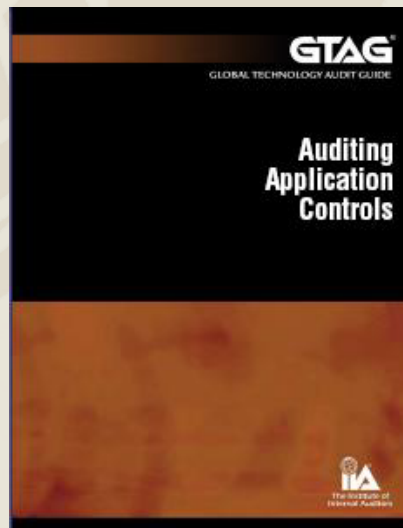


業務処理統制の監査



GTAG 8 (IT監査の国際的ガイダンス8)

このガイダンスの範囲

- 業務処理統制とその便益
 - 内部監査人の役割
 - リスク評価の実施方法
 - 業務処理統制レビューのスコープ
 - 業務処理レビューの方法
 - 共通する業務処理統制、想定されるテスト、レビュープログラムのサンプル
- * 訳者注:GTAG8における“レビュー”は、“監査”を意味すると考えられる。

業務処理統制

コントロール目標:

入力データが、正確で、完全で、承認され、適切であること

データが、許容時間内で処理されること

出力データと蓄積データが正確で、完全であること

入力、蓄積、出力のデータ処理の過程が記録されること

業務処理統制

- リスク管理のために、コスト効果に優れ、効率的な手段
- その効果は、IT全般統制の環境に依存する
- 実現方法は、環境が複雑か否かによって、様々である

業務処理統制の便益

- **信頼性**

手動操作に起因するエラーの可能性を減少させる

- **ベンチマーク**

IT全般統制に依存することにより、再テストを繰り返すことなく、業務処理統制が毎年有効であるという結論を導くことができる。

- **時間とコストの節約**

通常、IT全般統制が有効である限り、業務処理統制のテスト時間は少なくなり、一度だけテストすれば良いことになる。

内部監査人の役割

- 主要なITリスク、コントロール、監査技法の知識
- コンサルティングまたはアシュアランス
 - 独立したリスク評価
 - コントロールの設計
 - 教育
 - コントロールのテスト

リスク評価

- リスク評価

 - 技法

 - 主たるスコープの質問

- 手法

 - ユニバースの定義

 - リスクの定義

 - リスク要因の重み付け

 - リスクのランク付け

 - 結果に基づくレビュー計画の作成

レビューの範囲決め

- **ビジネスプロセスによる方法**
 - **トップダウンレビュー**
- **単一のアプリケーションによる方法**
 - **単一のアプリケーションやモジュールに焦点を当てる**
- **アクセス管理**
 - **いかなる方法が選択されても範囲に含む**

レビューの手順

- 計画
- 特定した資源の要求
- 文書化
- テスト
- コンピュータ支援監査技法 (CAATs)

共通した業務処理統制

- 入力とアクセスのコントロール
 - データのチェックと検証
 - 自動付与された権限付与、承認、オーバーライド
 - 自動化された職責分離
 - 未処理の項目
- ファイルとデータの転送のコントロール

共通した業務処理統制(続き)

- プロセスのコントロール
 - 自動化されたファイルの特定や検証
 - 自動化された機能や計算
 - 監査証跡やオーバーライド
 - データの抽出、選別、報告
 - インターフェースの整合
 - 自動化された機能や履歴
 - 重複のチェック
- 出力のコントロール
 - 総勘定元帳や補助簿の出力
 - 承認の更新

詳細なレビュープログラムのサンプル

- 想定されるテスト

トランザクションがアプリケーションに受け付けられ、重複することなく一度だけ処理されることを確実にする、入力コントロールをテストする。

トランザクションがアプリケーションに受け付けられ、妥当なロジックで処理され、全ての処理を通り、適切なファイルを更新することを確実にする、プロセスコントロールをテストする。

添付資料Bに、その他の詳細なテストを示す。

終わりに

- **業務処理統制は、リスク管理のために、コスト効果に優れ、効率的な手段である。**
- **内部監査人は、自らの組織の業務処理統制が適切に設計され、有効に機能していることを判断すべきである。**
- **テストにかかる労力を一層節減するために、ベンチマークを考慮する。**