The GAIT Principles

Last updated: Tuesday, January 02, 2007
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, which is generally accepted, enables an efficient assessment that focuses on the more likely and significant risks to financial reporting.

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. The Information Systems Audit and Control Association (ISACA) has also issued guidance 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\(^4\)) should be determined using the recommended top-down and risk-based approach.

Both management and the external auditors\(^5\) can use the principles in this Guide to the Assessment of IT General Controls Scope based on Risk (GAIT) 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. They are consistent with the methodology described both in the PCAOB’s Auditing Standard Number 2 (AS/2)\(^6\) and the IIA’s “Sarbanes-Oxley Section 404: A Guide for Management by Internal Controls Practitioners” (§404 Guide).

The authors of this document have developed a separate and complementary Methodology that expands the discussion and is based on these principles.

\(^1\) In their May 16 2005 “Commission Statement on Implementation of Internal Control Reporting Requirements.”

\(^2\) In Auditing Standard Number 2

\(^3\) 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.

\(^4\) ITGC are controls, generally within the IT organization’s general control processes (alternatively described as IT business 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)

\(^5\) This Guide refers to “users”, which are intended to include management responsible for the §404 program, independent auditors, and internal auditors, etc.

\(^6\) 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/2.
GAIT’s four core principles

Table 1: GAIT’s four core principles

<table>
<thead>
<tr>
<th>Principle</th>
<th>For Details, See...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Principle 1</strong>: 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.</td>
<td>Below</td>
</tr>
<tr>
<td><strong>Principle 2</strong>: 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.</td>
<td>Below</td>
</tr>
<tr>
<td><strong>Principle 3</strong>: 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.</td>
<td>Page 4</td>
</tr>
<tr>
<td><strong>Principle 4</strong>: Risks in IT general control processes are mitigated by the achievement of IT control objectives, not individual controls.</td>
<td>Page 4</td>
</tr>
</tbody>
</table>

**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.

The assessment of risk within IT general control processes should not start with a list or checklist of significant risks, but instead continue the risk assessment process. In their May 2005 FAQ’s, the PCAOB described this as starting with the identification of significant accounts and locations, related assertions, business processes and major classes of transactions, potential points of failure, and key controls within the business processes. Approaches that are not linked by a top-down approach (such as the above) to the risk of material misstatement of the financials may be ineffective and/or inefficient.

**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 IT general control processes that (indirectly, through their impact on automated controls and other functionality) represent a reasonably likely risk of material error in the financial statements. The top-down approach in AS/2 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 and risks to the functionality from defects in IT general control 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 IT general control processes. For example, companies may consider the activities that relate to ITGC exist in the change management, operations, and security business processes.

Each IT general control process operates at the various layers of the IT infrastructure of each application; some define these layers as 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 IT general control 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).

**Principle 4**

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

Each IT general control 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.

Controls in IT general control 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 IT general control 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.

**Closing Comments**

Each organization can use the above principles in developing a more detailed process for defining the scope of their IT general controls work for §404. The authors of this document have developed the GAIT Methodology and other related materials, which may be helpful in applying the principles discussed above.