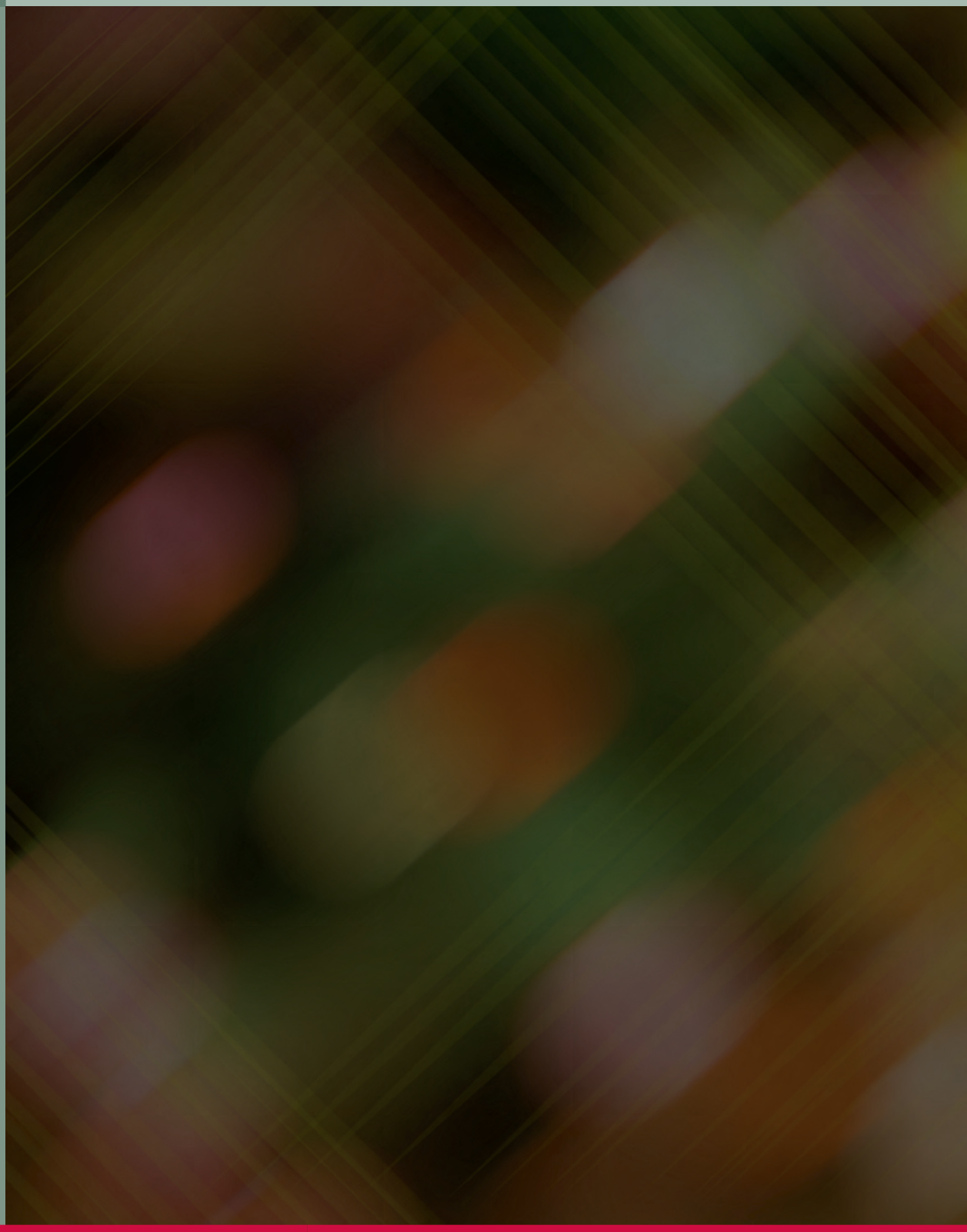
GAIT FOR IT GENERAL CONTROL DEFICIENCY ASSESSMENT



The Institute of Internal Auditors

PROFESSIONAL GUIDANCE

Setting the Standard

GAIT for IT General Control Deficiency Assessment

An approach for evaluating ITGC deficiencies in Sarbanes-Oxley Section 404 assessments of internal controls over financial reporting

The Institute of Internal Auditors
March 2008

Table of Contents

1. INTRODUCTION

Background

In 2004, representatives of nine certified public accounting firms, with a contribution by a Georgia State University professor, developed and published[1] A Framework for Evaluating Control Exceptions and Deficiencies. The framework[2] has guided audit firms and management in assessing whether deficiencies in the system of internal control over financial reporting (IFRC) are significant deficiencies or material weaknesses.

Since then, standards and practices related to assessments of Section 404 of the U.S. Sarbanes-Oxley Act of 2002 have changed extensively. The 2004 framework references Auditing Standard No. 2 (AS 2), which has been replaced by Auditing Standard No. 5 (AS 5); the definition of a significant deficiency has been revised; and we have three years' practical experience.

An additional development is the introduction of *The GAIT Methodology*[3]. This document explains how risk related to IT general controls (ITGCs) should be identified by continuing the top-down and risk-based scoping process recommended[4] by the U.S. Securities and Exchange Commission (SEC) and the U.S. Public Company Accounting Oversight Board (PCAOB).

Practice guides in the GAIT series describe the relationships among risk to the financial statements, key controls within business processes, automated controls and other critical IT functionality, and key controls within ITGC. Its methodology helps companies identify and assess the ITGCs necessary to ensure that material misstatements of the financials are prevented or detected on a timely basis.

This practice guide provides an updated approach to the assessment of ITGC deficiencies,[5] helping auditors or management assess whether they represent material weaknesses or significant deficiencies. The philosophies discussed in this guide can be leveraged extensively.

While this practice guide has been developed under the sponsorship of The Institute of Internal Auditors (IIA), the team included representatives from external audit firms. The guide and the methodology it describes can be used by management, external audit firms, internal auditors, and other stakeholders in the Sarbanes-Oxley Section 404 assessment process.

We believe the methodology presented herein is consistent with guidance from the SEC[6] and PCAOB.

1 The most recent version is No. 3, published in December 2004.
2 It should be noted that the framework was not formally adopted by either the SEC or the PCAOB.
3 GAIT stands for Guide to the Assessment of IT Risk and was published by The Institute of Internal Auditors in January 2007. Excerpts from *The GAIT Methodology* are included for reference purposes at the end of this practice guide. The full document is available at www.theiia.org.
4 The SEC and PCAOB have recommended a top-down approach since 2005. They have incorporated it into SEC guidance to management and public statements and in AS 5.
5 The practice guide is not intended for use in assessing deficiencies other than those in ITGCs.
6 For example, the description in the SEC guidance on the role of ITGCs is not only consistent with GAIT, but also uses many of the same terms and concepts.

The Effect of the Top-down Approach to Scoping

As noted above, both the SEC and the PCAOB recommend[7] the use of a top-down and risk-based approach to establishing the scope of work for Sarbanes-Oxley Section 404, including the identification of the key controls to assess and test. GAIT extends this approach to the identification of key ITGCs.

The top-down approach identifies the combination of key controls (i.e., entity-level and activity-level; manual, automated, and ITGC) relied upon to prevent or detect a material misstatement of the financial statements.

Should one or more of these key controls fail, the combination of controls may no longer provide reasonable assurance that material errors[8] will be prevented or detected.

However, controls can fail to different degrees (e.g., only failing with respect to part of the population of transactions, such as when application change approvals are performed well for some, but not all, systems) and the extent of failure needs to be understood and considered during the assessment.

In addition, imperfect scoping can result in the inclusion of redundant, overlapping, or other controls that are not truly key. An example is where the control objective is validity — the documented control includes the requirement for multiple approvals, but only one of the multiple approvals is required to achieve the control objective.

When assessing key control failures, including failures of key ITGCs, the assessor should place the burden of proof on demonstrating why the failures do not represent material weaknesses rather than on demonstrating why they are. The presumption is that the key controls are necessary to prevent or detect material errors — which is why they were included as key controls — and, therefore, are likely to be material weaknesses when they fail.

7 The PCAOB in AS 5 and the SEC in their guidance use different terms. For example, the PCAOB refers to *significant accounts* while the SEC uses the term *financial reporting elements*. This document uses the terms found in AS 5.

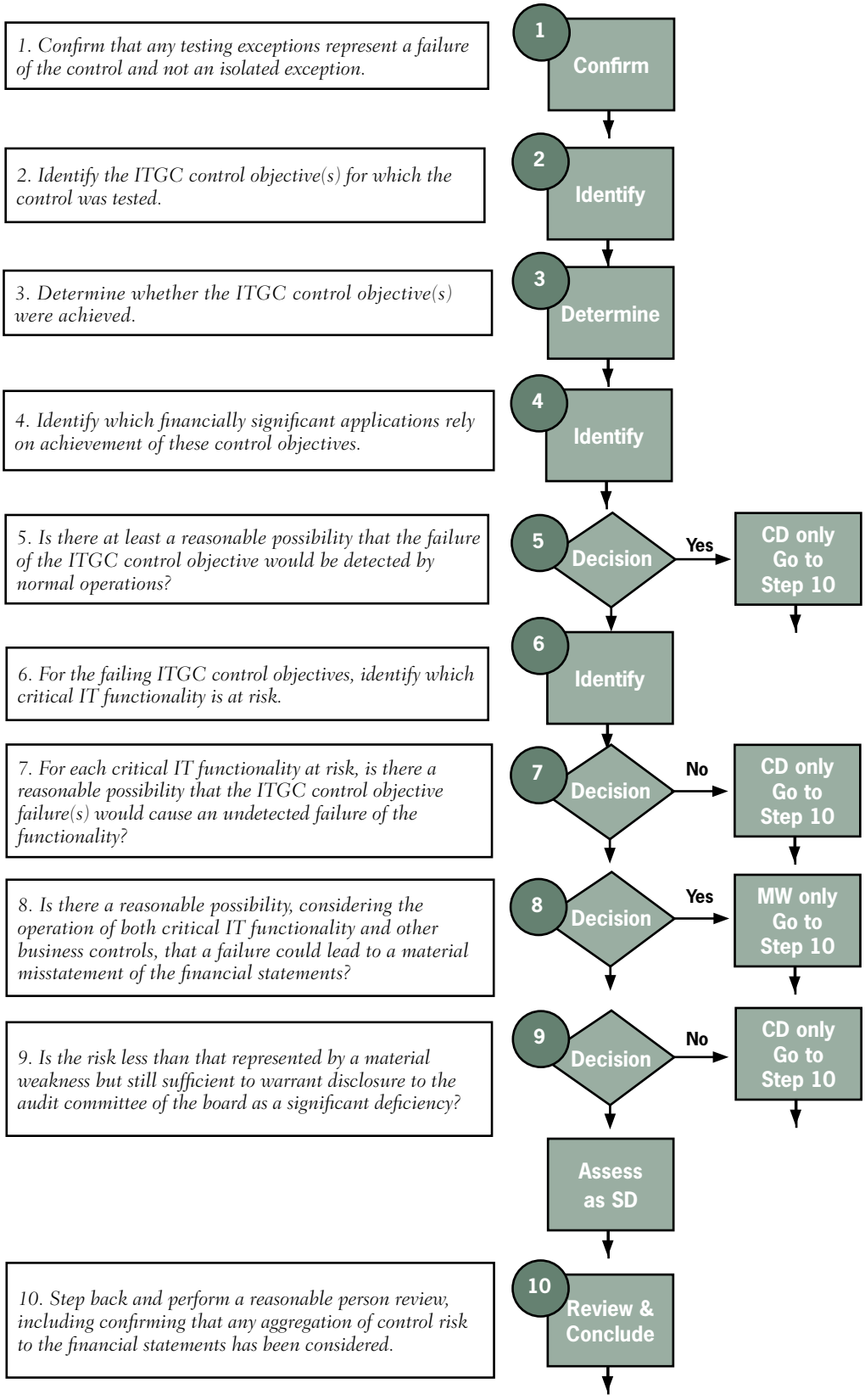
8 The term *material error* as used in this document is synonymous with *material misstatement of the financial statements*.

Overview

The methodology is based on six assessment principles, which are discussed in Section II.

ASSESSMENT PRINCIPLES
1. To assess ITGC deficiencies, it is necessary to understand the reliance chain between the financial statements and the ITGC key controls that have failed.
2. For there to be a material weakness, two tests have to be met: (a) likelihood and (b) impact (i.e., the potential misstatement of the financial statements).
3. Because an ITGC deficiency does not directly affect the financial statements, the assessment is similarly not direct. The assessment is in stages or steps, and the likelihood and impact tests are applied across a combination of the steps.
4. All ITGC deficiencies that relate to the same ITGC control objective should be assessed as a group.
5. All ITGC control objectives that are not achieved and relate to the same key automated controls, key reports, or other critical functionality should be assessed as a group.
6. The principle of aggregation requires that control deficiencies of all types — including manual and automated control deficiencies relating to the same significant account or disclosure — be considered as a group.

The assessment process consists of 10 steps as illustrated below. They are discussed in more detail in Section 3.


1. Confirm that any testing exceptions represent a failure of the control and not an isolated exception.
1
Confirm
2. Identify the ITGC control objective(s) for which the control was tested.
2
Identify
3. Determine whether the ITGC control objective(s) were achieved.
3
Determine
4. Identify which financially significant applications rely on achievement of these control objectives.
4
Identify
5. Is there at least a reasonable possibility that the failure of the ITGC control objective would be detected by normal operations?
5
Decision
Yes
CD only Go to Step 10
6. For the failing ITGC control objectives, identify which critical IT functionality is at risk.
6
Identify
7. For each critical IT functionality at risk, is there a reasonable possibility that the ITGC control objective failure(s) would cause an undetected failure of the functionality?
7
Decision
No
CD only Go to Step 10
8. Is there a reasonable possibility, considering the operation of both critical IT functionality and other business controls, that a failure could lead to a material misstatement of the financial statements?
8
Decision
Yes
MW only Go to Step 10
9. Is the risk less than that represented by a material weakness but still sufficient to warrant disclosure to the audit committee of the board as a significant deficiency?
9
Decision
No
CD only Go to Step 10
Assess as SD
10. Step back and perform a reasonable person review, including confirming that any aggregation of control risk to the financial statements has been considered.
10
Review & Conclude

2. PRINCIPLES

1. *To assess ITGC deficiencies, it is necessary to understand the reliance chain between the financial statements and the ITGC key controls that have failed.*

The assessment of deficiencies in ITGC for Sarbanes-Oxley Section 404 purposes is an assessment of the risk they represent of undetected errors in the financial statements. However, ITGC deficiencies do not have a direct relationship with the financial statements. The reliance chain described below represents the relationship and, therefore, the potential effect between ITGC deficiencies and the financial statements.

The reliance chain between the financial statements and the ITGC key controls is the same logical linkage that is used in a top-down approach to define which ITGC key controls should be in scope,[9] except that it is traveled in reverse.

The selection of ITGC key controls should be the result of a top-down, risk-based approach. The process can be summarized as follows:

- Identify significant accounts, locations, and related assertions.
- Identify the company- and activity-level business controls required to prevent or detect material errors in the significant accounts.
- Some of the identified company- and activity-level key controls are automated application controls or otherwise rely on automated functionality (e.g., through key reports, calculations, updates, etc). Reliance may be placed on ITGCs for the continued operation of this critical IT functionality.
- Critical IT functionality exists within significant applications.
- The top-down and risk-based approach identifies where there are risks within ITGC to each automated control (or key reports, etc.) and the appropriate ITGC control objectives to address those risks.
- Identify the key ITGCs required to achieve each ITGC control objective.
- In addition to reliance on functionality within applications, security of data from unauthorized change may be a risk. The assessment of that risk should consider the likelihood that an unauthorized change would not be detected by company- or activity-level controls and would result in a material error in the financial statements. The assessment is made for each application involved in significant business processes and major classes of transactions. If such material error from unauthorized change is considered at least reasonably possible,[10] related ITGC control objectives and individual key ITGC controls are identified.

The reliance chain — the linkage between individual ITGC and the financial statements — is the inverse of the above:

- Individual ITGCs relate to ITGC control objectives. The direct effect of ITGC failures is that they may result in the nonachievement of those objectives. It should be noted that a number of key controls may have been identified as necessary to the achievement of a control objective, and the failure or impairment of an individual ITGC does not necessarily mean that the control objective is not achieved.[11]

9 *The GAIT Methodology* should be referred to for more information on how the top-down approach discussed in SEC and PCAOB documents, including the SEC's guidance for management and the PCAOB's AS 5, can be continued and extended to the identification of key controls within ITGC processes.

10 See definition included in the Glossary of Terms.

11 Technically, control objectives are either achieved or not achieved. For ease of writing, the nonachievement of a control objective may be referred to in this document as the failure of that control objective.

- The first risk assessment is whether specific ITGC objectives are deemed to have failed as a result of control failures. When considering whether ITGC control objectives have failed, all failures of key ITGCs that relate to a control objective should be considered as a group.

  If compensating or mitigating controls within ITGCs reduce the impact of deficiencies, judgment should be applied in determining whether the control objective failed to the extent there is significant risk to the proper operation of automated controls.

- Each ITGC control objective relates to one or more automated application controls, which are identified during the top-down, risk-based scoping as necessary to prevent or detect a material error in the financial statements; other critical IT functionality (e.g., calculations and updates, which are not technically controls but need to operate consistently as designed and are, therefore, included with automated controls as *critical IT functionality*); or to the risk of unauthorized change to data. A failure of an ITGC control objective represents a risk to those key automated controls.

  Risk to each automated control must be assessed. This involves identifying the automated application controls or other functionality that cannot be assured of operating consistently as designed due to failures in underlying ITGC processes. The assessment also identifies which data is at risk from unauthorized change that could result in a material misstatement.

  Because critical IT functionality generally relies on the achievement of multiple ITGC control objectives, the combined or aggregate risk from all failing ITGC control objectives should be assessed.

- The potential impairment of — or lack of assurance relative to — key business automated controls or to the security of data represents a potential risk to the financial statements.

- Risk to the financial statements of a potential impairment of data, application controls, or other critical IT functionality is then assessed. This assessment relies on the application of judgment and should consider the presence of compensating or mitigating controls within business processes.

The reliance chain is illustrated below.

2. *For there to be a material weakness, two tests have to be met: (a) likelihood and (b) impact (i.e., the potential misstatement of the financial statements).*

The likelihood test requires at least a reasonable possibility that an error in the financial statements would result from the control deficiency.

The impact test determines whether the potential error would represent a material misstatement.

Both tests have to be met: There has to be at least a reasonable possibility of a material misstatement.

It should be noted that a significant deficiency is a lower level of risk than a material weakness (i.e., there is less than a reasonable possibility of a material misstatement). However, the risk to the financial statements is serious enough to warrant disclosure to the board's audit committee. Judgment, rather than tests of likelihood and impact, is used to make this determination.

3. *Because an ITGC deficiency does not directly affect the financial statements, the assessment is similarly not direct. The assessment is in stages or steps, and the likelihood and impact tests are applied across a combination of the steps.*

As discussed in principle 1 above and illustrated in the reliance chain diagram, there are three steps in the assessment process:

a. Is there a failure to achieve one or more ITGC control objectives?

b. If so, are any automated controls, key reports, or other critical IT functionality impaired (i.e., there is no assurance they will operate consistently as designed)? If so:

c. If so, is there a reasonable possibility of a material misstatement, because the automated control fails to prevent or detect the error?

Only if findings suggest a *yes* response to all three questions should ITGC deficiencies be considered at least reasonably likely[12] to result in the failure to prevent or detect a material misstatement of the financials. In other words:

There would have to be at least a reasonable possibility that …

the ITGC failure would cause a failure to achieve one or more ITGC control objectives …

such that there is at least a reasonable possibility that one or more key automated application controls (or key reports, etc.) would fail to operate effectively as designed …

such that there is at least a reasonable possibility that a material misstatement of the financials would not be detected.

4. *All ITGC deficiencies that relate to the same ITGC control objective should be assessed as a group.*

As discussed in principles 1 and 3, the risk to the financial statements is indirect. Only if the ITGC control objective is considered to have failed is there a potential material deficiency. To reach that assessment, all related ITGC failures should be assessed together to form an opinion as to whether one or more ITGC control objectives have failed.

5. *All ITGC control objectives that are not achieved and relate to the same key automated controls, key reports, or other critical functionality should be assessed as a group.*

The last link in the reliance chain is the critical IT functionality — the key automated controls, key reports, and other critical functionality (e.g., updates, interfaces, calculations) that are required to prevent or detect material errors in the financial statements.

The assessment of risk that critical IT functionality will fail should include all ITGC control objectives that have failed and relate to the functionality.

12 For editorial purposes, this document uses the terms *reasonably likely* and *reasonably possible* synonymously. Each has the same meaning and are defined in the Glossary of Terms under *reasonable possibility.*

In general, the more ITGC control objective failures that relate to an automated control, the higher the likelihood that automated control will not perform consistently as designed. Also, the higher the likelihood an automated control will fail, the higher the likelihood an error in the financial statements would not be prevented or detected.

6. *The principle of aggregation requires that control deficiencies of all types — including manual and automated control deficiencies relating to the same significant account or disclosure — be considered as a group.*

AS 5 provides a clear description of this requirement:

> *Multiple control deficiencies that affect the same financial statement account balance or disclosure increase the likelihood of misstatement and may, in combination, constitute a material weakness, even though such deficiencies may individually be less severe. Therefore, the auditor should determine whether individual control deficiencies that affect the same significant account or disclosure, relevant assertion, or component of internal control collectively result in a material weakness.*[13]

The top-down, risk-based scoping process will identify the combination of manual and automated controls within the business processes (e.g., within the procure-to-pay, order-to-cash, or equity processes) that are required to prevent or detect a material error. The assessor should take each impaired critical IT functionality and identify the associated significant accounts and disclosures. Then the effectiveness of the combination of manual and automated controls — including those which are effective and ineffective — should be considered and a determination made of the risk of a material misstatement.

13 In paragraph 65.

3. ASSESSMENT PROCESS

The Assessment Team

The effect of ITGC deficiencies on the financial statements is indirect as illustrated by the reliance chain. The assessment of ITGC deficiencies therefore requires an understanding not only of technical ITGC issues, but also of business processes, period-ending processes, and financial statements.

Accordingly, the assessment should be conducted by personnel with a collective understanding of all the stages in the reliance chain. While the full team may be involved in the entire assessment process, the early steps in the process rely more heavily on ITGC understanding and the later steps more heavily on business processes and controls.

Identification of Control Deficiencies

Control deficiencies may be identified during the assessment of the controls' design or during testing. The process discussed below assumes the issue is the result of control testing, as this is generally the case, and is worded accordingly. If the deficiency is the result of a review of the control's design, Step 1 is not required.

Step-by-step Process

1. *Confirm that any testing exceptions represent a failure of the control and not an isolated exception.*

The presence of a small number of test exceptions does not necessarily represent a control failure. Depending on the size of the control occurrence population, an additional exception-free sample may allow the tester to presume that the exception is isolated.

The tester should review testing results with management to confirm the understanding of the control and the test's design. An apparent failure could be the result of a misunderstanding of the control and how it operates, in which case the test should be redesigned and reperformed.

In addition, it is important to understand what elements of the control are required to satisfy the control objective or risk being addressed. The test should be designed to ensure those key elements are examined. For example, a control objective might state that a certain transaction must be authorized by management. However, the process could, for operational reasons, include multiple reviews and approvals (e.g., by two levels of management). As a result, the key control might include two levels of approvals. If one level of approval is missing, further review might find that approval by one manager is sufficient to achieve the control objective. The appropriate action, in that case, would be to change the definition of the key control to include only the approval required to achieve the control objective, without removing the additional layers of approval required for operational purposes, rather than considering the control to have failed.

If the test exceptions do not represent a control deficiency, the assessment process is concluded.

2. *Identify the ITGC control objective(s) for which the control was tested.*

Each key ITGC is tested because the determination was made during the planning and scoping for the assessment that it is required by one or more ITGC control objectives. When assessing failures of ITGC key controls, the first step is to identify which ITGC control objectives rely on them. Then, each ITGC control objective will be assessed to determine whether the failure of one or more key ITGCs means that the ITGC control objective should be considered as failed. It should be recognized that a single control may be relied on for more than one ITGC control objective, each of which could be at risk.

3. *Determine whether the ITGC control objective(s) were achieved.*

The determination of whether there is a significant deficiency or material weakness is based on whether ITGC control objectives have failed and not on the individual failure of ITGCs. As described in the discussion of Principle 1 and the reliance chain:

- Individual ITGCs relate to ITGC control objectives. The direct effect of ITGC failures is that they may result in the nonachievement of those objectives. It should be noted that a number of key controls may have been identified as necessary to the achievement of a control objective, and the failure or impairment of an individual ITGC does not necessarily mean that the control objective is not achieved.[14]
- The first risk assessment is whether specific ITGC control objectives are deemed to have failed as a result of the control failures. When considering whether ITGC control objectives have failed, all failures of key ITGCs that relate to a control objective should be considered as a group.

There are two aspects to this consideration:

a. Compensating[15] ITGCs

When multiple key ITGCs contribute to the achievement of an ITGC control objective, it is possible that strengths in one or more may compensate for weaknesses in another.

For example, two key controls may be identified for the control objective of limiting access by the database administrator (DBA) to the financial systems (i.e., the general ledger and sub-ledgers, including accounts payable, accounts receivable, inventories, fixed assets, etc.) The first control could limit the DBA capability to defined DBAs, and the second could be a monitoring access control to general ledger data. If the first key control failed, then second might be sufficient to reach the conclusion that the control objective as it relates to the general ledger system has not failed. On the other hand, if the monitoring control did not extend to access activities involving changes to accounts payable or inventories, the conclusion is likely that the control objective has failed with respect to those sub-ledgers.

In another example, there might be three controls related to the control objective of assuring only approved changes are made to the general ledger application. The first might be the approval by the corporate controller of all requests for change; the second the review and approval of all changes by a change control board in IT prior to implementation of the changes; and a third the testing of all changes by the accounting department. Even if the corporate controller's approval is frequently not obtained, the level of assurance provided by the other two controls might be sufficient to believe the control objective is still achieved.[16]

When considering compensating ITGCs, there has to be assurance that the compensating controls are operating effectively as designed. Normally, this includes limiting consideration to those ITGCs that have been identified as key controls that have been tested or otherwise assured.

14 Technically, control objectives are either achieved or not achieved. For ease of writing, the nonachievement of a control objective may be referred to in this document as the failure of that control objective.

15 The term *compensating controls* includes complementary and mitigating controls.

16 The assessment process might identify the presence of redundant controls, where two or more controls provide duplicate coverage of a risk. This may be the result of a deliberate decision during the scoping process to reduce the risk that control failures might represent to the overall Section 404 assessment. It also might be the result of an inefficient scoping process, perhaps because a top-down and risk-based process was not used. If the latter is the case, the scoping process might warrant revisiting and the removal of redundant controls from scope.

b. Failures of Multiple Key Controls

In general, it is more likely that the ITGC control objective will be assessed as failed when there are multiple key control failures affecting that control objective. Judgment should be used to determine whether the multiple failures represent an unmitigated risk such that the control objective has not been achieved.

The assessment requires the application of judgment. If the conclusion is that the ITGC control objectives have been achieved, considering the key ITGCs, then the assessment process is concluded.

4. *Identify which financially significant applications rely on the achievement of the control objectives.*

When ITGC control objectives are assessed, they must be in context. The control objectives are required to provide assurance for financially significant applications and the IT functionality they contain, and it is possible that different conclusions may be drawn for the same ITGC control objective with different applications. For example, a control objective to ensure that Unix root access is limited may fail for applications on some servers, but pass for applications on other servers.

5. *Determine whether there is at least a reasonable possibility that the failure of the ITGC control objective would be detected by normal operations.*

The nature of ITGC is that the failure of controls is often immediately apparent. One example is the failure to update antivirus protection. If this update failure were to result in a network infection, this would be evident in many situations as user functionality is impaired. Another example might be the failure to test updates to the network operating system provided by the vendor. The assessor should consider whether this is likely to result in a broad and obvious failure of related servers and their applications, rather than the undetected failure of functionality within financially significant applications.

The assessment should consider whether a reasonable person would conclude that, in the specific circumstances being reviewed, there is at least a reasonable possibility that an adverse event resulting from the control failure would not be detected by normal operations.

If it is concluded that there is no failure of an ITGC control objective, the exception is only a control deficiency.[17]

6. *For the failing ITGC control objectives, identify which critical IT functionality is at risk.*[18]

The assessment moves from considering individual control objectives to the consideration of groups of ITGC control objectives — those that have been determined to have failed and affect the same key automated control, key report, or other critical functionality. The more control objectives that fail for a specific key automated control, the more likely that the automated control will fail.

The planning and scoping for the ITGCs to be tested will have identified which ITGC control objectives need to be achieved for each key automated control. That documentation should be reviewed to determine which automated controls are affected by each failing ITGC control objective.

Because this step requires an understanding of the business processes and the role of automated controls, etc., the assessment team should include individuals with that knowledge and understanding of ITGC risks.

17 Similar to the discussion of redundant controls, the inclusion in scope of controls whose failure would be promptly apparent may be the result of an inefficient scoping process. The scope should be reassessed and consideration given to removing these controls from scope.

18 If *The GAIT Methodology* was used to define the scope of work for ITGC testing, the GAIT documentation will include a definition of which automated controls, key reports, etc. rely on the ITGC control objective being assessed.

The assessment process now moves to considering the risk to the financial statements from the failure of automated controls, key reports, etc. due to the failure of ITGC control objectives. Therefore, all members of the assessment team should be involved.

7. *For each critical IT functionality at risk, determine whether there is a reasonable possibility that the ITGC control objective failure(s) would cause an undetected functionality failure.*

Judgment is now applied to assessing whether there is at least a reasonable possibility that critical IT functionality (key automated controls, reports, etc.) would fail and not be detected.

The following should be considered.

a. *Have there been multiple failures of ITGC control objectives that affect the same critical IT functionality?*

   In general, the likelihood of failure in the operation of automated controls or other critical functionality will increase when there are multiple risks from a number of ITGC control objectives. Judgment must be used to assess whether the nature and extent of ITGC control objective failures implies that ITGCs cannot be relied on to assure the continued proper operation of critical IT functionality.

b. *Is there a reasonable possibility that the failure of the functionality would be detected in a timely fashion, for example by a compensating business control?*

   Consider the situation where the functionality at risk is a key report and the risk that has been identified is that the report will not be run. The manual key control of reviewing the key report would be sufficient to detect the failure to run the report. However, if the risk to the report is that its contents may be incomplete or inaccurate, whether the manual review would be sufficient to detect the errors would depend on specific facts and circumstances — the way in which the review is performed.

c. *Consider, as a risk indicator, whether there have been prior failures of the critical IT functionality.*

   A history of failures in key automated controls that were not detected on a timely basis is a prima facie indicator of higher risk of future failure. Judgment should be used to assess this risk indicator, including how quickly the failures were detected and whether there were failures in similar, but nonkey, functionality. For example, if there are key automated controls and key reports within the general ledger system, a history of failures in different functionality within the general ledger system may be relevant. Specific facts and circumstances should be considered when determining the level of risk to the functionality relied on to prevent or detect material misstatement of the financial statements.

If there is a nonreasonable possibility that there would be an undetected failure of any critical functionality, then there is only a control deficiency.

8. *Is there a reasonable possibility, considering the operation of critical IT functionality and other business controls, that a failure could lead to a material misstatement of the financial statements?*

The assessment process has established that there is at least a reasonable possibility that critical functionality will fail. Judgment is now applied, considering all the related facts and circumstances, including the effectiveness of related manual and other automated key controls at the entity level[19] and activity level, to assess whether the impact of the failure is at least reasonably likely to result in an undetected error in the financial statements that is material.

As described in principle 1, there has to be at least a reasonable possibility that …

> the ITGC failure would cause a failure to achieve one or more ITGC objectives …
>
> such that there is at least a reasonable possibility that one or more key automated application controls (or key reports, etc.) would fail to operate effectively as designed …
>
> such that there is at least a reasonable possibility that a material misstatement of the financials would not be detected.

The assessment should not be on the risk of a failure in critical functionality alone; it should consider the effectiveness of all controls relating to a significant account or disclosure, including:

- **Whether there are multiple control failures affecting the same account or disclosure.**

As described in Step 3, the presence of multiple control failures might indicate that the risk of a material misstatement is increased. However, the assessment should consider the specific nature of the control deficiencies. Where they are not related (e.g., they are not performed by the same people or using the same system), the likelihood of errors occurring in the same period may be low. For example, if two unrelated controls are each considered 10 percent likely to occur and result in an error of US $1 million, probability theory indicates that there is only a 1 percent likelihood that they will occur simultaneously and result in an error of US $2 million. However, if the two controls are related, then the likelihood of a US $2 million error could be much higher.

ITGC deficiencies may affect achievement of ITGC control objectives related to several automated controls or other IT critical functionality. If reliance on those automated controls is considered impaired, then the common cause (i.e., the key ITGCs and control objectives) means that they are related.[20]

- **Whether multiple significant accounts may be affected, either by one or multiple control deficiencies.**

As noted above, a single ITGC deficiency may be the root cause of errors in multiple accounts. This is because either the affected critical IT functionality is relied upon to prevent or detect errors in more than one significant account or because multiple automated controls are affected and, thereby, affecting multiple accounts.

19 The terms *company level* and *entity level* are considered equivalent.

20 This can be considered a form of aggregation. Others discuss this as the result of the pervasive nature of ITGC (i.e., that a defect in ITGC can affect multiple business process controls and multiple significant accounts).

The assessment team should consider whether there is an aggregated risk that is rising to the level of a material weakness.

- **Whether there are any compensating or mitigating controls.**

Step 3 describes how compensating controls could reduce the possibility of a material error in the financial statements. These compensating controls must have been found to be effective for reliance to be placed on them.

If a material weakness is identified, the assessment continues at Step 10, where any aggregation effect is considered.

9. *Assess whether the risk is less than that represented by a material weakness, but still sufficient to warrant disclosure to the board's audit committee as a significant deficiency.*

The SEC and PCAOB have defined a significant deficiency as:

> "… a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness yet important enough to merit attention by those responsible for oversight of the company's financial reporting."

This assessment will require the exercise of judgment by the assessment team. Since ITGC deficiencies generally have a potential impact on risks outside financial reporting (e.g., on risks relating to operational effectiveness or the protection of confidential information), we recommend that management's assessment considers and discusses all related risks with the audit committee.

10. *Step back and perform a reasonable person[21] review, including a confirmation that any aggregation of control risk to the financial statements has been considered.*

The assessment of ICFR is whether it provides reasonable assurance that material misstatements will either be prevented or detected on a timely basis. This requires that the assessment team consider all the deficiencies as a whole, especially their root causes, and determine:

- If there are weaknesses in the system of internal control. If so, have they been appropriately identified, including the identification of root causes?
- Have all aggregation risks been identified and considered?
- Would a reasonable person believe that the risk of a material misstatement, considering the nature of the business, the major risks to the financial statements, and the strengths and weaknesses of the key controls, is reasonably possible?

Experience has shown that control deficiencies frequently have the same root causes (e.g., an inadequately staffed IT security function, a lack of discipline over change management as a whole, or a lack of technical accounting experience and understanding). In this case, the team should assess whether the combined or aggregated effect of this underlying issue represents a material weakness or significant deficiency. It is also important that the root cause is identified and properly communicated, since only if the root cause is addressed will the weaknesses be effectively remediated.

21 The SEC and PCAOB guidance refer to a prudent official rather than a reasonable person, but the intent and the practice are the same.

The assessment so far has addressed some, but not necessarily all, aggregation issues. It has considered:

- Multiple key ITGC failures and their effect on a single ITGC objective (in Step 3).
- Multiple ITGC control objective failures and their effect on a single automated control or other critical IT functionality (in Step 7a).
- Multiple control failures, including a combination of manual, automated, and other controls, and their effect on the financial statements (in Step 8).
- Deficiencies with the same root cause (above).

The assessment team should review the entire set of control deficiencies and confirm that there are no additional significant deficiencies or material weaknesses when the entire set is viewed. For example, are there so many control deficiencies that a reasonable person would consider that management's focus on internal control is insufficient?

The review by a reasonable person, or prudent official, is recommended by the SEC and PCAOB as a final precautionary step. This is to ensure that the assessment has been neither overly conservative nor aggressive, as well as results in an assessment that is a fair representation of the internal control system's quality as of the reporting date.

4. GLOSSARY OF TERMS

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 Reviews, document G14).
Automated application control	As described above, application controls include "computerized controls built into the system, manually performed controls, or a combination of both." The term *application controls* is synonymous with the term *computerized controls* used in the ISACA definition.
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 Glossary).
Control deficiency	A deficiency in ICFR exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.
Control failure	A key control that is either inadequately designed or not operating effectively.
Critical IT functionality	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 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*.

Term	Definition
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 possibility 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 (e.g., 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 (IIA) is an international professional association of more than 122,000 members with global headquarters in Altamonte Springs, Fla., United States. Throughout the world, The IIA is recognized as the internal audit profession's leader in certification, education, research, and technological guidance.
ITGC	IT general controls (ITGCs) are controls over ITGC processes generally residing in the IT organization. Broadly speaking, ITGCs 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 data and programs from unauthorized change.
Key control	A control that, if it fails, means there is at least a reasonable possibility 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 detected in a timely basis. 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 AS 5, 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."

Term	Definition
Key report	A report used in a key control, usually one that is 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 (e.g., a journal entry) or is used as the control's basis (e.g., a review of aged receivables). • The manual part of the control would not necessarily detect an error in the report.
Material weakness	A deficiency, or a combination of deficiencies, in ICFR, such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis.
PCAOB	The U.S. Public Company Accounting Oversight Board (PCAOB) is a private sector, nonprofit 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 that regulate stock markets and other aspects of the financial markets in the United States.
Prudent official	See *reasonable person*.
Reasonable assurance	SEC's guidance includes the following: "The 'reasonable assurance' referred to in the Commission's implementing rules relates to similar language in the Foreign Corrupt Practices Act of 1977 (FCPA). Exchange Act Section 13(b) (7) defines reasonable assurance and reasonable detail as 'such level of detail and degree of assurance as would satisfy prudent officials in the conduct of their own affairs.' The Commission has long held that 'reasonableness' is not an 'absolute standard of exactitude for corporate records.' In addition, the Commission recognizes that while 'reasonableness' is an objective standard, there is a range of judgments that an issuer might make as to what is 'reasonable' in implementing Section 404 and the Commission's rules. Thus, the terms 'reasonable,' 'reasonably,' and 'reasonableness' in the context of Section 404 implementation do not imply a single conclusion or methodology, but encompass the full range of appropriate potential conduct, conclusions or methodologies upon which an issuer may reasonably base its decisions."
Reasonable person	The SEC's guidance states: "When evaluating the severity of a deficiency or combination of deficiencies in ICFR, management also should determine the level of detail and degree of assurance that would satisfy prudent officials in the conduct of their own affairs that they have reasonable assurance that transactions are recorded as necessary to permit the preparation of financial statements in conformity with GAAP."

Term	Definition
Reasonable possibility	The PCAOB's AS 5 states: "There is a reasonable possibility of an event, as used in this standard, when the likelihood of the event is either *reasonably possible* or *probable*, as those terms are used in Financial Accounting Standards Board Statement No. 5, Accounting for Contingencies (FAS 5)." The SEC, in its guidance, uses the same definition. FAS 5 states: "This Statement uses the terms *probable, reasonably possible*, and *remote* to identify three areas within that range, as follows: a. *Probable.* The future event or events are likely to occur. b. *Reasonably possible.* The chance of the future event or events occurring is more than remote but less than likely. c. *Remote.* The chance of the future event or events occurring is slight."
SEC	The United States Securities and Exchange Commission (SEC) is a 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. Section 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 U.S. Sarbanes-Oxley Act of 2002, and other statutes.
Significant deficiency	A significant deficiency is a deficiency, or a combination of deficiencies, in ICFR that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of the company's financial reporting.
Top-down approach	The PCAOB describes the top-down approach in AS 5: "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." Also see the next section on *The GAIT Methodology* for a short discussion of the top-down approach as it relates to ITGC.

5. APPENDIX: *The GAIT Methodology*

The following is excerpted from The GAIT Methodology, available on The Institute of Internal Auditors' Web site at www.theiia.org.

Executive Summary

The SEC and PCAOB have recommended a top-down and risk-based approach to defining Sarbanes-Oxley Section 404 scope and related key controls. 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.

Guidance has been provided by organizations such as The IIA and the PCAOB relative to the identification of key controls at the business level. Additional guidance also has been published by organizations including 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 ITGCs) should be determined using the recommended top-down and risk-based approach.

If key ITGCs — 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.

This methodology provides a scoping mechanism that both management and external auditors 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 AS 5, the SEC's interpretive guidance (published in June 2007), and The IIA's *Sarbanes-Oxley Section 404: A Guide for Management by Internal Controls Practitioners.*

The methodology 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 by identifying risks within ITGC processes where a control or security failure could lead to a control failure of material significance within the business process, in turn leading potentially to a material misstatement of the financial statements.

The methodology 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 key ITGCs.

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.

GAIT and the Top-down Approach

The figure below shows the steps in a top-down and risk-based process for defining key ITGCs for Sarbanes-Oxley Section 404 using the methodology. It shows the relationship between the steps discussed in AS 5 and the continuation described in *The GAIT Methodology*.