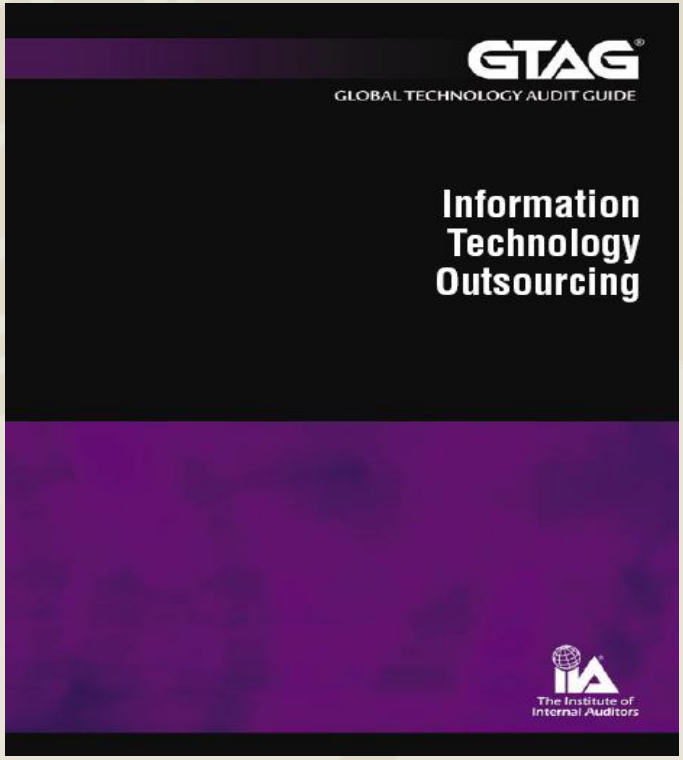
IT アウトソーシング



GTAG 7
（I T監査の国際的ガイダンス 7）

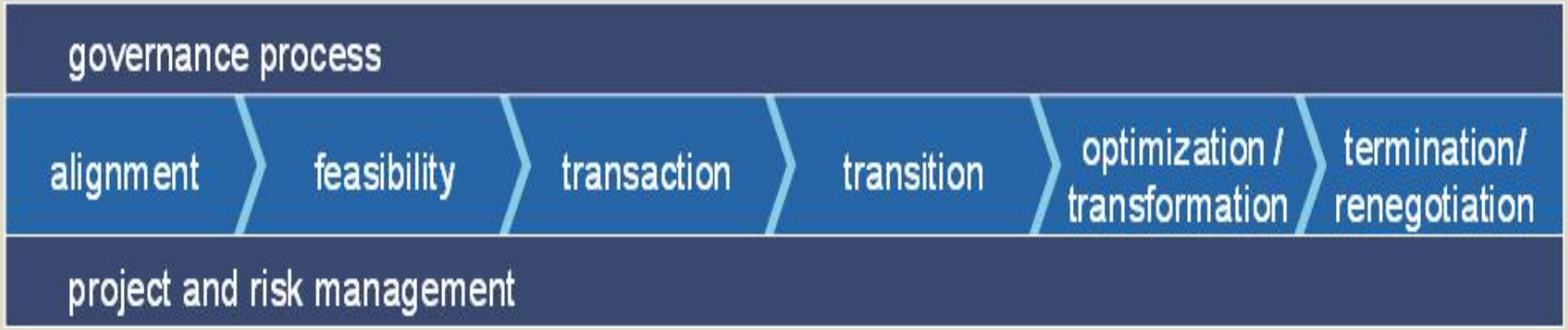
目次

- ITアウトソーシングの主要なタイプ
- アウトソーシングのライフサイクル
- ITアウトソーシングのリスク
- 考慮すべきキーコントロール – クライアント側の運用
- 考慮すべきキーコントロール – サービスプロバイダ側の運用
- 監査部門長が尋ねるべき10の質問

ITアウトソーシングの主要なタイプ

- アプリケーションの管理
- インフラの管理
- ヘルプデスク・サービス
- 独立したテストと有効性評価
- データセンターの管理
- システム統合
- R&D（研究開発）サービス
- セキュリティサービス

アウトソーシングのライフサイクル



ITアウトソーシングのリスク

IT アウトソーシングに関係するリスクの例

戦略:アウトソーシング戦略が企業の事業目的に整合していない
実行可能性: サプライヤーへの調査不充分や、組織による関連リスク評価の不十分さなどに起因して、元本回収期限、顧客およびサプライチェーンの影響度合、コスト削減などの掌握を誤る
実施: 調達規程が現実と合致していない、 正しいSLAが履行されていない、 運用、人的資源 (HR)、および規制による影響が考慮されていない、コンティンジェンシープランが計画されていない

ITアウトソーシングのリスク

リスクの例（続き）

移転: 公式な移転計画の欠如、適切なスキル保存計画の不備、IT運用上の問題点が効果的に伝達・解決されない
最適化と改善: アウトソーシング契約が有効に管理されておらず、その結果、アウトソーシングの利点と効率性が達成されない
終結と再交渉: アウトソーシング・プロセスの不適切な終結

考慮すべきキーコントロール – クライアント側の運用

ガバナンスのアウトソーシングにおけるフレームワーク

- 全てのITアウトソーシング契約の、組織の重要なビジネス目標への整合
- モニタリング機構の整備
- 複雑な事業ポートフォリオを横断するITプロジェクトとサービスの、変更管理
- ITの処理能力に対する、直接的かつ可視的な説明責任の確立
- 重要な契約事項についての所有権の特定
- 良好に統合された ITマネジメント・プロセスの、クライアント側およびサービスプロバイダ側に対する明確化

考慮すべきキーコントロール
– クライアント側の運用

整合性

- 戦略の有効性評価
- 選択肢の識別
- ビジネスモデルの準備
- 責任分担の合意およびチーム編成

実行可能性

- ビジネスモデルとケースの構築
- 最低基準線の設定
- 市場の理解
- 選択肢の評価とベンチマーキング

考慮すべきキーコントロール
– クライアント側の運用

契約

- 業務スキームの構築
- アウトソース資産に対する合意
- 契約交渉
- 取引とビジネスケースの実施

考慮すべきキーコントロール – クライアント側の運用

アウトソーシング契約における重要な構成要素

- サービスレベルとインセンティブ
- ベンダーの従業員
- データ保護、プライバシー、および知的資産
- 価格保護
- サードパーティーの割当て
- 提携先が使用または作成する資産の所有権
- 異なる複数の法体系におけるコンフリクト
- コンテンジェンシープランと変更管理
- 重要な悪影響への注意喚起
- 監査権限
- 終結

考慮すべきキーコントロール
– クライアント側の運用

移転

変更の実施
迅速な投資回収
文化の確立
人の管理

変更管理

最適化と改善

契約のモニタリングと紛争の解決
ビジネスの変質化
関係先の再評価
新たなビジネスケース – 利点の発見

考慮すべきキーコントロール – サービスプロバイダ側の運用

- 統制環境
- セキュリティに関する検討項目
  - データ保護リスク
  - セキュリティ： ネットワークへのアクセス、物理的なアクセス、環境面へのアクセス、人的なアクセス、論理的なアクセス
- SDLC（システム開発ライフサイクル）のコントロール
- 変更管理のコントロール
- HR（人的資源）に関する規程と手続き

監査部門長が尋ねるべき10の質問

1. アウトソースされているサービスは、クライアントにとって重要か？
2. クライアントは、適切に定められたアウトソース戦略を有しているか？
3. アウトソースされた業務に関するガバナンス構造には、どのようなものがあるか？　役割と責任は明確に定められているか？
4. アウトソーシングにあたり、詳細なリスク分析が行われたか？また通常のリスク分析は、常時行われているか？
5. アウトソーシング活動に関する、公式な契約書またはSLAは存在しているか？

監査部門長が尋ねるべき10の質問

6. ベンダーの実績をモニタリングするためのKPIは、SLA によって明確に定められているか？
7. 契約書またはSLAの遵守は、どのようにモニタリングされているか？
8. SLAを遵守していないことを特定するための仕組みには、どのようなものがあるか？
9. データ、システム、情報システム、OS、ユーティリティソフト、ならびにアプリケーションソフトの所有・管理責任は、明確に定められ、サービスプロバイダとの間で合意されているか？
10. 内部統制の運用有効性に対する保証を獲得するため、サービスプロバイダ側では、どのようなプロセスを有しているか？