audit Program

A review of the specific company data and the scope of the audit will determine the detailed test steps related to the following review activities.

Control Objective	Controls	Review Activities
Objective 1: Input data is accurate, complete, authorized, and correct.		
	Input controls are designed and operating effectively to ensure that all transactions have been authorized and approved prior to data entry.	Obtain data input procedures, gain an understanding of the authorization and approval process, and determine whether a review and approval process exists and has been communicated to users responsible for obtaining appropriate approvals. Verify that the application owner or process owner ensures that all data is authorized prior to input. This may be done through the granting of roles and responsibilities based on job duties. Obtain a copy of the approval levels and determine whether responsibility is assigned for verifying that appropriate approvals are consistently applied.

Sample Audit Program

Control Objective	Controls	Review Activities
	Input controls are designed and operating effectively to ensure that all entered transactions will be processed correctly and completely.	Obtain data input procedures and verify that individuals responsible for entering data have been trained on the preparation, entry, and control of input. Determine whether edit routines are embedded within the application that checks and subsequently rejects input information that does not meet certain criteria, including but not limited to, incorrect dates, incorrect characters, invalid field length, missing data, and duplicate transaction entries/numbers. Verify the existence and operation of manual data entry controls to prevent the entry of duplicate records. Manual data entry controls may include the pre-numbering of source documents and the marking of records as “input” after entry. Verify that added data is from an acceptable source and reconciled to the source utilizing control totals, record counts, and other techniques including the use of independent source reports. Determine whether appropriate segregation of duties exists to prevent users from both entering and authorizing transactions. Verify that appropriate segregation of duties exists between data entry personnel and those responsible for reconciling and verifying that the output is accurate and complete. Verify that controls exist to prevent unauthorized changes to system programs such as calculations and tables.
	Input controls are designed and operating effectively to ensure that all rejected transactions have been identified and reprocessed appropriately and completely.	Obtain data input procedures for handling rejected transactions and subsequent error correction and determine whether personnel responsible for error correction and data reentry have been adequately trained. Verify a mechanism is in place for notifying the process owner when transactions have been rejected or errors have occurred. Verify rejected items are reprocessed appropriately in a timely manner in accordance with the procedures, and errors are corrected before reentering into the system.

Sample Audit Program

Control Objective	Controls	Review Activities
	Controls are designed and operating effectively to ensure that data automatically posted from another system is processed accurately and completely.	Obtain procedures and verify that detailed information is included on how automated interfaces are authorized and what triggers the automated processing event. Verify that processing schedules are documented and problems are identified and corrected on a timely basis. Determine whether system to system record counts and total dollar values are systematically verified for automated interfaces and rejected items are prevented from posting and are flagged for follow-up and re-processing. Verify that files and data created for use by other applications or that are transferred to other applications are protected from unauthorized modification during the entire transfer process.
	Controls are designed and operating effectively to ensure that correct data files and databases are used in processing.	Validate that the test data and programs are segregated from production.
Objective 2: Data is processed as intended in an acceptable time period.		
	Processing controls are designed and operating effectively to ensure that all transactions are processed in a timely manner and within the correct accounting period.	Verify output is reviewed or reconciled against source documents for completeness and accuracy, including verification of control totals. Determine whether routines are embedded within the application that ensure all correctly entered transactions are actually processed and posted as intended in the correct accounting period.
	Processing controls are designed and operating effectively to ensure that all rejected transactions have been identified and reprocessed in a timely manner.	Obtain procedures for handling rejected transactions and subsequent error correction and determine whether personnel responsible for error correction and data reentry have been adequately trained. Verify a mechanism is in place for notifying the process owner when transactions have been rejected or errors have occurred. Verify rejected items are processed appropriately in a timely manner in accordance with the procedures, and errors are corrected before reentering into the system.

Sample Audit Program

Control Objective	Controls	Review Activities
Objective 3: Data stored is accurate and complete.		
	Logical access controls are designed and operating effectively to prevent unauthorized access, modification, or disclosure of system data.	Obtain password configuration and use policies and determine whether requirements for strong passwords, password resets, account lockout, and password re-use are present. Verify that the above policy has been applied to the application(s) under review. Verify that remote access controls are designed and operating effectively. Verify that users are restricted to specific functions based on their job responsibilities (role-based access). Verify unique user IDs are assigned to all users, including privileged users, and that user and administrative accounts are not shared. Verify proper approval of user account creation and modification is obtained prior to granting or changing access. (Users include privileged users, employees, contractors, vendors, and temporary personnel.) Verify access is removed immediately upon termination. Verify that the application owner is responsible for ensuring that a semi-annual review occurs of user and system accounts to ensure access to critical financial data, applications, and operating systems is correct and current.
	Controls are designed and operating effectively to ensure that data backups are accurate, complete, and occur in a timely manner.	Verify proper approval of user account creation and modification is obtained prior to granting or changing access. (Users include privileged users, employees, contractors, vendors, and temporary personnel.) Verify access is removed immediately upon termination. Verify that the application owner is responsible for ensuring that a semi-annual review occurs of user and system accounts to ensure access to critical financial data, applications, and operating systems is correct and current.
	Controls are designed and operating effectively to ensure that data is physically stored in a secured, offsite, environmentally-controlled location.	Verify that mechanisms are in place to store data offsite in a secured and environmentally-controlled location.

Sample Audit Program

Control Objective	Controls	Review Activities
Objective 4: Outputs are accurate and complete.		
	Output controls are designed and operating effectively to ensure that all transaction outputs are complete and accurate.	Obtain data output procedures and gain an understanding of the review process and verify that individuals responsible for data entry have been trained on the review and verification of data output. Verify output is reviewed or reconciled against source documents for completeness and accuracy, including verification of control totals.
	Output controls are designed and operating effectively to ensure that all transaction output has been distributed to appropriate personnel and that sensitive and confidential information is protected during distribution.	Review existing data output procedures and determine whether they document which personnel receive the data output and how the data will be protected during distribution.
	Output controls are designed and operating effectively to ensure that an output report is created at the designated time and covers the designated period.	Verify that an output report was created and identify that the date and time on the report is the designated time. Identify that the report covers the designated period via reconciliation against source documents from that period.
Objective 5: A record is maintained that tracks the process of data input, storage, and output.		
	Controls are designed and operating effectively to ensure that an audit trail is generated and maintained for all transactional data.	Verify processing audit trails and logs exist that assure all records have been processed and allow for tracing of the transaction from input to storage and output. Verify audit reports exist that track the identification and reprocessing of rejected transactions. Reports should contain a clear description of the rejected transaction, date, and time identified.

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.

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.

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.[18]

IT 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.

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.[19]

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.

[18] Taken from the ISACA's Certified Information Systems Auditor Glossary.

[19] Taken from the glossary of The IIA's International Professional Practices Framework.

References

- GTAG 4: *Management of IT Auditing*.
- GTAG 1: *Information Technology Controls*.
- ISACA, IS Auditing Guideline — Application Systems Review, Document G14.
- COSO's *Internal Control over Financial Reporting — Guidance for Smaller Public Companies*.
- PCAOB, Auditing Standard No. 5, An Audit of Internal Control Over Financial Reporting That is Integrated with An Audit of Financial Statements, paragraphs B29 - 30.
- IIA Standard 1220: Due Professional Care.
- IIA Standard 1210.A3.
- IIA Standard 1130.C1
- AXA Group, *Common Application Controls and Suggested Testing*.
- ISACA Certified Information Systems Auditor Glossary.
- The IIA's Professional Practices Framework.

Christine Bellino, CPA, CITP

Christine Bellino is the director of technology risk management for the Jefferson Wells' Denver practice and is a member of The IIA's Advanced Technology Committee. Bellino 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-sized 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, 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 1,000 mid-sized, 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 of 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 Co. Inc. – USA.
- Rune Berggren, IBM – Norway.
- Shirley Bernal, AXA Equitable Life Insurance Co. – USA.
- Lily Bi, The IIA.
- Claude Cargou, AXA – France.
- Maria Castellanos, AXA Equitable Life Insurance Co. – USA.
- Nelson Gibbs, Deloitte & Touche, LLP.
- Steven Markus, AXA Equitable Life Insurance Co. – 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 Co – USA.
- Joe Zhou, GM Audit Services – China.

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 CAEs 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

07526