GAIT (The Guide to the Assessment of IT Risk) メソドロジー

GAIT メソドロジーとは？ GAIT メソドロジー（別名 GAIT-M）は、トップダウン型のリスク・ベース・アプローチを用いたIT全般統制のスコーピングのためのガイドです。

誰のためのものか？ 経営者および外部監査人は、トップダウン型リスク・ベース・アプローチによる財務報告に係る内部統制のキー・コントロールのスコーピング（評価範囲の決定）の *一環として*、またその *継続として*、IT全般統制のキー・コントロールの識別に、このガイドを使用することができます。

どう役に立つのか？ IIAは、IT全般統制のキー・コントロール（ひとつの不備が間接的に財務諸表における重要な虚偽記載をもたらす可能性があります）の識別を容易にするため、このガイダンスを開発しました。つまりこのメソドロジーは、経営者や監査人がトップダウン、リスク・ベースのスコーピングで SOX404 条に対応する試みの一環かつ継続として、IT全般統制のキー・コントロールの識別を可能にします。

不具合(failure)が生じる場合、このメソドロジーは、IT全般統制プロセスの詳細なリスクおよび関連するIT全般統制の目標（達成された場合、それらのリスクを軽減するものです）を識別します。IT全般統制の目標に対応するキー・コントロールを識別するには CobiT その他のメソドロジーが使用できます。

原則

メソドロジーのベースとなる4つの原則は、PCAOB（米国公開企業会計監視委員会)AS5(監査基準書第5号)に記載されている次の方法論に整合しています。

■4つの原則

1. アプローチ:トップダウン、リスクベース
   IT全般統制プロセスのリスクおよび関連する統制（例えば、変更管理、導入・展開、アクセスセキュリティおよび運用等）の識別は、重要な勘定科目、これら勘定科目に関するリスクとビジネスプロセスのキー・コントロールの識別に用いられるトップダウン型リスク・ベース・アプローチを継続すべきである。
2. 識別すべきリスク:財務的に重要なアプリケーションに関連する重要なIT機能およびデータ
   識別すべきIT全般統制プロセスのリスクは、財務的に重要なアプリケーションに関連する重要なIT機能およびデータに影響するものである。
3. 識別すべきリスクのありか
   識別すべきIT全般統制プロセスのリスクは、プロセスにおける様々なITレイヤー（アプリケーションプログラムのコード、データベース、オペレーティングシステムおよびネットワーク）上に存在する。
   4. リスクの軽減:個別の統制ではなくIT統制目標の達成による

IT全般統制プロセスのリスクは、IT統制目標の達成によって軽減される。個別の統制の達成によってではない。

*GAIT メソドロジー*は、(IT全般統制を実施する)組織が4つの原則を実行することを可能にし、経営者や監査人にIT全般統制のスコーピングを行うためのガイダンスと、これらの意思決定を支援するツールを提供するものです。

関連資料

- Q&A about GAIT
- Less Complex GAIT Scenario
- More Complex GAIT Scenario
- Case Study (SOX2年目以降へのメソドロジーの適用)
- "New Scoping Methodology May Ease Section 404 Audits"
- GAIT Survey Executive Summary(2008 年2月に実施した GAIN (Global Audit Information Network) 調査の結果)

追加情報

GAIT シリーズに関するご意見・ご質問があれば、下記アドレス宛に CIA フォーラム研究会 No.12 までお寄せください。

⇒ ciaforum@iiajapan.com