GAIT-R

■GAIT-R： ビジネスとITリスクのためのGAIT

ビジネス目標の達成に必要な

IT統制/キー・コントロールの識別を助ける

ガイダンス

GAIT-R

■4つの原則

原則1： テクノロジーの問題点にかかるリスク

原則2： キー・コントロールの識別

原則3： ビジネスリスクの軽減

原則4： IT全般統制と自動化されたキー・コントロールの関係

GAIT-R

■ 4つの原則： 原則1

テクノロジーの不具合(failure)にかかるリスク

意図したとおりに動かないテクノロジーの不具合(failure)は、それがビジネスに対するリスクを示す場合には、評価、管理、監査すべき1つのリスクにすぎない。

GAIT-R

■ 4つの原則： 原則2

キー・コントロールの識別

キー・コントロールは、ビジネスリスク、リスク許容度、および統制（自動化された統制とIT全般統制を含む）のトップダウン評価の結果として、識別する。

GAIT-R

■ 4つの原則： 原則3

ビジネスリスクの軽減

ビジネスリスクは、手作業によるキー・コントロールと自動化されたキー・コントロールの組み合わせによって軽減される。ビジネスリスクを管理または軽減するための内部統制のシステムを評価するためには、自動化されたキー・コントロールを評価する必要がある。

GAIT-R

■ 4つの原則： 原則4

IT全般統制と自動化されたキー・コントロールの関係

IT全般統制は、自動化されたキー・コントロールの継続的かつ適切な運用を保証するために、依拠されている可能性がある。

GAIT-R

■ 4つの原則： 原則4（続き）

IT全般統制と
自動化されたキー・コントロールの関係

原則4a： 識別すべきIT全般統制プロセスのリスクは、重要なアプリケーションにおける重要なIT機能および当該アプリケーションに関連するデータである。

原則4b： 識別すべきIT全般統制プロセスのリスクは、各種プロセス中の様々な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）に存在する。

原則4c： IT全般統制におけるリスクは、IT統制目標を達成することにより軽減されるものであり、個別の統制によって、軽減されるものではない。

－－ **原則**4a～4cは、GAITメソドロジーの原則2～4に対応する

GAIT-R

■ GAITーRのトップダウンの方法（8つのステップ）

ステップ1： **ビジネス目標**を識別する

ステップ2： ビジネス目標の達成を合理的に保証する**キー・コントロール**をビジネスプロセス内から識別する

ステップ3： 依拠される**重要なIT機能**をビジネス統制のキー・コントロールの中から識別する

ステップ4： IT全般統制をテストすべき重要な**アプリケーション**を識別する

ステップ5： **IT全般統制プロセスのリスク**とそれに**関連する統制目標**を識別する

ステップ6： 統制目標に見合い、テストすべき、**IT全般統制**を識別する

ステップ7： 適切な人物によるレビューを実施する

ステップ8： レビュー範囲を決定し、適切なデザインと有効性テストプログラムを構築する

ーー　ステップ3～7は、GAIT Methodologyの5つのフェーズに対応。

GAIT-R

■ GAITメソドロジーの5つのフェーズ

フェーズ1

重要なIT機能を識別する（必要に応じてテストする）

フェーズ2

IT全般統制をテストすべき（重要な）アプリケーションを識別する

フェーズ3

IT全般統制プロセスのリスクとそれに関連する統制目標を識別する

フェーズ4

統制目標に合致し、テストすべき、IT全般統制のキー・コントロールを識別する

フェーズ5

適切な人物によるレビューを実施する