GAIT METHODOLOGY

The Institute of Internal Auditors

PROFESSIONAL GUIDANCE

Setting the Standard

GAIT Methodology

A risk-based approach to assessing the scope of IT general controls

The Institute of Internal Auditors
August 2007

Table of contents

Welcome 3
Part 1. Understanding GAIT 4
Executive summary 4
Understanding GAIT's four core principles 6
A word about entity-level controls 10
Part 2. Applying the GAIT methodology 11
GAIT: concisely 11
Documenting GAIT results 12
Customizing GAIT 13
Gathering the GAIT assessment team 13
GAIT methodology phases 13
Phase 1 Identify (and validate if necessary) the critical IT functionality 14
Phase 2 Identify the [significant] applications where ITGC need to be tested 16
Phase 3 Identify ITGC process risks and related control objectives 17
Phase 4 Identify the key ITGCs to test that meet the control objective 25
Phase 5 Perform a reasonable person review 28
Appendix 29
Sample GAIT matrix 29
GAIT template 31
Handling bottom-up risk assessments 34
Definitions 35

List of tables

Table 1: Sections in The GAIT Methodology 3
Table 2: Understanding GAIT 4
Table 3: GAIT's four core principles 6
Table 4: GAIT matrix 9
Table 5: Applying GAIT 11
Table 6: Empty GAIT matrix 12
Table 7: Additional application infrastructure and risk information 17
Table 8: Application layer IT general controls processes and typical risks 20
Table 9: Database layer IT general controls processes and typical risks 21
Table 10: Operating system layer IT general controls processes and typical risks 22
Table 11: Questions to ask for each cell in the GAIT matrix 23
Table 12: Evaluating pervasiveness 26
Table 13: Identifying key ITGCs 27
Table 14: Partially completed GAIT matrix 29
Table 15: GAIT template 31
Table 16: Glossary 35

List of procedures

☞ To apply the GAIT methodology 13
☞ To review the key manual and automated controls and key functionality 14
☞ To identify the applications where ITGC need to be tested 16
☞ To extend the understanding of the in-scope applications and their infrastructure 17
☞ To assess the risk of ITGC process failures 22
☞ To evaluate the pervasiveness of ITGC 26
☞ To select key controls for reliance and testing 27
☞ To review risks 28
☞ To handle a bottom-up risk assessment 34

Welcome

Welcome to *The GAIT Methodology*, a guide to assessing the scope of IT General Controls using a top-down and risk-based approach. *The GAIT Methodology* is based on *The GAIT Principles*, also published by The Institute of Internal Auditors. The *Methodology* is an approach to implementing the *GAIT Principles* from the developers of that document.

The Methodology is organized into sections, as described in Table 1 below.

Table 1: Sections in The GAIT Methodology

Part	Description	See
"Part 1. Understanding GAIT"	Information to help you understand the theory behind the GAIT methodology. It recaps and expands on *The GAIT Principles*.	Page 4
"Part 2. Applying the GAIT methodology"	Procedures to apply the GAIT methodology.	Page 11
"Appendix"	Supplementary information, such as samples and a glossary of terms.	Page 29

Part 1. Understanding GAIT

To guide you to a better understanding of GAIT, this part is divided into sections, described in Table 2 below.

Table 2: Understanding GAIT

Section	Description	See
"Executive summary"	High-level introduction to GAIT.	Page 4
"Understanding GAIT's four core principles"	Detailed discussion of GAIT's core principles.	Page 6
"A word about entity-level controls"	Brief discussion of entity-level controls as they relate to GAIT.	Page 10

Executive summary

A major challenge facing both management of organizations and their independent auditors is defining an effective and efficient scope for the annual assessments of internal control over financial reporting (ICFR) required by Section 404 ("§404") of the Sarbanes-Oxley Act of 2002.

The U.S. Securities and Exchange Commission (SEC)[1] and the Public Company Accounting Oversight Board (PCAOB)[2] have recommended a top-down and risk-based approach to defining §404 scope and related key controls[3]. That recommendation has been made, and generally accepted, as it enables an efficient assessment that is focused on the more likely and significant risks to financial reporting.

1. In its May 16, 2005 "Commission Statement on Implementation of Internal Control Reporting Requirements" and its interpretive guidance published in June 2007.
2. In Auditing Standard Number 5.
3. SEC and PCAOB guidance does not discuss the concept of a "key control". However, it has become a term recognized by both management and external auditors. See "Key control" on page 37.

Guidance has been provided by organizations such as The Institute of Internal Auditors (IIA) and the PCAOB relative to the identification of key controls at the business level. Additional guidance has also been published by organizations including the Information Systems Audit and Control Association (ISACA) relative to the assessment of controls within IT organizations. However, there remains less certainty about how the scope of work related to controls within IT organizations (IT general controls or ITGC[4, 5]) should be determined using the recommended top-down and risk-based approach.

If ITGC key controls (which exist within ITGC processes) are not identified as part of a top-down and risk-based approach that starts at the financial statement and significant account level and flows down to ITGC, there is a risk that:

- Controls may be assessed and tested that are not critical, resulting in unnecessary cost and diversion of resources.
- Controls that are key may not be tested, or may be tested late in the process, presenting a risk to the assessment or audit.[6]

This Guide to the Assessment of IT General Controls Scope based on Risk (GAIT) provides a methodology that both management and external auditors[7] can use in their identification of key controls within ITGC *as part* of and *a continuation* of their top-down and risk-based scoping of key controls for ICFR. It is consistent with the methodology described in the PCAOB's Auditing Standard Number 5 (AS/5),[8] the SEC's proposed interpretive guidance (published in June 2007), and The IIA's "Sarbanes-Oxley Section 404: A Guide for Management by Internal Controls Practitioners" (§404 Guide).

GAIT is a structured reasoning process that can be tailored for an organization. The business process risks and related key controls identified by the top-down and risk-based approach are its starting point. Those risks to the financial statements are taken to the next level using GAIT analysis: identifying risks within ITGC processes where a controls or security failure could lead to a controls failure of material significance within the business process — in turn leading potentially to a material misstatement of the financial statements.

4 ITGC are controls, generally within the IT organization's business processes (alternatively described as ITGC processes). They can be described as follows:

"Broadly speaking, ITGC provide assurance that applications are developed and subsequently maintained, such that they provide the functionality required to process transactions and provide automated controls. They also assure the proper operation of the applications and the protection of both data and programs from unauthorized change." (§404 Guide)

5 See "ITGC" on page 36.

6 It should be noted that key controls are also critical to business operations. Failure to identify and test all key controls represents a potential failure to test controls over important business risks – not just for financial reporting issues but also for other business risk management purposes.

7 This Guide refers to "users", which are intended to include management responsible for the §404 program, independent auditors, and internal auditors, etc.

8 As a matter of policy, the PCAOB will not endorse or otherwise publicly approve guidance such as this document, nor confirm that it is consistent with the principles of AS/5.

GAIT does not identify specific key controls. Rather, it identifies the ITGC processes and related IT control objectives for which key controls need to be identified. Users of GAIT will employ other tools, such as COBIT, to identify and then assess specific ITGC key controls.

Because the identification of risks within ITGC processes is a continuation of the top-down approach that starts with significant accounts and the related business processes, it should be performed by an integrated team of business and IT experts. Business experts alone will not appreciate the technical IT aspects and IT experts alone may not have a sufficient understanding of the extent of reliance on IT functionality.

At this time, GAIT focuses on ITGC risk assessment and scoping for the §404 assessment, but the principles can also be applied to the identification of controls for other assessment purposes (e.g., as part of an assessment of controls over compliance with applicable laws and regulations). Future editions are planned to provide guidance in some of those other areas.

Understanding GAIT's four core principles

This section provides information about GAIT's four core principles, found in *The GAIT Principles* and summarized in Table 3 below. For information about *applying* the principles, see "Applying the GAIT methodology" on page 11.

Table 3: GAIT's four core principles

	Principle	For Details, See…
1	The identification of risks and related controls in IT general control processes (e.g., in change management, deployment, access security, operations) should be a continuation of the top-down and risk-based approach used to identify significant accounts, risks to those accounts, and key controls in the business processes.	Page 7
2	The IT general control process risks that need to be identified are those that affect critical IT functionality in financially significant applications and related data.	Page 8
3	The IT general control process risks that need to be identified exist in processes and at various IT layers: application program code, databases, operating systems, and network.	Page 9
4	Risks in IT general control processes are mitigated by the achievement of IT control objectives, not individual controls.	Page 9

Principle 1

The identification of risks and related controls in IT general control processes (e.g., in change management, deployment, access security, operations) should be a continuation of the top-down and risk-based approach used to identify significant accounts, risks to those accounts, and key controls in the business processes.

GAIT continues the top-down approach stated in AS/5, using the results of the business process-related steps (specifically, identifying key controls that rely on IT functionality) to:

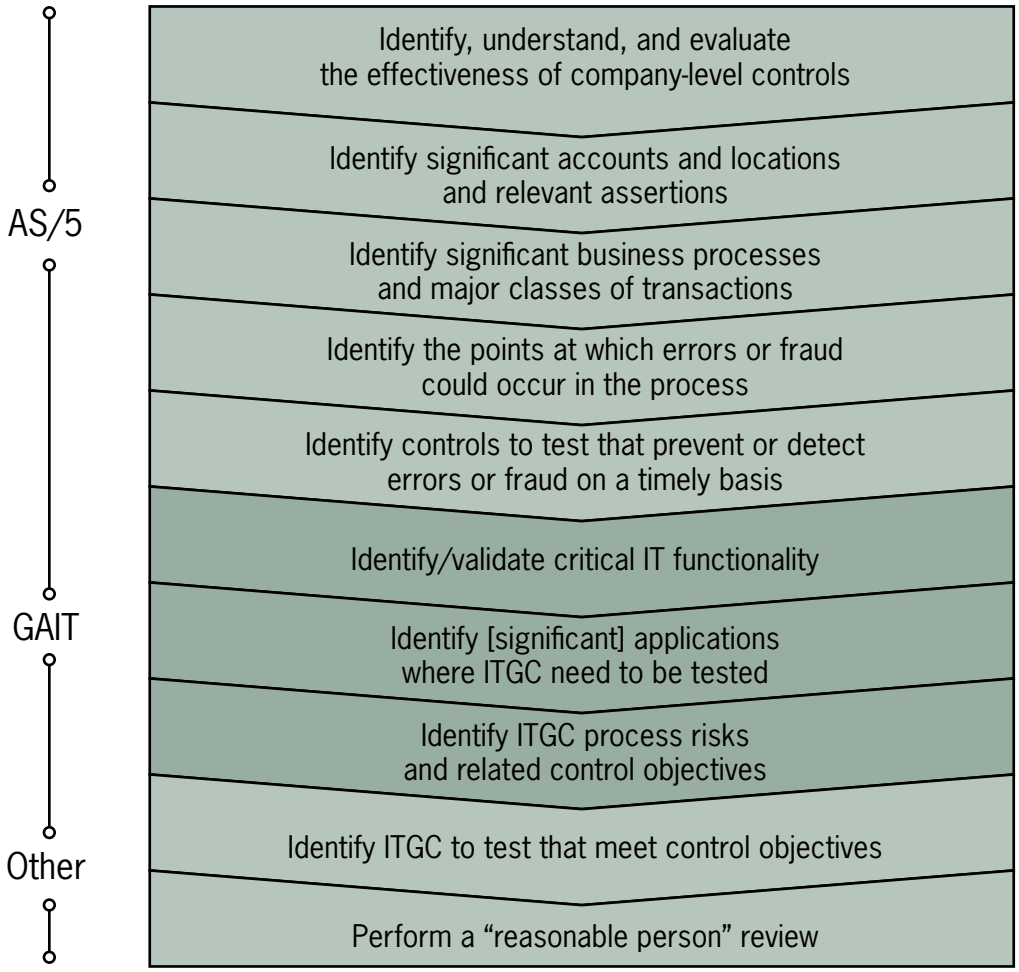
- Help users identify the potential points of failure in ITGC processes that could lead to errors or fraud and result in material misstatement of the financial statements, and
- Enable the identification of key ITGCs over those risks.

Figure 1 below is a summary representation of the top-down process (see also page 38) that includes GAIT activities. It includes:

1. **AS/2**, which starts with the identification of significant accounts and locations, then the business processes related to those significant accounts, the potential points of failure in the business processes that could lead to material misstatement, and then the key controls to prevent and detect material misstatements. ITGC is discussed in AS/2, but not in depth.
2. **GAIT** continues the process, identifying the critical IT functionality relied on to prevent or detect material misstatements (such as key automated controls and key reports), then significant applications[9] (those containing critical IT functionality and/or data), then ITGC processes related to significant applications, then IT control objectives required to assure continued operation of critical IT functionality in significant applications.
3. **Any methodology** for defining key controls in ITGC, such as COBIT .

9 In this context, "application" refers to the computer system. Some use the term for the business process as a whole, but here the intent is to identify computer systems that need to be assessed for their reliance on IT General Controls. Similarly, the term "financially significant applications" refers to computer systems rather than entire business processes.

Figure 1: Top-down process, including GAIT



Principle 2

The IT general control process risks that need to be identified are those that affect critical IT functionality in financially significant applications and related data.

The scope of work for §404 needs only address risks in ITGC processes that (indirectly, through their impact on critical IT functionality) represent a reasonably likely risk of material error in the financial statements. The top-down approach in AS/5 includes identifying potential points of failure in business processes and related key controls. Where IT functionality is relied upon (e.g., there is reliance on automated key controls or key reports, or where there is financially significant data), that application is considered financially significant (see "Financially significant" on page 36) and risks to the functionality from defects in ITGC processes need to be addressed.

Principle 3

The IT general control process risks that need to be identified exist in processes and at various IT layers: application program code, databases, operating systems, and network.

Activities in IT — such as performing network scans, maintaining routers, and testing changes to applications — belong to ITGC processes. GAIT assumes the activities that relate to ITGC exist in the change management, operations, and security business processes. Using these definitions of the ITGC processes (found in "Definitions" on page 36) is not critical to using GAIT. Each user of GAIT can substitute their definition without affecting the GAIT methodology.

Each ITGC process operates at the four layers of each application's IT infrastructure — application, database (including related structures such as the schema), operating system, and network infrastructure. These layers are also known as the "stack". Risks to the reliability of financially significant applications and data can be assessed for each ITGC process at each layer of the IT infrastructure (e.g., by assessing risk in the change management process at the application code layer, or in the security management process at the database level).

Table 4 below provides an example of an empty GAIT matrix, which illustrates how the stack relates to the ITGC processes. For information about filling out the GAIT matrix, see the section on "To assess the risk of ITGC process failures" on page 22. For a sample of a partially completed GAIT matrix, see "Sample GAIT matrix" on page 29.

Table 4: GAIT matrix

Layer	Change Management	Operations	Security
Application			
Database			
Operating system			
Network infrastructure			

Principle 4

Risks in IT general control processes are mitigated by the achievement of IT control objectives, not individual controls.

Each ITGC process contains controls that help achieve IT control objectives, such as:

- Systems are appropriately tested and validated prior to being placed into production.
- Data is protected from unauthorized change.
- Any problems or incidents in operations are properly responded to, recorded, investigated, and resolved.

Failure to achieve these objectives might imply that critical IT functionality fails to perform appropriately and consistently. GAIT helps identify the IT control objectives required for the financially significant applications.

Controls in ITGC processes do not directly relate to the risk of material errors in the financial statements. Individual ITGCs assure that relevant IT control objectives are achieved. Those control objectives assure that critical IT functionality operates consistently. That IT critical functionality is required for key controls in the business processes to function consistently. The key controls in the business processes are required to prevent or detect material errors in the financial statements.

As a result, it is important to first identify relevant IT control objectives and only when they have been defined should the key controls in ITGC be identified. The key ITGC controls that should be included in scope are those that are required to satisfy the IT control objectives. While certain ITGC controls might appear important, unless they are required to address an identified IT control objective they do not need to be included in the scope of assessment and testing for §404.

A word about entity-level controls[10]

The SEC and PCAOB recommend that an assessment of entity controls (see "Entity-level control" on page 35) be performed early in the §404 process. The information obtained from the assessment of risks and controls at the entity level (especially those related to the COSO Controls Environment layer) can be considered in assessing risks and related controls at lower levels, such as those in ITGC processes.

For that reason, GAIT does not include a detailed discussion of the assessment of IT entity controls. They are assumed to have been reviewed as part of the overall assessment of entity level controls.

The information obtained from the entity-level controls work should be considered when using GAIT, as it might affect the assessment of the likelihood of certain ITGC process failures. For example, the COSO Controls Environment includes questions related to staffing the organization with appropriately qualified and trained personnel. If there are issues in this area in IT, such that inexperienced individuals are testing applications, it might indicate a higher risk that the testing is less than adequate.

10 See Glossary on page 38. Note that the term "entity-level" is synonymous with "company-level", which is used in some publications.

Part 2. Applying the GAIT methodology

To help you get started in applying GAIT, this part is divided into sections, described in Table 5 below.

Table 5: Applying GAIT

Section	Description	See
"GAIT: concisely"	The essence of the GAIT methodology.	Below
"Documenting GAIT results"	Description of how to document the GAIT results.	Page 12
"Customizing GAIT"	Description of how to customize GAIT for your organization.	Page 13
"Gathering the GAIT assessment team"	Description of the team members necessary to apply GAIT.	Page 13
"GAIT methodology phases"	The step-by-step process for applying GAIT, in phases.	Page 13

GAIT: concisely

The GAIT methodology examines each financially significant application and determines whether failures in the ITGC processes at each layer in the stack represent a likely threat to the consistent operation of the application's critical functionality. If a failure is likely, GAIT identifies the ITGC process risks in detail and the related ITGC control objectives that, when achieved, mitigate the risks. COBIT and other methodologies can identify the key controls to address the ITGC control objectives.

In short, the GAIT methodology guides you through asking three questions in sequence:

1. What IT functionality in the financially significant applications is critical to the proper operation of the business process key controls that prevent/detect material misstatement (i.e., what is the critical IT functionality)?
2. For each IT process at each layer in the stack, is there a reasonable likelihood that a process failure would cause the critical functionality to fail — indirectly representing a risk of material misstatement (i.e., if that process failed at that layer, what effect would there be on the critical functionality? Would it cause the functionality to fail such that there would be a reasonably likely risk of material misstatement)?
3. If such ITGC process risks exist, what are the relevant IT control objectives (i.e., what IT control objectives need to be achieved to provide assurance over the critical functionality)?

For example:

- **Risk** (within the change management process at the application layer of the stack): Untested application changes could lead to a failure of critical functionality.
- **Control objective:** All program changes are appropriately tested and the results reviewed and approved prior to implementation.
- **Key controls:**
  - Program changes are tested in a separate test environment.
  - All test results are reviewed and approved by a manager.
  - User testing is performed for all major changes and the results approved by a manager.
  - Emergency changes are reviewed and approved by senior IT management.

Documenting GAIT results

This document provides two approaches to documenting the GAIT results: the GAIT matrix described below and the GAIT template (see "GAIT template" on page 29). However, no matter the approach you choose, you should document in enough detail to allow a reasonable reviewer to understand the rationale that led to the documented results.

The GAIT matrix (see Table 6 below) illustrates the methodology and lets you document the results for each financially significant application. You can record in each cell the assessment of whether there is a risk to the critical functionality for that business process at that layer of the stack, and identify the relevant IT control objectives.

Table 6: Empty GAIT matrix

Layer	Change Management	Operations	Security
Application			
Database			
Operating system			
Network infrastructure			

Customizing GAIT

GAIT is flexible. Users can customize its steps to accommodate their terminologies and IT control frameworks. In particular, users can use their own definitions of ITGC processes and levels — such as adding user access and privileged access to the already existing change management, operations, security — in the stack in the GAIT matrix. For more information about the stack, see "Principle 3" on page 9.

Gathering the GAIT assessment team

Experience has shown that business users do not always completely understand the IT functionality on the screens and reports they use, and IT experts do not always completely understand the business processes and what they rely on. An integrated team of internal control experts with both business and IT knowledge should perform the GAIT assessment.

GAIT is a continuation of the top-down and risk-based approach performed in its initial stages by those with business expertise. It is based on an understanding of the critical IT functionality relied upon to ensure the proper operation of business process key controls (which prevent and detect material misstatement of the financials) that were identified during the assessment of potential points of failure in the business processes.

As the GAIT assessment continues, into the more technical aspects of IT infrastructure and IT processes, IT expertise becomes more critical. That expertise should be sufficient to understand and identify critical IT functionality (including key automated controls, key reports, and other functionality), potential points of failure in related ITGC processes, and the appropriate ITGC control objectives and key controls.

An integrated team should review and confirm the results of the GAIT assessment to ensure that they are appropriate and reasonable.

GAIT methodology phases

To apply the GAIT methodology, follow the phases listed in the procedure below.

To apply the GAIT methodology

Phase 1: Identify (and validate if necessary) the critical IT functionality. See page 14.

Phase 2: Identify the [significant] applications where ITGC need to be tested. See page 16.

Phase 3: Identify ITGC process risks and related control objectives. See page 17. This is the core of the GAIT methodology.

Phase 4: Identify the ITGC to test that meet control objectives. See page 25.

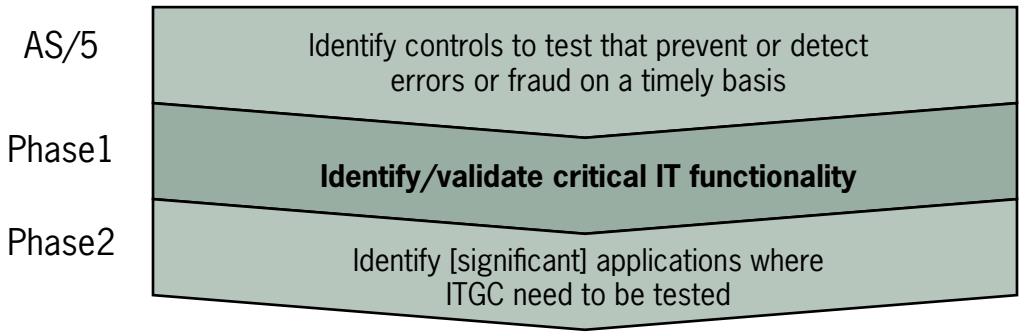
Phase 5: Perform a "reasonable person" review. See page 28.

For more information about using GAIT, including scenarios for applying it, visit The IIA Web site at www.theiia.org.

Phase 1 Identify (and validate if necessary) the critical IT functionality

The GAIT methodology begins with reviewing the key manual and automated business controls as well as other critical system functionality. (Figure 2 below illustrates how this and the next phase fit into GAIT). The top-down assessment of business processes will have identified these key manual and automated controls. GAIT continues the top-down process by confirming the list, which is the basis for the GAIT assessment, and ensuring all critical IT functionality has been identified. The list is used in Phase 2 to identify the financially significant applications, i.e., which applications will be considered "in scope" for §404 assessment and testing.

Figure 2: Phases 1 and 2



To review the key manual and automated controls and key functionality

1. Review the key controls, key reports, and other functionality in the company's financial processes and determine which are manual and which are automated.
2. Develop a list of critical IT functionality that is relied upon. This will include automated controls (see step 3 below) and other critical IT functionality (see step 4 below). The automated controls include:
   - Fully automated controls (e.g., matching or updating accounts in the general ledger.)
   - Application functionality that manual controls rely on[11], where an error in that functionality would not be detected (see also "Key report" on page 37). These are sometimes called "hybrid controls". For example, a key control to detect duplicate receipts might include the review of a system report. The manual part of the control should detect inaccuracies in the report but would not be able to ensure that the report was complete. Therefore, the report would be in scope as a key report. By way of contrast, a bank reconciliation might use a report from the entity's general ledger system showing the current balance, receipts, and disbursements. However, the normal operation of the reconciliation control would promptly detect an error in the report. So the automated portion of the control would not be key, only the manual portion.

11 ISACA's "IT Control Objectives for Sarbanes-Oxley" describes these as "IT-dependent manual controls" or "hybrid" controls.

3. Confirm the key automated controls:
   - Review the automated controls to ensure that they are key[12]. Organizations that had different teams determine risks and related controls in manual and automated processes, especially using a checklist or other bottoms-up approach, might have identified automated controls as key that should not be so classified.
   - Assess whether, if the automated controls failed, there is at least a reasonable likelihood that a material error would not be detected. Sometimes there are manual key controls that would detect either a failure in an automated key control before it could lead to a material error or an unauthorized change to the data that is potentially material. You might be able to ensure these manual controls are identified as key and take the automated controls off the list of key controls.
4. Determine whether there is additional critical IT functionality in the applications not identified as a key control, where a failure might not be detected and could reasonably lead to a material error in the financial statements. Many applications perform calculations and other procedures[13] that are relied upon in the processing of financial transactions and maintenance of related accounting records. These procedures are not strictly controls (see the definition of a control on page 35.) However, if the functionality failed, material errors might be introduced without detection from key manual or automated controls. Therefore, you need to include any such procedures as additional critical functionality and consider the risks to them.

At this point, all the critical IT functionality should have been identified for each financially significant application.

12 Consider the total cost involved when choosing between reliance and testing of manual or automated controls. Some have suggested that automated controls are more efficient and cost less than manual controls. The rationale is that testing manual controls is expensive as they have to be tested by sampling a (relatively) large number of transactions, and automated controls have to be tested only once. However, this assumes effective ITGC as the latter provide assurance that automated controls continue to function consistently, enabling a sample size of one. The cost of reliance on automated controls includes assessing and testing related IT general controls process key controls. While it is likely that many organizations benefit by relying more on automated than manual controls, each should make that determination carefully, considering all the costs and risks involved. Even if the automated controls remain key controls, manual key controls might be valuable when assessing risks in IT general controls processes related to the automated controls.

13 Some IT auditors use the term "programmed procedures" or "programmed accounting procedures" for these calculations, updating of ledger accounts, etc.

Phase 2 Identify the [significant] applications where ITGC need to be tested

Once the critical IT functionality has been confirmed, the financially significant applications can be identified. Financially significant applications are those where there is a potential ITGC process risk because they contain critical IT functionality or data (see the Glossary on page 35). Applications that are *involved* in the processing of financial transactions but neither contain critical IT functionality nor data that is subject to unauthorized change (that could lead to material error) are not in scope for §404; related ITGC do not need to be tested.

To identify the applications where ITGC need to be tested

1. Sort the critical IT functionality by application. The resulting list of applications with critical functionality is a list of the financially significant applications for which risks in ITGC processes will be assessed (subject only to the next step). See the definition of a financially significant application on page 36.
2. For applications that are not considered financially significant based on the presence of critical IT functionality, there is one additional step. That is to assess whether an unauthorized change directly to the application's data could result in an undetected material error (see also "Principle 1" on page 7). This step determines whether a change to the data, bypassing the normal process and controls (sometimes referred to as "backdoor access"), could result in a material error in the financials that would not be detected by the normal operation of controls. If that is possible, the application should be assessed using GAIT, as a financially significant application. If not, the application can be considered out of scope.

   It should be noted that on occasion calculations and other functionality use data created in a prior application. Where a change to that data could result in undetected material error, the risk may lie not only within the application that uses the data but also in other applications (for example, the application where the data was created and any other applications where the data was stored and therefore at risk). Each of those upstream applications may be financially significant, if changes to the data in those applications would not be detected there or elsewhere.
3. Continue *only* with financially significant applications.

> ***Key Point:***
>
> If none of the following exist within an application, it is not financially significant and there is no reliance on ITGC:
>
> a. Key automated (application) controls.
>
> b. Key reports or other hybrid controls (manual controls that depend on IT functions, screens, reports, etc.).
>
> c. Other critical IT functionality.
>
> d. An opportunity for data to be changed (even if pass-through) that could result either in a failure of a key control (which could be downstream) or otherwise in a material error. That data could be transaction or reference data (e.g., prices, credit limits, etc.).

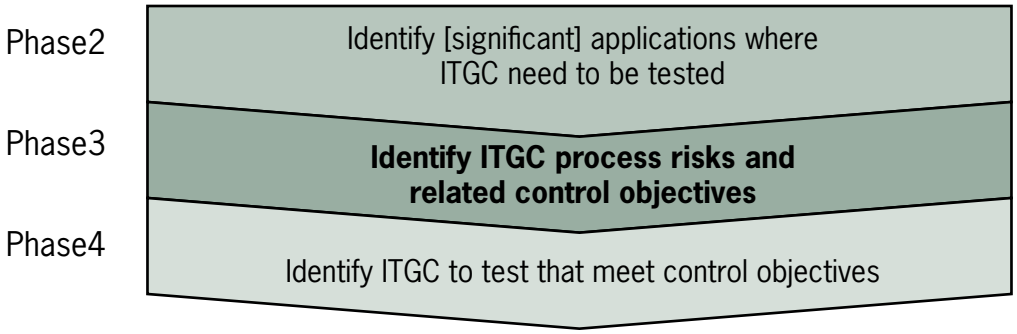
Phase 3 Identify ITGC process risks and related control objectives

This phase has two major activities:

- Obtain additional information for each significant application.
- Assess the ITGC process risks for each significant application: for each ITGC process at each layer of the stack.

The figure below illustrates how this phase fits into GAIT.

Figure 3: Phase 3



During the portion of the top-down process that looked at business processes, you obtained a broad understanding of each of the applications involved in processing financial information. It was needed to identify the appropriate controls to test in the business processes. Additional information is generally required to complete the risk assessment for each significant application of related ITGC processes.

To extend the understanding of the in-scope applications and their infrastructure

The information required to complete the GAIT assessment falls into three broad categories: application infrastructure, related ITGC processes, and risk indicators.

Table 7: Additional application infrastructure and risk information

Category	Description
Application infrastructure	The following are typical items that are obtained to understand and assess risks at each layer of the application's stack. • The infrastructure elements that support the applications (e.g., databases, operating systems, networks, and data centers). • The extent to which automated controls are the result of configuration settings rather than application code. • The database technology in use. Understand its nature and the frequency at which changes occur to database elements, such as schemas, that are essential to key automated controls. • Operating system (e.g., what is used for which application and how often are changes made).

Category	Description
	• Significant interfaces and the manual controls over them. You might need to add these to the list of key automated controls if they are not included as key controls, their failure would not be detected by the normal operation of key controls that have been identified, and they could lead to a material error. • The network infrastructure and its potential points of failure (e.g., the application and its key automated controls might be reliant on transmissions across the network, where a network failure or network security breach could reasonably likely result in an undetected material error in the financial statements). • Was the application developed in-house, or is it a purchased application? • Is the application maintained in-house or outsourced? • How are the applications and infrastructure supported: centrally through shared services, geographically, or individually by business units? • Are data center operations performed in-house or outsourced? • Which network and technical infrastructure operations are performed in-house, and which are outsourced? • How is IT organized? Is there separation of critical functions?
Risk indicators	Certain indicators could signal a higher level of risk in IT processes. These should be considered when assessing risk: • How many and which key controls failed during prior period testing for §404 or during internal audits? • What is the age of the application, and how often is it modified? • Are there known problems with the processing or data? • Are there known problems with any important application functionality? • How extensively has a purchased application been modified, customized, and configured? • What is the backlog of high-priority change requests? • How often do processing problems occur? • How often are emergency changes made? • What is the level of staff turnover in key positions? • How experienced are the staff and have they received sufficient training?

The core of the GAIT assessment is now performed. For each financially significant application, GAIT takes each IT process at each layer in the stack and identifies the IT process risks and related control objectives.

The challenge when assessing risk at this level, compared to risk in business processes, is that ITGC processes are only indirectly linked to the financial statements. In GAIT, IT process risk is assessed based on the risk it represents to the proper operation of the critical IT functionality.

Another factor affecting the risk assessment is that many failures in ITGC processes are more likely to be detected as part of normal operations than failures in general business processes. For example, if there is a security failure and a worm or virus invades the network, it is likely to be immediately apparent and its impact minimized. Therefore, there is a risk that an event may occur. However, if the nature of the event is such that it would be detected promptly, there is little risk of critical functionality failing without prompt detection — and therefore, the latter are unlikely to be the cause of a material error in the financial statements.

When assessing risk, consider:

- The ***likelihood*** of an IT process failure occurring and its ***potential impact***. There are a few steps involved in this assessment:
  - What is the likelihood of the IT process failing in such a way that it would cause the critical IT functionality to fail?
  - Is it at least reasonably likely that the critical functionality would fail without prompt detection and result in a material error in the financial statements?

For §404 purposes, the focus is on IT process failures that are likely to result (through their affect on critical IT functionality) in material errors, not just errors of any size. Including IT process risks that are only theoretically possible but not likely, might lead to an inefficient §404 scope.

- Whether the error is ***deliberate*** (for the purpose of fraud or other damage) or *inadvertent* (accidental). For deliberate errors (e.g., deliberately inserting unauthorized code or changing data without authorization), remember that the only risks that should be in the focus of §404 are risks that are at least reasonably likely. This document does not guide the assessment of fraud risk but suggests that you assess fraud in the same way as in the business process. In other words, you should assess not only whether deliberate error is possible but also whether there are factors that make it at least reasonably likely (such as access to liquid resources, incentives for management to create fictitious transactions, and other risks identified during the assessment of the control environment).

In this phase, you start to complete the GAIT matrix[14]. However, before you get to the steps of filling out the GAIT matrix (see "To assess the risk of ITGC process failures" on page 23), it is important to understand the how the ITGC processes vary at each layer of the stack:

- "Application layer IT general controls processes". See page 20.
- "Database layer IT general controls processes". See page 21.
- "Operating system layer IT general controls processes". See page 21.
- "Network infrastructure layer IT general controls processes". See page 22.

14. This discussion assumes that you are using the GAIT matrix. If you are using the template, it can be used to document all phases.

Application layer IT general controls processes

Table 8 below describes the application layer ITGC processes and risks that might considered.

Table 8: Application layer IT general controls processes and typical risks

IT general controls process

Change management	Change management includes a number of potential risk areas, including whether: • The new or changed functionality is appropriately designed and approved. • The change is adequately tested to ensure it functions properly. • The user accepts the change, confirming it functions as needed. • Unauthorized changes are prevented.
Operations	Operations has potential risk areas, including: • Controls to ensure applications run as intended (e.g., running as often as required, using the current reference files, and processing all input files). • Timely resolution of processing errors and exceptions. • Back-up of critical application and data files. • Physical security of processing. (Note: in the past, access to the operations console in the computer room was considered a major risk. In current times, this is of less consequence as individuals intending to breach security to manipulate data are much more likely to do so through the network).
Security	Security includes risk to the data and application code. Application security, the granting and revoking of access rights, and access to application code are typically included in this IT general controls process. Note: a common deficiency in the first years of §404 assessment was access by programmers to the production version of the code (especially for Web applications). In theory, the programmers could make unauthorized changes. However, further analysis and assessment often determined that the risk of this occurring and resulting (after assessing the impact on automated controls, etc.) in material error was low. There was usually little incentive for programmers to make unauthorized changes (for example, they did not have access to liquid assets), and the likelihood of material error being undetected was low. GAIT allows consideration of the potential risk *before* the control is tested, which is a more efficient approach: assess the risk and test only if likely, instead of test and then determine whether the risk is likely.

Database layer IT general controls processes

In general, the fewer the risks identified at the application or database layer, the less likely risks will exist at lower layers in the stack. For example, while it is theoretically possible that defects in change management at the operating system or network infrastructure layer can result in impaired functionality of an automated control, the probability of this happening to the extent that an automated control fails and results in a material error is often not reasonably likely.

Table 9 below describes the database layer ITGC processes.

Table 9: Database layer IT general controls processes and typical risks

IT general controls process	Description
Change management	Change management at this layer considers the risk of changes to non-data elements, such as schemas. Frequently overlooked, erroneous changes to how the database software presents data to the application can result in incomplete or inaccurate calculations and reports.
Operations	Risks in operations at this layer are often addressed by the same controls as identified for operations at the application layer.
Security	This is where unauthorized access to the data directly is addressed. While security of the data traditionally has been as one of the most critical areas in ITGC to address, you are encouraged to use your judgment and knowledge of the entire business process, including key manual controls, to identify security risks and focus on those at least reasonably likely to occur and result (directly or indirectly through their affect on critical IT functionality) in an undetected material error.

Operating system layer IT general controls processes

Defects at the operating system level are unlikely to result in material errors (either directly through unauthorized changes to data, or indirectly through their affect on the proper operation of critical IT functionality) as the impacts are often immediately apparent — in the form of production outages or processing failures. However, many organizations and their auditors have documented and tested controls over the operating system as if there were a true risk that defects could adversely affect automated controls.

You should review risks at this level using judgment and a broad understanding of the technology and key controls (not only in ITGC processes but in the business process, including high-level monitoring controls) to ensure the appropriate §404 focus.

Table 10 describes the operating system layer IT general controls processes.

Table 10: Operating system layer IT general controls processes and typical risks

IT general controls process	Description
Change management	Change management at this layer considers the risk of changes to the operating system environment, such as patching.
Operations	Risks in operations at this layer are often addressed by the same controls as identified for operations at the application layer.
Security	This is where unauthorized access to the operating system is addressed. You are encouraged to use your judgment and knowledge of the entire business process, including key manual controls, to identify security risks and focus on those at least reasonably likely to occur and result in an undetected material error (indirectly, through their affect on critical IT functionality or as a result of unauthorized changes directly to data). Typically, risks at the operating system layer rarely extend beyond access to "root" level and other privileged access.

Network infrastructure layer IT general controls processes

In general, organizations have fewer risks at this layer. The implications of issues at this layer are less direct and therefore less likely to result in the loss of functionality of key controls or the undetected change of data that causes a material error in the financial statements. The information gained from assessing the risk at the other layers assists in assessing the risk at this layer.

Proper scoping at this layer requires an understanding (obtained in Phase 2) of the application's technical infrastructure and an appreciation of the strengths of key controls in the business process and high-level monitoring processes. GAIT recommends identifying risks as specifically as possible to focus on the key controls in ITGC processes. For example, if a highly complex application receives and validates credit card charges across the network, you should identify potential points of failure in the network to limit the testing required.

To assess the risk of ITGC process failures

1. For each financially significant application, identify specific ITGC process risks and related control objectives for each layer in the IT infrastructure. In short, go through each cell in the GAIT matrix and answer the appropriate questions, listed in Table 11 below. Each question focuses on the risk of material error. As discussed earlier, ITGC process risks do not directly result in material error in the financial statements. They may result in a failure of key automated controls and other critical IT functionality (e.g., key reports) to perform consistently as required, and that could result in a failure to prevent or detect material error in the financial statements.

1. Record the results in the GAIT matrix (see "Sample GAIT matrix" on page 29) or in the GAIT template (see "GAIT template" on page 31). Use supplementary products as necessary, such as COBIT, to ensure a complete assessment.

Table 11: Questions to ask for each cell in the GAIT matrix

Layer	Change Management	Operations	Security
Application	Is a failure in ***change management*** at least reasonably likely to affect critical functionality such that one or more becomes ineffective and causes an undetected material error? • If so, identify the risks and related control objectives. • If not, controls in change management related to this ***application's code*** are not in scope. This, we believe, is highly unlikely.	Is a failure in ***operations*** at least reasonably likely to affect critical functionality such that one or more becomes ineffective and causes an undetected material error? • If so, identify the risks and related control objectives. • If not, controls in operations related to this ***application*** are not in scope.	Is a failure in ***security*** at least reasonably likely to affect critical functionality such that one or more becomes ineffective and causes an undetected material error? Alternatively, is it at least reasonably likely that a failure in security could result in an unauthorized change to data in an application (such as look-up tables) that results in an undetected material error in the financial statements? • If so, identify the risks and related control objectives. • If not, controls in security related to this ***application*** are not in scope.
Database	Is a failure in ***change management*** at least reasonably likely to affect critical functionality such that one or more becomes ineffective and causes an undetected material error? • If so, identify the risks and related control objectives. • If not, controls in change management related to this application's ***database*** are not in scope.	Is a failure in ***operations*** at least reasonably likely to affect critical functionality such that one or more becomes ineffective and causes an undetected material error? • If so, identify the risks and related control objectives. • If not, controls in operations related to this application's ***database*** are not in scope.	Is a failure in ***security*** at least reasonably likely to affect critical functionality such that one or more becomes ineffective and causes an undetected material error? Alternatively, is it at least reasonably likely that a failure in security could result in an unauthorized change to the data or other elements (such as schemas) that result in an undetected material error in the financial statements? • If so, identify the risks and related control objectives. • If not, controls in security related to this application's ***database*** are not in scope.

Layer	Change Management	Operations	Security
Operating system	Is a failure in ***change management*** at least reasonably likely to affect critical functionality such that one or more becomes ineffective and causes an undetected material error? • If so, identify the risks and related control objectives. • If not, controls in change management related to this application's operating system are not in scope.	Is a failure in ***operations*** at least reasonably likely to affect critical functionality such that one or more becomes ineffective and causes an undetected material error? • If so, identify the risks and related control objectives. • If not, controls in operations related to this application's operating system are not in scope.	Is a failure in ***security*** at least reasonably likely to affect critical functionality such that one or more becomes ineffective and causes an undetected material error? • If so, identify the risks and related control objectives. • If not, controls in security related to this application's ***operating system*** are not in scope.
Network infrastructure	Is a failure in ***change management*** at least reasonably likely to affect critical functionality such that one or more becomes ineffective and causes an undetected material error? • If so, identify the risks and related control objectives. • If not, controls in change management related to this application's ***network infrastructure*** are not in scope.	Is a failure in ***operations*** at least reasonably likely to affect critical functionality such that one or more becomes ineffective and causes an undetected material error? • If so, identify the risks and related control objectives. • If not, controls in operations related to this application's ***network infrastructure*** are not in scope.	Is a failure in ***security*** at least reasonably likely to affect critical functionality such that one or more becomes ineffective and causes an undetected material error? • If so, identify the risks and related control objectives. • If not, controls in security related to this application's ***network infrastructure*** are not in scope.

Phase 4 Identify the key ITGCs to test that meet the control objective

After all the risks and relevant IT control objectives are identified, the specific key controls in ITGC to address them can be determined. Frameworks, such as COBIT, can help significantly. This GAIT methodology does not extend to that next step in the §404 process. Our only recommendation is that every ITGC key control be specifically linked to the IT control objectives identified through GAIT and thus to the proper operation of the critical IT functionality at risk.

This section provides information about:

- "Evaluating the pervasiveness of ITGC". See below.
- "Selecting key controls for reliance and testing". See page 26.

Evaluating the pervasiveness of ITGC

ITGC is often considered pervasive because controls in ITGC processes tend to affect more than one automated control, and many affect more than one application. Up to this phase, the methodology:

- **Identifies**, for most organizations, identical risks when the risk assessment is performed for multiple applications. For example, different applications might use the same operating system or database.
- **Does not identify** the aggregate risk, where risks to critical IT functionality in multiple financially significant applications could be affected by a failure in a single ITGC process. That is, the potential failures in critical functionality could aggregate to a risk of a material error that is reasonably likely. A defect in a single ITGC process control could affect critical IT functionality, or multiple databases, in different financially significant applications. While none might individually be at high risk, the cumulative affect of the ITGC process defect could aggregate to high risk.

GAIT guides you through a separate assessment, using the results of the prior phases. This separate assessment tests whether a single ITGC process or risk affects multiple applications and is reasonably likely to cause multiple key control failures that, when aggregated, are at least reasonably likely to create a material error. In those cases, add the risks to those for which key controls in ITGC processes need to be identified.

To evaluate the pervasiveness of ITGC

- Consider the following questions, listed in Table 12 below.

Table 12: Evaluating pervasiveness

For Each Question...	Assess the Following...
With respect to: • **Applications**, are there risks in change management, operations, or security that are at least likely to affect multiple applications and their critical IT functionality? • **Databases**, are there risks in change management, operations, or security that are at least likely to affect multiple applications and their critical IT functionality? • **Operating systems**, are there risks in change management, operations, or security that are at least likely to affect multiple applications and their critical IT functionality? • **Network infrastructure**, are there risks in change management, operations, or security that are at least likely to affect multiple applications and their critical IT functionality? • **The entire IT environment**, are there any risks that potentially affect multiple applications at different layers with the stack? For example, is at least reasonably likely the same security exposure could lead to unauthorized data both in application code and data, such that an undetected material error is more than remotely likely?	• Where the answer is "no", that IT process is not in scope for that layer of the stack for that application. Document the rationale. • Where an answer is "yes", identify the risks. It is generally accepted IT audit practice to define IT control objectives that address these risks (see "Principle 4" on page 9). Document the rationale for the assessment and the applicable IT control objectives.

Selecting key controls for reliance and testing

GAIT provides a methodology for identifying risks and related ITGC control objectives for which key controls in ITGC processes should be included in the §404 scope. However, a consideration of key ITGCs is not complete without addressing the following issues:

To select key controls for reliance and testing

Address the issues, listed in Table 13 below:

Table 13: Identifying key ITGCs

Issue	Description
Relying on manual controls	Take a broad view of all the controls in place to determine the appropriate mix of preventive and detective controls on which to rely. Many organizations have strong monitoring and other controls that will likely detect a material error before it is included in the filed financial statements. When deciding which controls to designated as key and used for reliance, determine whether to include more detailed controls as key controls as a precaution or whether to rely on the higher-level controls. Periodic validation controls (such as physical inventories of inventories or other assets) might be sufficient to detect a defect in an automated control resulting in a material error.
Benchmarking	Benchmarking limits the testing of key automated controls and other critical IT functionality (e.g., key reports) and applies: • Generally where the change management controls at the application layer are strong. It enables reliance on a combination of those controls and prior period tests of automated controls instead of testing every key automated control every year. • Where the application is unchanged from the prior year, when all automated controls were successfully tested. For example, if the audit trail in SAP is reviewed and confirms no changes have been made, there is no need to test the automated control, and there is no risk in ITGC change management at the application layer.
Extended testing of automated controls	While ITGCs that have been effective through the year can limit the testing of automated controls to a sample of one, if there are only a few automated controls in an application, it might be more efficient not to rely on ITGC. The few automated controls could be tested more frequently, for example at each quarter-end, to confirm they are operating effectively rather than relying on controls in ITGC. If you take this approach, test the key automated controls using sampling methodologies based on the frequency of operation of the control. For example, if a key report is used monthly, then the sample size for testing the completeness and accuracy of the report should be based on that frequency. Consider this approach only after a full assessment, using GAIT, to understand all the risks to the application. For example, extended testing might not address risks at the database, operating system, or network infrastructure layers.

Phase 5 Perform a reasonable person review

A strict assessment of ITGC process risk might result in identifying relatively few risks compared to previous assessments, requiring correspondingly fewer key ITGCs. This is probably because the other risks are not considered as at least reasonably likely to lead to an undetected failure in critical functionality that would result in a material error. This does not mean that IT has no controls; it just means that they might not be in scope from a risk-based perspective for §404 testing.

To review risks

1. Confirm that the risks and key controls represent a reasonable view of risk to the financial statements in the eyes of an independent, prudent official.
1. Ensure that the selection of risk is reasonable, given the organization's risk tolerance in the §404 scope. That is, has the approach taken been conservative or aggressive?

Appendix

This section contains supplementary information, including:

- "Sample GAIT matrix". See below.
- "GAIT template". See page 31.
- "Handling bottom-up risk assessments". See page 34.
- "Definitions". See page 35.

Sample GAIT matrix

Table 14 below provides an example of a partially completed GAIT matrix with explanatory notes.

Table 14: Partially completed GAIT matrix

Layer	Change Management	Operations	Security
Application	Yes The application contains numerous key automated controls and other critical functionality (including key reports, calculations, and the updating of the general ledger) whose consistent functionality is at least reasonably likely to be adversely affected if there are failures in change management processes at the application code level. Control objectives to be addressed include: • All program changes are approved prior to implementation by both IT and user management. • Program changes are appropriately tested and the results of testing approved prior to implementation.	Yes The application contains a number of interface batch jobs that are reliant on controls in this process. Control objectives include: • Batch jobs are monitored to ensure normal completion; all processing incidents are reported and appropriate corrective actions taken. • Batch jobs are included in an automated schedule that assures they are executed as required.	Yes User access controls are relevant as the application includes automated controls relative to restricting authorization of transactions to certain individuals and functions. Relevant control objectives include: • Access is limited based on defined job roles appropriate to each user's responsibilities. • Access granted employees and contractors is removed promptly on termination of employment. • Periodic reviews are performed to ensure only authorized individuals have privileged access.

Layer	Change Management	Operations	Security
Database	Assessment not completed		
Operating system	No Changes, including emergency patches, to the operating system are not considered likely to affect critical IT functionality to the extent that they fail. In particular, inappropriate changes or changes made without sufficient testing would be immediately apparent, as the entire application would fail.		
Network infrastructure	Assessment not completed		

GAIT template

The GAIT template is an alternative to the GAIT matrix (see page 29) for documenting the results of the GAIT assessment.

Table 15: GAIT template

Application:

(Application name)

Business processes:

Assessment performed by and date:

Reviewed and approved:

Application overview:

(In general, include a short description of the application, whether it is a purchased product or an in-house development, its age, the frequency of modification, critical interfaces, operating system and database technology, where it is hosted, and other information relevant to the assessment.)

Critical IT functionality:

(Include the full text of each.)

Key automated controls:

Key manual controls reliant on application functionality:
(These are manual controls reliant on application functionality where a defect in the latter would not be detected through the normal operation of the manual control and could result in a material error (e.g., key reports). Clearly highlight the functionality at risk.)

Other critical IT functionality:

(Describe IT functionality that is not included as an automated control, but where a failure could go undetected and result in a material error.)

Relevant manual key controls:

(In this optional section, list in full manual key controls relevant to the assessment. It is useful to include them to support the assessment of risk to the automated controls from ITGC defects. For example, they might assist the assessment of risk from security defects.)

Assessment at the application layer of the stack:

Is a failure in change management at least reasonably likely to affect the proper operation of the critical IT functionality such that one or more becomes ineffective and (indirectly) causes an undetected material error?

- If so, identify the risks and related control objectives in change management for application code.
- If not, controls in change management related to this application's code are not in scope.

Is a failure in operations at least reasonably likely to affect the proper operation of the critical IT functionality such that one or more becomes ineffective and (indirectly) causes an undetected material error?

- If so, identify the risks and related control objectives in operations for application code.
- If not, controls in operations related to this application's code are not in scope.

Is a failure in security at least reasonably likely to affect the proper operation of the critical IT functionality such that one or more becomes ineffective and (indirectly) causes an undetected material error? Alternatively, is it at least reasonably likely that a failure in the security process could result in an unauthorized change to data in an application (such as look-up tables) that results in an undetected material error in the financial statements?

- If so, identify the risks and control objectives in security for application code.
- If not, controls in security related to this application's code are not in scope.

Assessment at the database layer of the stack:

Is a failure in change management at least reasonably likely to affect the proper operation of the critical IT functionality such that one or more becomes ineffective and (indirectly) causes an undetected material error?

- If so, identify the risks and related control objectives in change management for database elements.
- If not, controls in change management related to this application's database are not in scope.

Is a failure in operations at least reasonably likely to affect the proper operation of the critical IT functionality such that one or more becomes ineffective and (indirectly) causes an undetected material error?

- If so, identify the risks and related control objectives in operations for database elements.
- If not, controls in operations related to this application's database are not in scope.

Is a failure in security at least reasonably likely to affect the proper operation of the critical IT functionality such that one or more becomes ineffective and (indirectly) causes an undetected material error? Alternatively, is it at least reasonably likely that a failure in security could result in an unauthorized change to the data or other elements (such as schemas), and in turn result in an undetected material error in the financial statements?

- If so, identify the risks and related control objectives in security for database elements that could cause a material error.
- If not, controls in security related to this application's database are not in scope.

Assessment at the operating system layer of the stack:

Is a failure in change management at least reasonably likely to affect the proper operation of the critical IT functionality such that one or more becomes ineffective and (indirectly) causes an undetected material error?

- If so, identify the risks and related control objectives in change management for the operating system.
- If not, controls in change management related to this application's operating system are not in scope.

Is a failure in operations at least reasonably likely to affect the proper operation of the critical IT functionality such that one or more becomes ineffective and (indirectly) causes an undetected material error?

- If so, identify the risks and related control objectives in operations for the operating system.
- If not, controls in operations related to this application's operating system are not in scope.

Is a failure in security at least reasonably likely to affect the proper operation of the critical IT functionality such that one or more becomes ineffective and (indirectly) causes an undetected material error?

- If so, identify the risks and related control objectives in security for the operating system.
- If not, controls in security related to this application's operating system are not in scope.

Assessment at the network infrastructure layer of the stack:

Is a failure in change management at least reasonably likely to affect the proper operation of the critical IT functionality such that one or more becomes ineffective and (indirectly) causes an undetected material error?

- If so, identify the risks and related control objectives in change management for the network infrastructure.
- If not, controls in change management related to this application's network infrastructure are not in scope.

Is a failure in operations at least reasonably likely to affect the proper operation of the critical IT functionality such that one or more becomes ineffective and (indirectly) causes an undetected material error?

- If so, identify the risks and related control objectives in operations for the network infrastructure.
- If not, controls in operations related to this application's network infrastructure are not in scope.

Is a failure in security at least reasonably likely to affect the proper operation of the critical IT functionality such that one or more becomes ineffective and (indirectly) causes an undetected material error?

- If so, identify the risks and related control objectives in security for the network infrastructure.
- If not, controls in security related to this application's network infrastructure are not in scope.

Consideration of additional ITGC risks that are pervasive

Identification of key controls in ITGC

(Summarize the ITGC process risks and related control objectives that have been identified and for each determine which key controls in ITGC should be included in the §404 scope)

Handling bottom-up risk assessments

GAIT uses a top-down and risk-based approach. However, an ITGC process risk might arise using a bottom-up approach. For example, an auditor, advisor, or IT manager might reference an article or checklist that suggests that a certain risk is important and question why it has not been included in the ITGC scope. It is improbable that an issue brought up in this manner (bottom-up rather than top-down) represents a likely risk of material error when evaluated using GAIT.

To handle a bottom-up risk assessment

1. Identify the applications potentially affected by the issue. For example, if the issue is router configuration, then identify the applications potentially affected. If the issue is database administrator access to the data, identify the applications that use that database.
2. For each application so identified, review its risk assessment:
   - Is there any critical IT functionality in that application?
   - Does the issue represent a risk of unauthorized change to the data that could (indirectly) result in an undetected material error? Or does the combination of manual and automated controls reduce the risk from the issue to below the level where a material error is at least reasonably likely?
   - Does the risk assessment appropriately consider the layer in the stack that is potentially affected and its related ITGC process? If not, update the assessment as necessary.
3. If additional risks:
   - **Have not been identified**, consider whether the issue should be added as a risk based on aggregation. Did the review identify potential risks that are not individually potentially material, but might aggregate to at least a reasonable likelihood of a material error?
   - **Have been identified**, determine whether additional ITGC key controls should be added to the §404 scope.

Definitions

Table 16 below provides definitions of the terms used in this document.

Table 16: Glossary

Term	Definition
Application control	"Application controls to address the application level risks may be in the form of computerized controls built into the system, manually performed controls, or a combination of both. Examples include the computerized matching of documents (purchase order, invoice and goods received report), the checking and signing of a computer generated check and the review by senior management of exception reports." ISACA, Application Systems Review, document G14.
Change management and initial development	The process of developing, implementing, and maintaining applications, operating systems, and database elements.
COBIT	Control Objectives for Information and related Technology (COBIT) is a framework for IT management, created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1992 and updated in 2006.
Control	The policies, procedures, practices and organizational structures, designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected. (COBIT)
COSO	Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a U.S. private-sector initiative, formed in 1985. Its major objective is to identify the factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence. COSO has established a common definition of internal controls, standards, and criteria against which companies and organizations can assess their control systems.
Critical IT functionality	As described in Phase 2 on page 16, critical IT functionality includes: • Key automated controls • IT functionality that is relied on for the proper operation of key manual controls • Key reports • Other critical functionality such as calculations or posting to the general ledger, where a failure might not be detected and could lead to a material error in the financial statements. Some use the term "programmed accounting procedures" for this.
Entity-level control	COSO describes controls as existing at both the entity-level and detail process level. Risks at the entity level can be more pervasive in nature as they may affect the entire organization and the effectiveness of multiple controls at the detail process level. The term "entity-level" is synonymous with "company-level", which the proposed revision of AS/2 uses and is a more accurate term.

ERP	Enterprise resource planning (ERP) systems are management information systems that integrate and automate many of the business practices associated with the operations or production aspects of a company.
Financially significant	Financially significant: • **Applications** contain functionality relied upon to assure the integrity of the financial reporting process, including key automated application controls, key reports and other key automated processes. If that functionality does not operate consistently and correctly, there is at least a reasonable likelihood of a material misstatement that would not be prevented or detected. To be included, the functionality has to be necessary to detect or prevent material misstatements (e.g., part of a key control). • **Data** is data that, if affected by unauthorized change that bypasses normal application controls (for example, as a result of an ITGC failure), is at least reasonably likely to result in a material misstatement that would not be prevented or detected. This might occur when the data is financial data or where the data is relied upon for the consistent operation of an automated procedure.
ICFR	Internal control over financial reporting
IIA	The Institute of Internal Auditors is an international professional association of more than 130,000 members with global headquarters in Altamonte Springs, Florida, United States. Throughout the world, The IIA is recognized as the internal audit profession's leader in certification, education, research, and technological guidance.
IT general controls process	Activities in IT — such as performing network scans, maintaining routers, and testing changes to applications — belong to IT general controls processes. GAIT assumes the activities that relate to ITGC exist in the change management, operations, and security business processes. Using these definitions of the ITGC processes is not critical to using GAIT. Each user of GAIT can substitute their definition without affecting the GAIT methodology. (See also Principle 3).

ITGC	IT General Controls are controls over the IT general controls processes, generally residing in the IT organization. "Broadly speaking, ITGC provide assurance that applications are developed and subsequently maintained, such that they provide the functionality required to process transactions and provide automated controls. They also assure the proper operation of the applications and the protection of both data and programs from unauthorized change." (§404 Guide) In their December 2004 "Framework for Evaluating Control Exceptions and Deficiencies", representatives of nine independent auditing firms developed a document that included portions concerning ITGC. The document describes the relationship between ITGC and applications controls (or automated key controls) as follows: "ITGCs may affect the continued effective operation of application controls. For example, an effective security administration function supports the continued effective functioning of application controls that restrict access. As another example, effective program change controls support the continued effective operation of programmed application controls, such as a three-way match. ITGCs also may serve as controls at the application level. For example, ITGCs may directly achieve the control objective of restricting access and thereby prevent initiation of unauthorized transactions."
Key control	A control that, if it fails, means there is at least a reasonable likelihood that a material error in the financial statements would not be prevented or detected on a timely basis. In other words, a key control is one that provides reasonable assurance that material errors will be prevented or timely detected. The failure could be individual or together with other controls that are likely to fail at the same time. This is given the term "aggregation" in the literature. While the failure of one control might not be likely to result in a material misstatement, several might fail at the same time, increasing the risk to more than remote. In aggregation, controls have to be likely to fail at the same time, for example, because they are performed at the same time by the same people or with the same computer system. The timely detection of an error is critical. Otherwise, detection might occur after the financial statements have been filed with the SEC, leading to the potential need for restatement. In AS5, the PCAOB states the following, which essentially describes key controls: *"The auditor should test those controls that are important to the auditor's conclusion about whether the company's controls sufficiently address the assessed risk of misstatement to each relevant assertion."*

Key report	A report used in a key control, usually system-generated. To be a key report, the following conditions apply: • An error in the report could result in a material error if undetected, for example, because information in the report is used to generate a transaction (such as a journal entry) or is used as the basis of the control (such as a review of aged receivables) • The manual part of the control would not necessarily detect an error in the report
Material error	A material misstatement of the financial statements filed with the SEC.
Operations management	The process of operating or running applications and systems. This process typically includes physical security back-up and recovery, and other aspects of data center operations.
PCAOB	The Public Company Accounting Oversight Board (PCAOB) is a private sector, non-profit corporation created by the Sarbanes-Oxley Act to oversee the auditors of public companies. Its stated purpose is to "protect the interests of investors and further the public interest in the preparation of informative, fair, and independent audit reports". Although a private entity, the PCAOB has many government-like regulatory functions, making it similar to the private Self Regulatory Organizations (SROs) that regulate stock markets and other aspects of the financial markets in the United States.
SEC	The United States Securities and Exchange Commission (SEC) is a United States government agency having primary responsibility for enforcing the Federal securities laws and regulating the securities industry. The SEC was created by section 4 of the Securities Exchange Act of 1934 (now codified as 15 U.S.C. §78d). In addition to the 1934 Act that created it, the SEC enforces the Securities Act of 1933, the Trust Indenture Act of 1939, the Investment Company Act of 1940, the Investment Advisers Act of 1940, the Sarbanes-Oxley Act of 2002, and other statutes.
Security management	The process of ensuring the integrity of the applications, data, operating systems, and network infrastructure by restricting access to systems and data.
Stack	Each IT general controls process operates at the four layers of each application's IT infrastructure — application, database (including related structures such as the schema), operating system, and network infrastructure. These layers are also known as the "stack". Users of GAIT can modify the stack definition to suit their organization.

Top-down approach	The PCAOB describes the top-down approach in AS5: The auditor should use a top-down approach to the audit of internal control over financial reporting to select the controls to test. A top-down approach begins at the financial statement level and with the auditor's understanding of the overall risks to internal control over financial reporting. The auditor then focuses on entity-level controls and works down to significant accounts and disclosures and their relevant assertions. This approach directs the auditor's attention to accounts, disclosures, and assertions that present a reasonable possibility of material misstatement to the financial statements and related disclosures. The auditor then verifies his or her understanding of the risks in the company's processes and selects for testing those controls that sufficiently address the assessed risk of misstatement to each relevant assertion