ITGC でキーコントロールといえば GAIT

IT 全般統制の評価範囲を決定するに当たっては、The GAIT Principles http://www.theiia.org/guidance/technology/gait/ が発行されているものの中で最も簡潔明瞭な指針となるだろう。

GAIT では４つの原則が示されている。以下意訳すると、

原則１

IT 全般統制プロセスにおけるリスクの認識とそれに関係する統制を識別するには、重要な勘定やそれに関係するリスクやキーコントロールを識別したトップダウン＆リスクベースアプローチの延長として行なわなければならない。

チェックリスト方式などは非効果的で非効率である。

原則２

識別すべき IT 全般統制リスクとは、財務会計上重要なアプリケーションとデータにおける重要な IT 機能に対して影響を与えるものであるべき。

トップダウン＆リスクベースアプローチとは、業務プロセスにおいて虚偽記載をもたらすリスクのあるポイントとそれに関係するキーコントロールを識別する。その上で、それが IT 機能（すなわち、自動化されたキーコントロールや、キーレポート、重要な財務データ）に拠っている場合に、そのアプリケーションは財務会計上重要となるから、IT 全般統制プロセスの欠陥からもたらされる IT 機能のリスクを識別しなければならない。

原則３

識別すべき IT 全般統制プロセスのリスクは、業務プロセス中にあり、かつ、各 IT レイヤ（アプリケーション、データベース、オペレーションシステム、ネットワーク）上に存在している。

原則４

IT 全般統制プロセスにおけるリスクは、IT 統制目標の達成によって軽減されるものであり、個々別々のコントロール手続ではない。

各 IT 全般統制プロセスには、IT 統制目標を支援する手続が埋め込まれている。IT 統制目標とは、

・システムが実装される前に、適切にテストされ評価される
・データは未承認の変更から保護されている
・運用における支障や事故は、適切に対応され、記録され、調査され、解決される

先ず第一に、財務報告に関連する IT 統制目標を識別することが肝要であり、その後にその統制目標を満たす IT 全般統制のキーコントロールを識別すべきである。識別された IT 統制目標に関係ない IT 全般統制手続は、たとえ重要であっても、ICFR の評価対象に含める必要はない。