Deloitte.
デロイト トーマツ

トーマツ.

システム導入・更改における統制構築・高度化に関するサービス

有限責任監査法人トーマツ

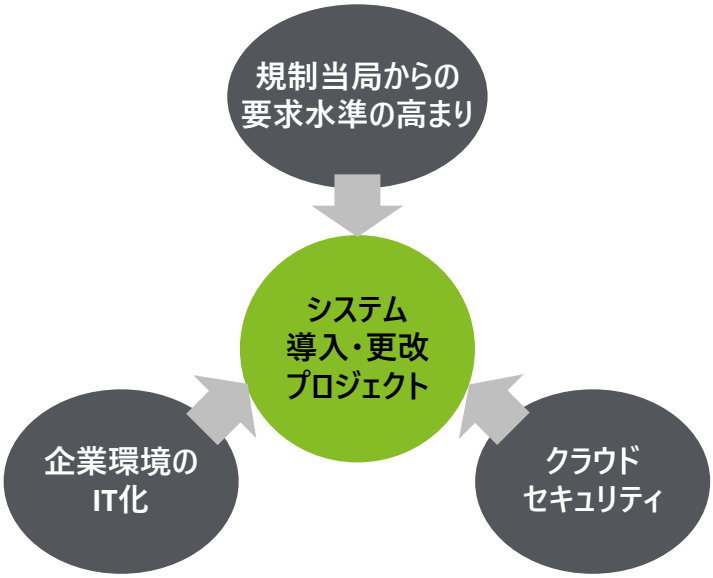
システム導入・更改に伴う内部統制の高度化

企業のIT環境高度化に対応できる内部統制の高度化が求められています

■規制当局からの要求水準の高まり
各国規制当局の連携実態及びJICPAの動向を踏まえると、ISA（国際監査基準）でも**PCAOB基準で要求される高い水準**での監査手続が求められるようになっており、**遠からず日本基準でも高い水準での監査手続きに対応した内部統制の高度化が求められる**ことが想定される

■企業環境のIT化
進化するビジネス環境において、**企業によるITの利用環境および利用状況の進化に**より、システム導入・更改プロジェクトにおいては、ガバナンス強化を目的とした統制機能の構築が求められている

■クラウドセキュリティ
組織がクラウドサービス（SaaS、PaaS、IaaSなど）を利用する際に、情報漏えい・不正アクセス・サービス停止等のリスクを適切に管理・低減するために、内部統制の仕組みや運用を強化することが求められている



システム導入・更改プロジェクトにおいては、以下のような領域について、特に留意する必要があります

。

主な領域	主なPitfall
プロジェクト・ガバナンス テスト データ移行 カットオーバー・ハイパーケア	• **経営者のプロジェクト関与が不十分**で、経営者の意図に即さないシステムが構築される • **内部統制要件/セキュリティ要件の検討が不十分**で、財務諸表監査に影響を及ぼす • ベンダー主導による要件検討による業務処理パターンの検討が不十分で、要件の再検討のためにスケジュールが遅延する。 • 標準機能、内部統制の知識が不十分で、稼働後に新規帳票作成などの追加開発が発生する • **ユーザトレーニングの検討が不十分**で、稼働後に正しい処理（マスタ・伝票登録時の入力ミス・入力情報の不足等）が行われない • **データ移行の検討が不十分**で、マスタ不備、データ不整合が発生する • **本番稼働判定基準作成されておらず、テスト結果が不十分**にもかかわらず、バグが残存した状態でシステムを稼働させる • ハイパーケア体制の検討が不十分で、稼働後にシステムが適切に運用されない
IT全般統制	• **IT全般統制上の課題に対する検討が不十分**で、稼働後に不備が識別される • **ログ出力機能、パスワード設定などのシステム設定機能の検討が不十分**で、稼働後に不備が識別されたり、追加開発が必要になる
業務プロセス統制 職務分掌	• **業務処理パターンの検討が不十分**で、稼働後に手作業による修正が発生し、決算処理に影響を及ぼす • **権限ロール設計、ユーザー設定の検討が不正確**で、アクセスセキュリティが不十分なままシステムを稼働させる • **業務記述書・業務フロー図、RCMなどの内部統制関連文書が更新されない**
クラウドセキュリティ	• クラウド内のセキュリティの設定が不完全であるか、過剰な特権アクセスが許可される • リスク軽減のためのログが利用できない

サービスの概要

システム開発プロジェクトにともない内部統制の見直し、高度化を図るための助言を実施します。

①システム導入・更改と並行した内部統制高度化に関する助言

システム導入・更改プロジェクトの計画に合わせて、内部統制の現状評価・分析を行い、課題を識別した上で対応計画を策定し本番リリースまでに内部統制が構築されていることを確認するための助言を実施します。

内部統制高度化の流れ

フェーズ	現状評価・分析			統制設計・文書化		ウォークスルー		
ステップ	①現状理解	②課題・ToDoとりまとめ	③統制整備・文書化計画	①統制設計	②内部統制文書の作成	①ウォークスルー	②プレ評価	③監査人レビュー課題・ToDo
目的・ゴール	• 再構築する基幹システムの全体構想や業務フローをレビューし、業務実施上及び監査上のリスクや課題を洗い出す			• 評価・分析結果、SaaS固有リスク等を踏まえた効率的かつ実効性のある統制設計のための提案を実施 • 統制の要点をまとめた３点セットの作成助言		• ウォークスルーを通じ、整備状況のプレ評価が実施され、発見された課題・ToDoの対応方針が策定され、調書を監査人レビューに供されている		
タスク	● ①現状理解 ➢ 資料の閲覧および関係者へのインタビューにより、現行の統制、新システムで計画されている統制を理解する ● ②課題・ToDoとりまとめ ➢ 既知の課題、現状理解で抽出した課題、チェックリスト等と突合して検出した課題等を取り纏め対応の方向性を決定する ● ③統制整備・文書化計画 ➢ 後続フェーズへの影響を検討し、計画を詳細化する ➢ 内部統制上の課題を整理し、監査部門等との認識合わせを行う			● ①統制設計 （IT全般統制、業務処理統制を対象） ➢ 前フェーズで特定された課題に対して改善案を、業務部門・システム部門と討議する ➢ 業務部門・システム部門と合意した統制活動を最終化する ● ②内部統制文書の更新 ➢ IT全般統制領域については、RCMを作成する ➢ 業務処理統制の領域については３点セット（プロセスフロー、業務記述書、RCM）を作成する		● ①ウォークスルーの実施 ➢ IT全般統制、IT業務処理統制のウォークスルーを実施 ➢ 母集団の網羅性を確認する ● ②プレ評価の実施 ➢ 本番環境と同等の環境でIT全般統制、IT業務処理統制の評価を実施 ● ③監査人レビュー、課題・ToDo ➢ 監査人のレビューに供する ➢ 課題・ToDoを取りまとめる		

②IT統制監査に関するワークショップ

現在実施しているIT統制（IT全般統制、IT業務処理統制）を対象に、トーマツのチェックリストや統制事例等の説明を受けるとともに、ワークショップとして自社で課題について検討し、IT統制への理解を深めることを目的としています。

また、ワークショップを通じて、現状評価・分析工程で作成した課題や統制設計・文書化を進めるための知見を身に着けることを目的とします。

ワークショップの流れ

STEP	1. 事前準備	2. ワークショップ開催	3. 振り返り
クライアント	● 依頼書に基づく事前資料のご準備 ● 現状業務・課題の情報共有 ● 事前協議（対象範囲の検討含） ● ご参加メンバーの決定 ● 事前勉強会・WS開催日程の決定 ● 事前勉強会への参加 ● 資料の事前読込・課題検討	● WSへのご参加 ➢ WSの狙いの理解 ➢ WS実施（ハンズオン） ➢ ハンズオン結果についてのディスカッション	● WS振り返りへのご参加 ➢ WSを通じて得た気付きや、今後に向けてのアクションプランに関するディスカッション
当法人	● 事前に協議・決定したテーマに基づく事前資料準備依頼書の作成・ご提示 ● 現状業務・課題の情報確認 ● 事前協議 ● WSのコンテンツ作成 ● 事前勉強会・WS開催日程の調整 ● 事前勉強会の実施	● WSのファシリテート ➢ IT監査基礎知識の説明 ➢ WS実施（ファシリテート） ➢ ハンズオン結果についてのディスカッション	● WS振り返りのファシリテート ➢WSを通じて得た気付きや、今後に向けてのアクションプランに関するディスカッション ➢WSを通じて検出した課題を現行分析・評価に反映

トーマツの強み

①J-SOX対応の専門知見

J-SOX対応に関し監査法人の知見を活用したアプローチを有しています

アプローチを活用した、効果的・効率的な構築・文書案作成を立案・実施いたします

「トーマツ内部統制報告制度対応アプローチ」「タスクリスト」


V. 内部統制報告制度対応アプローチ・タスクリスト

②テクノロジーフレームワークの活用

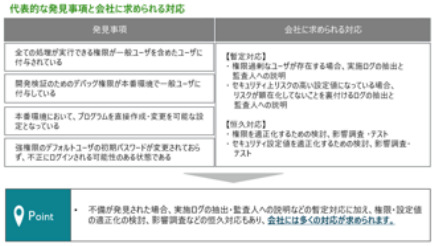
デロイトの知見を集約した、IT全般統制の標準化された評価の枠組みであるテクノロジーフレームワークを有しています

テクノロジー毎のリスク対応のリーディングプラクティスに基づいた評価手法であり、実質的なリスク領域を識別することで監査品質を向上し、標準化された手続きを実施することができます

③内部統制高度化の知見

内部統制の高度化に多くの知見を有しています

内部統制文書の整備、評価の過程で発見した内部統制の課題「リスクのある統制処理」「非効率/効率化の余地のある統制」「電子化の可能性」「効果的な評価」等余地がある点について、課題提起が可能です



※貴社および貴社との関係会社とデロイト トーマツ グループの関係において監査人としての独立性が要求される場合、本サービス内容が提供できない可能性があります。詳細はお問合わせください。

Deloitte. トーマツ.
デロイト トーマツ

Member of
Deloitte Touche Tohmatsu Limited

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

IS/BCMSそれぞれの認証範囲はこちらをご覧ください
http://www.bsigroup.com/clientDirectory