

GAIT: New Guideline in Conducting IT General Controls SOX compliance assessments

Sometime last February, the IIA released the Guide to the Assessment of IT (GAIT) General Controls Scope Based on Risk, a guidance on identifying IT General Controls that should be tested as a part of an annual assessment of internal controls over financial reporting. The objective of this guidance is to help reduce SOX compliance costs incurred by auditors through a more efficient risk based approach in doing annual SOX compliance assessments.

GAIT consists of 4 core principles:

Principle 1: The identification of risks and related controls in ITGC processes 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.

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.

Principle 3: The IT general control process risks that need to be identified exist in processes and at various IT layers: application program code, database, operating systems, and network.

Principle 4: Risks in IT general control processes are mitigated by the achievement of IT control objectives, not individual controls.

GAIT's four principles and methodology and a presentation used during the release of the GAIT through a web event are available for free download on The IIA's website at <http://www.theiia.org./recent-ia-news/index.cfm?i=3168>.