ＩＴ監査のマネジメント

ＧＴＡＧ４
（ＩＴ監査の国際的ガイダンス４）

このガイドの内容

- ITの定義
- IT関連リスク
- IT監査領域の定義
- IT監査の実施
- IT監査の管理
- 新たな問題

ITの定義

第1層 – IT管理

- この層は、IT環境を管理する人、ポリシー、手続き、プロセスの集合から構成される
  - システムのモニタリング
  - プログラミング
  - プランニング
  - 外部委託ベンダーの管理
  - ITガバナンス

ITの定義

第2層 – 技術的インフラ

- この層は、重要な業務アプリケーションの基礎になり、これを支援し、可能にするシステムを指す
  - オペレーティングシステム
  - データベース
  - ネットワーク

ITの定義

第3層 – アプリケーション

- 業務運用に関連した特定のタスクを行うプログラム
  - 取引用アプリケーション: ビジネス取引を処理し記録する
  - 支援アプリケーション: 取引処理は一般的には行わないが業務活動を支援する

第4層 – 外部との接続

- インターネット、EDI、その他の外部ネットワーク

IT関連リスク

リスクとなりうるものは?

可用性、セキュリティ、インテグリティ、機密性、有効性、効率性

- リスクのタイプ
  - 広範囲のリスク: 企業へ全体として影響する
  - 特定のリスク
- 3つの次元の考察
  - 各会社が特定のリスクプロファイルをもつ
  - IT関連リスクは、静的でなく、ダイナミックに変化する
  - 増殖:IT関連リスクを評価する際、それに付随する特性に留意する

IT関連リスク

リスク評価

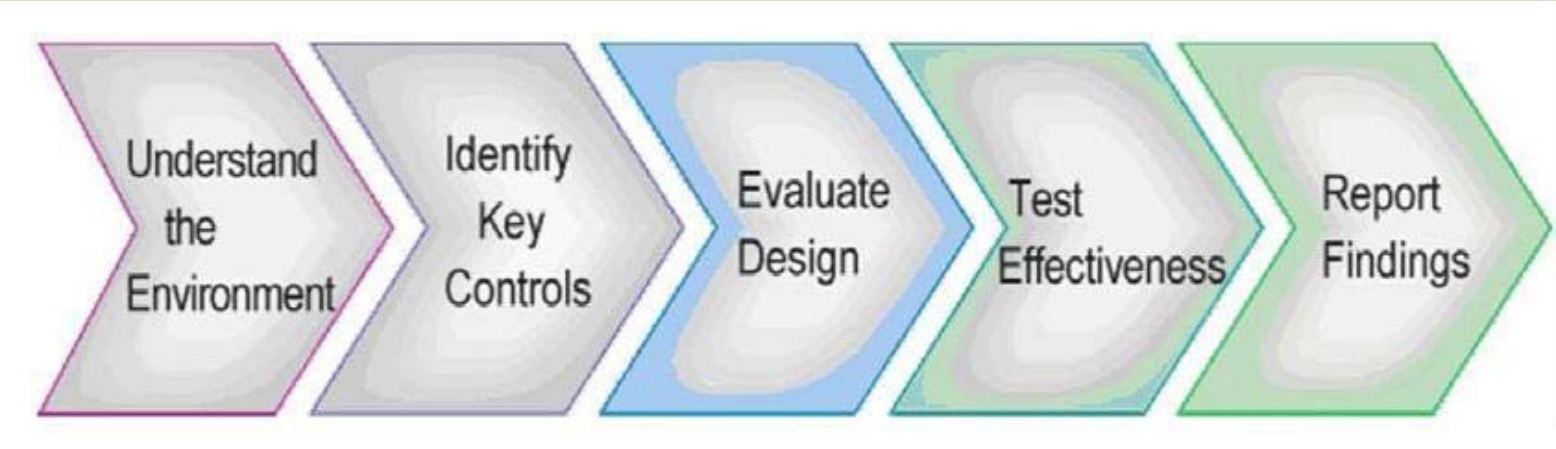
- 影響度と発生可能性を考察する
- 伝統的なリスク評価プロセスはITリスク評価には適さないこともある
- ITリスク評価プロセスの強い推奨事項:
  - 前年のアップデートを行うだけではなく、毎年、詳細に実施
  - IT環境のすべての層(レイヤー)を考慮
  - 静的・動的(ダイナミック)リスクの両方を考慮
  - インタビューにのみ頼るのでなく、そのほかの発見技法を用いる
  - 発見後、適切なレベルの分析で補う
  - 適切な要員によって実施

IT監査領域の定義

- IT監査に十分に広い定義をあてる
- IT環境のすべての層（レイヤー）を扱う
- IT監査のリソース（人的資源）は一般的に得がたく、IT監査の需要は大きい→IT監査のニーズと限られたリソースを効果的にバランスさせるIT監査計画をどのように構築するかを理解する

IT監査の実施

- 通常の監査プロセス



- 次のようなフレームワークや基準を用い、IT監査を検討する
  - COSO, CoBIT, ISO27001/17799...

IT監査の管理

- 新たな管理手法および手続きが必要である
- IT監査のリソース（人的資源）を管理する
  - 優秀なIT監査のプロフェッショナルを選別、雇用、訓練、確保する
  - 資格、配置転換、継続的教育を検討する
  - IT監査機能のコソーシング

IT監査の管理

IT監査の推進要素（促進剤）

- 次のような監査支援ツール類
  - 電子調書
  - プロジェクト管理ソフト
  - フローチャート作成ソフト
- 次のようなテスト支援ツール類
  - データ分析ソフト
  - セキュリティ分析ツール

新たな問題

- ワイヤレスネットワーク
- モバイル装置
- データ管理
- プライバシー
- 職責分離
- 管理者権限アクセス
- 著作権侵害
- …