ビジネスとITリスクのための GAIT（The Guide to the Assessment of IT Risk）

GAIT-R とは？

「ビジネスとITリスクのための GAIT」、別名 GAIT-R は、ビジネスの目標を達成するために不可欠なキー・コントロールを識別することに焦点を当てています。

誰のためのものか？

GAIT-R は、内部監査の実務家向けに作られましたが、ITガバナンスやセキュリティの管理者や、組織の中でITリスク(体系)を管理しIT統制を整備する担当者にも使用いただけます。

どう役に立つのか？

GAIT-R は、ビジネスリスクに焦点を当て、組織にとって重要ではないITリスクへの注意を最小限にすることで、内部監査機能の効率性と有効性を向上させます。内部監査部門長（CAE）はITに関連する問題が適切なレベルで考慮されるという安心感をもってビジネスリスクを保証することができます。

GAIT シリーズの他の実務ガイド同様に、GAIT-R 方法論は一連の原則で構成されています。

■4つの原則

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。
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、識別すべきである。
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。
4. IT全般統制と自動化されたキー・コントロールとの関係
   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は、識別された各ビジネス目標に対するリスクに基づいた評価範囲についても解説しています。それは各ビジネスプロセス中の手動のキー・コントロール、自動化されたキー・コントロール、（両者の混成である）ハイブリッド・コントロールや、IT全般統制プロセスの中にあるキー・コントロール、および COSO 内部統制モデルの統制環境、情報と伝達、その他の階層における（統制）活

動を含有するエンティティレベルのコントロールを含んでいます。

『PCI コンプライアンスのスコープに GAIT-R を使ったケーススタディ』は、GAIT-R の原則と方法論にもとづき、GAI-R を PCI コンプライアンスに適用した二つのケーススタディを提供しています。

追加情報

GAIT シリーズに関するご意見・ご質問があれば、下記アドレス宛に CIA フォーラム研究会 No.12 までお寄せください。

⇒ ciaforum@iiajapan.com